Nathan Jacobson
Università di Yale

Algebra di base II

Seconda edizione

Volume secondo

Traduzione italiana di *Basic Algebra II*, seconda edizione
W. H. Freeman and Company, New York, 1989

A Mike e Polly

Dati di catalogazione della Library of Congress
(Scheda riveduta per il volume 2)

Jacobson, Nathan, 1910–
Basic algebra.
Contiene riferimenti bibliografici e indici.
1. Algebra. I. Titolo.
QA154.2.J32 1985 512.9 84-25836
ISBN 0-7167-1480-9 (vol. 1)
ISBN 0-7167-1933-9 (vol. 2)

Copyright © 1989 W. H. Freeman and Company.

Nessuna parte di questo libro può essere riprodotta con procedimenti meccanici, fotografici o elettronici, né sotto forma di registrazione fonografica, né può essere memorizzata in un sistema di recupero delle informazioni, trasmessa o altrimenti copiata per uso pubblico o privato senza il permesso scritto dell'editore.

Stampato negli Stati Uniti d'America.
1 2 3 4 5 6 7 8 9 0 VB 7 6 5 4 3 2 1 0 8 9

Indice del volume

Sommario del volume II **viii**

Sommario del volume I **xii**

Prefazione alla seconda edizione **xv**

Prefazione alla prima edizione **xvi**

Introduzione **1**

0.1 Il lemma di Zorn 1
0.2 Aritmetica dei numeri cardinali 2
0.3 Numeri ordinali e cardinali 3
0.4 Insiemi e classi 4

1 Categorie **6**

1.1 Definizione ed esempi di categorie 6
1.2 Alcune nozioni fondamentali sulle categorie 11
1.3 Funtori e trasformazioni naturali 14
1.4 Equivalenza di categorie 19
1.5 Prodotti e coprodotti 23
1.6 I funtori hom. Funtori rappresentabili 27
1.7 Universali 30
1.8 Funtori aggiunti 34

2 Algebra universale **39**

2.1 Ω-algebre 39
2.2 Sottoalgebre e prodotti 43
2.3 Omomorfismi e congruenze 45
2.4 Il reticolo delle congruenze. Prodotti sottodiretti 49
2.5 Limiti diretti e inversi 51
2.6 Ultraprodotti 56
2.7 Le Ω-algebre libere 58
2.8 Varietà 60
2.9 Prodotti liberi di gruppi 65
2.10 Caratterizzazione interna delle varietà 68

3 Moduli **70**

3.1 Le categorie R-mod e mod-R 70
3.2 Moduli artiniani e noetheriani 74
3.3 Il teorema di raffinamento di Schreier e il teorema di Jordan–Hölder 76

3.4 Il teorema di Krull–Schmidt . . . 81
3.5 Moduli completamente riducibili . . . 86
3.6 Relazioni astratte di dipendenza. Invarianza della dimensione . . . 89
3.7 Prodotti tensoriali di moduli . . . 92
3.8 Bimoduli . . . 97
3.9 Algebre e coalgebre . . . 100
3.10 Moduli proiettivi . . . 108
3.11 Moduli iniettivi. Inviluppo iniettivo . . . 114
3.12 Contesti di Morita . . . 119
3.13 Il teorema di Wedderburn–Artin per gli anelli semplici . . . 125
3.14 Generatori e progeneratori . . . 126
3.15 Equivalenza di categorie di moduli . . . 129

4 Fondamenti della teoria della struttura degli anelli 134
4.1 Primitività e semiprimitività . . . 134
4.2 Il radicale di un anello . . . 140
4.3 Teoremi di densità . . . 143
4.4 Anelli artiniani . . . 147
4.5 Teoria della struttura delle algebre . . . 153
4.6 Algebre semplici centrali di dimensione finita . . . 156
4.7 Il gruppo di Brauer . . . 165
4.8 Algebre di Clifford . . . 167

5 Teoria classica delle rappresentazioni dei gruppi finiti 180
5.1 Rappresentazioni e rappresentazioni matriciali dei gruppi . . . 180
5.2 Completa riducibilità . . . 183
5.3 Applicazione della teoria delle rappresentazioni delle algebre . . . 187
5.4 Rappresentazioni irriducibili di S_n . . . 193
5.5 Caratteri. Relazioni di ortogonalità . . . 196
5.6 Prodotti diretti di gruppi. Caratteri dei gruppi abeliani . . . 204
5.7 Alcune considerazioni aritmetiche . . . 206
5.8 Il teorema di Burnside sui gruppi di ordine $p^a q^b$ . . . 208
5.9 Moduli indotti . . . 210
5.10 Proprietà dell'induzione. Teorema di reciprocità di Frobenius . . . 214
5.11 Ulteriori risultati sui moduli indotti . . . 220
5.12 Il teorema di Brauer sui caratteri indotti . . . 224
5.13 Il teorema di Brauer sui campi di spezzamento . . . 230
5.14 L'indice di Schur . . . 231
5.15 Gruppi di Frobenius . . . 233

6 Elementi di algebra omologica e applicazioni **241**

6.1 Categorie additive e abeliane . . . 241
6.2 Complessi e omologia . . . 244
6.3 La successione esatta lunga di omologia . . . 246
6.4 Omotopia . . . 248
6.5 Risoluzioni . . . 249
6.6 Funtori derivati . . . 251
6.7 Ext . . . 255
6.8 Tor . . . 260
6.9 Coomologia dei gruppi . . . 261
6.10 Estensioni di gruppi . . . 268
6.11 Coomologia delle algebre . . . 274
6.12 Dimensione omologica . . . 278
6.13 Il complesso di Koszul e il teorema delle sizigie di Hilbert . . . 280

7 Teoria degli ideali negli anelli commutativi: teoria generale e anelli noetheriani **288**

7.1 Ideali primi. Nilradicale . . . 288
7.2 Localizzazione degli anelli . . . 291
7.3 Localizzazione dei moduli . . . 294
7.4 Localizzazione rispetto al complementare di un ideale primo. Relazioni locali e globali . . . 297
7.5 Lo spettro primo di un anello commutativo . . . 299
7.6 Dipendenza intera . . . 303
7.7 Domini integralmente chiusi . . . 306
7.8 Rango dei moduli proiettivi . . . 307
7.9 Gruppo delle classi proiettive . . . 311
7.10 Anelli noetheriani . . . 311
7.11 Anelli artiniani commutativi . . . 315
7.12 Varietà algebriche affini. Il Nullstellensatz di Hilbert . . . 317
7.13 Decomposizioni primarie . . . 321
7.14 Il lemma di Artin–Rees. Il teorema di intersezione di Krull . . . 327
7.15 Il polinomio di Hilbert di un modulo graduato . . . 329
7.16 Il polinomio caratteristico di un anello locale noetheriano . . . 332
7.17 Dimensione di Krull . . . 334
7.18 Topologie I-adiche e completamenti . . . 337

8 Teoria dei campi **343**

8.1 Chiusura algebrica di un campo . . . 343
8.2 La corrispondenza di Jacobson–Bourbaki . . . 346

8.3 La teoria di Galois finita . . . 348
8.4 Prodotti incrociati e gruppo di Brauer . . . 351
8.5 Algebre cicliche . . . 357
8.6 Teoria di Galois infinita . . . 358
8.7 Separabilità e normalità . . . 361
8.8 Campi di spezzamento separabili . . . 366
8.9 Estensioni di Kummer . . . 367
8.10 Anelli dei vettori di Witt . . . 370
8.11 p-estensioni abeliane . . . 375
8.12 Basi di trascendenza . . . 380
8.13 Basi di trascendenza dei domini. Algebre affini . . . 381
8.14 Il teorema di Lüroth . . . 383
8.15 Separabilità delle estensioni arbitrarie . . . 388
8.16 Derivazioni . . . 391
8.17 Teoria di Galois per le estensioni puramente inseparabili di esponente uno . . . 399
8.18 Prodotti tensoriali di campi . . . 402
8.19 Compositi liberi di campi . . . 406

9 Teoria delle valutazioni **411**
9.1 Valori assoluti . . . 411
9.2 Il teorema di approssimazione . . . 414
9.3 Valori assoluti su $\mathbb{Q}$ e $F(x)$ . . . 416
9.4 Completamento di un campo . . . 417
9.5 Estensioni di dimensione finita di campi completi. Il caso archimedeo . . . 419
9.6 Valutazioni . . . 422
9.7 Anelli di valutazione e posti . . . 425
9.8 Estensione degli omomorfismi e delle valutazioni . . . 427
9.9 Determinazione dei valori assoluti di un'estensione di dimensione finita . . . 431
9.10 Indice di ramificazione e grado residuo. Valutazioni discrete . . . 433
9.11 Lemma di Hensel . . . 436
9.12 Campi locali . . . 439
9.13 Anelli con divisione localmente compatti totalmente sconnessi . . . 442
9.14 Il gruppo di Brauer di un campo locale . . . 448
9.15 Forme quadratiche sui campi locali . . . 450

10 Domini di Dedekind **456**
10.1 Ideali frazionari. Domini di Dedekind . . . 456
10.2 Caratterizzazioni dei domini di Dedekind . . . 460
10.3 Estensioni intere di domini di Dedekind . . . 464
10.4 Relazioni con la teoria delle valutazioni . . . 466

10.5 Ideali primi ramificati e discriminante 470
10.6 Moduli finitamente generati su un dominio di Dedekind 473

11 Campi formalmente reali **479**
11.1 Campi formalmente reali 479
11.2 Chiusure reali 482
11.3 Elementi totalmente positivi 483
11.4 Il diciassettesimo problema di Hilbert 485
11.5 La teoria di Pfister delle forme quadratiche 488
11.6 Somme di quadrati in $R(x_1, \ldots, x_n)$, con R campo reale chiuso 492
11.7 La caratterizzazione di Artin–Schreier dei campi reali chiusi 497

Indice analitico **500**

I numeri di pagina in questo indice rinviano alla traduzione italiana. Nei due sommari che seguono, nei rimandi di Jacobson e nell'indice analitico si conserva la paginazione delle edizioni inglesi. La sigla BAI indica il primo volume.

Sommario del volume II

Le pagine indicate sono quelle della seconda edizione inglese.

Sommario del volume I x
Prefazione alla seconda edizione xiii
Prefazione alla prima edizione xv

Introduzione **1**
0.1 Il lemma di Zorn 2
0.2 Aritmetica dei numeri cardinali 3
0.3 Numeri ordinali e cardinali 4
0.4 Insiemi e classi 6
Riferimenti bibliografici 7

1 Categorie **8**
1.1 Definizione ed esempi di categorie 9
1.2 Alcune nozioni fondamentali sulle categorie 15
1.3 Funtori e trasformazioni naturali 18
1.4 Equivalenza di categorie 26
1.5 Prodotti e coprodotti 32
1.6 I funtori hom. Funtori rappresentabili 37
1.7 Universali 40
1.8 Funtori aggiunti 45
Riferimenti bibliografici 51

2 Algebra universale **52**
2.1 Ω-algebre 53
2.2 Sottoalgebre e prodotti 58
2.3 Omomorfismi e congruenze 60
2.4 Il reticolo delle congruenze. Prodotti sottodiretti 66
2.5 Limiti diretti e inversi 70
2.6 Ultraprodotti 75
2.7 Ω-algebre libere 78
2.8 Varietà 81
2.9 Prodotti liberi di gruppi 87
2.10 Caratterizzazione interna delle varietà 91
Riferimenti bibliografici 93

3 Moduli **94**
3.1 Le categorie R-**mod** e **mod**-R 95
3.2 Moduli artiniani e noetheriani 100
3.3 Il teorema di raffinamento di Schreier. Il teorema di Jordan–Hölder 104
3.4 Il teorema di Krull–Schmidt 110
3.5 Moduli completamente riducibili 117
3.6 Relazioni astratte di dipendenza. Invarianza della dimensione 122
3.7 Prodotti tensoriali di moduli 125
3.8 Bimoduli 133
3.9 Algebre e coalgebre 137
3.10 Moduli proiettivi 148
3.11 Moduli iniettivi. Inviluppo iniettivo 156
3.12 Contesti di Morita 164
3.13 Il teorema di Wedderburn–Artin per gli anelli semplici 171
3.14 Generatori e progeneratori 173
3.15 Equivalenza di categorie di moduli 177
Riferimenti bibliografici 183

4 Fondamenti della teoria della struttura degli anelli . . . 184
4.1 Primitività e semiprimitività . . . 185
4.2 Il radicale di un anello . . . 192
4.3 Teoremi di densità . . . 197
4.4 Anelli artiniani . . . 202
4.5 Teoria della struttura delle algebre . . . 210
4.6 Algebre semplici centrali di dimensione finita . . . 215
4.7 Il gruppo di Brauer . . . 226
4.8 Algebre di Clifford . . . 228
Riferimenti bibliografici . . . 245

5 Teoria classica delle rappresentazioni dei gruppi finiti . . . 246
5.1 Rappresentazioni e rappresentazioni matriciali di gruppi . . . 247
5.2 Completa riducibilità . . . 251
5.3 Applicazione della teoria delle rappresentazioni delle algebre . . . 257
5.4 Rappresentazioni irriducibili di S_n . . . 265
5.5 Caratteri. Relazioni di ortogonalità . . . 269
5.6 Prodotti diretti di gruppi. Caratteri dei gruppi abeliani . . . 279
5.7 Alcune considerazioni aritmetiche . . . 282
5.8 Il teorema di Burnside sui gruppi di ordine $p^a q^b$ . . . 284
5.9 Moduli indotti . . . 286
5.10 Proprietà dell'induzione. Il teorema di reciprocità di Frobenius . . . 292
5.11 Ulteriori risultati sui moduli indotti . . . 299
5.12 Il teorema di Brauer sui caratteri indotti . . . 305
5.13 Il teorema di Brauer sui campi di spezzamento . . . 313
5.14 L'indice di Schur . . . 314
5.15 Gruppi di Frobenius . . . 317
Riferimenti bibliografici . . . 325

6 Elementi di algebra omologica con applicazioni . . . 326
6.1 Categorie additive e abeliane . . . 327
6.2 Complessi e omologia . . . 331
6.3 La successione esatta lunga di omologia . . . 334
6.4 Omotopia . . . 337
6.5 Risoluzioni . . . 339
6.6 Funtori derivati . . . 342
6.7 Ext . . . 346
6.8 Tor . . . 353
6.9 Coomologia dei gruppi . . . 355
6.10 Estensioni di gruppi . . . 363
6.11 Coomologia delle algebre . . . 370
6.12 Dimensione omologica . . . 375
6.13 Il complesso di Koszul e il teorema delle sizigie di Hilbert . . . 378
Riferimenti bibliografici . . . 387

7 Teoria degli ideali negli anelli commutativi. Teoria generale e anelli noetheriani 388
7.1 Ideali primi. Nilradicale . . . 389
7.2 Localizzazione di anelli . . . 393
7.3 Localizzazione di moduli . . . 397
7.4 Localizzazione rispetto al complementare di un ideale primo. Relazioni fra proprietà locali e globali . . . 400
7.5 Spettro primo di un anello commutativo . . . 403
7.6 Dipendenza integrale . . . 408
7.7 Domini integralmente chiusi . . . 412
7.8 Rango dei moduli proiettivi . . . 414
7.9 Il gruppo delle classi proiettive . . . 419
7.10 Anelli noetheriani . . . 420
7.11 Anelli commutativi artiniani . . . 425
7.12 Varietà algebriche affini. Il teorema degli zeri di Hilbert . . . 427
7.13 Decomposizioni primarie . . . 433
7.14 Il lemma di Artin–Rees. Il teorema di intersezione di Krull . . . 440
7.15 Il polinomio di Hilbert di un modulo graduato . . . 443
7.16 Il polinomio caratteristico di un anello locale noetheriano . . . 448
7.17 Dimensione di Krull . . . 450
7.18 Topologie I-adiche e completamenti . . . 455
Riferimenti bibliografici . . . 462

8 Teoria dei campi . . . 463
8.1 Chiusura algebrica di un campo . . . 464
8.2 La corrispondenza di Jacobson–Bourbaki . . . 468
8.3 Teoria di Galois finita . . . 471
8.4 Prodotti incrociati e gruppo di Brauer . . . 475
8.5 Algebre cicliche . . . 484
8.6 Teoria di Galois infinita . . . 486
8.7 Separabilità e normalità . . . 489
8.8 Campi di spezzamento separabili . . . 495
8.9 Estensioni di Kummer . . . 498
8.10 Anelli di vettori di Witt . . . 501
8.11 p-estensioni abeliane . . . 509
8.12 Basi di trascendenza . . . 514
8.13 Basi di trascendenza per domini. Algebre affini . . . 517
8.14 Il teorema di Lüroth . . . 520
8.15 Separabilità per estensioni di campi arbitrarie . . . 525
8.16 Derivazioni . . . 530
8.17 Teoria di Galois per estensioni puramente inseparabili di esponente uno . . . 541
8.18 Prodotti tensoriali di campi . . . 544
8.19 Compositi liberi di campi . . . 550
Riferimenti bibliografici . . . 556

9 Teoria delle valutazioni **557**
9.1 Valori assoluti 558
9.2 Il teorema di approssimazione 562
9.3 Valori assoluti su $\mathbb{Q}$ e su $F(x)$ 564
9.4 Completamento di un campo 566
9.5 Estensioni di grado finito di campi completi. Il caso archimedeo 569
9.6 Valutazioni 573
9.7 Anelli di valutazione e posti 577
9.8 Estensione di omomorfismi e valutazioni 580
9.9 Determinazione dei valori assoluti di un'estensione di grado finito 585
9.10 Indice di ramificazione e grado residuo. Valutazioni discrete 588
9.11 Il lemma di Hensel 592
9.12 Campi locali 595
9.13 Corpi totalmente sconnessi localmente compatti 599
9.14 Il gruppo di Brauer di un campo locale 608
9.15 Forme quadratiche su campi locali 611
Riferimenti bibliografici 618

10 Domini di Dedekind **619**
10.1 Ideali frazionari. Domini di Dedekind 620
10.2 Caratterizzazioni dei domini di Dedekind 625
10.3 Estensioni integrali di domini di Dedekind 631
10.4 Relazioni con la teoria delle valutazioni 634
10.5 Ideali primi ramificati e discriminante 639
10.6 Moduli finitamente generati su un dominio di Dedekind 643
Riferimenti bibliografici 649

11 Campi formalmente reali **650**
11.1 Campi formalmente reali 651
11.2 Chiusure reali 655
11.3 Elementi totalmente positivi 657
11.4 Il diciassettesimo problema di Hilbert 660
11.5 La teoria di Pfister delle forme quadratiche 663
11.6 Somme di quadrati in $R(x_1, \ldots, x_n)$, con R campo reale chiuso 669
11.7 La caratterizzazione di Artin–Schreier dei campi reali chiusi 674
Riferimenti bibliografici 677

Indice analitico **679**

Sommario del volume I

Le pagine indicate sono quelle della seconda edizione inglese del primo volume.

Introduzione. Nozioni di teoria degli insiemi. Gli interi **1**
0.1 L'insieme delle parti di un insieme 3
0.2 Il prodotto cartesiano. Applicazioni 4
0.3 Relazioni di equivalenza. Fattorizzazione di un'applicazione attraverso una relazione di equivalenza 10
0.4 I numeri naturali 15
0.5 Il sistema $\mathbb{Z}$ dei numeri interi 19
0.6 Alcuni fatti aritmetici fondamentali su $\mathbb{Z}$ 22
0.7 Un cenno ai numeri cardinali 24

1 Monoidi e gruppi **26**
1.1 Monoidi di trasformazioni e monoidi astratti 28
1.2 Gruppi di trasformazioni e gruppi astratti 31
1.3 Isomorfismo. Il teorema di Cayley 36
1.4 Associatività generalizzata. Commutatività 39
1.5 Sottomonoidi e sottogruppi generati da un sottoinsieme. Gruppi ciclici 42
1.6 Decomposizione delle permutazioni in cicli 48
1.7 Orbite. Classi laterali di un sottogruppo 51
1.8 Congruenze. Monoidi e gruppi quoziente 54
1.9 Omomorfismi 58
1.10 Sottogruppi di un'immagine omomorfa. Due teoremi fondamentali di isomorfismo . . . 64
1.11 Oggetti liberi. Generatori e relazioni 67
1.12 Gruppi che agiscono su insiemi 71
1.13 I teoremi di Sylow 79

2 Anelli **85**
2.1 Definizione e proprietà elementari 86
2.2 Tipi di anelli 90
2.3 Anelli di matrici 92
2.4 Quaternioni 98
2.5 Ideali e anelli quoziente 101
2.6 Ideali e anelli quoziente di $\mathbb{Z}$ 103
2.7 Omomorfismi di anelli. Teoremi fondamentali 106
2.8 Anti-isomorfismi 111
2.9 Campo delle frazioni di un dominio commutativo 115
2.10 Anelli di polinomi 119
2.11 Alcune proprietà degli anelli di polinomi e loro applicazioni 127
2.12 Funzioni polinomiali 134
2.13 Polinomi simmetrici 138
2.14 Monoidi e anelli fattoriali 140
2.15 Domini a ideali principali e domini euclidei 147
2.16 Estensioni polinomiali dei domini fattoriali 151
2.17 «Rng»: anelli senza unità 155

3 Moduli su un dominio a ideali principali **157**
3.1 L'anello degli endomorfismi di un gruppo abeliano 158
3.2 Moduli sinistri e destri 163
3.3 Nozioni e risultati fondamentali 166
3.4 Moduli liberi e matrici 170
3.5 Somme dirette di moduli 175
3.6 Moduli finitamente generati su un dominio a ideali principali. Risultati preliminari . . 179
3.7 Equivalenza delle matrici a coefficienti in un dominio a ideali principali 181
3.8 Teorema di struttura dei moduli finitamente generati su un dominio a ideali principali . 187
3.9 Moduli di torsione e componenti primarie. Teorema di invarianza 189
3.10 Applicazioni ai gruppi abeliani e alle trasformazioni lineari 194
3.11 L'anello degli endomorfismi di un modulo finitamente generato su un dominio a ideali principali 204

4 Teoria di Galois delle equazioni **210**
4.1 Risultati preliminari, alcuni già noti, altri nuovi 213
4.2 Costruzioni con riga e compasso 216
4.3 Campo di spezzamento di un polinomio 224
4.4 Radici multiple 229
4.5 Il gruppo di Galois. La corrispondenza fondamentale di Galois 234
4.6 Alcuni risultati sui gruppi finiti 244
4.7 Il criterio di Galois per la risolubilità per radicali 251
4.8 Il gruppo di Galois come gruppo di permutazioni delle radici 256
4.9 L'equazione generale di grado n 262
4.10 Equazioni a coefficienti razionali aventi per gruppo di Galois il gruppo simmetrico . . . 267
4.11 Poligoni regolari costruibili di n lati 271
4.12 Trascendenza di e e di π. Il teorema di Lindemann–Weierstrass 277
4.13 Campi finiti 287
4.14 Basi speciali per le estensioni di grado finito 290
4.15 Tracce e norme 296
4.16 Riduzione modulo p 301

5 Equazioni e disuguaglianze polinomiali reali **306**
5.1 Campi ordinati. Campi reali chiusi 307
5.2 Il teorema di Sturm 311
5.3 Formalizzazione dell'algoritmo euclideo e teorema di Sturm 316
5.4 Procedimenti di eliminazione. Risultanti 322
5.5 Un metodo di decisione per una curva algebrica 327
5.6 Il teorema di Sturm generalizzato. Il principio di Tarski 335

6 Spazi vettoriali metrici e gruppi classici 342
6.1 Funzionali lineari e forme bilineari 343
6.2 Forme alternanti 349
6.3 Forme quadratiche e forme bilineari simmetriche 354
6.4 Nozioni fondamentali di geometria ortogonale 361
6.5 Il teorema di cancellazione di Witt 367
6.6 Il teorema di Cartan–Dieudonné 371
6.7 Struttura del gruppo lineare generale $\mathrm{GL}_n(F)$ 375
6.8 Struttura dei gruppi ortogonali 382
6.9 Geometria simplettica. Il gruppo simplettico 391
6.10 Ordini dei gruppi ortogonali e simplettici su un campo finito 398
6.11 Postilla sulle forme hermitiane e sulla geometria unitaria 401

7 Algebre su un campo 405
7.1 Definizione ed esempi di algebre associative 406
7.2 Algebre esterne. Applicazione ai determinanti 411
7.3 Rappresentazioni matriciali regolari delle algebre associative. Norme e tracce 422
7.4 Cambiamento del campo di base. Transitività della traccia e della norma 426
7.5 Algebre non associative. Algebre di Lie e di Jordan 430
7.6 Il problema di Hurwitz. Algebre di composizione 438
7.7 I teoremi di Frobenius e di Wedderburn sulle algebre associative di divisione 451

8 Reticoli e algebre di Boole 455
8.1 Insiemi parzialmente ordinati e reticoli 456
8.2 Distributività e modularità 461
8.3 Il teorema di Jordan–Hölder–Dedekind 466
8.4 Il reticolo dei sottospazi di uno spazio vettoriale. Il teorema fondamentale della geometria proiettiva 468
8.5 Algebre di Boole 474
8.6 La funzione di Möbius di un insieme parzialmente ordinato 480

Prefazione alla seconda edizione

Le modifiche più ampie di questa edizione riguardano la parte del libro dedicata all'algebra commutativa, in particolare il capitolo 7, *Teoria degli ideali negli anelli commutativi: teoria generale e anelli noetheriani*, il capitolo 8, *Teoria dei campi*, e il capitolo 9, *Teoria delle valutazioni*. Nel capitolo 7 abbiamo rielaborato l'esposizione della dipendenza integrale, mettendo in risalto le relazioni fra un anello e le sue estensioni intere (teoremi di *lying over*, *going up* e *going down*). Il § 7.7, *Domini integralmente chiusi*, è nuovo, come pure tre paragrafi del capitolo 8: il § 8.13, *Basi di trascendenza per i domini*, il § 8.18, *Prodotti tensoriali di campi*, e il § 8.19, *Compositi liberi di campi*. Questi ultimi due sono tratti dal terzo volume delle nostre *Lectures in Abstract Algebra* (D. Van Nostrand, 1964; Springer-Verlag, 1980). L'aggiunta più significativa al capitolo 9 è il lemma di Krasner, di cui ci serviamo per dare una dimostrazione migliore di un classico teorema di Kürschák del 1913. Abbiamo anche migliorato la dimostrazione del teorema che riguarda il prolungamento dei valori assoluti a un'estensione di grado finito di un campo (teorema 9.13), basandoci sulla nozione di composito di campi considerata nel nuovo § 8.18.

Nel capitolo 4, *Fondamenti della teoria della struttura degli anelli*, abbiamo migliorato l'esposizione di due argomenti: la caratterizzazione dei campi di spezzamento di grado finito delle algebre semplici centrali e il fatto che le classi di Brauer delle algebre semplici centrali su un campo assegnato costituiscono un insieme, fatto necessario per definire il gruppo di Brauer $\mathrm{Br}(F)$. Nel capitolo sull'algebra omologica (capitolo 6) abbiamo migliorato la dimostrazione dell'esistenza di una risoluzione proiettiva di una successione esatta corta di moduli.

Abbiamo aggiunto alcuni esercizi nuovi ed eliminato alcuni esercizi difettosi.

Alcune delle modifiche sono nate da suggerimenti dei nostri colleghi Walter Feit, George Seligman e Tsuneo Tamagawa. A loro, a Ronnie Lee, a Sidney Porter (già nostro studente di dottorato) e ai traduttori cinesi del libro, i professori Cao Xi-hua e Wang Jian-pan, dobbiamo la segnalazione di alcuni errori della prima edizione, ora corretti. Siamo loro davvero grati per l'interesse dimostrato e per l'importante contributo alla nuova edizione. Ringraziamo di cuore anche F. D. Jacobson, che ha letto le bozze del testo e, soprattutto, ha aggiornato l'indice analitico.

Nathan Jacobson
Gennaio 1989

Prefazione alla prima edizione

Questo volume è un testo per un secondo corso di algebra. Presuppone un corso introduttivo in cui si sia trattata materia del tipo di quella contenuta nell'introduzione e nei primi tre o quattro capitoli di *Algebra di base I*. Tali capitoli riguardavano i rudimenti della teoria degli insiemi, la teoria dei gruppi, gli anelli, i moduli, in particolare quelli su un dominio a ideali principali, e la teoria di Galois, imperniata sui problemi classici della risolubilità per radicali delle equazioni e delle costruzioni con riga e compasso.

Algebra di base II contiene ben più materiale di quanto si possa svolgere in un corso annuale. Per costruire un programma realistico occorrerà scegliere i capitoli e delimitare gli argomenti anche al loro interno. Indichiamo brevemente alcune possibilità. Si potrebbero svolgere il capitolo 1, aggiungendo il § 2.9 a complemento del § 1.5, i capitoli 3 e 4, il capitolo 6 fino al § 6.11, il capitolo 7 fino al § 7.13, i §§ 8.1–8.3, 8.6 e 8.12 e il capitolo 9 fino al § 9.13. Una lieve variante consisterebbe nel sostituire i §§ 4.6–4.8 con i §§ 5.1–5.5 e 5.9. Per gli studenti che non abbiano mai studiato la teoria di Galois sarà opportuno integrare il § 8.3 con una parte del capitolo 4 di *Algebra di base I*. Se uno degli obiettivi principali del corso è comprendere i fondamenti delle strutture algebriche e il rapporto fra algebra e logica matematica, converrà includervi l'intero capitolo 2. Naturalmente ciò imporrà di ridurre altre parti, per esempio l'algebra omologica. Vi sono molte altre possibilità per un corso annuale basato su questo testo.

Ogni capitolo approfondisce la materia quanto basta perché il testo possa servire anche a corsi specialistici. Per esempio, i capitoli 3, 4 e 5 potrebbero costituire un corso semestrale sulla teoria delle rappresentazioni dei gruppi finiti. Il capitolo 7 e parti dei capitoli 8, 9 e 10 potrebbero servire per un corso semestrale di algebra commutativa. I capitoli 1, 3 e 6 si prestano a un corso introduttivo di algebra omologica.

Il capitolo 11 sui campi reali è piuttosto indipendente dal resto del volume. Costituisce tuttavia una prosecuzione diretta del capitolo 5 di *Algebra di base I* e comprende una soluzione del problema di Hilbert sulle funzioni razionali semidefinite positive, basata su un teorema di Tarski dimostrato nel capitolo 5 del primo volume. Il capitolo 11 contiene anche la bella teoria delle forme quadratiche di Pfister, che permette di stabilire il numero minimo di quadrati occorrenti per esprimere una somma di quadrati di funzioni razionali di n variabili reali (si veda il § 11.5).

Oltre che come testo per un corso, il libro è concepito per la lettura autonoma da parte di studenti con la preparazione indicata. Vi abbiamo raccolto molto materiale. Crediamo tuttavia che quasi tutto possa interessare matematici di orientamento diverso, anche al di fuori della cerchia degli specialisti di algebra. A questo pubblico più vasto abbiamo pensato anche cercando di ridurre al minimo la terminologia tecnica ed evitando di costruire un apparato troppo elaborato prima di presentare i risultati di interesse. Talvolta ne abbiamo pagato il prezzo con dimostrazioni che allo specialista potranno apparire un po' pesanti.

Il testo comprende numerosi esercizi. Alcuni enunciano ulteriori risultati interessanti, accompagnati da un abbozzo di dimostrazione. A relegarli fra gli esercizi ci ha indotti semplicemente il desiderio di contenere un poco la mole del testo. Consigliamo al lettore di svolgerne un buon numero.

Una bibliografia estesa ci è parsa poco adatta a un testo di questo tipo. Al suo posto abbiamo indicato, alla fine di ogni capitolo, uno o due testi specialistici nei quali il lettore troverà ampie bibliografie sull'argomento. Di tanto in tanto abbiamo incluso nel nostro breve elenco anche uno o due articoli di importanza storica. Nel farlo non abbiamo seguito criteri sistematici né aspirato alla completezza.

Mi è ancora una volta gradito riconoscere l'aiuto di tanti amici che mi hanno suggerito come

migliorare le precedenti stesure del testo. Desidero ricordare per primi gli studenti, che con occhio attento hanno scoperto difetti nell'esposizione e talvolta mi hanno suggerito dimostrazioni migliori incontrate altrove. Fra gli studenti che così hanno contribuito ricordo Monica Barattieri, Ying Cheng, Daniel Corro, William Ellis, Craig Huneke e Kenneth McKenna. Preziosi suggerimenti mi sono venuti dai professori Kevin McCrimmon, James D. Reid, Robert L. Wilson e Daniel Zelinsky, come pure dai miei colleghi Walter Feit, George Seligman e Tsuneo Tamagawa. Del gravoso compito di correggere le bozze si sono fatti carico in gran parte Ying Cheng, la professoressa Florence Jacobson e James Reid. Florence Jacobson ha collaborato alla compilazione dell'indice analitico. Desidero infine ricordare l'ottimo lavoro di dattiloscrittura di Joyce Harry e Donna Belli. A tutti loro devo molto e colgo l'occasione per esprimere il mio sincero ringraziamento.

Nathan Jacobson
Gennaio 1980

Introduzione

Nell'introduzione a *Basic Algebra I* (che abbrevieremo sempre in «BAI») abbiamo esposto le nozioni di teoria degli insiemi necessarie per quel volume. Fra queste figuravano l'insieme delle parti $\mathcal{P}(S)$ di un insieme S, il prodotto cartesiano $S_1 \times S_2$ di due insiemi S_1 e S_2, le applicazioni (o funzioni) e le relazioni di equivalenza. Nel primo volume abbiamo generalmente preferito argomenti costruttivi e abbiamo evitato del tutto i metodi transfiniti.

I risultati presentati in questo volume richiedono strumenti più potenti, in particolare per la dimostrazione di certi teoremi di esistenza. Molte di queste dimostrazioni si baseranno su un risultato detto *lemma di Zorn*. Fu Max Zorn a osservare per primo quanto fosse utile per dimostrare teoremi di esistenza di questo tipo. Ci occorreranno anche alcuni risultati sull'aritmetica dei numeri cardinali. Tutto ciò rientra nel quadro dell'assiomatizzazione di Zermelo–Fraenkel della teoria degli insiemi, comprendente l'assioma della scelta (la cosiddetta teoria degli insiemi ZFC). Per i particolari che ometteremo nella nostra esposizione si possono consultare due ottimi testi, *Naive Set Theory* di P. R. Halmos e il più ampio *Set Theory and the Continuum Hypothesis* di P. J. Cohen.

La matematica classica si occupa quasi esclusivamente di strutture definite su insiemi. La teoria delle categorie, che introdurremo nel capitolo 1, si occupa invece di collezioni di insiemi, come la collezione di tutti i gruppi, che richiedono un trattamento diverso da quello riservato agli insiemi. Tali collezioni si chiamano *classi*. Nell'ultimo paragrafo di questa introduzione accenneremo a un possibile fondamento della teoria delle categorie.

0.1 Il lemma di Zorn

Formuleremo ora un principio di massimalità della teoria degli insiemi, detto lemma di Zorn. Lo enunciamo dapprima per i sottoinsiemi di un insieme dato. Ricordiamo che un insieme C di sottoinsiemi di un insieme S (ossia un sottoinsieme dell'insieme delle parti $\mathcal{P}(S)$) si chiama *catena* se C è totalmente ordinato per inclusione, vale a dire se, comunque si scelgano $A, B \in C$, si ha $A \subset B$ oppure $B \subset A$. Un insieme T di sottoinsiemi di S si dice *induttivo* se l'unione $\bigcup A_\alpha$ di ogni catena $C = \{A_\alpha\} \subset T$ appartiene a T. Possiamo ora enunciare il seguente lemma.

Lemma di Zorn (prima formulazione). *Sia T un insieme non vuoto di sottoinsiemi di un insieme S. Supponiamo che T sia induttivo. Allora T contiene un elemento massimale, ossia esiste $M \in T$ tale che nessun $A \in T$ contenga propriamente M.*

Esiste un'altra formulazione del lemma di Zorn in termini di insiemi parzialmente ordinati (BAI, p. 456). Sia $(P, \geq)$ un insieme parzialmente ordinato. Diremo che $(P, \geq)$ è *totalmente* (o *linearmente*) *ordinato* se per ogni $a, b \in P$ si ha $a \geq b$ oppure $b \geq a$. Diremo che P è *induttivo* se ogni sottoinsieme non vuoto C di P, totalmente ordinato dalla relazione $\geq$ definita in P, ammette un estremo superiore in P. Ciò significa che esiste un $u \in P$ tale che $u \geq a$ per ogni $a \in C$ e che, se $v \geq a$ per ogni $a \in C$, allora $v \geq u$. Si ha quindi il seguente enunciato.

Lemma di Zorn (seconda formulazione). *Sia $(P, \geq)$ un insieme parzialmente ordinato induttivo.*[1] *Allora P contiene elementi massimali, ossia esiste $m \in P$ tale che nessun $a \in P$ soddisfi $m < a$.*

Si vede facilmente che le due formulazioni del lemma di Zorn sono equivalenti, sicché possiamo riferirci indifferentemente all'una o all'altra come al «lemma di Zorn». Si può dimostrare che il lemma di Zorn equivale all'assioma seguente.

Assioma della scelta. *Siano S un insieme e $\mathcal{P}(S)^*$ l'insieme dei sottoinsiemi non vuoti di S.*

[1] Si sottintende che P sia non vuoto. [N.d.T.]

Esiste allora un'applicazione f (una «funzione di scelta») di $\mathcal{P}(S)^*$ in S tale che $f(A) \in A$ per ogni $A \in \mathcal{P}(S)^*$.

Anche il seguente enunciato è equivalente all'assioma della scelta. Se $\{A_\alpha\}$ è un insieme di insiemi non vuoti A_α, allora il prodotto cartesiano $\prod A_\alpha$ è diverso da $\varnothing$.

Che l'assioma della scelta implichi il lemma di Zorn si può dimostrare mediante un argomento di cui E. Zermelo si servì per provare che ogni insieme può essere ben ordinato (si veda Halmos, pp. 62–65). Un insieme S è *ben ordinato* da una relazione d'ordine $\geq$ se ogni sottoinsieme non vuoto di S ha un minimo. Anche il teorema del buon ordinamento equivale al lemma di Zorn e all'assioma della scelta. Nel prossimo paragrafo illustreremo l'uso del lemma di Zorn.

0.2 Aritmetica dei numeri cardinali

Seguendo Halmos, enunceremo dapprima i principali risultati dell'aritmetica cardinale senza definire i numeri cardinali. Diciamo che gli insiemi A e B hanno la *stessa cardinalità*, e scriviamo $|A| = |B|$, se esiste un'applicazione biiettiva di A su B. Scriviamo $|A| \leq |B|$ se esiste un'applicazione iniettiva di A in B, e $|A| < |B|$ se $|A| \leq |B|$ e $|A| \neq |B|$. Con queste notazioni, il teorema di Schröder–Bernstein (BAI, p. 25) si enuncia così: $|A| \leq |B|$ e $|B| \leq |A|$ se e solo se $|A| = |B|$. Un insieme F è *finito* se $|F| = |N|$ per un certo $N = \{0, 1, \ldots, n-1\}$, mentre A è *infinito numerabile* se $|A| = |\omega|$, dove $\omega = \{0, 1, 2, \ldots\}$. Dall'assioma della scelta segue che, se A è infinito (cioè non finito), allora $|\omega| \leq |A|$. Abbiamo anche il teorema di Cantor, secondo il quale $|A| < |\mathcal{P}(A)|$ per ogni A.

Per insiemi A, B, C scriviamo $C = A \dot\cup B$ se $C = A \cup B$ e $A \cap B = \varnothing$. È chiaro che, se $|A_1| \leq |A_2|$ e $|B_1| \leq |B_2|$, allora $|A_1 \dot\cup B_1| \leq |A_2 \dot\cup B_2|$. Sia $C = F \dot\cup \omega$, con F finito, ad esempio $F = \{x_0, \ldots, x_{n-1}\}$ con $x_i \neq x_j$ per $i \neq j$. L'applicazione di C in ω definita da $x_i \mapsto i$ e da $k \mapsto k + n$ per $k \in \omega$ è biiettiva. Dunque $|C| = |\omega|$. Poiché $|\omega| \leq |A|$ per ogni insieme infinito A, ne segue che, se $C = F \dot\cup A$, allora $|C| = |A|$. Infatti possiamo scrivere $A = D \dot\cup B$ con $|D| = |\omega|$. Abbiamo allora una biiezione di $F \cup D$ su D, che possiamo estendere con l'identità su B ottenendo una biiezione di C su A.

Possiamo servirci del risultato precedente e del lemma di Zorn per dimostrare il risultato fondamentale sull'«addizione dei cardinali», che si enuncia così: se A è infinito e $C = A \cup B$, con $|B| = |A|$, allora $|C| = |A|$. Per A numerabile ciò è evidente dalla decomposizione $\omega = \{0, 2, 4, \ldots\} \dot\cup \{1, 3, 5, \ldots\}$. È inoltre chiaro che il risultato equivale all'uguaglianza $|A \times 2| = |A|$, dove $2 = \{0, 1\}$, poiché $|A \times 2| = |A \dot\cup B|$. Dimostriamo dunque che $|A \times 2| = |A|$ per A infinito. Consideriamo l'insieme delle coppie (X, f) in cui X è un sottoinsieme infinito di A e f è un'applicazione biiettiva di $X \times 2$ su X. Questo insieme non è vuoto, poiché A contiene sottoinsiemi infiniti numerabili X e, per ciascuno di essi, esistono biiezioni di $X \times 2$ su X. Ordiniamo l'insieme $\{(X, f)\}$ ponendo $(X, f) \leq (X', f')$ se $X \subset X'$ e f' è un prolungamento di f. È chiaro che $(\{(X, f)\}, \leq)$ è un insieme parzialmente ordinato induttivo. Per il lemma di Zorn esiste dunque un elemento massimale (Y, g) di $\{(X, f)\}$. Affermiamo che $A - Y$ è finito. Infatti, se $A - Y$ fosse infinito, conterrebbe un sottoinsieme infinito numerabile D e g si potrebbe prolungare a una biiezione di $(Y \dot\cup D) \times 2$ su $Y \dot\cup D$, contro la massimalità di (Y, g). Dunque $A - Y$ è finito. Allora

$$\begin{aligned} |A \times 2| &= \big|\big((Y \times 2) \cup (A - Y)\big) \times 2\big| = |Y \times 2| \\ &= |Y| = |A|. \end{aligned}$$

Possiamo estendere leggermente quest'ultimo risultato e scrivere

$$|A \dot\cup B| = |B| \tag{1}$$

se B è infinito e $|B| \geq |A|$. Ciò segue dalle relazioni

$$|B| \leq |A \cup B| \leq |B \times 2| = |B|.$$

Al lettore è certamente noto che $|A \times A| = |A|$ se A è infinito numerabile. Lo si vede enumerando $\omega \times \omega$ nell'ordine

$$(0,0),\ (0,1),\ (1,0),\ (0,2),\ (1,1),\ (2,0),\ \ldots .$$

Più in generale si ha $|A \times A| = |A|$ per ogni insieme infinito A. La dimostrazione è simile a quella data per l'addizione. Consideriamo l'insieme delle coppie (X, f) in cui X è un sottoinsieme infinito di A e f è una biiezione di $X \times X$ su X, e ordiniamo l'insieme $\{(X, f)\}$ come prima. Per il lemma di Zorn esiste in questo insieme un elemento massimale (Y, g). Se $|Y| = |A|$, segue il risultato che vogliamo dimostrare. Supponiamo dunque $|Y| < |A|$. Dalla relazione $A = Y \dot{\cup} (A - Y)$ e dal risultato sull'addizione segue che $|A| = |A - Y|$. Pertanto $|A - Y| > |Y|$. Allora $A - Y$ contiene un sottoinsieme Z tale che $|Z| = |Y|$. Poniamo $W = Y \cup Z$. Si ha così $W = Y \dot{\cup} Z$ e $W \times W$ è l'unione disgiunta degli insiemi $Y \times Y$, $Y \times Z$, $Z \times Y$ e $Z \times Z$. Abbiamo

$$|(Y \times Z) \cup (Z \times Y) \cup (Z \times Z)| = |Z \times Z| = |Z|.$$

Possiamo dunque prolungare g a una biiezione di $W \times W$ su W. Ciò contraddice la massimalità di (Y, g). Quindi $|Y| = |A|$ e la dimostrazione è completa.

Vale anche un risultato più forte: se $A \neq \varnothing$, B è infinito e $|B| \geq |A|$, allora

$$|A \times B| = |B|. \tag{2}$$

Ciò segue dalle relazioni

$$|B| \leq |A \times B| \leq |B \times B| = |B|.$$

0.3 Numeri ordinali e cardinali

Nella teoria assiomatica degli insiemi non si distingue fra insiemi ed elementi. Si scrive $A \in B$ per dire «l'insieme A è un elemento dell'insieme B». Occorre distinguere questa scrittura da $A \subset B$, che si legge «A è un sottoinsieme di B». (Nei testi di teoria degli insiemi si trova $A \subseteq B$ per il nostro $A \subset B$, e $A \subset B$ per il nostro $A \subsetneq B$.) Per definizione, $A \subset B$ significa che $C \in A$ implica $C \in B$. Uno degli assiomi della teoria degli insiemi afferma che, dato un insieme arbitrario C di insiemi, esiste un insieme che è l'unione degli insiemi appartenenti a C. In altre parole, per ogni insieme C esiste un insieme U tale che $A \in U$ se e solo se esiste un B tale che $A \in B$ e $B \in C$. In particolare, per ogni insieme A possiamo formare il *successore* $A^+ = A \cup \{A\}$, dove $\{A\}$ è l'insieme il cui unico elemento è A.

Il procedimento di formazione dei successori permette di definire l'insieme ω ($= \mathbb{N}$) dei numeri naturali. Poniamo $0 = \varnothing$, $1 = \varnothing^+ = \{\varnothing\}$, $2 = 1^+, \ldots, n+1 = n^+, \ldots$, e definiamo ω come l'unione dell'insieme dei numeri naturali n. Il numero naturale n e l'insieme ω sono numeri ordinali nel senso che preciseremo ora. Diciamo anzitutto che un insieme S è *transitivo* se da $A \in S$ e $B \in A$ segue $B \in S$. Ciò equivale a dire che ogni elemento di S è un sottoinsieme di S. Possiamo ora dare la definizione seguente.

Definizione 0.1. *Un ordinale è un insieme α ben ordinato da $\in$ e transitivo.*

La condizione $A \in A$ è esclusa dagli assiomi della teoria degli insiemi. Per $A, B \in \alpha$ scriviamo $A \leq B$ se $A \in B$ oppure $A = B$. Si vede facilmente che ogni numero naturale n è un ordinale e che l'insieme ω dei numeri naturali è un ordinale. Anche $\omega^+, (\omega^+)^+, \ldots$ sono ordinali. L'unione di questi insiemi è a sua volta un ordinale, che si indica con $\omega + \omega$ o con $\omega \times 2$.

Enunceremo ora senza dimostrazione alcune delle principali proprietà dei numeri ordinali.

Due insiemi parzialmente ordinati $(S_1, \leq_1)$ e $(S_2, \leq_2)$ si dicono *simili* se esiste una biiezione di S_1 su S_2 che conservi l'ordine. Gli ordinali costituiscono un sistema di rappresentanti delle classi di similitudine degli insiemi ben ordinati. Vale infatti il seguente teorema: se $(S, \leq)$ è ben ordinato, esistono un unico ordinale α e un'unica biiezione di S su α che conservi l'ordine. Se α e β sono ordinali, si ha $\alpha = \beta$, oppure $\alpha < \beta$, oppure $\beta < \alpha$. Un ordinale α si chiama *successore* se esiste un ordinale β tale che $\alpha = \beta^+$. In caso contrario, α si chiama *ordinale limite*. Ogni insieme non vuoto di ordinali ha un minimo.

Definizione 0.2. *Un numero cardinale è un ordinale α tale che, per ogni ordinale β di cardinalità $|\beta| = |\alpha|$, si ha $\alpha \leq \beta$.*

Un numero cardinale o è finito o è un ordinale limite. D'altra parte, non tutti gli ordinali limite sono cardinali. Ad esempio, $\omega + \omega$ non è un cardinale. Il più piccolo cardinale infinito è ω. Per indicare i cardinali si usa spesso la lettera ebraica «aleph» $\aleph$ munita di un indice. In questa notazione si scrive $\aleph_0$ per ω.

Poiché ogni insieme può essere ben ordinato, per ogni insieme dato S esiste un unico cardinale α tale che $|\alpha| = |S|$. Chiameremo d'ora in avanti α il *numero cardinale*, o la *cardinalità*, di S, e scriveremo $|S| = \alpha$. Dai risultati del paragrafo precedente ricaviamo le seguenti formule per le cardinalità:

$$|A \cup B| = |B| \tag{3}$$

se B è infinito e $|B| \geq |A|$. Qui, a differenza di quanto accade nella formula (1), $|S|$ indica il numero cardinale dell'insieme S. Analogamente si ha

$$|A \times B| = |B| \tag{4}$$

se A non è vuoto e $|B|$ è infinito e maggiore o uguale a $|A|$.

0.4 Insiemi e classi

Esiste un'assiomatizzazione della teoria degli insiemi, diversa dal sistema ZF, che permette di trattare collezioni di insiemi che possono non essere a loro volta insiemi. Si tratta del sistema di assiomi di Gödel–Bernays (o sistema GB). Gli oggetti primitivi di questo sistema sono le «classi» e gli «insiemi» o, più precisamente, le variabili di classe e le variabili di insieme, insieme con una relazione $\in$. Una caratteristica del sistema è che le classi che appartengono ad altre classi sono insiemi. Vale cioè l'assioma: se $Y \in X$, allora Y è un insieme.

Intuitivamente si può pensare alle classi come a collezioni di insiemi definite da certe proprietà. Una parte del sistema GB riguarda le operazioni che si possono eseguire sulle classi e che corrispondono a combinazioni di proprietà. Un esempio tipico è l'intersezione di classi, espressa come segue: per ogni X e Y esiste uno Z tale che $u \in Z$ se e solo se $u \in X$ e $u \in Y$. Abbiamo dato qui il significato intuitivo dell'assioma

$$\forall X\, \forall Y\, \exists Z\, \forall u\, (u \in Z \iff (u \in X \text{ e } u \in Y)),$$

dove $\forall$ si legge «per ogni» e $\exists$ si legge «esiste». Un altro esempio è il seguente: per ogni X esiste un Y tale che $u \in Y$ se e solo se $u \notin X$. In simboli,

$$\forall X\, \exists Y\, \forall u\, (u \in Y \iff \sim(u \in X)),$$

dove $\sim(\ldots)$ è la negazione di $(\ldots)$. Altre costruzioni di classi corrispondono alle unioni, e così via. Per una trattazione dei sistemi ZF e GB e delle loro relazioni rimandiamo al libro di Cohen.

Qui ci limitiamo a osservare che si può dimostrare che ogni teorema di ZF è un teorema di GB e che ogni teorema di GB che si riferisca soltanto a insiemi è un teorema di ZF.

Nel seguito faremo uso delle classi nello studio delle categorie e in pochi altri punti, nei quali incontreremo classi che poi dimostreremo essere insiemi, facendo vedere che si possono considerare elementi di altre classi. Le consuete strutture algebriche (gruppi, anelli, campi, moduli ecc.) si intenderanno sempre «piccole», cioè definite su insiemi.

Bibliografia

Paul R. Halmos, *Naive Set Theory*, Springer, New York, 1960.

Paul J. Cohen, *Set Theory and the Continuum Hypothesis*, Addison-Wesley, Reading, Mass., 1966.

1 Categorie

In questo capitolo e nel successivo, dedicato all'algebra universale, consideriamo due concetti unificatori che permettono di studiare simultaneamente certi aspetti di numerose strutture matematiche. Qui studieremo il concetto di categoria e le nozioni, ad esso collegate, di funtore e di trasformazione naturale. Eilenberg e Mac Lane le introdussero nel 1945 per dare un significato preciso all'affermazione che certi isomorfismi sono «naturali». Un esempio tipico è l'isomorfismo naturale fra uno spazio vettoriale V di dimensione finita su un campo e il suo biduale V^{**}, ossia lo spazio delle forme lineari sullo spazio V^* delle forme lineari su V. L'isomorfismo di V su V^{**} è l'applicazione lineare che associa a ogni vettore $x \in V$ la funzione di valutazione $f \mapsto f(x)$, definita per ogni $f \in V^*$. Per descrivere la «naturalità» di questo isomorfismo, Eilenberg e Mac Lane dovettero considerare simultaneamente tutti gli spazi vettoriali di dimensione finita, le applicazioni lineari fra essi, i loro biduali e le corrispondenti applicazioni lineari fra questi ultimi. Giunsero così ai concetti di categoria e di funtore come preliminari alla definizione di trasformazione naturale. Nel § 1.3 discuteremo in dettaglio una generalizzazione di questo esempio.

Nel concetto di categoria entrano due ingredienti: una classe di oggetti e una classe di morfismi fra essi. Di solito gli oggetti sono insiemi e i morfismi sono determinate applicazioni fra questi insiemi: si pensi, per esempio, agli spazi topologici e alle applicazioni continue. La definizione pone sullo stesso piano oggetti e morfismi. Adottando il punto di vista categoriale si sposta l'accento rispetto all'impostazione abituale, nella quale gli oggetti hanno un ruolo primario e i morfismi un ruolo secondario. Si guadagna così in precisione, specificando fin dall'inizio quali morfismi si ammettono fra gli oggetti riuniti in una categoria.

Il linguaggio e i risultati elementari della teoria delle categorie sono ormai penetrati in una parte considerevole della matematica. Al di là dell'uso quotidiano di questi concetti e risultati, occorre osservare che le nozioni categoriali sono alla base di alcuni fra i più notevoli sviluppi recenti della matematica. Uno di questi è l'estensione della geometria algebrica, nata per studiare le soluzioni nel campo dei numeri complessi di sistemi di equazioni polinomiali a coefficienti complessi, allo studio di equazioni analoghe su un anello commutativo arbitrario. La fondazione rigorosa di tale studio, dovuta soprattutto ad A. Grothendieck, poggia sul concetto categoriale di schema. Un'altra profonda applicazione è la teoria dell'equivalenza di K. Morita per i moduli. Essa getta nuova luce sul classico teorema di struttura di Wedderburn–Artin per gli anelli semplici e svolge un ruolo importante nell'estensione di buona parte della teoria strutturale delle algebre sui campi alle algebre sugli anelli commutativi.

Un esempio tipico di categoria è la categoria dei gruppi. Qui si considerano «tutti» i gruppi. Per evitare i paradossi della teoria degli insiemi occorre pertanto trattare i fondamenti con maggiore cautela di quanta sia necessaria nello studio della teoria dei gruppi in sé. Un modo di superare le ben note difficoltà consiste nell'adottare la distinzione di Gödel e Bernays fra insiemi e classi. Seguiremo questa via, già brevemente indicata nell'Introduzione.

In questo capitolo introduciamo le principali definizioni della teoria delle categorie: funtori, trasformazioni naturali, prodotti, coprodotti, universali e aggiunti. Le illustreremo con molti esempi algebrici, passando così in rassegna numerosi concetti dell'algebra. Abbiamo incluso qualche esempio non banale per dare un po' di sapore a una trattazione che altrimenti potrebbe sembrare troppo insipida.

1.1 Definizione ed esempi di categorie

Definizione 1.1. Una *categoria* **C** è costituita dai dati seguenti.

1. Una classe $\mathrm{ob}\,\mathbf{C}$ di *oggetti*, di solito indicati con $A, B, C, \ldots$

2. Per ogni coppia ordinata di oggetti (A, B), un insieme $\hom_{\mathbf{C}}(A, B)$, o semplicemente $\hom(A, B)$ quando la categoria è chiara dal contesto. I suoi elementi si chiamano *morfismi di dominio A e codominio B*, o morfismi *da A a B*.

3. Per ogni terna ordinata di oggetti (A, B, C), un'applicazione $(f, g) \mapsto gf$ dell'insieme prodotto $\hom(A, B) \times \hom(B, C)$ in $\hom(A, C)$.

Si richiede che gli oggetti e i morfismi soddisfino le condizioni seguenti.

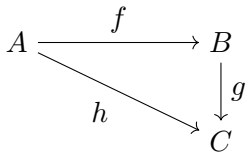
C1. Se $(A, B) \neq (C, D)$, gli insiemi $\hom(A, B)$ e $\hom(C, D)$ sono disgiunti.

C2. *Associatività.* Se $f \in \hom(A, B)$, $g \in \hom(B, C)$ e $h \in \hom(C, D)$, allora $(hg)f = h(gf)$. Come di consueto, abbreviamo questa espressione in hgf.

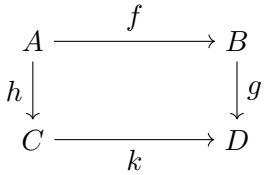
C3. *Unità.* Per ogni oggetto A esiste un elemento $1_A \in \hom(A, A)$ tale che $f1_A = f$ per ogni $f \in \hom(A, B)$ e $1_A g = g$ per ogni $g \in \hom(B, A)$. L'elemento 1_A è unico.

Se $f \in \hom(A, B)$ scriviamo $f\colon A \to B$ oppure $A \xrightarrow{f} B$ (talvolta $A \underset{f}{\to} B$) e chiamiamo f una *freccia* da A a B. Si noti che gf è definito se e solo se il dominio di g coincide con il codominio di f. Il suo dominio è quello di f e il suo codominio è quello di g.

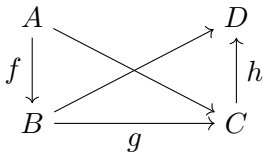
Il fatto che $gf = h$ si esprime dicendo che il diagramma



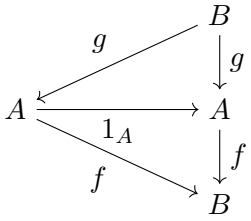
è *commutativo*. I diagrammi più complicati hanno lo stesso significato che nel caso delle applicazioni fra insiemi (BAI, pp. 7–8). Per esempio, la commutatività del diagramma



significa che $gf = kh$, mentre l'associatività $(hg)f = h(gf)$ si esprime mediante la commutatività di



La condizione che 1_A sia l'unità in $\hom(A, A)$ si può esprimere mediante la commutatività del diagramma



per ogni $f \in \hom(A, B)$ e ogni $g \in \hom(B, A)$.

Osserviamo che, nel definire una categoria, non è necessario che gli insiemi $\hom(A, B)$ e $\hom(C, D)$ siano disgiunti fin dall'inizio ogni volta che $(A, B) \neq (C, D)$. Data una classe di insiemi $\hom(A, B)$, basta sostituire ciascuno di essi con l'insieme delle terne ordinate (A, B, f), dove $f \in \hom(A, B)$. Avremo così una libertà assai maggiore nel costruire esempi di categorie (si vedano gli esercizi 3–6).

Presentiamo ora un lungo elenco di esempi.

Esempi

1. **Set**, la categoria degli insiemi. La classe $\operatorname{ob}\mathbf{Set}$ è la classe di tutti gli insiemi. Se A e B sono insiemi, $\hom(A, B) = B^A$ è l'insieme delle applicazioni da A a B. Il prodotto gf è l'usuale composizione di applicazioni e 1_A è l'applicazione identica sull'insieme A. La validità degli assiomi C1, C2 e C3 è evidente.

2. **Mon**, la categoria dei monoidi. La classe $\operatorname{ob}\mathbf{Mon}$ è la classe dei monoidi (BAI, p. 28). Per due monoidi M, N, $\hom(M, N)$ è l'insieme degli omomorfismi di M in N, gf è il composto degli omomorfismi f e g, e 1_M è l'applicazione identica su M, che è un omomorfismo. Gli assiomi sono evidentemente soddisfatti.

3. **Grp**, la categoria dei gruppi. La definizione si ottiene da quella dell'esempio 2 sostituendo i monoidi con i gruppi.

4. **Ab**, la categoria dei gruppi abeliani. La classe $\operatorname{ob}\mathbf{Ab}$ è la classe dei gruppi abeliani. Per il resto, tutto procede come nell'esempio 2.

Una categoria $\mathbf{D}$ si chiama *sottocategoria* di $\mathbf{C}$ se $\operatorname{ob}\mathbf{D}$ è una sottoclasse di $\operatorname{ob}\mathbf{C}$ e, per ogni $A, B \in \operatorname{ob}\mathbf{D}$, si ha $\hom_{\mathbf{D}}(A, B) \subseteq \hom_{\mathbf{C}}(A, B)$. La definizione richiede inoltre che 1_A, per $A \in \operatorname{ob}\mathbf{D}$, e il prodotto dei morfismi in $\mathbf{D}$ siano quelli di $\mathbf{C}$. La sottocategoria $\mathbf{D}$ si dice *piena* se $\hom_{\mathbf{D}}(A, B) = \hom_{\mathbf{C}}(A, B)$ per ogni $A, B \in \operatorname{ob}\mathbf{D}$. È chiaro che **Grp** e **Ab** sono sottocategorie piene di **Mon**. Per contro, poiché un monoide non è soltanto un insieme, bensì una terna $(M, p, 1)$, dove p è una composizione binaria associativa in M e 1 ne è l'unità, la categoria **Mon** non è una sottocategoria di **Set**. Più avanti daremo un esempio di sottocategoria che non è piena (esempio 10).

Riprendiamo l'elenco degli esempi.

5. Sia M un monoide. Esso definisce una categoria $\mathbf{M}$ ponendo $\operatorname{ob}\mathbf{M} = \{A\}$, insieme con un solo elemento A, e $\hom(A, A) = M$. Si prende per 1_A l'unità di M e per xy, con $x, y \in \hom(A, A)$, il prodotto di x e y in M. È chiaro che $\mathbf{M}$ è una categoria con un solo oggetto. Viceversa, sia $\mathbf{M}$ una categoria con un solo oggetto: $\operatorname{ob}\mathbf{M} = \{A\}$. Allora $M = \hom(A, A)$ è un monoide. Possiamo dunque identificare i monoidi con le categorie la cui classe degli oggetti è un insieme con un solo elemento.

Una categoria $\mathbf{C}$ si dice *piccola* se $\operatorname{ob}\mathbf{C}$ è un insieme. L'esempio 5 è una categoria piccola, mentre gli esempi da 1 a 4 non lo sono.

Un elemento $f \in \hom(A, B)$ si chiama *isomorfismo* se esiste $g \in \hom(B, A)$ tale che $fg = 1_B$ e $gf = 1_A$. È chiaro che g è univocamente determinato da f, perciò possiamo indicarlo con f^{-1}. Anch'esso è un isomorfismo e $(f^{-1})^{-1} = f$. Se f e h sono isomorfismi e fh è definito, allora fh è un isomorfismo e $(fh)^{-1} = h^{-1}f^{-1}$. In **Set** gli isomorfismi sono le applicazioni biiettive e in **Grp** sono gli isomorfismi usuali, ossia gli omomorfismi biiettivi.

6. Sia G un gruppo e sia $\mathbf{G}$ la categoria con un solo oggetto che esso definisce come nell'esempio 5. La proprietà caratteristica di una categoria di questo tipo è quella di avere un solo oggetto e di avere per frecce (ossia per morfismi) soltanto isomorfismi.

7. Un *gruppoide* è una categoria piccola in cui tutti i morfismi sono isomorfismi.

8. Una *categoria discreta* è una categoria nella quale $\hom(A, B) = \varnothing$ se $A \neq B$ e $\hom(A, A) = \{1_A\}$. Le categorie discrete piccole si possono identificare con i loro insiemi di oggetti.

9. **Ring**, la categoria degli anelli associativi con unità per la moltiplicazione. La classe $\operatorname{ob}\mathbf{Ring}$ è la classe degli anelli e i morfismi sono gli omomorfismi che mandano 1 in 1.

10. **Rng**, la categoria degli anelli associativi per i quali non si richiede un'unità (BAI, p. 155), con gli omomorfismi usuali. La categoria **Ring** è una sottocategoria di **Rng**, ma non è piena, poiché esistono applicazioni fra anelli con unità che conservano addizione e moltiplicazione senza mandare 1 in 1. (Si dia un esempio.)

11. R-**mod**, la categoria dei moduli sinistri su un anello fissato R. In un R-modulo sinistro M supponiamo che $1x = x$ per ogni $x \in M$. La classe degli oggetti è la classe degli R-moduli sinistri e i morfismi sono gli omomorfismi di R-moduli. Il prodotto è la composizione di applicazioni. Se $R = \Delta$ è un anello di divisione (in particolare, un campo), allora R-**mod** è la categoria degli spazi vettoriali sinistri su Δ. Si definisce in modo analogo **mod**-R, la categoria dei moduli destri sull'anello R.

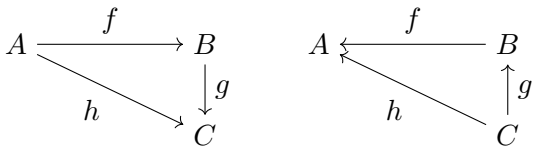
12. Sia S un insieme preordinato, ossia un insieme munito di una relazione binaria $a \leq b$ tale che $a \leq a$ e tale che da $a \leq b$ e $b \leq c$ segua $a \leq c$. Si definisce una categoria $\mathbf{S}$ ponendo $\operatorname{ob}\mathbf{S} = S$ e, per $a, b \in S$, prendendo $\hom(a, b)$ vuoto se $a \not\leq b$ e costituito da un solo elemento se $a \leq b$. Se $f \in \hom(a, b)$ e $g \in \hom(b, c)$, allora gf è l'unico elemento di $\hom(a, c)$. È chiaro che gli assiomi di categoria sono soddisfatti. Per converso, ogni categoria piccola nella quale $\hom(A, B)$ è vuoto o ha un solo elemento per ogni coppia A, B è la categoria di un insieme preordinato appena descritta.

13. **Top**, la categoria degli spazi topologici. Gli oggetti sono gli spazi topologici e i morfismi le applicazioni continue. Gli assiomi si verificano immediatamente.

Concludiamo il paragrafo con due costruzioni generali per ottenere nuove categorie da categorie date. La prima è analoga alla costruzione dell'opposto di un anello (BAI, p. 113). Data una categoria $\mathbf{C}$, definiamo $\mathbf{C}^{\mathrm{op}}$ ponendo $\operatorname{ob}\mathbf{C}^{\mathrm{op}} = \operatorname{ob}\mathbf{C}$ e, per $A, B \in \operatorname{ob}\mathbf{C}^{\mathrm{op}}$,

$$\hom_{\mathbf{C}^{\mathrm{op}}}(A, B) = \hom_{\mathbf{C}}(B, A).$$

Se $f \in \hom_{\mathbf{C}^{\mathrm{op}}}(A, B)$ e $g \in \hom_{\mathbf{C}^{\mathrm{op}}}(B, C)$, allora $g \cdot f$ in $\mathbf{C}^{\mathrm{op}}$ è il prodotto fg in $\mathbf{C}$. L'identità 1_A è quella di $\mathbf{C}$. È chiaro che si ottiene una categoria, che chiamiamo *categoria duale* di $\mathbf{C}$. In termini di frecce, se $A \xrightarrow{f} B$ in $\mathbf{C}$, allora $A \xleftarrow{f} B$ in $\mathbf{C}^{\mathrm{op}}$. Se il diagramma a sinistra è commutativo in $\mathbf{C}$, quello a destra è commutativo in $\mathbf{C}^{\mathrm{op}}$:



Più in generale, da qualsiasi diagramma commutativo in $\mathbf{C}$ si ottiene un diagramma commutativo in $\mathbf{C}^{\mathrm{op}}$ invertendo tutte le frecce.

Siano ora $\mathbf{C}$ e $\mathbf{D}$ due categorie. Definiamo la *categoria prodotto* $\mathbf{C} \times \mathbf{D}$ secondo la ricetta seguente: $\operatorname{ob}(\mathbf{C} \times \mathbf{D}) = \operatorname{ob}\mathbf{C} \times \operatorname{ob}\mathbf{D}$. Per $A, B \in \operatorname{ob}\mathbf{C}$ e $A', B' \in \operatorname{ob}\mathbf{D}$ poniamo

$$\hom_{\mathbf{C}\times\mathbf{D}}\left((A, A'), (B, B')\right) = \hom_{\mathbf{C}}(A, B) \times \hom_{\mathbf{D}}(A', B'), \qquad 1_{(A,A')} = (1_A, 1_{A'}).$$

Se $f \in \hom_{\mathbf{C}}(A, B)$, $g \in \hom_{\mathbf{C}}(B, C)$, $f' \in \hom_{\mathbf{D}}(A', B')$ e $g' \in \hom_{\mathbf{D}}(B', C')$, allora

$$(g, g')(f, f') = (gf, g'f').$$

Si verifica immediatamente che questi dati definiscono una categoria. La costruzione si può generalizzare per definire il prodotto di una famiglia indicizzata di categorie. Lasciamo al lettore il compito di eseguirla.

Esercizi

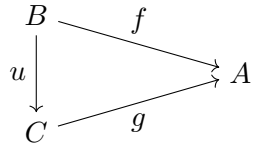
1. Mostrare che i dati seguenti definiscono una categoria $\mathbf{Ring}^*$. La classe $\operatorname{ob}\mathbf{Ring}^*$ è la classe degli anelli. Se R e S sono anelli, $\hom_{\mathbf{Ring}^*}(R, S)$ è l'insieme degli omomorfismi e degli antiomomorfismi di R in S. Il prodotto gf dei morfismi è la composizione delle applicazioni f e g, eseguite in quest'ordine, e 1_R è l'applicazione identica su R.

2. Per *anello con involuzione* intendiamo una coppia (R, j) dove R è un anello con unità e j è un'involuzione di R. Ciò significa che, scrivendo $j\colon a \mapsto a^*$, si ha

   $$(a + b)^* = a^* + b^*, \qquad (ab)^* = b^*a^*, \qquad 1^* = 1, \qquad (a^*)^* = a.$$

   (Si diano alcuni esempi.) Per omomorfismo di un anello con involuzione (R, j) in un altro (S, k) intendiamo un'applicazione η di R in S che sia un omomorfismo di anelli, mandi 1 in 1 e soddisfi $\eta(ja) = k(\eta a)$ per ogni $a \in R$. Mostrare che i dati seguenti definiscono una categoria $\mathbf{Rinv}$. La classe $\operatorname{ob}\mathbf{Rinv}$ è la classe degli anelli con involuzione. Dati due di questi anelli (R, j) e (S, k), l'insieme $\hom((R, j), (S, k))$ è l'insieme degli omomorfismi di (R, j) in (S, k). Il prodotto gf è la composizione delle applicazioni e $1_{(R,j)} = 1_R$.

3. Siano $\mathbf{C}$ una categoria e A un suo oggetto. Poniamo $\operatorname{ob}(\mathbf{C}/A) = \bigcup_{X\in\operatorname{ob}\mathbf{C}} \hom(X, A)$: è la classe delle frecce di $\mathbf{C}$ che terminano in A. Se $f \in \hom(B, A)$ e $g \in \hom(C, A)$, definiamo $\hom(f, g)$ come l'insieme degli $u\colon B \to C$ tali che sia commutativo il diagramma

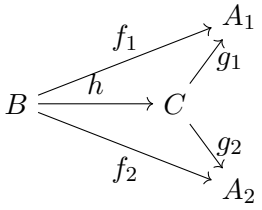
   

   Si noti che $\hom(f, g)$ e $\hom(f', g')$ possono non essere disgiunti per $(f, g) \neq (f', g')$. Se $u \in \hom(f, g)$ e $v \in \hom(g, h)$, con $h\colon D \to A$, allora $vu \in \hom(f, h)$. Usare questo fatto per definire un prodotto da $\hom(f, g) \times \hom(g, h)$ in $\hom(f, h)$. Porre $1_f = 1_B$ per $f\colon B \to A$. Mostrare che questi dati, insieme con l'osservazione fatta a p. 11 dell'originale, permettono di definire una categoria $\mathbf{C}/A$, detta *categoria degli oggetti di* $\mathbf{C}$ *sopra* A.

4. Usare $\mathbf{C}^{\mathrm{op}}$ per dualizzare l'esercizio 3. Si definisce così la categoria $\mathbf{C}\backslash A$ degli *oggetti di* $\mathbf{C}$ *sotto* A.

5. Siano $\mathbf{C}$ una categoria e $A_1, A_2 \in \operatorname{ob}\mathbf{C}$. Mostrare che i dati seguenti definiscono una categoria $\mathbf{C}/\{A_1, A_2\}$. Gli oggetti sono le terne (B, f_1, f_2) con $f_i \in \hom_{\mathbf{C}}(B, A_i)$. Un

morfismo $h\colon (B, f_1, f_2) \to (C, g_1, g_2)$ è un morfismo $h\colon B \to C$ di $\mathbf{C}$ che rende commutativo il diagramma



Fare in modo che gli insiemi di morfismi siano disgiunti, come sopra. Porre $1_{(B,f_1,f_2)} = 1_B$ e definire il prodotto dei morfismi come in $\mathbf{C}$. Verificare gli assiomi C2 e C3.

6. Dualizzare l'esercizio 5 applicando la costruzione a $\mathbf{C}^{\mathrm{op}}$ e interpretandola in $\mathbf{C}$. La categoria che ne risulta si indica con $\mathbf{C}\backslash\{A_1, A_2\}$.

7. *Definizione alternativa di gruppoide.* Sia $\mathbf{G}$ un gruppoide nel senso dell'esempio 7 e sia $G = \bigcup_{A,B \in \mathrm{ob}\,\mathbf{G}} \hom(A, B)$. Allora G è un insieme munito di una composizione definita per certe coppie (f, g) di elementi di G e tale che valgono le condizioni seguenti.

   (i) Per ogni $f \in G$ esiste un'unica coppia (u, v) di elementi di G tali che uf e fv sono definiti e $uf = f = fv$. Questi elementi si chiamano rispettivamente *unità sinistra* e *unità destra* di f.

   (ii) Se u è un'unità (sinistra e destra per qualche $f \in G$), allora u è la propria unità sinistra e quindi anche la propria unità destra.

   (iii) Il prodotto fg è definito se e solo se l'unità destra di f coincide con l'unità sinistra di g.

   (iv) Se fg e gh sono definiti, allora anche $(fg)h$ e $f(gh)$ sono definiti e $(fg)h = f(gh)$.

   (v) Se f ha unità sinistra u e unità destra v, esiste un elemento g con unità destra u e unità sinistra v tale che $fg = u$ e $gf = v$.

   Mostrare, viceversa, che se G è un insieme munito di una composizione parziale che soddisfa le condizioni (i)–(v), allora G definisce una categoria gruppoide $\mathbf{G}$ nella quale $\mathrm{ob}\,\mathbf{G}$ è l'insieme delle unità di G. Per ogni coppia di oggetti u, v, $\hom(u, v)$ è il sottoinsieme degli elementi di G che hanno u come unità sinistra e v come unità destra. La composizione su $\hom(u, v) \times \hom(v, w)$ è quella di G.[2]

8. Sia G come nell'esercizio 7 e sia G^* l'unione disgiunta di G e dell'insieme $\{0\}$. Estendere la composizione da G a G^* ponendo $0a = 0 = a0$ per ogni $a \in G^*$ e $fg = 0$ se $f, g \in G$ e il loro prodotto non è definito in G. Mostrare che G^* è un semigruppo (BAI, p. 29).

1.2 Alcune nozioni fondamentali sulle categorie

Abbiamo detto che in una categoria $\mathbf{C}$ un morfismo $f\colon A \to B$ è un isomorfismo se esiste $g\colon B \to A$ tale che $fg = 1_B$ e $gf = 1_A$. Se $f\colon A \to B$, $g\colon B \to A$ e $gf = 1_A$, si dice che f è una *sezione* di g e che g è una *retrazione* di f. Più interessanti di queste due nozioni sono quelle di monomorfismo e di epimorfismo, definite da proprietà di cancellazione. Un morfismo $f\colon A \to B$ si dice *monomorfismo* (rispettivamente *epimorfismo*) se in $\mathbf{C}$ è cancellabile a sinistra (rispettivamente a destra). In altre parole, per ogni oggetto C e per ogni $g_1, g_2 \in \hom(C, A)$,

[2] Con la convenzione $gf = g \circ f$ adottata nel capitolo, un morfismo da u a v ha u come unità *destra* e v come unità *sinistra*. Nella descrizione di questo insieme di morfismi l'originale scambia i due termini. [N.d.T.]

da $fg_1 = fg_2$ deve seguire $g_1 = g_2$; nel secondo caso, per ogni $g_1, g_2 \in \hom(B, C)$, da $g_1 f = g_2 f$ deve seguire $g_1 = g_2$. Dalle definizioni discendono immediatamente i fatti seguenti.

1. Se $A \xrightarrow{f} B \xrightarrow{g} C$ e f, g sono monomorfismi (epimorfismi), allora gf è un monomorfismo (epimorfismo).

2. Se $A \xrightarrow{f} B \xrightarrow{g} C$ e gf è un monomorfismo (epimorfismo), allora f è un monomorfismo (g è un epimorfismo).

3. Se f ammette una sezione, è un epimorfismo. Se ammette una retrazione, è un monomorfismo.

Sia f un'applicazione di un insieme A in un insieme B. Si vede facilmente che f è iniettiva, ossia che $f(a) \neq f(a')$ per $a \neq a'$ in A, se e solo se, per ogni insieme C e ogni coppia di applicazioni g_1, g_2 di C in A, l'uguaglianza $fg_1 = fg_2$ implica $g_1 = g_2$ (BAI, p. 10, esercizio 3). Dunque $f \in \hom_{\mathbf{Set}}(A, B)$ è un monomorfismo se e solo se è iniettiva. Analogamente, f è un epimorfismo in **Set** se e solo se è suriettiva, cioè $f(A) = B$. Risultati analoghi valgono nelle categorie R-**mod** e **Grp**.

Proposizione 1.1. *Un morfismo f in R-**mod** o in **Grp** è un monomorfismo (epimorfismo) se e solo se l'applicazione fra gli insiemi sottostanti è iniettiva (suriettiva).*

Dimostrazione. Sia $f\colon A \to B$ in R-**mod** o in **Grp**. Se f è iniettiva (suriettiva) come applicazione di insiemi, è cancellabile a sinistra (a destra) in **Set**. Segue che f è un monomorfismo (epimorfismo) in R-**mod** o in **Grp**. Supponiamo ora che l'applicazione f non sia iniettiva. Allora $C = \ker f$ è diverso da 0 nel caso di R-**mod** e da 1 nel caso di **Grp**. Sia g l'omomorfismo di inclusione di C in A, indicato con $C \hookrightarrow A$: si ha $g(x) = x$ per ogni $x \in C$. Il composto fg è l'omomorfismo di C in B che manda ogni $x \in C$ nell'elemento neutro di B. Sia poi h l'omomorfismo di C in A che manda ogni elemento di C nell'elemento neutro di A. Allora $h \neq g$ perché $C \neq 0$ (oppure $C \neq 1$), eppure $fg = fh$. Quindi f non è un monomorfismo.

Supponiamo ora di trovarci nella categoria R-**mod** e che f non sia suriettiva. L'immagine $f(A)$ è un sottomodulo di B, e possiamo formare il modulo $C = B/f(A)$. Esso è diverso da 0 perché $f(A) \neq B$. Siano g l'omomorfismo canonico di B su C e h l'omomorfismo di B in C che manda ogni elemento di B in 0. Allora $g \neq h$ ma $gf = hf$. Quindi f non è un epimorfismo.

Supponiamo infine di trovarci in **Grp** e che f non sia suriettiva. Il ragionamento precedente si applica quando $C = f(A) \trianglelefteq B$, ossia quando C è un sottogruppo normale di B. In generale ciò non accade, benché accada sempre se $[B : C] = 2$. Supponiamo dunque $[B : C] > 2$. Completeremo la dimostrazione mostrando che esistono due omomorfismi distinti g, h di B nel gruppo $\operatorname{Sym} B$ delle permutazioni di B tali che $gf = hf$. Prendiamo per g l'omomorfismo $b \mapsto b_L$ di B in $\operatorname{Sym} B$, dove b_L è la traslazione sinistra $x \mapsto bx$ in B. Sceglieremo h della forma kg, dove k è un automorfismo interno di $\operatorname{Sym} B$. Dunque k è della forma $y \mapsto pyp^{-1}$, con $y \in \operatorname{Sym} B$ e p elemento fissato di $\operatorname{Sym} B$. Allora $h = kg$ avrà la forma $b \mapsto pb_L p^{-1}$ e vogliamo che sia distinto da $g\colon b \mapsto b_L$. Occorre cioè che la permutazione p non commuti con tutte le b_L. Poiché le permutazioni che commutano con tutte le traslazioni sinistre sono le traslazioni destre (BAI, p. 42, esercizio 1), avremo $h = kg \neq g$ se p non è una traslazione destra. Le traslazioni diverse dall'identità non hanno punti fissi: basterà dunque che p sia una permutazione diversa dall'identità e con un punto fisso. D'altra parte, per ottenere $gf = hf$, occorre che p commuti con ogni c_L, $c \in C$. Per costruire una p che soddisfi tutte queste condizioni, scegliamo una permutazione π dell'insieme $C\backslash B$ delle classi laterali destre Cb, $b \in B$, diversa dall'identità e con un punto fisso. Ciò è possibile perché $|C\backslash B| > 2$. Sia I un insieme di rappresentanti delle classi laterali destre Cb. Ogni elemento di B si scrive in uno e un solo modo come prodotto cu,

con $c \in C$ e $u \in I$. Definiamo ora p ponendo $p(cu) = cu'$, dove $\pi(Cu) = Cu'$ e $u' \in I$. Allora $p \in \operatorname{Sym} B$, $p \neq 1$ e p ha punti fissi, poiché $\pi \neq 1$ e π ha punti fissi. È chiaro che p commuta con ogni d_L, $d \in C$. Dunque p soddisfa tutte le condizioni richieste e f non è un epimorfismo. □

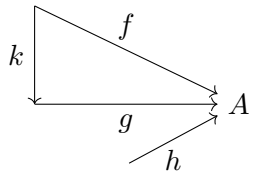
Che cosa si può dire dei monomorfismi e degli epimorfismi nella categoria **Ring**? Anzitutto, la dimostrazione della proposizione 1.1 mostra che gli omomorfismi iniettivi sono monomorfismi e quelli suriettivi sono epimorfismi. Il passo successivo del ragionamento, con il quale si dimostrava che i monomorfismi sono iniettivi, qui viene meno del tutto. Il nucleo di un omomorfismo di anelli è infatti un ideale, che può non essere un anello con unità; e, anche se lo fosse, la sua inclusione non sarebbe in generale un omomorfismo di anelli. Mostriamo ora con un ragionamento diverso, che generalizzeremo più avanti (p. 82 dell'originale), che i monomorfismi in **Ring** sono iniettivi.

Sia f un omomorfismo non iniettivo dell'anello A nell'anello B. Formiamo l'anello $A \oplus A$ delle coppie (a_1, a_2) con $a_i \in A$, con somma e prodotto componente per componente e unità $1 = (1, 1)$. Sia K il sottoinsieme di $A \oplus A$ costituito dagli elementi (a_1, a_2) per i quali $f(a_1) = f(a_2)$. È chiaro che K è un sottoanello di $A \oplus A$ che contiene propriamente $D = \{(a, a) \mid a \in A\}$. Indichiamo con g_1 l'applicazione $(a_1, a_2) \mapsto a_1$ e con g_2 l'applicazione $(a_1, a_2) \mapsto a_2$ da K ad A. Entrambe sono omomorfismi di anelli e, per definizione di K, si ha $fg_1 = fg_2$. D'altra parte, poiché $K \neq D$, esiste una coppia $(a_1, a_2) \in K$ con $a_1 \neq a_2$. Allora $g_1(a_1, a_2) = a_1 \neq a_2 = g_2(a_1, a_2)$. Dunque $g_1 \neq g_2$, e ciò mostra che f non è un monomorfismo.

Possiamo ora mostrare con un esempio che in **Ring** gli epimorfismi non sono necessariamente suriettivi. Consideriamo l'omomorfismo di inclusione f dell'anello $\mathbb{Z}$ degli interi nel campo $\mathbb{Q}$ dei razionali. Se g e h sono omomorfismi di $\mathbb{Q}$ in un anello R, allora $gf = hf$ se e solo se le restrizioni $g|_{\mathbb{Z}}$ e $h|_{\mathbb{Z}}$ coincidono. Poiché un omomorfismo di $\mathbb{Q}$ è determinato dalla sua restrizione a $\mathbb{Z}$, segue che $gf = hf$ implica $g = h$. Dunque f è un epimorfismo e, evidentemente, non è suriettivo. Abbiamo dimostrato la seguente proposizione.

Proposizione 1.2. *Un morfismo in* **Ring** *è un monomorfismo se e solo se è iniettivo. In* **Ring** *esistono tuttavia epimorfismi non suriettivi.*

Il concetto di monomorfismo permette di definire i *sottoggetti* di un oggetto A di una categoria $\mathbf{C}$. Consideriamo la classe dei monomorfismi che terminano in A:



Su questa classe introduciamo un preordine ponendo $f \leq g$ se esiste k tale che $f = gk$. Ne segue che k è un monomorfismo. Scriviamo $f \equiv g$ se $f \leq g$ e $g \leq f$. In tal caso k è un isomorfismo. La relazione $\equiv$ è una relazione di equivalenza e le sue classi si chiamano *sottoggetti* di A.

Per dualità otteniamo la nozione di *oggetto quoziente* di A. Consideriamo ora gli epimorfismi che escono da A e poniamo $f \geq g$ se esiste k tale che $f = kg$. Si ha una relazione di equivalenza $f \equiv g$, definita dall'esistenza di un isomorfismo k per il quale $f = kg$. Le classi di equivalenza così determinate si chiamano *oggetti quoziente* di A.

Considerando il caso particolare $\mathbf{C} = \mathbf{Grp}$, il lettore si convincerà che la terminologia di sottoggetti e oggetti quoziente di A è ragionevole. Si osservi tuttavia che gli oggetti quoziente definiti in **Ring** costituiscono una classe più ampia di quella fornita dagli omomorfismi suriettivi.

Esercizi

1. Dare un esempio in **Top** di un morfismo che sia contemporaneamente un monomorfismo

e un epimorfismo, ma non ammetta una retrazione.

2. Siano G un gruppo finito e H un sottogruppo. Mostrare che il numero delle permutazioni di G che commutano con tutte le h_L, $h \in H$ (agenti su G), è $[G:H]!\,|H|^{[G:H]}$, dove $[G:H]$ è l'indice di H in G.

1.3 Funtori e trasformazioni naturali

In questa sezione introduciamo il concetto di *funtore*, ossia di morfismo da una categoria a un'altra, e quello di applicazione fra funtori, che prende il nome di *trasformazione naturale*. Prima delle definizioni consideriamo un esempio.

Sia R un anello e sia $U(R)$ il gruppo moltiplicativo delle unità (elementi invertibili) di R. La corrispondenza $R \mapsto U(R)$ è un'applicazione dagli anelli ai gruppi, ossia da $\operatorname{ob}\mathbf{Ring}$ in $\operatorname{ob}\mathbf{Grp}$. Inoltre, dato un omomorfismo di anelli $f : R \to S$, la restrizione $f|_{U(R)}$ manda $U(R)$ in $U(S)$ e può dunque essere considerata come un'applicazione di $U(R)$ in $U(S)$. Evidentemente è un omomorfismo di gruppi. È chiaro anche che, se $g : S \to T$ è un omomorfismo di anelli, allora

$$(gf)|_{U(R)} = (g|_{U(S)})(f|_{U(R)}).$$

Inoltre la restrizione $1_R|_{U(R)}$ è l'applicazione identica su $U(R)$.

Le applicazioni $R \mapsto U(R)$ dagli anelli ai gruppi e $f \mapsto f|_{U(R)}$ dagli omomorfismi di anelli agli omomorfismi di gruppi costituiscono un funtore da **Ring** a **Grp** nel senso della definizione che segue.

Definizione 1.2. *Se* $\mathbf{C}$ *e* $\mathbf{D}$ *sono categorie, un funtore (covariante)* F *da* $\mathbf{C}$ *a* $\mathbf{D}$ *consiste dei seguenti dati.*

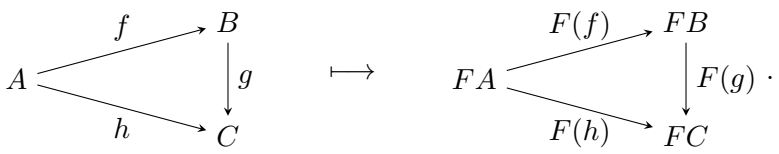
1. *Un'applicazione* $A \mapsto FA$ *da* $\operatorname{ob}\mathbf{C}$ *in* $\operatorname{ob}\mathbf{D}$.
2. *Per ciascuna coppia* (A, B) *di oggetti di* $\mathbf{C}$*, un'applicazione* $f \mapsto F(f)$ *da* $\hom_{\mathbf{C}}(A, B)$ *in* $\hom_{\mathbf{D}}(FA, FB)$.

Richiediamo che siano soddisfatte le condizioni seguenti.

F1. *Se* gf *è definito in* $\mathbf{C}$*, allora* $F(gf) = F(g)F(f)$.

F2. $F(1_A) = 1_{FA}$.

La condizione F1 afferma che ogni triangolo commutativo in $\mathbf{C}$ viene mandato in un triangolo commutativo in $\mathbf{D}$:



Un *funtore controvariante* da $\mathbf{C}$ a $\mathbf{D}$ è un funtore da $\mathbf{C}^{\mathrm{op}}$ a $\mathbf{D}$. Più direttamente, esso consiste di un'applicazione F da $\operatorname{ob}\mathbf{C}$ in $\operatorname{ob}\mathbf{D}$ e, per ciascuna coppia (A, B) di oggetti di $\mathbf{C}$, di un'applicazione F da $\hom(A, B)$ in $\hom(FB, FA)$, tali che $F(fg) = F(g)F(f)$ e $F(1_A) = 1_{FA}$. Un funtore da $\mathbf{B} \times \mathbf{C}$ a $\mathbf{D}$ si dice *bifuntore* da $\mathbf{B}$ e $\mathbf{C}$ in $\mathbf{D}$. Possiamo anche combinare i bifuntori con i funtori controvarianti, ottenendo funtori da $\mathbf{B}^{\mathrm{op}} \times \mathbf{C}$ a $\mathbf{D}$ e da $\mathbf{B}^{\mathrm{op}} \times \mathbf{C}^{\mathrm{op}}$ a $\mathbf{D}$. Il primo si dice bifuntore controvariante in $\mathbf{B}$ e covariante in $\mathbf{C}$, il secondo bifuntore controvariante sia in $\mathbf{B}$ sia in $\mathbf{C}$.

Esempi

1. Sia $\mathbf{D}$ una sottocategoria di $\mathbf{C}$. Abbiamo allora il *funtore di inclusione* di $\mathbf{D}$ in $\mathbf{C}$, che manda ciascun oggetto di $\mathbf{D}$ nello stesso oggetto di $\mathbf{C}$ e ciascun morfismo di $\mathbf{D}$ nello stesso morfismo di $\mathbf{C}$. Nel caso particolare in cui $\mathbf{D} = \mathbf{C}$ esso si chiama *funtore identità* $1_{\mathbf{C}}$.

2. Si ottiene un funtore da **Grp** a **Set** associando a ogni gruppo il suo insieme soggiacente e a ogni omomorfismo di gruppi la corrispondente applicazione di insiemi. Un funtore che dimentica parte della struttura assegnata si dice *funtore dimenticante*. Nell'esempio seguente ne incontriamo altri due.

3. A ogni anello $(R, +, \cdot, 0, 1)$ sono associati il gruppo additivo $(R, +, 0)$ e il monoide moltiplicativo $(R, \cdot, 1)$. Un omomorfismo di anelli è in particolare un omomorfismo dei gruppi additivi e dei monoidi moltiplicativi. Queste osservazioni conducono in modo evidente alle definizioni dei funtori dimenticanti da **Ring** ad **Ab** e da **Ring** a **Mon**.

4. Sia n un intero positivo. Per ogni anello R possiamo formare l'anello $M_n(R)$ delle matrici $n \times n$ a elementi in R. Un omomorfismo di anelli $f : R \to S$ determina un omomorfismo $(r_{ij}) \mapsto (f(r_{ij}))$ da $M_n(R)$ in $M_n(S)$. In questo modo si ottiene un funtore M_n da **Ring** in **Ring**.

5. Siano n e R come nell'esempio 4 e sia $\mathrm{GL}_n(R)$ il gruppo delle unità di $M_n(R)$, ossia il gruppo delle matrici invertibili $n \times n$ a elementi in R. Le corrispondenze $R \mapsto \mathrm{GL}_n(R)$ e $f \mapsto [(r_{ij}) \mapsto (f(r_{ij}))]$ definiscono un funtore GL_n da **Ring** a **Grp**.

6. Definiamo il *funtore delle parti* in **Set** associando a ogni insieme A il suo insieme delle parti $\mathcal{P}(A)$ e a ogni applicazione $f : A \to B$ l'applicazione indotta $f_{\mathcal{P}}$ da $\mathcal{P}(A)$ in $\mathcal{P}(B)$, che manda ogni sottoinsieme A_1 di A nella sua immagine $f(A_1) \subseteq B$ ($\varnothing \mapsto \varnothing$).

7. Il *funtore di abelianizzazione* da **Grp** ad **Ab**. A ogni gruppo G associamo il gruppo abeliano $G/(G, G)$, dove (G, G) è il sottogruppo dei commutatori di G (BAI, p. 238). Se f è un omomorfismo di G in un altro gruppo H, allora f manda (G, G) in (H, H) e induce un omomorfismo $\bar{f}$ da $G/(G, G)$ in $H/(H, H)$. La corrispondenza $f \mapsto \bar{f}$ completa la definizione del funtore di abelianizzazione.

8. Sia **Poset** la categoria degli insiemi parzialmente ordinati. I suoi oggetti sono gli insiemi parzialmente ordinati (BAI, p. 456) e i suoi morfismi le applicazioni che conservano l'ordine. Si ottiene un funtore da R-**mod** a **Poset** associando a ogni R-modulo M l'insieme $L(M)$ dei suoi sottomoduli, ordinato per inclusione. Se $f : M \to N$ è un omomorfismo di moduli, f determina un'applicazione da $L(M)$ in $L(N)$ che conserva l'ordine. Queste applicazioni definiscono un funtore.

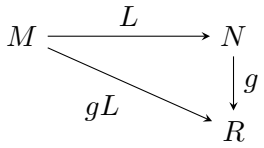
9. Definiamo un *funtore di proiezione* da $\mathbf{C} \times \mathbf{D}$ in $\mathbf{C}$ associando a ogni oggetto (A, B) di $\mathbf{C} \times \mathbf{D}$ l'oggetto A di $\mathbf{C}$ e a $(f, g) \in \hom((A, B), (A', B'))$ il morfismo $f \in \hom(A, A')$.

10. Definiamo il *funtore diagonale* $\mathbf{C} \to \mathbf{C} \times \mathbf{C}$ mediante $A \mapsto (A, A)$ e associando a $f : A \to B$ il morfismo $(A, A) \xrightarrow{(f,f)} (B, B)$.

11. Consideriamo le categorie R-**mod** e **mod**-R degli R-moduli sinistri e destri, rispettivamente, sull'anello R. Definiamo un funtore controvariante D da R-**mod** a **mod**-R nel modo seguente. Se M è un R-modulo sinistro, consideriamo l'insieme $M^* = \hom_R(M, R)$ degli omomorfismi di M in R, dove R è considerato come R-modulo sinistro nel modo consueto. Dunque M^* è l'insieme delle applicazioni da M in R tali che

$$f(x + y) = f(x) + f(y), \qquad f(rx) = rf(x) \quad (x, y \in M,\ r \in R).$$

Se $f, g \in M^*$ e $s \in R$, allora appartengono a M^* sia $f+g$, definita da $(f+g)(x) = f(x) + g(x)$, sia fs, definita da $(fs)(x) = f(x)s$. In tal modo M^* diventa un R-modulo destro e si ha la corrispondenza $M \mapsto M^*$ da ob(R-**mod**) in ob(**mod**-R). Sia ora $L : M \to N$ un omomorfismo dall'R-modulo M all'R-modulo N. L'*applicazione trasposta* $L^* : N^* \to M^*$ è definita da $L^* : g \mapsto gL$, dove gL è la composta di g e L:



Se $M_1 \xrightarrow{L_1} M_2 \xrightarrow{L_2} M_3$ in R-**mod** e $g \in M_3^*$, allora

$$(L_2L_1)^*(g) = gL_2L_1 = (gL_2)L_1 = L_1^*L_2^*(g).$$

Dunque $(L_2L_1)^* = L_1^*L_2^*$. È chiaro che $(1_M)^* = 1_{M^*}$. Ne segue che $D : M \mapsto M^*,\ L \mapsto L^*$ definisce un funtore controvariante, il *funtore di dualità* D da R-**mod** a **mod**-R. In modo analogo si ottiene il funtore di dualità D da **mod**-R a R-**mod**.

È chiaro che un funtore manda un isomorfismo in un isomorfismo: se $fg = 1_B$ e $gf = 1_A$, allora $F(f)F(g) = 1_{FB}$ e $F(g)F(f) = 1_{FA}$. Analogamente, i funtori mandano sezioni in sezioni e retrazioni in retrazioni. È invece facile fornire esempi in cui l'immagine di un monomorfismo (epimorfismo) non è un monomorfismo (epimorfismo): si veda l'esercizio 3.

Dati un funtore F da $\mathbf{C}$ a $\mathbf{D}$ e un funtore G da $\mathbf{D}$ a $\mathbf{E}$, si ottiene un funtore GF da $\mathbf{C}$ a $\mathbf{E}$ ponendo $(GF)A = G(FA)$ per $A \in \operatorname{ob}\mathbf{C}$ e $(GF)(f) = G(F(f))$ per $f \in \hom_{\mathbf{C}}(A, B)$. In modo analogo si può definire la composizione quando uno dei funtori o entrambi sono controvarianti. Il composto è controvariante se uno dei due funtori è controvariante e l'altro covariante, ed è covariante se entrambi sono controvarianti. L'esempio 5 si può descrivere come il composto UM_n, dove M_n è il funtore dell'esempio 4 e U è il funtore da **Ring** a **Grp** definito all'inizio della sezione. Come vedremo tra poco, il funtore *biduale* D^2 da R-**mod** in sé è un funtore covariante particolarmente interessante.

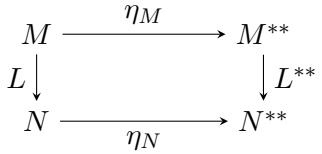
Un funtore F si dice *fedele* (rispettivamente *pieno*) se, per ogni coppia di oggetti A, B di $\mathbf{C}$, l'applicazione $f \mapsto F(f)$ da $\hom_{\mathbf{C}}(A, B)$ in $\hom_{\mathbf{D}}(FA, FB)$ è iniettiva (rispettivamente suriettiva). Tra gli esempi precedenti, il funtore dell'esempio 1 è fedele ed è pieno se e solo se $\mathbf{D}$ è una sottocategoria piena di $\mathbf{C}$. Quelli degli esempi 2 e 3 sono fedeli ma non pieni (perché?), mentre quello dell'esempio 9 è pieno ma non fedele.

Passiamo ora all'importante concetto di trasformazione naturale fra funtori. Prima della definizione sarà istruttivo esaminare nei dettagli l'esempio accennato nell'introduzione a questo capitolo. Consideriamo la situazione più generale dei moduli. Partiamo dunque dalla categoria R-**mod**, per un anello R, e dal funtore biduale D^2 in questa categoria. Esso manda un R-modulo sinistro M in $M^{**} = (M^*)^*$ e un omomorfismo $L : M \to N$ in $L^{**} = (L^*)^* : M^{**} \to N^{**}$. Se $x \in M$ e $g \in N^*$, allora $L^*g \in M^*$ e $(L^*g)(x) = g(Lx)$. Se $\varphi \in M^{**}$, allora $L^{**}\varphi \in N^{**}$ e $(L^{**}\varphi)(g) = \varphi(L^*g)$. Consideriamo ora l'applicazione

$$\eta_M(x) : f \longmapsto f(x)$$

da M^* in R. Essa appartiene a $M^{**} = \hom_R(M^*, R)$ e l'applicazione $\eta_M : x \mapsto \eta_M(x)$ è un R-omomorfismo di M in M^{**}. Per ogni omomorfismo $L : M \to N$ il diagramma

(1)



è commutativo. Infatti, se $x \in M$, allora $\eta_N(Lx)$ è l'applicazione $g \mapsto g(Lx)$ da N^* in R, e per $\varphi = \eta_M(x) \in M^{**}$ si ha $(L^{**}\varphi)(g) = \varphi(L^*g)$. Dunque

$$(L^{**}\eta_M(x))(g) = \eta_M(x)(L^*g) = (L^*g)(x) = g(Lx).$$

Introduciamo ora la seguente definizione di «naturalità».

Definizione 1.3. *Siano F e G funtori da $\mathbf{C}$ a $\mathbf{D}$. Una trasformazione naturale η da F a G è un'applicazione che a ciascun oggetto A di $\mathbf{C}$ associa un morfismo $\eta_A \in \hom_{\mathbf{D}}(FA, GA)$ in modo che, per ogni coppia di oggetti A, B di $\mathbf{C}$ e per ogni $f \in \hom_{\mathbf{C}}(A, B)$, il rettangolo nel diagramma*

$$\begin{array}{ccc} A & & FA \xrightarrow{\eta_A} GA \\ f\downarrow & \qquad & F(f)\downarrow \qquad\qquad \downarrow G(f) \\ B & & FB \xrightarrow[\eta_B]{} GB \end{array}$$

sia commutativo. Se inoltre ogni η_A è un isomorfismo, η si dice isomorfismo naturale.

Nell'esempio precedente prendiamo il funtore identità $1_{R\text{-}\mathbf{mod}}$ e il funtore biduale D^2 sulla categoria degli R-moduli sinistri. A ogni oggetto M di R-**mod** possiamo associare il morfismo η_M da M in M^{**}. La commutatività di (1) mostra che $\eta : M \mapsto \eta_M$ è una trasformazione naturale dal funtore identità al funtore biduale.

Restringendoci agli spazi vettoriali di dimensione finita su un corpo Δ, possiamo enunciare un risultato più forte. Questi spazi formano una sottocategoria di Δ-**mod**. Se V ha dimensione finita su Δ, scegliamo una base $(e_1, e_2, \ldots, e_n)$ di V su Δ. Sia e_i^* la forma lineare su V tale che $e_i^*(e_j) = \delta_{ij}$. Allora $(e_1^*, e_2^*, \ldots, e_n^*)$ è una base di V^* come spazio vettoriale destro su Δ, la *base duale* (o *complementare*) della base $(e_1, \ldots, e_n)$. Ciò mostra che V^* ha la stessa dimensione n di V. Anche V^{**} ha dunque la stessa dimensione di V. Poiché ogni vettore non nullo x può essere preso come elemento e_1 di una base $(e_1, e_2, \ldots, e_n)$, per ogni $x \neq 0$ in V esiste un $g \in V^*$ tale che $g(x) \neq 0$. Ne segue che per ogni $x \neq 0$ l'applicazione $\eta_V(x) : f \mapsto f(x)$ è non nulla. Quindi $\eta_V : x \mapsto \eta_V(x)$ è un'applicazione lineare iniettiva da V in V^{**}. Poiché $\dim V^{**} = \dim V$, η_V è un isomorfismo. Pertanto, in questo caso, η è un isomorfismo naturale dal funtore identità della categoria degli spazi vettoriali di dimensione finita su Δ al funtore biduale su tale categoria.

Nel seguito incontreremo molti esempi di trasformazioni naturali. Per ora basterà registrarne altri due.

Esempi

1. Definiamo il funtore $\bigoplus_n$ in R-**mod** associando a ogni modulo M la somma diretta $M^{(n)}$ di n copie di M (BAI, p. 175) e a ogni omomorfismo $f : M \to N$ l'omomorfismo

$$f^{(n)} : (a_1, \ldots, a_n) \longmapsto (f(a_1), \ldots, f(a_n)).$$

   Per ogni M definiamo l'omomorfismo diagonale $\delta_M^{(n)} : a \mapsto (a, \ldots, a)$. Allora $\delta^{(n)} : M \mapsto \delta_M^{(n)}$ è una trasformazione naturale da $1_{R\text{-}\mathbf{mod}}$ a $\bigoplus_n$, perché si ha il diagramma commutativo

$$\begin{array}{ccc} M & \xrightarrow{\delta_M^{(n)}} & M^{(n)} \\ f\downarrow & & \downarrow f^{(n)} \\ N & \xrightarrow[\delta_N^{(n)}]{} & N^{(n)} \end{array}.$$

2. Consideriamo il funtore di abelianizzazione definito nell'esempio 7, prendendo però **Grp** sia come categoria di partenza sia come categoria di arrivo, al posto di **Ab** come categoria di arrivo. (È l'analogo di cambiare il codominio di una funzione.) Sia ν_G l'omomorfismo canonico di G sul gruppo quoziente. Il diagramma commutativo

$$\begin{array}{ccc} G & \xrightarrow{\nu_G} & G/(G,G) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \bar{f}} \\ H & \xrightarrow[\nu_H]{} & H/(H,H) \end{array}$$

mostra che $\nu : G \mapsto \nu_G$ è una trasformazione naturale dal funtore identità di **Grp** in sé al funtore di abelianizzazione.

Siano F, G, H funtori da $\mathbf{C}$ a $\mathbf{D}$, sia η una trasformazione naturale da F a G e sia ζ una trasformazione naturale da G ad H. Per $A \in \operatorname{ob}\mathbf{C}$ abbiamo $\eta_A \in \hom_{\mathbf{D}}(FA, GA)$ e $\zeta_A \in \hom_{\mathbf{D}}(GA, HA)$. Dunque $\zeta_A\eta_A \in \hom_{\mathbf{D}}(FA, HA)$. I due rettangoli piccoli nel diagramma

$$\begin{array}{ccccc} FA & \xrightarrow{\eta_A} & GA & \xrightarrow{\zeta_A} & HA \\ {\scriptstyle F(f)}\downarrow & & {\scriptstyle G(f)}\downarrow & & \downarrow{\scriptstyle H(f)} \\ FB & \xrightarrow[\eta_B]{} & GB & \xrightarrow[\zeta_B]{} & HB \end{array}$$

sono commutativi, dunque lo è anche il rettangolo grande con vertici FA, HA, FB, HB. Ne segue che $A \mapsto \zeta_A\eta_A$ è una trasformazione naturale da F ad H. La indichiamo con $\zeta\eta$ e la chiamiamo *prodotto* di ζ e η.

Se F è un funtore da $\mathbf{C}$ a $\mathbf{D}$, si ottiene una trasformazione naturale 1_F da F in sé associando a ogni $A \in \operatorname{ob}\mathbf{C}$ il morfismo $1_{FA} \in \hom_{\mathbf{D}}(FA, FA)$. Se η è una trasformazione naturale da F a un funtore G da $\mathbf{C}$ a $\mathbf{D}$, allora evidentemente $\eta 1_F = \eta = 1_G\eta$.

Sia η un isomorfismo naturale da F a G. Allora per ogni $A \in \operatorname{ob}\mathbf{C}$ il morfismo $\eta_A : FA \to GA$ è un isomorfismo. Abbiamo quindi l'isomorfismo $\eta_A^{-1} : GA \to FA$. La commutatività richiesta è evidente, perciò $A \mapsto \eta_A^{-1}$ è un isomorfismo naturale da G a F. Lo chiamiamo *inverso* η^{-1} di η, sicché $(\eta^{-1})_A = (\eta_A)^{-1}$. È chiaro che $\eta^{-1}\eta = 1_F$ ed $\eta\eta^{-1} = 1_G$. Viceversa, se η è una trasformazione naturale da F a G e ζ è una trasformazione naturale da G a F tale che $\zeta\eta = 1_F$ ed $\eta\zeta = 1_G$, allora η è un isomorfismo naturale e $\eta^{-1} = \zeta$.

Se η è un isomorfismo naturale fra il funtore identità $1_{\mathbf{C}}$ e un funtore E da $\mathbf{C}$ a $\mathbf{C}$, la commutatività del diagramma

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & EA \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle E(f)} \\ B & \xrightarrow[\eta_B]{} & EB \end{array}$$

mostra che $E(f) = \eta_B f \eta_A^{-1}$. Dunque l'applicazione $f \mapsto E(f)$ da $\hom(A, B)$ in $\hom(EA, EB)$ è biiettiva.

Esercizi

1. Sia F un funtore fedele e pieno da $\mathbf{C}$ a $\mathbf{D}$ e sia $f \in \hom_{\mathbf{C}}(A, B)$. Mostrare che ciascuna delle proprietà seguenti di $F(f)$ implica la proprietà corrispondente per f: essere un monomorfismo, essere un epimorfismo, avere una sezione, avere una retrazione, essere un isomorfismo.

2. Siano M e N monoidi, considerati come categorie con un solo oggetto come nell'esempio 5 di p. 12. Mostrare che, con questa identificazione, un funtore è un omomorfismo da M in N e che una trasformazione naturale da un funtore F a un funtore G corrisponde a un elemento $b \in N$ tale che $b(Fx) = (Gx)b$ per ogni $x \in M$.

3. Usare l'esercizio 2 per costruire un funtore F e un monomorfismo (epimorfismo) f tali che $F(f)$ non sia un monomorfismo (epimorfismo).

4. Sia G un gruppo e sia $\mathbf{G}$ la categoria con un solo oggetto determinata da G, come nell'esempio 6 di p. 12. Mostrare che dare un funtore da $\mathbf{G}$ a $\mathbf{Set}$ equivale a dare un omomorfismo di G nel gruppo $\operatorname{Sym} S$ delle permutazioni di un insieme S o, equivalentemente, un'azione di G su S (BAI, p. 72). Mostrare che due funtori di questo tipo sono naturalmente isomorfi se e solo se le azioni di G sono equivalenti (BAI, p. 74).

5. Siano $\mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}$ categorie, F e G funtori da $\mathbf{C}$ a $\mathbf{D}$, K un funtore da $\mathbf{B}$ a $\mathbf{C}$ e H un funtore da $\mathbf{D}$ a $\mathbf{E}$. Mostrare che, se η è una trasformazione naturale da F a G, allora $A \mapsto H(\eta_A)$, per $A \in \operatorname{ob}\mathbf{C}$, è una trasformazione naturale da HF a HG, e $B \mapsto \eta_{KB}$, per $B \in \operatorname{ob}\mathbf{B}$, è una trasformazione naturale da FK a GK.

6. Si definisca il *centro* di una categoria $\mathbf{C}$ come la classe delle trasformazioni naturali dal funtore identità $1_{\mathbf{C}}$ in sé. Sia $\mathbf{C} = R\text{-}\mathbf{mod}$ e sia c un elemento del centro di R. Per ogni $M \in \operatorname{ob}(R\text{-}\mathbf{mod})$ denotiamo con $\eta_M(c)$ l'applicazione $x \mapsto cx$, $x \in M$. Mostrare che $\eta(c) : M \mapsto \eta_M(c)$ appartiene al centro di $\mathbf{C}$ e che ogni elemento del centro ha questa forma. Mostrare che $c \mapsto \eta(c)$ è una biiezione e dunque che il centro di $R\text{-}\mathbf{mod}$ è un insieme.

1.4 Equivalenza di categorie

Diciamo che le categorie $\mathbf{C}$ e $\mathbf{D}$ sono *isomorfe* se esistono funtori $F : \mathbf{C} \to \mathbf{D}$ (da $\mathbf{C}$ a $\mathbf{D}$) e $G : \mathbf{D} \to \mathbf{C}$ tali che $GF = 1_{\mathbf{C}}$ e $FG = 1_{\mathbf{D}}$. La condizione è piuttosto forte, tanto che nella maggior parte dei casi in cui è soddisfatta si tende a identificare le categorie isomorfe. Eccone un esempio. Siano $\mathbf{C} = \mathbf{Ab}$ e $\mathbf{D} = \mathbb{Z}\text{-}\mathbf{mod}$. Se M è un gruppo abeliano (scritto additivamente), diventa uno $\mathbb{Z}$-modulo definendo nx, per $n \in \mathbb{Z}$ e $x \in M$, come l'n-esimo multiplo di x (BAI, p. 164). D'altra parte, se M è uno $\mathbb{Z}$-modulo, il suo gruppo additivo è abeliano. In tal modo abbiamo due applicazioni, da $\operatorname{ob}\mathbf{Ab}$ in $\operatorname{ob}(\mathbb{Z}\text{-}\mathbf{mod})$ e da $\operatorname{ob}(\mathbb{Z}\text{-}\mathbf{mod})$ in $\operatorname{ob}\mathbf{Ab}$, inverse l'una dell'altra. Se f è un omomorfismo dal gruppo abeliano M nel gruppo abeliano N, allora $f(nx) = nf(x)$ per $n \in \mathbb{Z}$ e $x \in M$. Dunque f è un omomorfismo da M a N considerati come $\mathbb{Z}$-moduli. Viceversa, ogni $\mathbb{Z}$-omomorfismo è un omomorfismo di gruppi. È quindi chiaro che $\mathbf{Ab}$ e $\mathbb{Z}\text{-}\mathbf{mod}$ sono categorie isomorfe e abitualmente le si identifica.

Un altro esempio di categorie isomorfe è dato da $R\text{-}\mathbf{mod}$ e $\mathbf{mod}\text{-}R^{\mathrm{op}}$ per un anello qualsiasi R. Se M è un R-modulo sinistro, esso diventa un R^{op}-modulo destro ponendo $xr = rx$ per $x \in M$ e $r \in R^{\mathrm{op}} = R$ (come insiemi). Analogamente ogni R^{op}-modulo destro diventa un R-modulo sinistro invertendo il procedimento. È chiaro inoltre che un omomorfismo da ${}_RM$, cioè M considerato come R-modulo sinistro, in ${}_RN$ è un omomorfismo da $M_{R^{\mathrm{op}}}$, cioè M considerato come R^{op}-modulo destro, in $N_{R^{\mathrm{op}}}$. Si hanno così gli ovvi funtori F e G per i quali $GF = 1_{R\text{-}\mathbf{mod}}$ e $FG = 1_{\mathbf{mod}\text{-}R^{\mathrm{op}}}$. Le due categorie sono dunque isomorfe.

La nozione di isomorfismo di categorie è alquanto restrittiva. Ampliandola nel modo che segue si ottiene una nozione assai più interessante. Si dice che $\mathbf{C}$ e $\mathbf{D}$ sono categorie *equivalenti* se esistono funtori $F : \mathbf{C} \to \mathbf{D}$ e $G : \mathbf{D} \to \mathbf{C}$ tali che $GF \cong 1_{\mathbf{C}}$ e $FG \cong 1_{\mathbf{D}}$, dove $\cong$ indica l'isomorfismo naturale di funtori. Evidentemente l'isomorfismo di categorie implica l'equivalenza.

È chiaro anche che la relazione di equivalenza fra categorie è, come suggerisce il nome, riflessiva, simmetrica e transitiva.

Osserviamo che nella definizione di equivalenza il funtore G non è determinato univocamente da F. È quindi naturale spostare l'attenzione dalla coppia (F, G) al funtore F e cercare condizioni affinché, dato $F : \mathbf{C} \to \mathbf{D}$, esista $G : \mathbf{D} \to \mathbf{C}$ tale che (F, G) dia un'equivalenza, ossia $GF \cong 1_{\mathbf{C}}$ e $FG \cong 1_{\mathbf{D}}$. Abbiamo visto che $GF \cong 1_{\mathbf{C}}$ implica che $f \mapsto GF(f)$ è una biiezione da $\hom_{\mathbf{C}}(A, B)$ su $\hom_{\mathbf{C}}(GFA, GFB)$. Analogamente $g \mapsto FG(g)$ è una biiezione da $\hom_{\mathbf{D}}(A', B')$ su $\hom_{\mathbf{D}}(FGA', FGB')$. Ora l'iniettività di $f \mapsto GF(f)$ implica l'iniettività di $f \mapsto F(f)$ dall'insieme $\hom_{\mathbf{C}}(A, B)$ in $\hom_{\mathbf{D}}(FA, FB)$, e la suriettività di $g \mapsto FG(g)$ implica la suriettività di $f \mapsto F(f)$. Vediamo così che F è fedele e pieno. Osserviamo anche che, dato un qualunque $A' \in \operatorname{ob}\mathbf{D}$, l'isomorfismo naturale $FG \cong 1_{\mathbf{D}}$ fornisce un isomorfismo $\eta_{A'} \in \hom_{\mathbf{D}}(A', FGA')$. Ponendo $A = GA' \in \operatorname{ob}\mathbf{C}$, si ha dunque un isomorfismo in $\hom_{\mathbf{D}}(A', FA)$ o, equivalentemente, in $\hom_{\mathbf{D}}(FA, A')$.

Mostriamo ora che le condizioni così individuate sono anche sufficienti. Otteniamo pertanto il seguente importante criterio.

Proposizione 1.3. *Sia F un funtore da $\mathbf{C}$ a $\mathbf{D}$. Esiste un funtore $G : \mathbf{D} \to \mathbf{C}$ tale che (F, G) sia un'equivalenza se e solo se F è fedele e pieno e, per ogni oggetto A' di $\mathbf{D}$, esiste un oggetto A di $\mathbf{C}$ tale che FA e A' siano isomorfi in $\mathbf{D}$, ossia tale che $\hom_{\mathbf{D}}(FA, A')$ contenga un isomorfismo.*

Dimostrazione. Resta da verificare la sufficienza delle condizioni. Supponiamole soddisfatte. Per ogni $A' \in \operatorname{ob}\mathbf{D}$ scegliamo $A \in \operatorname{ob}\mathbf{C}$ tale che FA e A' siano isomorfi e scegliamo un isomorfismo $\eta_{A'} : A' \to FA$. Definiamo un'applicazione G da $\operatorname{ob}\mathbf{D}$ in $\operatorname{ob}\mathbf{C}$ mediante $A' \mapsto A$, dove A è l'oggetto appena scelto. Allora $\eta_{A'} : A' \to FGA'$. Sia B' un secondo oggetto di $\mathbf{D}$ e sia $f' \in \hom_{\mathbf{D}}(A', B')$. Consideriamo il diagramma

$$\begin{array}{ccc} A' & \xrightarrow{\eta_{A'}} & FGA' \\ {\scriptstyle f'}\downarrow & & \\ B' & \xrightarrow[\eta_{B'}]{} & FGB' \end{array}$$

Poiché $\eta_{A'}$ è un isomorfismo, vi è un unico morfismo $\eta_{B'} f' \eta_{A'}^{-1} : FGA' \to FGB'$ che rende commutativo il rettangolo. Poiché F è pieno e fedele, esiste in $\mathbf{C}$ un unico $f : GA' \to GB'$ tale che $F(f) = \eta_{B'} f' \eta_{A'}^{-1}$. Definiamo l'applicazione G da $\hom_{\mathbf{D}}(A', B')$ in $\hom_{\mathbf{C}}(GA', GB')$ mediante $f' \mapsto f$. Si ha quindi il rettangolo commutativo

$$\begin{array}{ccc} A' & \xrightarrow{\eta_{A'}} & FGA' \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle FG(f')} \\ B' & \xrightarrow[\eta_{B'}]{} & FGB' \end{array} \tag{2}$$

e $G(f')$ è l'unico morfismo $GA' \to GB'$ tale che (2) sia commutativo.

Sia ora $g' \in \hom_{\mathbf{D}}(B', C')$. Si ha il diagramma

$$\begin{array}{ccc} A' & \xrightarrow{\eta_{A'}} & FGA' \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle FG(f')} \\ B' & \xrightarrow{\eta_{B'}} & FGB' \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle FG(g')} \\ C' & \xrightarrow[\eta_{C'}]{} & FGC' \end{array}$$

nel quale sono commutativi i due rettangoli piccoli e quindi anche quello grande. Poiché F è un funtore, abbiamo il rettangolo commutativo

$$\begin{array}{ccc} A' & \xrightarrow{\eta_{A'}} & FGA' \\ {\scriptstyle g'f'}\downarrow & & \downarrow{\scriptstyle F(G(g')G(f'))} \\ C' & \xrightarrow[\eta_{C'}]{} & FGC' \end{array} \cdot \tag{3}$$

D'altra parte abbiamo il rettangolo commutativo

$$\begin{array}{ccc} A' & \xrightarrow{\eta_{A'}} & FGA' \\ {\scriptstyle g'f'}\downarrow & & \downarrow{\scriptstyle F(G(g'f'))} \\ C' & \xrightarrow[\eta_{C'}]{} & FGC' \end{array} \tag{4}$$

e $G(g'f') : GA' \to GC'$ è l'unico morfismo che rende commutativo (4). Dunque $G(g')G(f') = G(g'f')$. In modo analogo si vede che $G(1_{A'}) = 1_{GA'}$. Pertanto le applicazioni $G : A' \mapsto GA'$ e $G : f' \mapsto G(f')$ per tutti gli insiemi di morfismi $\hom_{\mathbf{D}}(A', B')$ costituiscono un funtore da $\mathbf{D}$ a $\mathbf{C}$. Inoltre, la commutatività di (2) mostra che $\eta' : A' \mapsto \eta_{A'}$ è un isomorfismo naturale da $1_{\mathbf{D}}$ a FG.

Osserviamo ora che, essendo F fedele e pieno, se $A, B \in \operatorname{ob}\mathbf{C}$ e $f' : FA \to FB$ è un isomorfismo, allora il morfismo $f : A \to B$ tale che $F(f) = f'$ è un isomorfismo (esercizio 1 del §1.3). Poiché $\eta_{FA} : FA \to FGFA$ è un isomorfismo, ne segue che esiste un unico isomorfismo $\zeta_A : A \to GFA$ tale che $F(\zeta_A) = \eta_{FA}$. Ponendo in (2) $A' = FA$, $B' = FB$ e $f' = F(f)$ con $f : A \to B$ in $\mathbf{C}$, vediamo che il diagramma

$$\begin{array}{ccc} FA & \xrightarrow{F(\zeta_A)} & FGFA \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle FGF(f)} \\ FB & \xrightarrow[F(\zeta_B)]{} & FGFB \end{array}$$

è commutativo. Poiché F è fedele, ne segue la commutatività di

$$\begin{array}{ccc} A & \xrightarrow{\zeta_A} & GFA \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle GF(f)} \\ B & \xrightarrow[\zeta_B]{} & GFB \end{array} \cdot$$

Dunque $\zeta : A \mapsto \zeta_A$ è un isomorfismo naturale da $1_{\mathbf{C}}$ a GF. □

Come applicazione di questo criterio dimostriamo la seguente proposizione, particolarmente interessante.

Proposizione 1.4. *Sia R un anello e sia $M_n(R)$ l'anello delle matrici $n \times n$ a elementi in R. Le categorie* **mod**-R *e* **mod**-$M_n(R)$ *dei moduli destri rispettivamente su R e su $M_n(R)$ sono equivalenti.*

Prima di procedere alla dimostrazione, ricordiamo alcuni fatti elementari sulle unità matriciali in $M_n(R)$ (BAI, pp. 94–95). Per $i, j = 1, \ldots, n$ denotiamo con e_{ij} la matrice il cui elemento di posto (i, j) è 1 e i cui altri elementi sono 0. Per $a \in R$ poniamo $a' = \operatorname{diag}(a, \ldots, a)$, la matrice diagonale in cui tutti gli elementi diagonali sono a. Si ha la tavola di moltiplicazione

$$e_{ij}e_{kl} = \delta_{jk}e_{il} \tag{5}$$

e si ha

$$\sum_i e_{ii} = 1. \tag{6}$$

Inoltre

$$a' e_{ij} = e_{ij} a' \tag{7}$$

e questa matrice ha a nel posto (i, j) e zero altrove. Se dunque

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \qquad a_{ij} \in R, \tag{8}$$

allora

$$A = \sum_{i,j} a'_{ij} e_{ij} = \sum_{i,j} e_{ij} a'_{ij}. \tag{9}$$

Possiamo ora dare la

Dimostrazione della proposizione 1.4. Sia M un R-modulo destro e sia $M^{(n)}$ la somma diretta di n copie di M (BAI, p. 175). Se $x = (x_1, x_2, \ldots, x_n) \in M^{(n)}$ e $A \in M_n(R)$ è la matrice (8), definiamo xA mediante il prodotto matriciale

$$(x_1, x_2, \ldots, x_n) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = (y_1, y_2, \ldots, y_n), \tag{10}$$

dove

$$y_i = \sum_j x_j a_{ji}, \qquad 1 \leq i \leq n, \tag{11}$$

e il secondo membro si calcola in M. L'associatività del prodotto matriciale (in questo caso misto di moltiplicazione di «vettori» per matrici) permette di verificare che, con l'azione appena definita, $M^{(n)}$ è un $M_n(R)$-modulo destro. Si ha dunque un'applicazione $M \mapsto M^{(n)}$ da ob(**mod**-R) in ob(**mod**-$M_n(R)$). Se f è un omomorfismo di moduli da M in N, l'omomorfismo diagonale

$$f^{(n)} : (x_1, x_2, \ldots, x_n) \longmapsto (f(x_1), f(x_2), \ldots, f(x_n))$$

è un omomorfismo di $M_n(R)$-moduli destri da $M^{(n)}$ in $N^{(n)}$. Le applicazioni $M \mapsto M^{(n)}$, $f \mapsto f^{(n)}$ costituiscono un funtore F da **mod**-R a **mod**-$M_n(R)$. Verifichiamo che F soddisfa le condizioni della proposizione 1.3.

1. *F è fedele.* È evidente.

2. *F è pieno.* Sia g un $M_n(R)$-omomorfismo da $M^{(n)}$ in $N^{(n)}$, dove M e N sono R-moduli destri. Ora $M^{(n)}e_{11}$ è l'insieme degli elementi $(x, 0, \ldots, 0)$, $x \in M$, e $N^{(n)}e_{11}$ è l'insieme degli elementi $(y, 0, \ldots, 0)$, $y \in N$. Poiché g è un $M_n(R)$-omomorfismo, si ha $g(M^{(n)}e_{11}) \subseteq N^{(n)}e_{11}$. Dunque $g(x, 0, \ldots, 0) = (f(x), 0, \ldots, 0)$. È chiaro che f è additiva, e l'uguaglianza $f(xa) = f(x)a$ per $a \in R$ segue da

$$g((x, 0, \ldots, 0)a') = g(x, 0, \ldots, 0)a'.$$

Pertanto f è un R-omomorfismo di M in N. Inoltre $(x,0,\dots,0)e_{1i} = (0,\dots,0,x,0,\dots,0)$, con x nell'i-esimo posto. L'uguaglianza $g((x,0,\dots,0)e_{1i}) = g(x,0,\dots,0)e_{1i}$ implica quindi

$$g(0,\dots,0,\overset{i}{x},0,\dots,0) = (0,\dots,0,\overset{i}{f(x)},0,\dots,0).$$

Allora $g = f^{(n)}$ e F è pieno.

3. *Ogni $M_n(R)$-modulo destro M' è isomorfo a un modulo FM, con M un R-modulo destro.* L'applicazione $a \mapsto a'$ è un omomorfismo di R in $M_n(R)$. Combinandolo con l'azione di $M_n(R)$ su M', si fa di M' un R-modulo destro ponendo $x'a = x'a'$ per $x' \in M'$. Allora $M = M'e_{11}$ è un R-sottomodulo di M', poiché $e_{11}a' = a'e_{11}$ per $a \in R$. Inoltre, per ogni i, $x'e_{i1} = x'e_{i1}e_{11} \in M$. Definiamo un'applicazione $\eta_{M'} : M' \to FM = M^{(n)}$ mediante

$$x' \longmapsto (x'e_{11}, x'e_{21}, \dots, x'e_{n1}). \tag{12}$$

Una verifica diretta mediante (9) e la definizione di $x'a$ mostra che $\eta_{M'}$ è un $M_n(R)$-omomorfismo. Se $x'e_{i1} = 0$ per $1 \le i \le n$, allora $x' = \sum_i x'e_{ii} = \sum_i x'e_{i1}e_{1i} = 0$. Dunque $\eta_{M'}$ è iniettiva. È anche suriettiva: se $(x_1, x_2, \dots, x_n) \in M^{(n)}$, allora $x_i = x_i'e_{11} = (x_i'e_{1i})e_{i1}$ e

$$\begin{aligned}(x_1, x_2, \dots, x_n) = {} & \big((x_1'e_{11})e_{11}, (x_1'e_{11})e_{21}, \dots, (x_1'e_{11})e_{n1}\big) \\ & + \big((x_2'e_{12})e_{11}, (x_2'e_{12})e_{21}, \dots, (x_2'e_{12})e_{n1}\big) + \cdots .\end{aligned}$$

Pertanto $\eta_{M'}$ è un isomorfismo. □

Esercizi

1. Sia (F, G) un'equivalenza da $\mathbf{C}$ a $\mathbf{D}$ e sia $f \in \hom_{\mathbf{C}}(A, B)$. Mostrare che ciascuna delle seguenti proprietà di f implica la proprietà corrispondente per $F(f)$: essere un monomorfismo, essere un epimorfismo, avere una sezione, avere una retrazione, essere un isomorfismo.

2. Le categorie **mod**-R e **mod**-$M_n(R)$ sono isomorfe per $n > 1$?

1.5 Prodotti e coprodotti

Molte costruzioni fondamentali della matematica, e in particolare dell'algebra, si possono caratterizzare in modo semplice mediante proprietà delle applicazioni. Ne sono esempi il prodotto cartesiano di insiemi, il prodotto diretto di gruppi, l'unione disgiunta di insiemi e il prodotto libero di gruppi. Questo fatto, noto da tempo, trova posto nella teoria delle categorie con la definizione di prodotto e di coprodotto in una categoria e con gli esempi che la illustrano. Cominciamo dal prodotto diretto di due gruppi.

Sia $G = G_1 \times G_2$ il prodotto diretto dei gruppi G_1 e G_2. Gli elementi di G sono le coppie (g_1, g_2), con $g_i \in G_i$, e la moltiplicazione è definita da

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

L'unità è $1 = (1_1, 1_2)$, dove 1_i è l'unità di G_i, e $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. Si hanno le proiezioni $p_i : G \to G_i$ definite da

$$p_1 : (g_1, g_2) \longmapsto g_1, \qquad p_2 : (g_1, g_2) \longmapsto g_2. \tag{13}$$

Esse sono omomorfismi, poiché

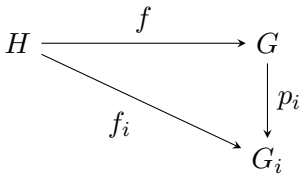
$$p_1\big((g_1, g_2)(h_1, h_2)\big) = p_1(g_1h_1, g_2h_2) = g_1h_1 = p_1(g_1, g_2)\, p_1(h_1, h_2)$$

e $p_1(1) = 1_1$. Relazioni analoghe valgono per p_2.

Sia ora H un altro gruppo e, per $i = 1, 2$, sia $f_i : H \to G_i$ un omomorfismo di H in G_i. Definiamo un'applicazione f di H in $G = G_1 \times G_2$ ponendo

$$h \longmapsto (f_1(h), f_2(h)).$$

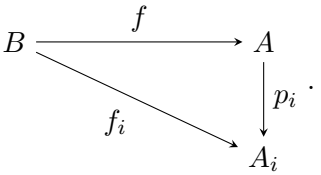
È chiaro che f è un omomorfismo e che $p_i f(h) = f_i(h)$. È dunque commutativo il diagramma

(14)


Sia f' un qualsiasi omomorfismo di H in G tale che $p_i f' = f_i$, $i = 1, 2$. Allora $f'(h) = (f_1(h), f_2(h)) = f(h)$, sicché $f' = f$. Pertanto f è l'unico omomorfismo $H \to G$ che rende commutativo il diagramma (14).

Formuliamo ora la seguente definizione.

Definizione 1.4. *Siano A_1, A_2 oggetti di una categoria $\mathbf{C}$. Un prodotto di A_1 e A_2 in $\mathbf{C}$ è una terna (A, p_1, p_2), con $A \in \operatorname{ob}\mathbf{C}$ e $p_i \in \hom_{\mathbf{C}}(A, A_i)$, avente la seguente proprietà. Per ogni oggetto B di $\mathbf{C}$ e ogni coppia di morfismi $f_i \in \hom_{\mathbf{C}}(B, A_i)$, $i = 1, 2$, esiste un unico $f \in \hom_{\mathbf{C}}(B, A)$ che rende commutativi i diagrammi*

(15)


Da quanto precede è chiaro che, se G_1, G_2 sono gruppi, $(G = G_1 \times G_2, p_1, p_2)$ è un prodotto di G_1 e G_2 nella categoria dei gruppi. Il fatto che $(G_1 \times G_2, p_1, p_2)$ sia un prodotto di G_1 e G_2 in **Grp** caratterizza il prodotto diretto $G_1 \times G_2$ e le proiezioni p_i. Si tratta di un caso particolare della seguente proposizione.

Proposizione 1.5. *Siano (A, p_1, p_2) e (A', p_1', p_2') prodotti di A_1 e A_2 in $\mathbf{C}$. Esiste allora un unico isomorfismo $h : A \to A'$ tale che $p_i = p_i' h$ per $i = 1, 2$.*

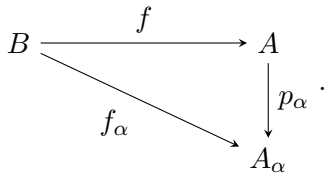
Dimostrazione. Poiché (A', p_1', p_2') è un prodotto di A_1, A_2, esiste un unico morfismo $h : A \to A'$ tale che $p_i = p_i' h$, $i = 1, 2$. Scambiando i ruoli di (A, p_1, p_2) e (A', p_1', p_2'), si ottiene un unico morfismo $h' : A' \to A$ tale che $p_i' = p_i h'$. Abbiamo dunque $p_i = p_i h' h$ e $p_i' = p_i' h h'$. D'altra parte, applicando la definizione 1.4 a $B = A$ e $f_i = p_i$, si vede che l'unico morfismo $u : A \to A$ tale che $p_i = p_i u$ è 1_A. Quindi $h'h = 1_A$ e, analogamente, $hh' = 1_{A'}$. Pertanto h è un isomorfismo e $h' = h^{-1}$. □

In virtù di questa essenziale unicità, indicheremo con $A_1 \amalg A_2$ un qualsiasi prodotto di A_1 e A_2 nella categoria $\mathbf{C}$. Il concetto di prodotto in una categoria si può generalizzare a più di due oggetti.

Definizione 1.4′**.** *Sia $\{A_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di oggetti di una categoria $\mathbf{C}$. Un prodotto $\prod A_\alpha$ degli A_α è costituito da un oggetto $A \in \operatorname{ob}\mathbf{C}$ e da una famiglia di morfismi $p_\alpha \in \hom_{\mathbf{C}}(A, A_\alpha)$, $\alpha \in I$, tali che, dati $B \in \operatorname{ob}\mathbf{C}$ e $f_\alpha \in \hom_{\mathbf{C}}(B, A_\alpha)$, $\alpha \in I$, esista un unico*

$f \in \hom_{\mathbf{C}}(B, A)$ *che renda commutativo ciascun diagramma*

(15′)



Non si suppone che l'applicazione $\alpha \mapsto A_\alpha$ sia iniettiva. Gli A_α possono anche essere tutti uguali. Inoltre, se un prodotto esiste, esso è unico nel senso precisato nella proposizione 1.5, la cui dimostrazione si estende senza modifiche al caso generale. Consideriamo alcuni esempi di prodotti in categorie.

Esempi.

1. Sia $\{A_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di insiemi. L'insieme prodotto $A = \prod A_\alpha$ è formato dalle applicazioni $a : I \to \bigcup A_\alpha$ tali che $a(\alpha) \in A_\alpha$ per ogni $\alpha \in I$. A ciascun α corrisponde la proiezione $p_\alpha : a \mapsto a(\alpha)$. Affermiamo che $\{A, p_\alpha\}$ è un prodotto degli A_α nella categoria **Set**. Infatti, dati un insieme B e, per ogni $\alpha \in I$, un'applicazione $f_\alpha : B \to A_\alpha$, si ha l'applicazione $f : B \to A$ che a b associa l'applicazione $\alpha \mapsto f_\alpha(b)$. Allora $p_\alpha f = f_\alpha$ ed è chiaro che f è l'unica applicazione $B \to A$ che verifica queste condizioni. Pertanto $\{A, p_\alpha\}$ soddisfa la condizione che definisce un prodotto degli A_α.

2. Sia $\{G_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di gruppi. Definiamo in $G = \prod G_\alpha$ una moltiplicazione ponendo $(gg')(\alpha) = g(\alpha)g'(\alpha)$, per $g, g' \in G$, e definiamo $1 \in G$ ponendo, per ogni $\alpha \in I$, $1(\alpha) = 1_\alpha$, l'unità di G_α. Si verifica facilmente che si ottiene così una struttura di gruppo su G, ed è chiaro che le proiezioni definite in **Set** sono omomorfismi. Come nell'esempio 1, $\{G, p_\alpha\}$ è un prodotto dei G_α nella categoria dei gruppi.

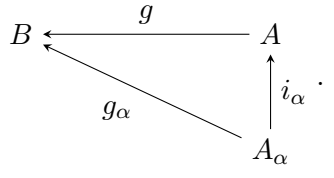
3. Il ragionamento dell'esempio 2 si applica anche alla categoria degli anelli. Se $\{R_\alpha \mid \alpha \in I\}$ è una famiglia indicizzata di anelli, si può munire $\prod R_\alpha$ di una struttura di anello per la quale le proiezioni p_α siano omomorfismi di anelli. Allora $\{\prod R_\alpha, p_\alpha\}$ è un prodotto degli R_α nella categoria **Ring**.

4. In modo analogo si possono definire i prodotti di famiglie indicizzate di moduli in R-**mod**, per ogni anello R.

Consideriamo ora il concetto duale di quello di prodotto.

Definizione 1.5. *Sia $\{A_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di oggetti di una categoria $\mathbf{C}$. Un coprodotto degli A_α è costituito da un oggetto $A \in \operatorname{ob}\mathbf{C}$ e da una famiglia di morfismi $i_\alpha \in \hom_{\mathbf{C}}(A_\alpha, A)$, $\alpha \in I$, tali che, dati $B \in \operatorname{ob}\mathbf{C}$ e $g_\alpha \in \hom_{\mathbf{C}}(A_\alpha, B)$, $\alpha \in I$, esista un unico $g \in \hom_{\mathbf{C}}(A, B)$ che renda commutativo ciascun diagramma*

(16)



Si vede subito che, se $\{A, i_\alpha \mid \alpha \in I\}$ e $\{A', i'_\alpha \mid \alpha \in I\}$ sono coprodotti in $\mathbf{C}$ di $\{A_\alpha \mid \alpha \in I\}$, esiste un unico isomorfismo $k : A' \to A$ tale che $i_\alpha = ki'_\alpha$ per ogni $\alpha \in I$.

Se $\{A_\alpha \mid \alpha \in I\}$ è una famiglia indicizzata di insiemi, esiste un insieme $\bigsqcup A_\alpha$ che è unione disgiunta degli A_α. Indichiamo con i_α l'iniezione di A_α in $\bigsqcup A_\alpha$. Dati un insieme B e, per ogni

α, un'applicazione $g_\alpha : A_\alpha \to B$, esiste un'unica applicazione $g : \bigsqcup A_\alpha \to B$ la cui restrizione a A_α è g_α, per ogni $\alpha \in I$. Ne segue che $\{\bigsqcup A_\alpha, i_\alpha\}$ è un coprodotto degli A_α in **Set**.

Nel prossimo capitolo mostreremo che in **Grp** e in **Ring** esistono i coprodotti di ogni famiglia indicizzata di oggetti (si veda p. 84 dell'originale). Nel caso di R-**mod** lo si vede facilmente. Sia $\{M_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di R-moduli sinistri e sia $\prod M_\alpha$ l'insieme prodotto degli M_α, munito della struttura di R-modulo sinistro per la quale, dati $x, y \in \prod M_\alpha$ e $r \in R$,

$$(x + y)(\alpha) = x(\alpha) + y(\alpha), \qquad (rx)(\alpha) = r\big(x(\alpha)\big).$$

Sia $\bigoplus M_\alpha$ il sottoinsieme di $\prod M_\alpha$ costituito dagli x per i quali $x(\alpha) = 0$ salvo che per un numero finito di indici $\alpha \in I$. Chiaramente $\bigoplus M_\alpha$ è un sottomodulo di $\prod M_\alpha$. Per $x_\alpha \in M_\alpha$, indichiamo con $i_\alpha x_\alpha$ l'elemento di $\bigoplus M_\alpha$ che vale x_α in α e 0 in ogni $\beta \in I$ diverso da α. L'applicazione $i_\alpha : x_\alpha \mapsto i_\alpha x_\alpha$ è un omomorfismo di moduli da M_α in $\bigoplus M_\alpha$. Sia ora N un R-modulo sinistro e supponiamo dato, per ogni $\alpha \in I$, un omomorfismo $g_\alpha : M_\alpha \to N$. Per $x \in \bigoplus M_\alpha$, $x(\alpha) = 0$ salvo che per un numero finito di indici, dunque la somma $\sum_\alpha g_\alpha x(\alpha)$ è ben definita. Definiamo $g : \bigoplus M_\alpha \to N$ ponendo

$$x \longmapsto \sum_\alpha g_\alpha x(\alpha).$$

Si verifica subito che g è un omomorfismo da $\bigoplus M_\alpha$ in N e che è l'unico tale che $gi_\alpha = g_\alpha$ per ogni α. Pertanto $\{\bigoplus M_\alpha, i_\alpha\}$ è un coprodotto degli M_α in R-**mod**. Chiamiamo $\bigoplus M_\alpha$ la *somma diretta* dei moduli M_α.

Poiché la categoria **Ab** è isomorfa a $\mathbb{Z}$-**mod**, in **Ab** esistono i coprodotti di famiglie indicizzate arbitrarie di oggetti.

Esercizi.

1. Siano S un insieme parzialmente ordinato e **S** la categoria associata, definita nell'esempio 12 del § 1.1. Sia $\{a_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di elementi di S. Dare una condizione su $\{a_\alpha\}$ affinché la famiglia corrispondente di oggetti di **S** ammetta un prodotto (un coprodotto). Servirsene per costruire un esempio di categoria in cui ogni sottoinsieme finito di oggetti abbia un prodotto (un coprodotto), ma in cui vi siano insiemi infiniti di oggetti che non ne hanno.

2. Una categoria **C** si dice *con prodotto* (*con coprodotto*) se ogni coppia di suoi oggetti ha un prodotto (un coprodotto) in **C**. Mostrare che, in tal caso, ogni famiglia di oggetti di **C** indicizzata da un insieme finito ha un prodotto (un coprodotto).

3. Un oggetto A di una categoria **C** si dice *iniziale* (*terminale*) se, per ogni oggetto X di **C**, $\hom_{\mathbf{C}}(A, X)$ (rispettivamente $\hom_{\mathbf{C}}(X, A)$) è costituito da un solo elemento. Un oggetto al tempo stesso iniziale e terminale si dice *oggetto zero* di **C**. Mostrare che, se A, A' sono iniziali (terminali), esiste un unico isomorfismo h in $\hom_{\mathbf{C}}(A, A')$.

4. Siano A_1, A_2 oggetti di una categoria **C** e sia $\mathbf{C}/\{A_1, A_2\}$ la categoria definita nell'esercizio 5 del § 1.1. Mostrare che A_1, A_2 hanno un prodotto in **C** se e solo se $\mathbf{C}/\{A_1, A_2\}$ ha un oggetto terminale. Si osservi che questo risultato e l'esercizio 3 forniscono un'altra dimostrazione della proposizione 1.5. Generalizzare alle famiglie indicizzate di oggetti di **C**.

5. Servirsi dell'esercizio 6 del § 1.1 per dare un'altra definizione di coprodotto di oggetti di una categoria.

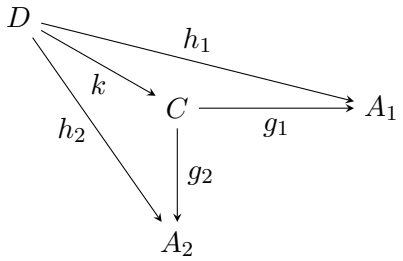
6. Siano $f_i : A_i \to B$, $i = 1, 2$, morfismi di una categoria $\mathbf{C}$. Si chiama *diagramma di pullback* di $\{f_1, f_2\}$ un diagramma commutativo

(17)
$$\begin{array}{ccc} C & \xrightarrow{g_1} & A_1 \\ {\scriptstyle g_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ A_2 & \xrightarrow[f_2]{} & B \end{array}$$

con la proprietà seguente. Per ogni rettangolo commutativo

$$\begin{array}{ccc} D & \xrightarrow{h_1} & A_1 \\ {\scriptstyle h_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ A_2 & \xrightarrow[f_2]{} & B \end{array}$$

che contenga f_1 e f_2, esiste un unico $k : D \to C$ che rende commutativo il diagramma



Mostrare che, se (C, g_1, g_2) e (C', g_1', g_2') determinano pullback di f_1, f_2 come in (17), esiste un unico isomorfismo $k : C' \to C$ tale che $g_i' = g_i k$, $i = 1, 2$.

7. Siano $f_i : G_i \to H$ in **Grp**. Si formi $G_1 \times G_2$ e si consideri il sottoinsieme M costituito dagli elementi (a_1, a_2) tali che $f_1(a_1) = f_2(a_2)$. Esso è un sottogruppo. Sia $m_i = p_i|_M$, dove p_i è la proiezione di $G_1 \times G_2$ su G_i. Mostrare che $\{m_1, m_2\}$ definisce un diagramma di pullback di f_1, f_2.

8. Dualizzare l'esercizio 6 per definire il *diagramma di pushout* determinato da $f_i : B \to A_i$, $i = 1, 2$, in $\mathbf{C}$. Siano $f_i : B \to A_i$, $i = 1, 2$, in R-**mod**. Si formi $A_1 \oplus A_2$ e si definisca $f : B \to A_1 \oplus A_2$ ponendo $f(b) = (-f_1(b), f_2(b))$. Siano $I = \operatorname{Im} f$, $N = (A_1 \oplus A_2)/I$. Si definiscano $n_i : A_i \to N$ ponendo $n_1 a_1 = (a_1, 0) + I$, $n_2 a_2 = (0, a_2) + I$. Verificare che $\{n_1, n_2\}$ definisce un diagramma di pushout di f_1, f_2.

1.6 I funtori hom. Funtori rappresentabili

Definiremo ora alcuni importanti funtori dalla categoria $\mathbf{C}$ e dalle categorie ad essa associate, $\mathbf{C}^{\mathrm{op}}$ e $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$, alla categoria degli insiemi. Consideriamo anzitutto il funtore hom di dominio $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$. Ricordiamo che gli oggetti di quest'ultima categoria sono le coppie (A, B), con $A, B \in \operatorname{ob} \mathbf{C}$, e che un morfismo da (A, B) ad (A', B') è una coppia (f, g), dove $f : A' \to A$ e $g : B \to B'$. Se (f', g') è un morfismo da (A', B') ad (A'', B''), cosicché $f' : A'' \to A'$ e $g' : B' \to B''$, si ha $(f', g')(f, g) = (ff', g'g)$. Inoltre $1_{(A,B)} = (1_A, 1_B)$.

Definiamo il funtore hom da $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$ a **Set** nel modo seguente. All'oggetto (A, B) esso associa l'insieme $\hom(A, B)$, che è un oggetto di **Set**, e al morfismo $(f, g) : (A, B) \to (A', B')$ associa l'applicazione da $\hom(A, B)$ a $\hom(A', B')$ definita da

$$\hom(f, g) : k \longmapsto gkf. \tag{18}$$

La definizione ha senso poiché $f : A' \to A$, $g : B \to B'$, $k : A \to B$, e dunque $gkf : A' \to B'$. Queste regole definiscono un funtore. Infatti, se $(f', g') : (A', B') \to (A'', B'')$, allora $(f', g')(f, g) = (ff', g'g)$ e

$$\begin{aligned} \hom(ff', g'g)(k) &= (g'g)k(ff') \\ &= g'(gkf)f' \\ &= g'\big(\hom(f, g)(k)\big)f' \\ &= \hom(f', g')\big(\hom(f, g)(k)\big). \end{aligned}$$

Ne segue che $\hom\big((f', g')(f, g)\big) = \hom(f', g')\hom(f, g)$. Se poi $f = 1_A$ e $g = 1_B$, la (18) mostra che $\hom(1_A, 1_B)$ è l'applicazione identica dell'insieme $\hom(A, B)$. Sono così soddisfatte le condizioni che definiscono un funtore da $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$ a **Set**.

Fissato un oggetto A di $\mathbf{C}$, definiamo ora un funtore $\hom(A, -)$ da $\mathbf{C}$ a **Set**. Sugli oggetti poniamo

$$\hom(A, -)B = \hom(A, B).$$

Per $g : B \to B'$, $\hom(A, -)(g)$ è l'applicazione da $\hom(A, B)$ a $\hom(A, B')$ data da

$$\hom(A, g) : k \longmapsto gk. \tag{19}$$

È chiaro che ciò definisce un funtore. Lo chiamiamo *funtore hom (covariante) determinato dall'oggetto* A di $\mathbf{C}$.

In modo analogo definiamo il *funtore hom controvariante* $\hom(-, B)$ *determinato da* $B \in \mathrm{ob}\,\mathbf{C}$. Sugli oggetti poniamo

$$\hom(-, B)A = \hom(A, B).$$

Per $f : A' \to A$, $\hom(-, B)(f)$ è l'applicazione da $\hom(A, B)$ a $\hom(A', B)$ data da

$$\hom(f, B) : k \longmapsto kf. \tag{20}$$

Siano ora $f : A' \to A$, $g : B \to B'$, $k : A \to B$. Allora

$$\begin{aligned} \hom(f, B')\hom(A, g)(k) &= (gk)f, \\ \hom(A', g)\hom(f, B)(k) &= g(kf), \end{aligned}$$

e $(gk)f = g(kf) = \hom(f, g)(k)$. Pertanto il diagramma

$$\begin{array}{ccc} \hom(A, B) & \xrightarrow{\hom(A, g)} & \hom(A, B') \\ {\scriptstyle \hom(f, B)}\downarrow & & \downarrow{\scriptstyle \hom(f, B')} \\ \hom(A', B) & \xrightarrow[\hom(A', g)]{} & \hom(A', B') \end{array} \tag{21}$$

è commutativo. Da questa commutatività si deducono due trasformazioni naturali. Fissiamo dapprima $g : B \to B'$ e consideriamo l'applicazione

$$A \longmapsto \hom(A, g) \in \hom_{\mathbf{Set}}\big(\hom(A, B), \hom(A, B')\big).$$

La commutatività del diagramma precedente esprime il fatto che $A \mapsto \hom(A, g)$ è una trasformazione naturale dal funtore controvariante $\hom(-, B)$ al funtore controvariante $\hom(-, B')$. Similmente, per $f : A' \to A$ si può interpretare la commutatività di (21) dicendo che $B \mapsto \hom(f, B)$ è una trasformazione naturale da $\hom(A, -)$ a $\hom(A', -)$.

Nelle applicazioni si desidera spesso «rappresentare» un funtore dato mediante un funtore hom. Prima di precisare il significato di rappresentazione determiniamo le trasformazioni naturali da un funtore $\hom_{\mathbf{C}}(A, -)$, che va da $\mathbf{C}$ a $\mathbf{Set}$, a un qualsiasi funtore F da $\mathbf{C}$ a $\mathbf{Set}$. Siano a un elemento dell'insieme FA, $B \in \operatorname{ob}\mathbf{C}$ e $k \in \hom_{\mathbf{C}}(A, B)$. Allora $F(k)$ è un'applicazione di FA in FB, e il suo valore in a è $F(k)(a) \in FB$. Si ha così un'applicazione

$$a_B : k \longmapsto F(k)(a) \tag{22}$$

di $\hom_{\mathbf{C}}(A, B)$ in FB. Vale il seguente importante lemma.

Lemma di Yoneda. *Siano F un funtore da $\mathbf{C}$ a $\mathbf{Set}$, A un oggetto di $\mathbf{C}$ e a un elemento dell'insieme FA. Per ogni $B \in \operatorname{ob}\mathbf{C}$, sia a_B l'applicazione da $\hom_{\mathbf{C}}(A, B)$ a FB data da $k \mapsto F(k)(a)$. Allora $B \mapsto a_B$ è una trasformazione naturale $\eta(a)$ da $\hom_{\mathbf{C}}(A, -)$ a F. Inoltre $a \mapsto \eta(a)$ è una biiezione dall'insieme FA sulla classe delle trasformazioni naturali da $\hom_{\mathbf{C}}(A, -)$ a F. L'inversa di $a \mapsto \eta(a)$ è l'applicazione $\eta \mapsto \eta_A(1_A) \in FA$.*

Dimostrazione. Abbiamo osservato che la (22) è un'applicazione da $\hom_{\mathbf{C}}(A, B)$ a FB. Sia ora $g : B \to C$. Allora

$$\begin{aligned} F(g)a_B(k) &= F(g)F(k)(a) = F(gk)(a), \\ a_C \hom(A, g)(k) &= a_C(gk) = F(gk)(a). \end{aligned}$$

È dunque commutativo il diagramma

$$\begin{array}{ccc} \hom(A, B) & \xrightarrow{\quad a_B \quad} & FB \\ {\scriptstyle \hom(A,-)(g)}\downarrow & & \downarrow{\scriptstyle F(g)} \\ \hom(A, C) & \xrightarrow[\quad a_C \quad]{} & FC \end{array}$$

e $\eta(a) : B \mapsto a_B$ è una trasformazione naturale da $\hom(A, -)$ a F. Inoltre

$$\eta(a)_A(1_A) = a_A(1_A) = F(1_A)(a) = a.$$

Sia ora η una qualsiasi trasformazione naturale da $\hom(A, -)$ a F e sia $f \in \hom_{\mathbf{C}}(A, B)$. Dalla commutatività del diagramma

$$\begin{array}{ccc} \hom(A, A) & \xrightarrow{\quad \eta_A \quad} & FA \\ {\scriptstyle \hom(A,f)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \hom(A, B) & \xrightarrow[\quad \eta_B \quad]{} & FB \end{array}$$

segue che

$$\begin{aligned} \eta_B(f) &= \eta_B(f1_A) = \eta_B\big(\hom(A, f)(1_A)\big) \\ &= F(f)\eta_A(1_A) = F(f)(a), \qquad a = \eta_A(1_A) \in FA. \end{aligned}$$

Ciò mostra che $\eta = \eta(a)$, con la notazione introdotta sopra. I due risultati così ottenuti dimostrano il lemma. □

Diremo che un funtore F da $\mathbf{C}$ a $\mathbf{Set}$ è *rappresentabile* se esiste un isomorfismo naturale tra F e un funtore $\hom(A,-)$, per qualche $A \in \operatorname{ob}\mathbf{C}$. Se $\eta : \hom(A,-) \to F$ è tale isomorfismo naturale, il lemma di Yoneda mostra che η è determinato da A e dall'elemento $a = \eta_A(1_A)$ di FA. La coppia (A,a) si chiama un *rappresentante* del funtore rappresentabile F.

Esercizi.

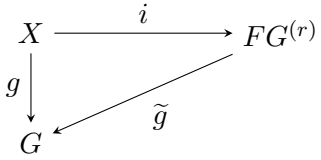
1. Applicare il lemma di Yoneda per ottenere una biiezione fra la classe delle trasformazioni naturali da $\hom(A,-)$ a $\hom(A',-)$ e l'insieme $\hom_{\mathbf{C}}(A',A)$.

2. Mostrare che $f : B \to B'$ è un monomorfismo in $\mathbf{C}$ se e solo se $\hom(A,f)$ è iniettiva per ogni $A \in \operatorname{ob}\mathbf{C}$.

3. Dualizzare il lemma di Yoneda per mostrare che, se F è un funtore controvariante da $\mathbf{C}$ a $\mathbf{Set}$ e $A \in \operatorname{ob}\mathbf{C}$, ogni trasformazione naturale da $\hom_{\mathbf{C}}(-,A)$ a F è della forma $B \mapsto a_B$, dove a_B è un'applicazione da $\hom_{\mathbf{C}}(B,A)$ a FB determinata da un elemento $a \in FA$ mediante
$$a_B : k \longmapsto F(k)a.$$
Mostrare che si ottiene in tal modo una biiezione fra l'insieme FA e la classe delle trasformazioni naturali da $\hom_{\mathbf{C}}(-,A)$ a F.

1.7 Universali

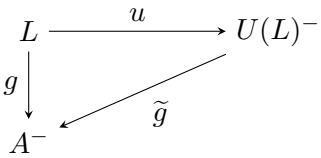
Fra i primi esempi del concetto di universale si trovano il gruppo libero determinato da un insieme X e l'algebra inviluppante universale (associativa) di un'algebra di Lie. Abbiamo studiato il primo per un insieme finito X in BAI, pp. 68–69. Per un insieme X di cardinalità $r < \infty$ vi abbiamo costruito un gruppo $FG^{(r)}$ e un'applicazione $i\colon x \mapsto \bar{x}$ di X in $FG^{(r)}$ tali che, per ogni gruppo G e ogni applicazione g di X in G, esista un unico omomorfismo $\widetilde{g}\colon FG^{(r)} \to G$ che renda commutativo il diagramma



Qui $\widetilde{g}$ è considerato come un'applicazione fra insiemi.

Ricordiamo che un'algebra di Lie L su un campo è uno spazio vettoriale dotato di un prodotto bilineare $[xy]$ tale che
$$[xx] = 0, \qquad [[xy]z] + [[yz]x] + [[zx]y] = 0.$$
Se A è un'algebra associativa, essa definisce un'algebra di Lie A^- in cui la legge di composizione è il prodotto di Lie (o commutatore additivo) $[xy] = xy - yx$, dove xy è il prodotto associativo dato in A (BAI, pp. 431 e 434). È chiaro che, se A e B sono algebre associative e f è un omomorfismo di A in B, allora f è anche un omomorfismo di algebre di Lie di A^- in B^-.

Se L è un'algebra di Lie, un'*algebra inviluppante universale* di L è una coppia $(U(L),u)$, dove $U(L)$ è un'algebra associativa e u è un omomorfismo di L nell'algebra di Lie $U(L)^-$, con la seguente proprietà. Per ogni omomorfismo g di L in un'algebra di Lie A^- ottenuta da un'algebra associativa A, esiste un unico omomorfismo $\widetilde{g}$ dell'algebra associativa $U(L)$ in A tale che



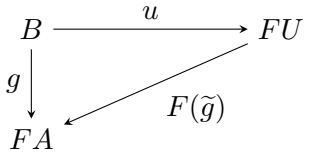
sia un diagramma commutativo di omomorfismi di algebre di Lie. Daremo una costruzione di $(U(L), u)$ nel capitolo 3 (p. 142 dell'originale).

Entrambi gli esempi si possono formulare in termini di categorie e funtori. Nel primo consideriamo le categorie **Grp** e **Set**. Sia F il funtore dimenticante da **Grp** a **Set** che a un gruppo associa l'insieme sottostante e a un omomorfismo di gruppi la corrispondente applicazione fra insiemi. Dato un insieme X, un gruppo libero determinato da X è una coppia (U, u), dove U è un gruppo e u un'applicazione di X in U, tale che, per ogni gruppo G e ogni applicazione g di X in G, esista un unico omomorfismo $\widetilde{g}$ di U in G per il quale, come applicazioni fra insiemi, si abbia $\widetilde{g}u = g$.

Per il secondo esempio consideriamo la categoria **Alg** delle algebre associative e la categoria **Lie** delle algebre di Lie su un campo fissato. Abbiamo il funtore F da **Alg** a **Lie** definito da $FA = A^-$ per ogni algebra associativa A e, se $f\colon A \to B$ è un omomorfismo di algebre associative, da $F(f) = f\colon A^- \to B^-$ per le corrispondenti algebre di Lie. Per una data algebra di Lie L, un inviluppo universale è una coppia $(U(L), u)$, dove $U(L)$ è un'algebra associativa e u è un omomorfismo di algebre di Lie di L in $U(L)^-$, tale che per ogni omomorfismo g di L in un'algebra di Lie A^-, con A associativa, esista un unico omomorfismo $\widetilde{g}$ di $U(L)$ in A tale che $\widetilde{g}u = g$.

Diamo ora la definizione generale di universale.

Definizione 1.6. *Siano* **C** *e* **D** *categorie, F un funtore da* **C** *a* **D** *e B un oggetto di* **D**. *Un* universale da B al funtore F *è una coppia (U, u), dove U è un oggetto di* **C** *e u è un morfismo da B a FU, tale che per ogni morfismo g da B a FA esista un unico morfismo $\widetilde{g}$ da U ad A in* **C** *che renda commutativo il diagramma*



Si dice che U è un oggetto universale *di* **C** *per B e che u è la corrispondente* applicazione universale.

I due esempi già considerati sono evidentemente casi particolari di questa definizione. Eccone altri.

Esempi.

1. *Campo delle frazioni di un dominio commutativo.* Indichiamo con **Dom** la sottocategoria di **Ring** i cui oggetti sono i domini commutativi (anelli commutativi privi di divisori dello zero diversi da zero) e i cui morfismi sono i monomorfismi. È evidente che si ottiene così una sottocategoria di **Ring**. Inoltre **Dom** contiene la sottocategoria piena **Field**, i cui oggetti sono i campi e i cui morfismi sono i monomorfismi. Se D è un dominio commutativo, esso ammette un campo delle frazioni F (BAI, p. 115). La proprietà importante di F è la seguente. Abbiamo il monomorfismo $u\colon a \mapsto a/1$ di D in F e, per ogni monomorfismo g di D in un campo F', esiste un unico monomorfismo $\widetilde{g}$ di F in F' tale che $g = \widetilde{g}u$. Possiamo identificare D con l'insieme delle frazioni $d/1$, prendendo così per u l'inclusione. Il risultato appena enunciato significa allora che ogni monomorfismo di D ($\subset F$) in F' si estende in modo unico a un monomorfismo di F in F' (BAI, teorema 2.9, p. 117).

Per ricondurre questo risultato alla definizione di universale, consideriamo il funtore inclusione della sottocategoria **Field** nella categoria **Dom** (esempio 1 del § 1.3, p. 20 dell'originale). Se D è un dominio commutativo, dunque un oggetto di **Dom**, prendiamo come oggetto universale per D in **Field** il campo F delle frazioni di D e come applicazione universale u l'inclusione di

D in F. Allora (F, u) è un universale da D al funtore inclusione nel senso della definizione 1.6.

2. *Moduli liberi.* Siano R un anello e X un insieme non vuoto. Definiamo il *R-modulo (sinistro) libero* $\bigoplus_X R$ come la somma diretta di una famiglia di copie di R indicizzata da X, ossia $\bigoplus_X R = \bigoplus_{a\in X} M_a$, con $M_a = R$ per ogni a. Dunque $\bigoplus_X R$ è l'insieme delle applicazioni f di X in R tali che $f(x) = 0$ per tutti gli x, salvo un numero finito. L'addizione e l'azione di R sono quelle consuete:

$$(f + g)(x) = f(x) + g(x), \qquad (rf)(x) = rf(x).$$

Abbiamo l'applicazione $u\colon x \mapsto \bar{x}$ di X in $\bigoplus_X R$, dove $\bar{x}$ è definita da

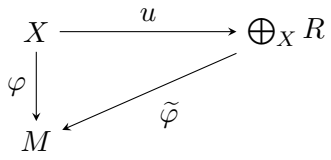
$$\bar{x}(x) = 1, \qquad \bar{x}(y) = 0 \quad \text{se } y \neq x.$$

Se $f \in \bigoplus_X R$ e $\{x_1, \ldots, x_n\}$ è un sottoinsieme di X tale che $f(y) = 0$ per $y \notin \{x_1, \ldots, x_n\}$, allora $f = \sum r_i \bar{x}_i$, dove $r_i = f(x_i)$. Inoltre, se gli $\bar{x}_i$ sono distinti, è chiaro che $\sum r_i \bar{x}_i = 0$ implica $r_i = 0$ per ogni i. Pertanto l'insieme $\bar{X} = \{\bar{x} \mid x \in X\}$ è una base di $\bigoplus_X R$, nel senso che ogni elemento del modulo è una somma $\sum_{x\in X} r_x \bar{x}$, finita nel senso che soltanto un numero finito dei coefficienti r_x è diverso da zero, e che per una somma di questo tipo $\sum r_x \bar{x} = 0$ implica $r_x = 0$ per ogni x.

Sia ora M un R-modulo (sinistro) qualsiasi e sia $\varphi\colon x \mapsto m_x$ un'applicazione di X in M. Allora

$$\widetilde{\varphi}\colon \sum r_x \bar{x} \longmapsto \sum r_x m_x$$

è un'applicazione ben definita di $\bigoplus_X R$ in M. È chiaro che si tratta di un omomorfismo di moduli. Inoltre $\widetilde{\varphi}(\bar{x}) = m_x$, sicché il diagramma



è commutativo. Poiché un omomorfismo di moduli è determinato dalla sua restrizione a un insieme di generatori, $\widetilde{\varphi}$ è evidentemente l'unico omomorfismo del modulo libero $\bigoplus_X R$ in M che renda commutativo il diagramma.

Consideriamo ora il funtore dimenticante F da R-**mod** a **Set** che a un R-modulo associa l'insieme sottostante e a ogni omomorfismo di moduli la corrispondente applicazione fra insiemi. Se X è un insieme non vuoto, i risultati precedenti significano che $(\bigoplus_X R, u)$ è un universale da X al funtore F.

3. *Algebre libere e algebre di polinomi.* Se K è un anello commutativo, definiamo un'*algebra (associativa) su K* come una coppia costituita da un anello $(A, +, \cdot, 0, 1)$ e da un K-modulo A, tali che l'insieme sottostante e l'addizione siano gli stessi nell'anello e nel modulo (in altre parole, l'anello e il modulo hanno lo stesso gruppo additivo) e tali che

$$a(xy) = (ax)y = x(ay)$$

per $a \in K$, $x, y \in A$ (cfr. BAI, p. 407). L'algebra A si dice *commutativa* se la sua moltiplicazione è commutativa. Gli omomorfismi di K-algebre sono gli omomorfismi di K-moduli tali che $1 \mapsto 1$ e, se $x \mapsto x'$ e $y \mapsto y'$, allora $xy \mapsto x'y'$. Si hanno una categoria K-**alg** delle K-algebre e una categoria K-**comalg** delle K-algebre commutative. Nella prima, gli oggetti sono le K-algebre e i morfismi sono gli omomorfismi di K-algebre. La categoria K-**comalg** è la sottocategoria piena delle K-algebre commutative.

Abbiamo i funtori dimenticanti da K-**alg** e da K-**comalg** a **Set**. Se X è un insieme non vuoto, un universale da X al primo funtore dimenticante ha la forma $(K\{X\}, u)$, dove $K\{X\}$ è una K-algebra e u è un'applicazione di X in $K\{X\}$, tale che per ogni applicazione g di X in una K-algebra A esista un unico omomorfismo di K-algebre $\widetilde{g}$ di $K\{X\}$ in A con $\widetilde{g}u = g$ (come applicazioni fra insiemi). Se $(K\{X\}, u)$ esiste, $K\{X\}$ si chiama *K-algebra libera determinata da X*. In modo analogo possiamo sostituire K-**alg** con K-**comalg**. Un universale da X al funtore dimenticante a valori in **Set** si indica con $(K[X], u)$. Se $X = \{x_1, x_2, \dots, x_n\}$, sia $K[X_1, \dots, X_n]$ l'anello dei polinomi nelle indeterminate X_i con coefficienti in K. Se g è un'applicazione di X in una K-algebra commutativa A, esiste un unico omomorfismo di K-algebre di $K[X_1, \dots, X_n]$ in A tale che $X_i \mapsto g(x_i)$, $1 \leq i \leq n$ (BAI, p. 124). Dunque $K[X_1, \dots, X_n]$, insieme all'applicazione $x_i \mapsto X_i$, è un universale da X al funtore dimenticante da K-**comalg** a **Set**.

4. *Coprodotti.* Sia $\mathbf{C}$ una categoria. Abbiamo il funtore diagonale Δ da $\mathbf{C}$ a $\mathbf{C} \times \mathbf{C}$, che a un oggetto A di $\mathbf{C}$ associa l'oggetto (A, A) di $\mathbf{C} \times \mathbf{C}$ e a un morfismo $f\colon A \to B$ il morfismo $(f, f)\colon (A, A) \to (B, B)$. Un universale da (A_1, A_2) a Δ è una coppia (U, u) dove U è un oggetto di $\mathbf{C}$ e $u = (u_1, u_2)$, $u_i\colon A_i \to U$, tale che, se $C \in \operatorname{ob}\mathbf{C}$ e $g_i\colon A_i \to C$, esista un unico $\widetilde{g}\colon U \to C$ tale che $g_i = \widetilde{g}u_i$, $i = 1, 2$. Ciò equivale a dire che (U, u_1, u_2) è un coprodotto di A_1 e A_2 in $\mathbf{C}$. Si ha un'immediata generalizzazione ai coprodotti di famiglie indicizzate di oggetti di $\mathbf{C}$. Se l'insieme degli indici è $I = \{\alpha\}$, il coprodotto $\coprod_\alpha C_\alpha$ è un universale dalla famiglia (C_α) al funtore diagonale da $\mathbf{C}$ alla categoria prodotto $\mathbf{C}^I$, dove $\mathbf{C}^I$ è il prodotto di una famiglia di copie di $\mathbf{C}$ indicizzata da I (cfr. § 1.3, p. 21 dell'originale).

Spesso gli universali si possono costruire in più modi. È indifferente quale costruzione si scelga, come mostra la seguente proprietà forte di unicità.

Proposizione 1.6. *Se (U, u) e (U', u') sono universali da un oggetto B a un funtore F, esiste un unico isomorfismo $h\colon U \to U'$ tale che $u' = F(h)u$.*

Lasciamo la dimostrazione al lettore. Osserviamo che il risultato segue anche dall'esercizio 4 qui sotto, mostrando che (U, u) è l'oggetto iniziale di una certa categoria.

Come ci si può attendere, il concetto di universale da un oggetto a un funtore ha un duale. Lo dà la definizione seguente.

Definizione 1.7. *Siano $\mathbf{C}$ e $\mathbf{D}$ categorie, G un funtore da $\mathbf{D}$ a $\mathbf{C}$ e $A \in \operatorname{ob}\mathbf{C}$. Un* universale da G ad A *è una coppia (V, v), con $V \in \operatorname{ob}\mathbf{D}$ e $v \in \hom_{\mathbf{C}}(GV, A)$, tale che per ogni $B \in \operatorname{ob}\mathbf{D}$ e ogni $g \in \hom_{\mathbf{C}}(GB, A)$ esista un unico $\widetilde{g}\colon B \to V$ per cui $vG(\widetilde{g}) = g$.*

Per illustrare la definizione prendiamo $\mathbf{C} = R$-**mod**, $\mathbf{D} = \mathbf{Set}$, come nell'esempio 2. Se X è un insieme non vuoto, poniamo $GX = \bigoplus_X R$, il modulo libero determinato da X. Conviene identificare l'elemento $x \in X$ con il corrispondente elemento $\bar{x}$ di $\bigoplus_X R$, e d'ora in poi adotteremo questa convenzione. Allora $\bigoplus_X R$ contiene X e X è una base del modulo libero. La proprietà fondamentale di X è che ogni applicazione φ di X in un modulo M si estende in modo unico a un omomorfismo di $\bigoplus_X R$ in M. Per $X = \varnothing$ poniamo $\bigoplus_X R = 0$. Se X e Y sono insiemi e φ è un'applicazione di X in Y, allora φ ammette un unico prolungamento a un omomorfismo $\widetilde{\varphi}$ di $\bigoplus_X R$ in $\bigoplus_Y R$. Ponendo $G(X) = \bigoplus_X R$ e $G(\varphi) = \widetilde{\varphi}$ otteniamo un funtore G da **Set** a R-**mod**.

Sia ora M un R-modulo (sinistro) e sia FM l'insieme sottostante, cosicché $GFM = \bigoplus_{FM} R$. Sia v l'omomorfismo di GFM in M che estende l'applicazione identica su FM. Siano X un insieme e g un omomorfismo di $\bigoplus_X R$ in M. Poniamo $\widetilde{g} = g|_X$. Allora $G(\widetilde{g})$ è l'omomorfismo di $\bigoplus_X R$ in $\bigoplus_{FM} R$ tale che $G(\widetilde{g})(x) = g(x)$ per $x \in X$, e $vG(\widetilde{g})(x) = g(x)$. Dunque $vG(\widetilde{g}) = g$. Inoltre $\widetilde{g}$ è l'unica applicazione di X in FM che soddisfi questa condizione. Ne segue che (FM, v) è un universale dal funtore G al modulo M.

Esercizi

1. Siano $\mathbf{D}$ una categoria e Δ il funtore diagonale da $\mathbf{D}$ a $\mathbf{D} \times \mathbf{D}$. Dimostrare che (V, v), con $v = (v_1, v_2)$, è un universale da Δ ad (A_1, A_2) se e solo se (V, v_1, v_2) è un prodotto di A_1 e A_2 in $\mathbf{D}$.

2. Siano **Rng** la categoria degli anelli senza unità e F il funtore da **Ring** a **Rng** che dimentica l'unità. Dimostrare che per ogni oggetto di **Rng** esiste un universale da tale oggetto a F. (Si veda BAI, p. 155.)

3. Siano F_1 un funtore da $\mathbf{C}_1$ a $\mathbf{C}_2$ e F_2 un funtore da $\mathbf{C}_2$ a $\mathbf{C}_3$. Siano (U_2, u_2) un universale da B a F_2 e (U_1, u_1) un universale da U_2 a F_1. Dimostrare che $(U_1, F_2(u_1)u_2)$ è un universale da B a F_2F_1.

4. Siano F un funtore da $\mathbf{C}$ a $\mathbf{D}$ e B un oggetto di $\mathbf{D}$. Verificare che i dati seguenti definiscono una categoria $\mathbf{D}(B, F)$. Gli oggetti sono le coppie (A, g), dove $A \in \operatorname{ob}\mathbf{C}$ e $g \in \hom_{\mathbf{D}}(B, FA)$. Si definisca $\hom((A, g), (A', g'))$ come il sottoinsieme di $\hom_{\mathbf{C}}(A, A')$ formato dagli h tali che $g' = F(h)g$, avendo cura di rendere disgiunti questi insiemi di morfismi. Si definisca la moltiplicazione dei morfismi come in $\mathbf{C}$ e si ponga $1_{(A,g)} = 1_A$. Dimostrare che (U, u) è un universale da B a F se e solo se (U, u) è un oggetto iniziale di $\mathbf{D}(B, F)$. Dare l'enunciato duale.

1.8 Funtori aggiunti

Esaminiamo ora la situazione in cui è dato un funtore F da $\mathbf{C}$ a $\mathbf{D}$ tale che, per ogni oggetto B di $\mathbf{D}$, esista un universale (U, u) da B a F. Tutti gli esempi del paragrafo precedente sono di questo tipo. Occorre dapprima considerare alcune definizioni equivalenti degli universali.

Siano F un funtore da $\mathbf{C}$ a $\mathbf{D}$, B un oggetto di $\mathbf{D}$ e (U, u) una coppia con $U \in \operatorname{ob}\mathbf{C}$ e $u \in \hom_{\mathbf{D}}(B, FU)$. Se $f \in \hom_{\mathbf{C}}(U, A)$, allora $F(f) \in \hom_{\mathbf{D}}(FU, FA)$ e $F(f)u \in \hom_{\mathbf{D}}(B, FA)$. Abbiamo dunque l'applicazione

$$\eta_A \colon f \longmapsto F(f)u \tag{23}$$

dell'insieme $\hom_{\mathbf{C}}(U, A)$ nell'insieme $\hom_{\mathbf{D}}(B, FA)$. Per definizione, (U, u) è un universale da B a F se per ogni oggetto A di $\mathbf{C}$ e ogni morfismo $g \colon B \to FA$ in $\mathbf{D}$ vi è uno e un solo $\widetilde{g} \colon U \to A$ tale che $g = F(\widetilde{g})u$. Ciò significa precisamente che (U, u) è un universale da B a F se e solo se, per ogni $A \in \operatorname{ob}\mathbf{C}$, l'applicazione η_A da $\hom_{\mathbf{C}}(U, A)$ a $\hom_{\mathbf{D}}(B, FA)$ definita in (23) è biiettiva. Se ciò accade e $h \colon A \to A'$ in $\mathbf{C}$, il diagramma

$$\begin{array}{ccc} \hom_{\mathbf{C}}(U, A) & \xrightarrow{\eta_A} & \hom_{\mathbf{D}}(B, FA) \\ \Big\downarrow{\scriptstyle \hom_{\mathbf{C}}(U, h)} & & \Big\downarrow{\scriptstyle \hom_{\mathbf{D}}(B, F(h))} \\ \hom_{\mathbf{C}}(U, A') & \xrightarrow[\eta_{A'}]{} & \hom_{\mathbf{D}}(B, FA') \end{array}$$

è commutativo. Infatti, partendo da un $f \in \hom_{\mathbf{C}}(U, A)$, uno dei due cammini dà $F(hf)u$ e l'altro $F(h)F(f)u$, che sono uguali perché $F(hf) = F(h)F(f)$. Ne segue che $\eta \colon A \mapsto \eta_A$ è un isomorfismo naturale dal funtore $\hom_{\mathbf{C}}(U, -)$ al funtore $\hom_{\mathbf{D}}(B, F-)$, ottenuto componendo F con $\hom_{\mathbf{D}}(B, -)$. Si osservi che entrambi sono funtori da $\mathbf{C}$ a **Set**. Poiché $\eta_U(1_U) = F(1_U)u = 1_{FU}u = u$, concludiamo che $\hom_{\mathbf{D}}(B, F-)$ è rappresentabile e ha (U, u) come rappresentante.

Viceversa, supponiamo che $\hom_{\mathbf{D}}(B, F-)$ sia rappresentabile con rappresentante (U, u). Per il lemma di Yoneda, per ogni oggetto A di $\mathbf{C}$ l'applicazione η_A di (23) è una biiezione di $\hom_{\mathbf{C}}(U, A)$ su $\hom_{\mathbf{D}}(B, FA)$. Quindi (U, u) è un universale da B a F.

Considerazioni analoghe si applicano all'altro tipo di universale. Siano G un funtore da $\mathbf{D}$ a $\mathbf{C}$, A un oggetto di $\mathbf{C}$ e (V, v) una coppia tale che $V \in \operatorname{ob}\mathbf{D}$ e $v \in \hom_{\mathbf{C}}(GV, A)$. Per ogni $B \in \operatorname{ob}\mathbf{D}$ abbiamo l'applicazione

$$\zeta_B \colon g \longmapsto vG(g) \tag{24}$$

di $\hom_{\mathbf{D}}(B, V)$ in $\hom_{\mathbf{C}}(GB, A)$, e (V, v) è un universale da G ad A se e solo se ζ_B è biiettiva per ogni $B \in \operatorname{ob}\mathbf{D}$. Ciò accade a sua volta se e solo se $\zeta \colon B \mapsto \zeta_B$ è un isomorfismo naturale del funtore controvariante $\hom_{\mathbf{D}}(-, V)$ sul funtore controvariante $\hom_{\mathbf{C}}(G-, A)$, ottenuto componendo G con $\hom_{\mathbf{C}}(-, A)$.

Supponiamo ora che per ogni $B \in \operatorname{ob}\mathbf{D}$ esista un universale da B al funtore F da $\mathbf{C}$ a $\mathbf{D}$. Per ogni B scegliamo un universale, che indichiamo con (GB, u_B). Per ogni $A \in \operatorname{ob}\mathbf{C}$ abbiamo allora l'applicazione biiettiva

$$\eta_{B,A} \colon f \longmapsto F(f)u_B \tag{25}$$

di $\hom_{\mathbf{C}}(GB, A)$ su $\hom_{\mathbf{D}}(B, FA)$. Fissato B, $A \mapsto \eta_{B,A}$ è un isomorfismo naturale dal funtore $\hom_{\mathbf{C}}(GB, -)$ al funtore $\hom_{\mathbf{D}}(B, F-)$.

Sia B' un secondo oggetto di $\mathbf{D}$ e sia $h \colon B \to B'$. Abbiamo il diagramma

$$\begin{array}{ccc} B & \xrightarrow{\;h\;} & B' \\ {\scriptstyle u_B}\downarrow & & \downarrow{\scriptstyle u_{B'}} \\ FGB & & FGB' \end{array}$$

e dunque $u_{B'}h \in \hom_{\mathbf{D}}(B, FGB')$. Poiché (GB, u_B) è un universale da B a F, esiste un unico morfismo $G(h) \colon GB \to GB'$ tale che il diagramma diventi commutativo inserendovi la freccia orizzontale $FG(h)$, ossia

$$FG(h)u_B = u_{B'}h. \tag{26}$$

La commutatività del diagramma

$$\begin{array}{ccccc} B & \xrightarrow{\;h\;} & B' & \xrightarrow{\;k\;} & B'' \\ {\scriptstyle u_B}\downarrow & & {\scriptstyle u_{B'}}\downarrow & & \downarrow{\scriptstyle u_{B''}} \\ FGB & \xrightarrow[FG(h)]{} & FGB' & \xrightarrow[FG(k)]{} & FGB'' \end{array}$$

e la proprietà funtoriale $(FG(k))(FG(h)) = F(G(k)G(h))$ implicano che anche

$$\begin{array}{ccc} B & \xrightarrow{\;kh\;} & B'' \\ {\scriptstyle u_B}\downarrow & & \downarrow{\scriptstyle u_{B''}} \\ FGB & \xrightarrow[F(G(k)G(h))]{} & FGB'' \end{array}$$

è commutativo. Poiché $G(kh)$ è l'unico morfismo da GB a GB'' tale che $FG(kh)u_B = u_{B''}kh$, segue che $G(kh) = G(k)G(h)$. Analogamente si ha $G(1_B) = 1_{GB}$. Dunque G è un funtore da $\mathbf{D}$ a $\mathbf{C}$.

Vogliamo studiare le relazioni fra i due funtori F e G. Sia $A \in \operatorname{ob}\mathbf{C}$. Allora $FA \in \operatorname{ob}\mathbf{D}$. Applicando la definizione di universale da FA a F al morfismo $g = 1_{FA}$, otteniamo un unico $v_A\colon GFA \to A$ tale che

$$F(v_A)u_{FA} = 1_{FA}. \tag{27}$$

Per ogni $B \in \operatorname{ob}\mathbf{D}$ abbiamo allora l'applicazione

$$\zeta_{A,B}\colon g \longmapsto v_A G(g) \tag{28}$$

di $\hom_{\mathbf{D}}(B, FA)$ in $\hom_{\mathbf{C}}(GB, A)$. Sia ora $g \in \hom_{\mathbf{D}}(B, FA)$. Per (26) e (27),

$$\eta_{B,A}\zeta_{A,B}(g) = F(v_A G(g))u_B = F(v_A)(FG(g))u_B = F(v_A)u_{FA}g = g.$$

Poiché $\eta_{B,A}$ è biiettiva, segue che $\zeta_{A,B} = \eta_{B,A}^{-1}$, ed è quindi una biiezione di $\hom_{\mathbf{D}}(B, FA)$ su $\hom_{\mathbf{C}}(GB, A)$.

Il fatto che per ogni $B \in \operatorname{ob}\mathbf{D}$ l'applicazione $\zeta_{A,B}\colon g \mapsto v_A G(g)$ sia una biiezione di $\hom_{\mathbf{D}}(B, FA)$ su $\hom_{\mathbf{C}}(GB, A)$ implica che (FA, v_A) è un universale da G ad A, e questo vale per ogni $A \in \operatorname{ob}\mathbf{C}$. Inoltre, fissato A, $B \mapsto \zeta_{A,B}$ è un isomorfismo naturale dal funtore controvariante $\hom_{\mathbf{D}}(-, FA)$ al funtore controvariante $\hom_{\mathbf{C}}(G-, A)$. Di conseguenza $B \mapsto \eta_{B,A} = \zeta_{A,B}^{-1}$ è un isomorfismo naturale da $\hom_{\mathbf{C}}(G-, A)$ a $\hom_{\mathbf{D}}(-, FA)$.

Riassumiamo i risultati ottenuti finora.

Proposizione 1.7. *Sia F un funtore da $\mathbf{C}$ a $\mathbf{D}$ tale che per ogni $B \in \operatorname{ob}\mathbf{D}$ esista un universale da B a F. Per ogni B se ne scelga uno e lo si indichi con (GB, u_B). Se $h\colon B \to B'$ in $\mathbf{D}$, si definisca $G(h)\colon GB \to GB'$ come l'unico elemento di $\hom_{\mathbf{C}}(GB, GB')$ tale che $F(G(h))u_B = u_{B'}h$. Allora G è un funtore da $\mathbf{D}$ a $\mathbf{C}$. Se $A \in \operatorname{ob}\mathbf{C}$, esiste un unico $v_A\colon GFA \to A$ tale che $F(v_A)u_{FA} = 1_{FA}$. Allora (FA, v_A) è un universale da G ad A. Se $\eta_{B,A}$ è l'applicazione $f \mapsto F(f)u_B$ di $\hom_{\mathbf{C}}(GB, A)$ in $\hom_{\mathbf{D}}(B, FA)$, per B fissato $A \mapsto \eta_{B,A}$ è un isomorfismo naturale da $\hom_{\mathbf{C}}(GB, -)$ a $\hom_{\mathbf{D}}(B, F-)$, e per A fissato $B \mapsto \eta_{B,A}$ è un isomorfismo naturale da $\hom_{\mathbf{C}}(G-, A)$ a $\hom_{\mathbf{D}}(-, FA)$.*

L'ultima affermazione di questa proposizione si può formulare in termini dell'importante concetto di funtori aggiunti, dovuto a D. M. Kan.

Definizione 1.8. *Siano F un funtore da $\mathbf{C}$ a $\mathbf{D}$ e G un funtore da $\mathbf{D}$ a $\mathbf{C}$. Si dice che F è un* aggiunto destro *di G e che G è un* aggiunto sinistro *di F se per ogni coppia (B, A), con $B \in \operatorname{ob}\mathbf{D}$ e $A \in \operatorname{ob}\mathbf{C}$, si ha una biiezione $\eta_{B,A}$ di $\hom_{\mathbf{C}}(GB, A)$ su $\hom_{\mathbf{D}}(B, FA)$, naturale in A e in B nel senso seguente. Per ogni B, $A \mapsto \eta_{B,A}$ è un isomorfismo naturale da $\hom_{\mathbf{C}}(GB, -)$ a $\hom_{\mathbf{D}}(B, F-)$ e, per ogni A, $B \mapsto \eta_{B,A}$ è un isomorfismo naturale da $\hom_{\mathbf{C}}(G-, A)$ a $\hom_{\mathbf{D}}(-, FA)$. Si chiama $\eta\colon (B, A) \mapsto \eta_{B,A}$ un* isomorfismo di aggiunzione *da G a F, e la terna (F, G, η) un'*aggiunzione.

L'ultima affermazione della proposizione 1.7 implica evidentemente che (F, G, η) è un'aggiunzione. Mostreremo che, viceversa, ogni aggiunzione (F, G, η) determina degli universali, dai quali si può riottenere l'aggiunzione come nella proposizione 1.7.

Supponiamo dunque che (F, G, η) sia un'aggiunzione. Sia $B \in \operatorname{ob}\mathbf{D}$ e poniamo $u_B = \eta_{B,GB}(1_{GB}) \in \hom_{\mathbf{D}}(B, FGB)$. Tenendo fisso B, abbiamo l'isomorfismo naturale $A \mapsto \eta_{B,A}$ da $\hom_{\mathbf{C}}(GB, -)$ a $\hom_{\mathbf{D}}(B, F-)$. Per il lemma di Yoneda, se $f \in \hom_{\mathbf{C}}(GB, A)$, allora

$$\eta_{B,A}(f) = \hom_{\mathbf{D}}(B, F(f))u_B = F(f)u_B.$$

Pertanto $f \mapsto F(f)u_B$ è una biiezione di $\hom_{\mathbf{C}}(GB, A)$ su $\hom_{\mathbf{D}}(B, FA)$. Il fatto che ciò valga per ogni $A \in \operatorname{ob}\mathbf{C}$ implica che (GB, u_B) è un universale da B a F.

Siano $k \in \hom_{\mathbf{C}}(A, A')$, $f \in \hom_{\mathbf{C}}(GB, A)$, $g \in \hom_{\mathbf{C}}(GB', A)$ e $h \in \hom_{\mathbf{D}}(B, B')$. L'isomorfismo naturale $A \mapsto \eta_{B,A}$ da $\hom_{\mathbf{C}}(GB, -)$ a $\hom_{\mathbf{D}}(B, F-)$ dà la relazione

$$\eta_{B,A'}(kf) = F(k)\eta_{B,A}(f), \tag{29}$$

mentre l'isomorfismo naturale $B \mapsto \eta_{B,A}$ da $\hom_{\mathbf{C}}(G-, A)$ a $\hom_{\mathbf{D}}(-, FA)$ dà

$$\eta_{B,A}(gG(h)) = \eta_{B',A}(g)h. \tag{30}$$

(Si disegnino i diagrammi.) Da queste relazioni segue che

$$\begin{aligned} F(G(h))u_B &= F(G(h))\eta_{B,GB}(1_{GB}) \\ &= \eta_{B,GB'}(G(h)1_{GB}), \end{aligned}$$

per (29), con $A = GB$, $A' = GB'$, $k = G(h)$, $f = 1_{GB}$. Proseguendo, si ottiene

$$\eta_{B,GB'}(1_{GB'}G(h)) = \eta_{B',GB'}(1_{GB'})h = u_{B'}h$$

per (30), con $A = GB'$, $g = 1_{GB'}$. La relazione $F(G(h))u_B = u_{B'}h$, che coincide con (26), mostra che il funtore G dato è proprio quello determinato dalla scelta dell'universale (GB, u_B) per ogni $B \in \operatorname{ob}\mathbf{D}$. Siamo così tornati alla situazione da cui eravamo partiti.

Una conseguenza immediata del legame fra aggiunti e universali è la seguente.

Proposizione 1.8. *Due aggiunti sinistri G e G' di uno stesso funtore F da $\mathbf{C}$ a $\mathbf{D}$ sono naturalmente isomorfi.*

Dimostrazione. Siano η e η' gli isomorfismi di aggiunzione rispettivamente da G e da G' a F. Per $B \in \operatorname{ob}\mathbf{D}$, le coppie (GB, u_B) e $(G'B, u'_B)$, dove u_B e u'_B sono determinati come sopra, sono universali da B a F. Esiste dunque un unico isomorfismo $\lambda_B \colon GB \to G'B$ tale che $u'_B = F(\lambda_B)u_B$ (proposizione 1.6).[3] Per concludere che $\lambda \colon B \mapsto \lambda_B$ è un isomorfismo naturale da G a G' basta mostrare che, per ogni $h \colon B \to B'$, il diagramma

$$\begin{array}{ccc} GB & \xrightarrow{\lambda_B} & G'B \\ {\scriptstyle G(h)}\downarrow & & \downarrow{\scriptstyle G'(h)} \\ GB' & \xrightarrow[\lambda_{B'}]{} & G'B' \end{array}$$

è commutativo. Applichiamo a tal fine $\eta_{B,G'B'}$ a $G'(h)\lambda_B$ e a $\lambda_{B'}G(h)$. Otteniamo, usando in entrambi i casi la (26),

$$\begin{aligned} F(G'(h))F(\lambda_B)u_B &= F(G'(h))u'_B = u'_{B'}h, \\ F(\lambda_{B'})F(G(h))u_B &= F(\lambda_{B'})u_{B'}h = u'_{B'}h. \end{aligned}$$

Poiché $\eta_{B,G'B'}$ è un isomorfismo, segue che $G'(h)\lambda_B = \lambda_{B'}G(h)$, e il diagramma è quindi commutativo.

Tutto quanto precede si può dualizzare per gli universali da un funtore a un oggetto. Lasciamo al lettore la verifica.

Esercizi

[3] L'edizione inglese rinvia qui alla proposizione 1.5. Nello stesso argomento si legge $\eta_{B,GB'}$: il secondo indice è $G'B'$, codominio dei due morfismi cui si applica η. [N.d.T.]

1. Determinare gli aggiunti sinistri dei funtori definiti negli esempi del § 1.7 (pp. 42–44 dell'originale).

2. Sia (F, G, η) un'aggiunzione. Si ponga $u_B = \eta_{B,GB}(1_{GB}) \in \hom_{\mathbf{D}}(B, FGB)$. Verificare che $u\colon B \mapsto u_B$ è una trasformazione naturale da $1_{\mathbf{D}}$ a FG. Si chiama u l'*unità* dell'isomorfismo di aggiunzione η. Analogamente, $v\colon A \mapsto v_A = \eta^{-1}_{FA,A}(1_{FA})$ è una trasformazione naturale da GF a $1_{\mathbf{C}}$, detta *counità* di η.

3. Sia data un'aggiunzione per i funtori $F_1\colon \mathbf{C}_1 \to \mathbf{C}_2$, $G_1\colon \mathbf{C}_2 \to \mathbf{C}_1$, con isomorfismo di aggiunzione η_1, e un'aggiunzione per $F_2\colon \mathbf{C}_2 \to \mathbf{C}_3$, $G_2\colon \mathbf{C}_3 \to \mathbf{C}_2$, con isomorfismo di aggiunzione η_2. Dimostrare che G_1G_2 è un aggiunto sinistro di F_2F_1 e determinare l'isomorfismo di aggiunzione.

4. Sia data un'aggiunzione fra G e F, con isomorfismo di aggiunzione η. Dimostrare che $F\colon \mathbf{C} \to \mathbf{D}$ conserva i prodotti, ossia che, se $A = \prod A_\alpha$ con applicazioni $p_\alpha\colon A \to A_\alpha$, allora $FA = \prod FA_\alpha$ con applicazioni $F(p_\alpha)$. Dare l'enunciato duale.

Riferimenti bibliografici

S. Eilenberg e S. MacLane, General theory of natural equivalences, *Trans. Amer. Math. Soc.*, vol. 58 (1945), 231–294.

S. MacLane, *Categories for the Working Mathematician*, New York, Springer, 1971.

2 Algebra universale

L'idea di un'algebra «universale», intesa come studio comparato delle strutture algebriche, sembra risalire al filosofo e matematico Alfred North Whitehead. Nel suo libro *A Treatise on Universal Algebra with Applications*, apparso nel 1898, Whitehead indicava come particolarmente meritevoli di uno studio comparato «i quaternioni di Hamilton, il calcolo delle estensioni di Grassmann e la logica simbolica di Boole». Forse i tempi non erano ancora maturi per un'indagine del genere. Sta di fatto che i primi risultati significativi di algebra universale giunsero parecchio più tardi, negli anni Trenta e Quaranta, con i lavori di G. Birkhoff, di Tarski, di Jónsson e Tarski e di altri.

La nozione fondamentale di cui ci occuperemo è quella di «Ω-algebra»: in prima approssimazione, un insieme non vuoto dotato di un insieme di operazioni finitarie. A questa nozione si accompagna un'opportuna nozione di omomorfismo. Adotteremo il seguente punto di vista. È dato a priori un insieme Ω di simboli di operazione (per esempio $+$, $\cdot$, $\wedge$) ed è data una classe di insiemi non vuoti, i *sostegni*, sui quali tali simboli si realizzano come operazioni. Un medesimo simbolo ω si realizza su ogni sostegno con la stessa «arità»: determina sempre un'operazione binaria, oppure sempre un'operazione ternaria, e così via. Fissato Ω, le Ω-algebre costituiscono una categoria i cui morfismi sono gli omomorfismi di Ω-algebre. Le idee della teoria delle categorie avranno una parte importante nella nostra esposizione.

La nozione di Ω-algebra si può ampliare fino a includere, accanto alle operazioni, anche le relazioni. Si ottiene così la nozione fondamentale di struttura relazionale, mediante la quale la logica matematica trova applicazione all'algebra. Qui non considereremo questa nozione più generale.

Svilupperemo dapprima alcuni risultati generali sugli omomorfismi e sugli isomorfismi di Ω-algebre che il lettore ha già incontrato in casi particolari. Introdurremo poi il prodotto sottodiretto di algebre e alcune importanti costruzioni: i limiti diretti, i limiti inversi e gli ultraprodotti di Ω-algebre. Ci interesseremo in particolare delle varietà (o classi equazionali) di Ω-algebre, delle algebre libere e dei prodotti liberi in una varietà. Dimostreremo un importante teorema di G. Birkhoff che dà una caratterizzazione interna delle varietà. Tratteremo più in dettaglio il caso particolarmente importante dei prodotti liberi di gruppi e dei gruppi liberi.

2.1 Ω-algebre

Richiamiamo brevemente alcune nozioni insiemistiche di cui ci serviremo nello studio delle algebre generali (o universali).

Dati due insiemi A e B, si chiama *corrispondenza da A a B* un qualunque sottoinsieme di $A \times B$. Un'applicazione $f\colon A \to B$ è una corrispondenza tale che per ogni $a \in A$ esiste un $b \in B$ per cui $(a, b) \in f$ e, se (a, b) e (a, b') appartengono a f, allora $b = b'$. L'unico b tale che $(a, b) \in f$ si indica con $f(a)$. Si passa così dalla notazione delle corrispondenze a quella usuale delle funzioni o applicazioni. Se Φ è una corrispondenza da A a B, la *corrispondenza inversa* Φ^{-1}, da B ad A, è l'insieme delle coppie (b, a) tali che $(a, b) \in \Phi$. Se Φ è una corrispondenza da A a B e Ψ una corrispondenza da B a C, si indica con $\Psi\Phi$ la corrispondenza da A a C formata dalle coppie (a, c), con $a \in A$ e $c \in C$, per le quali esiste un $b \in B$ tale che $(a, b) \in \Phi$ e $(b, c) \in \Psi$. Nel caso di due applicazioni f da A a B e g da B a C, il prodotto gf delle corrispondenze è l'usuale composizione di f seguita da g: $(gf)(a) = g(f(a))$. Come di consueto, indichiamo con 1_A l'applicazione identica su A. È la corrispondenza da A ad A costituita dalle coppie (a, a) con $a \in A$ e prende anche il nome di *diagonale* di A. Se Φ, Ψ, Θ sono corrispondenze, rispettivamente

da A a B, da B a C e da C a D, si verificano facilmente le seguenti relazioni insiemistiche:

$$(\Theta\Psi)\Phi = \Theta(\Psi\Phi), \tag{1}$$

$$(\Psi\Phi)^{-1} = \Phi^{-1}\Psi^{-1}, \tag{2}$$

$$(\Phi^{-1})^{-1} = \Phi, \tag{3}$$

$$\Phi 1_A = \Phi = 1_B\Phi. \tag{4}$$

Indichiamo con B^A l'insieme delle applicazioni da A a B. Se $A = \{1, 2, \ldots, n\}$, scriviamo $B^{(n)}$ per B^A e ne chiamiamo gli elementi *n-uple* (o successioni di n elementi) di B. Identifichiamo $B^{(1)}$ con B. Una *relazione n-aria* su A è un sottoinsieme R di $A^{(n)}$. Una relazione binaria ($n = 2$) su A è dunque una corrispondenza da A ad A. Invece di $(a, b) \in R$ si scrive anche aRb e si dice allora che a è in relazione R con b.

Una *relazione di equivalenza* E su A è una relazione binaria riflessiva (aEa per ogni $a \in A$), simmetrica (se aEb, allora bEa) e transitiva (se aEb e bEc, allora aEc). Queste condizioni si esprimono più concisamente così:

$$\begin{aligned} 1_A &\subset E \quad && \text{(riflessività)},\\ E &= E^{-1} && \text{(simmetria)},\\ EE &\subset E && \text{(transitività)}. \end{aligned}$$

Indichiamo con $\bar{a}_E$, o semplicemente con $\bar{a}$ se E è chiara dal contesto, l'elemento dell'insieme delle parti $\mathcal{P}(A)$ costituito dai b tali che bEa. L'insieme di queste classi $\bar{a}$ forma una partizione di A, chiamata *insieme quoziente* A/E di A rispetto a E (si veda, per esempio, BAI, p. 11). Per partizione di A intendiamo un insieme di sottoinsiemi non vuoti di A dei quali A è l'unione disgiunta: la loro unione è A e l'intersezione di due sottoinsiemi distinti è vuota. Le partizioni di A e le relazioni di equivalenza su A si corrispondono biunivocamente (BAI, pp. 11–12).

Un'altra relazione importante su un insieme A è un *ordine parziale* $\geq$. Le proprietà che lo definiscono sono la riflessività ($a \geq a$), l'antisimmetria (se $a \geq b$ e $b \geq a$, allora $a = b$) e la transitività (se $a \geq b$ e $b \geq c$, allora $a \geq c$). Se O è il sottoinsieme di $A \times A$ formato dalle coppie (a, b) tali che $a \geq b$, queste condizioni diventano, nell'ordine,

$$O \supset 1_A, \qquad O \cap O^{-1} \subset 1_A, \qquad OO \subset O.$$

Per n intero positivo, chiamiamo *prodotto n-ario* su A un'applicazione da $A^{(n)}$ ad A. I prodotti n-ari sono dunque gli elementi dell'insieme $A^{A^{(n)}}$. Per $n = 1, 2, 3, \ldots$ si hanno prodotti unari, binari, ternari e così via. Conviene introdurre anche i *prodotti nullari*, che sono semplicemente elementi distinti assegnati in A (per esempio lo zero di un anello). Estendiamo la notazione ponendo $A^{A^{(0)}} = A$, l'insieme dei prodotti nullari su A. Abbiamo così prodotti n-ari per ogni $n \in \mathbb{N} = \{0, 1, 2, 3, \ldots\}$. Se $n \geq 1$ e $\omega \in A^{A^{(n)}}$, cosicché ω è un'applicazione $(a_1, \ldots, a_n) \mapsto \omega(a_1, \ldots, a_n) \in A$, l'insieme degli elementi

$$(a_1, \ldots, a_n, \omega(a_1, \ldots, a_n))$$

è un sottoinsieme di $A^{(n+1)}$, ossia una relazione $(n + 1)$-aria su A. Poiché i prodotti nullari sono gli elementi di A, per ogni $n \in \mathbb{N}$ la nozione di relazione $(n + 1)$-aria comprende quella di prodotto n-ario.

Possiamo ora definire un'algebra «generale» o Ω-algebra. Informalmente, è un insieme non vuoto A munito di un insieme Ω di prodotti n-ari, $n = 0, 1, 2, \ldots$. Per confrontare algebre diverse, e più precisamente per definirne gli omomorfismi, conviene considerare Ω indipendentemente da A: ogni suo elemento deve determinare prodotti su insiemi diversi $A, B, \ldots$ in modo che, fissato

$\omega \in \Omega$, i prodotti che esso determina su $A, B, \ldots$ abbiano tutti la stessa arità, ossia siano n-ari per un medesimo n. Partiamo dunque da un insieme Ω e da una sua decomposizione in unione disgiunta di sottoinsiemi $\Omega(n)$, $n = 0, 1, 2, \ldots$. Gli elementi di $\Omega(n)$ si chiamano *simboli di prodotto* (o *di operatore*) *n-ari*. Fissati Ω e la decomposizione $\Omega = \bigcup_n \Omega(n)$, diamo la seguente definizione.

Definizione 2.1. *Una Ω-algebra è un insieme non vuoto A munito di un'applicazione di Ω nell'insieme dei prodotti su A, tale che a ogni $\omega \in \Omega(n)$ corrisponda un prodotto n-ario su A. L'insieme sottostante A si chiama sostegno dell'algebra. Di solito indicheremo l'algebra con lo stesso simbolo del suo sostegno.*

Se ω è nullario, ossia $\omega \in \Omega(0)$, il corrispondente elemento distinto di A si denota con ω_A o, quando non vi sia pericolo di confusione, con ω (si scrive per esempio 1 in ogni gruppo G, invece di 1_G). Se $n \geq 1$ e $\omega \in \Omega(n)$, il prodotto corrispondente su A è

$$(a_1, a_2, \ldots, a_n) \longmapsto \omega(a_1, a_2, \ldots, a_n), \qquad a_i \in A.$$

D'ora innanzi abbrevieremo il secondo membro in $\omega a_1 a_2 \cdots a_n$, sopprimendo parentesi e virgole. L'osservazione che ciò è possibile senza ambiguità, anche in presenza di più simboli di operatore, è dovuta a Łukasiewicz. Per esempio, se ω è quinario, φ ternario, ψ unario e λ nullario, allora

$$\varphi(a_1, a_2, \omega(a_3, \lambda, a_4, a_5, \psi(a_6)))$$

nella notazione di Łukasiewicz diventa $\varphi a_1 a_2 \omega a_3 \lambda a_4 a_5 \psi a_6$. Se si conoscono le arità di $\varphi, \omega, \lambda, \psi$, è facile vedere che l'elemento scritto sopra è l'unico significato che si possa attribuire a quest'ultima espressione. Il lettore faccia ancora qualche esperimento con questa notazione. Vi torneremo trattando le Ω-algebre libere. Osserviamo inoltre che due simboli distinti $\omega, \omega' \in \Omega(n)$ possono determinare su A lo stesso prodotto n-ario.

Esempi

1. Un monoide è una Ω-algebra con $\Omega = \{p, 1\}$, dove p è binario e 1 nullario, che soddisfa le identità (o leggi) $ppabc = papbc$ (associatività di p) e $pa1 = a = p1a$.

2. Un gruppo è una Ω-algebra con $\Omega = \{p, 1, i\}$, dove p è binario, 1 nullario e i unario. Agli assiomi di gruppo corrispondono le identità $ppabc = papbc$, $pa1 = a = p1a$, $paia = 1$, $piaa = 1$. Dunque ia è l'usuale a^{-1}. L'introduzione di questa operazione unaria è necessaria perché la teoria generale delle Ω-algebre, specializzata ai gruppi, restituisca in modo soddisfacente la teoria usuale.

3. Un anello è una Ω-algebra con $\Omega = \{s, p, 0, 1, -\}$, dove s e p sono binari, 0 e 1 nullari e $-$ unario. Qui s dà la somma, p il prodotto, 0 e 1 hanno il significato consueto e $-a$ è l'opposto di a. Lasciamo al lettore il compito di formulare le identità necessarie per completare la definizione di anello. Per esempio, una delle leggi distributive si scrive $pasbc = spabpac$.

4. *Gruppi con operatori.* Questa nozione permette di studiare un gruppo rispetto a un insieme assegnato di endomorfismi, per esempio gli automorfismi interni, tutti gli automorfismi o tutti gli endomorfismi. Dal punto di vista delle Ω-algebre prendiamo $\Omega = \Lambda \cup \{p, 1, i\}$, dove Λ è un insieme di simboli unari distinti da i, e $p, 1, i$ sono come nella definizione di gruppo. Oltre agli assiomi di gruppo su $p, 1, i$ richiediamo che per $\lambda \in \Lambda$ valga

$$\lambda pab = p\lambda a\lambda b, \tag{5}$$

ossia, nella notazione usuale,

$$(5') \qquad \lambda(ab) = (\lambda a)(\lambda b).$$

Quindi $a \mapsto \lambda a$ è un endomorfismo del gruppo. Questa algebra si chiama *gruppo con operatori* o Λ-*gruppo*. Ogni modulo M, sinistro o destro, su un anello R si può considerare come un gruppo abeliano avente R come insieme di operatori.

5. *Reticoli.* Qui Ω consta di due simboli di prodotto binario. Se L è il sostegno, indichiamo i risultati della loro applicazione ad $a, b \in L$ nel modo consueto con $a \vee b$ e $a \wedge b$, detti rispettivamente *supremo* e *infimo* di a e b. Gli assiomi del reticolo sono

$$\begin{aligned} a \vee b &= b \vee a, & a \wedge b &= b \wedge a, \\ (a \vee b) \vee c &= a \vee (b \vee c), & (a \wedge b) \wedge c &= a \wedge (b \wedge c), \\ a \vee a &= a, & a \wedge a &= a, \\ (a \vee b) \wedge a &= a, & (a \wedge b) \vee a &= a. \end{aligned}$$

Un altro modo di definire un reticolo è quello di considerarlo come un insieme parzialmente ordinato di un certo tipo. Si parte da un insieme L con un ordine parziale $\geq$. Per $S \subset L$, si dice *maggiorante* u (rispettivamente *minorante* l) di S un elemento di L tale che $u \geq s$ (rispettivamente $l \leq s$) per ogni $s \in S$. Un *estremo superiore*, o *sup*, di S è un maggiorante B tale che $B \leq u$ per ogni maggiorante u di S. Un *estremo inferiore*, o *inf*, di S è un minorante b tale che $b \geq l$ per ogni minorante l di S. Il sup e l'inf, quando esistono, sono unici, come risulta dalla definizione. Si può definire un reticolo come un insieme parzialmente ordinato in cui ogni coppia di elementi ammette un sup $a \vee b$ e un inf $a \wedge b$. È facile vedere che le due definizioni sono equivalenti. Si dimostra che sup e inf soddisfano le relazioni dell'esempio 5 e, viceversa, che in ogni reticolo algebrico si ottiene un ordine parziale ponendo $a \geq b$ se $a \wedge b = b$ (equivalentemente, se $a \vee b = a$). Gli elementi assegnati $a \vee b$ e $a \wedge b$ di L sono allora sup e inf per quest'ordine. I dettagli si verificano facilmente e sono esposti per esteso in BAI, pp. 459–460.

Un reticolo, considerato come insieme parzialmente ordinato, si dice *completo* se ogni suo sottoinsieme non vuoto ammette sup e inf. Allora $1 = \sup\{a \mid a \in L\}$ soddisfa $1 \geq a$ per ogni $a \in L$, e $0 = \inf\{a \mid a \in L\}$ soddisfa $0 \leq a$ per ogni a. Questi elementi si chiamano rispettivamente il *massimo* e il *minimo* del reticolo. Il seguente teorema è assai utile.

Teorema 2.1. *Un insieme parzialmente ordinato L è un reticolo completo se e soltanto se contiene un massimo* 1 *($1 \geq a$ per ogni a) e ogni suo sottoinsieme non vuoto ha un estremo inferiore.*

Per dimostrarlo si osserva che, se S è un sottoinsieme non vuoto di L, l'insieme U dei suoi maggioranti è non vuoto e il suo estremo inferiore è un estremo superiore di S (BAI, p. 458).

Gli esempi precedenti mostrano quanto la teoria delle Ω-algebre abbia a che fare con lo studio di numerose strutture algebriche importanti. Va osservato tuttavia che alcune strutture, per esempio i campi, non sono Ω-algebre, poiché una delle operazioni di un campo, l'inversione rispetto alla moltiplicazione, non è definita ovunque. Anche nella teoria dei moduli i risultati sulle Ω-algebre hanno applicazioni limitate: passando al punto di vista delle Ω-algebre si perde interamente di vista la struttura di anello dell'insieme degli operatori.

Esercizi

1. Siano Φ, Φ' corrispondenze da A a B e Ψ, Ψ' corrispondenze da B a C. Mostrare che, se $\Phi \subset \Phi'$ e $\Psi \subset \Psi'$, allora $\Psi\Phi \subset \Psi'\Phi'$.

2. Siano E, F relazioni di equivalenza su A. Mostrare che EF è una relazione di equivalenza se e soltanto se $EF = FE$.

3. Sia H un sottogruppo di un gruppo G e si ponga $a \equiv_H b$ se $b^{-1}a \in H$. Si ottiene una relazione di equivalenza. Mostrare che, dato un secondo sottogruppo K, le relazioni $\equiv_H$ e $\equiv_K$ commutano se e soltanto se $HK = KH$. Dedurne che, se $H \triangleleft G$ (H è normale in G), il prodotto delle relazioni $\equiv_H$ e $\equiv_K$ è una relazione di equivalenza.

4. Elencare tutte le partizioni di $\{1, 2, \ldots, n\}$ per $n = 1, 2, 3, 4$.

5. Sia $E(n)$ l'insieme delle relazioni di equivalenza su un insieme di n elementi, e sia $|E(n)|$ la sua cardinalità. Dimostrare la formula di ricorrenza

$$|E(n)| = |E(n-1)| + \tbinom{n-1}{1}|E(n-2)| + \tbinom{n-1}{2}|E(n-3)| + \cdots + \tbinom{n-1}{n-2}|E(1)| + 1.$$

6. Sia A una Ω-algebra e sia $\omega_j^{(i)}$ un simbolo di operatore i-ario. Scrivere con parentesi e virgole l'espressione

$$\omega_1^{(2)}\omega_2^{(3)}\omega_3^{(2)}\omega_4^{(0)}\omega_5^{(4)}a_1a_2a_3a_4a_5a_6\omega_6^{(3)}a_7a_8a_9.$$

2.2 Sottoalgebre e prodotti

Sia A una Ω-algebra arbitraria. Un sottoinsieme non vuoto B di A si dice *sottoalgebra* di A se, per ogni $\omega \in \Omega(n)$ e per ogni $(b_1, b_2, \ldots, b_n)$ con $b_i \in B$, si ha $\omega b_1 b_2 \cdots b_n \in B$. In particolare, se $n = 0$, B contiene l'elemento distinto ω_A associato a ω. Se, ad esempio, A è un gruppo, un sottoinsieme B è un sottogruppo se e solo se contiene bc, 1 e b^{-1} per ogni $b, c \in B$. Si ritrova così la consueta definizione di sottogruppo. Osserviamo che ciò non sarebbe accaduto se, nella definizione di un gruppo come Ω-algebra, avessimo omesso il simbolo di operazione unaria i. Se A è un Λ-gruppo, una sottoalgebra è un sottogruppo B tale che $\lambda b \in B$ per $b \in B$, $\lambda \in \Lambda$. Lo si chiama Λ-*sottogruppo* di A.

Se B è una sottoalgebra di A, si fa di B una Ω-algebra definendo l'azione di ogni $\omega \in \Omega$ mediante la restrizione a B della sua azione in A. È chiaro che, se B è una sottoalgebra di A e C è una sottoalgebra di B, allora C è una sottoalgebra di A. È chiaro altresì che, se $\{B_\alpha \mid \alpha \in I\}$ è un insieme di sottoalgebre, $\bigcap B_\alpha$ è una sottoalgebra oppure è vuoto. Conviene aggiungere $\varnothing$ all'insieme delle sottoalgebre di A. Se ordiniamo parzialmente per inclusione l'insieme così ottenuto, il teorema 2.1 ci permette di concludere che esso è un reticolo completo. La dimostrazione che abbiamo abbozzato mostra inoltre come si ricavi l'estremo superiore di un insieme assegnato $\{B_\alpha\}$ di sottoalgebre: si prende l'intersezione dell'insieme delle sottoalgebre C che contengono ogni B_α. In generale tale estremo superiore non è l'unione $\bigcup B_\alpha$ degli insiemi B_α, che ne è l'estremo superiore nell'insieme parzialmente ordinato $\mathcal{P}(A)$, poiché $\bigcup B_\alpha$ può non essere una sottoalgebra.

Vi è tuttavia un caso importante in cui esso coincide con $\bigcup B_\alpha$: quando $\{B_\alpha\}$ è *diretto* rispetto all'inclusione, nel senso che, per ogni coppia B_β, B_γ di elementi di $\{B_\alpha\}$, esiste nello stesso insieme un B_δ tale che $B_\delta \supseteq B_\beta$ e $B_\delta \supseteq B_\gamma$. Ciò avviene ad esempio quando $\{B_\alpha\}$ è una catena (ossia è totalmente ordinato). Se $\{B_\alpha\}$ è diretto e $\{B_{\beta_1}, \ldots, B_{\beta_n}\}$ è un suo qualunque sottoinsieme finito, esiste un $B_\delta \in \{B_\alpha\}$ tale che $B_\delta \supseteq B_{\beta_i}$ per $1 \leq i \leq n$.

Teorema 2.2. *Se $\{B_\alpha\}$ è un insieme diretto di sottoalgebre, allora $\bigcup B_\alpha$ è una sottoalgebra.*

Dimostrazione. Sia $\omega \in \Omega(n)$. Se $n = 0$, è chiaro che $\omega_A \in B = \bigcup B_\alpha$. Siano ora $n \geq 1$ e $(b_1, \ldots, b_n) \in B^{(n)}$. Ogni b_i appartiene a un $B_{\beta_i} \in \{B_\alpha\}$ e quindi, per un opportuno B_δ di $\{B_\alpha\}$,

tutti i b_i appartengono a B_δ. Allora $\omega b_1 \cdots b_n \in B_\delta \subseteq \bigcup B_\alpha$. Dunque $\bigcup B_\alpha$ è una sottoalgebra. □

È chiaro che, se $\bigcup B_\alpha$ è una sottoalgebra, essa è l'estremo superiore delle B_α.

Sia X un sottoinsieme non vuoto della Ω-algebra A. Sia $\{B_\alpha\}$ l'insieme delle sottoalgebre di A che contengono X e si ponga $[X] = \bigcap B_\alpha$. Allora $[X]$ è una sottoalgebra che contiene X ed è contenuta in ogni sottoalgebra di A che contiene X. Chiaramente queste proprietà determinano $[X]$ in modo univoco. Chiamiamo $[X]$ la *sottoalgebra di A generata dall'insieme X*. Possiamo anche darne una definizione costruttiva. Poniamo $X_0 = X \cup U$, dove U è l'insieme degli elementi distinti ω_A, $\omega \in \Omega(0)$. Per $k \geq 0$ poniamo

$$X_{k+1} = X_k \cup \{y \mid y = \omega x_1 \cdots x_n,\ x_i \in X_k,\ \omega \in \Omega(n),\ n \geq 1\}.$$

Evidentemente $X_0 \subseteq X_1 \subseteq \cdots$, ed è chiaro che $\bigcup X_k$ è una sottoalgebra che contiene X. D'altra parte, se B è una qualunque sottoalgebra contenente X, si vede per induzione su k che B contiene ogni X_k. Dunque $B \supseteq \bigcup X_k$ e $[X] = \bigcup X_k$.

Sia $\{A_\alpha \mid \alpha \in I\}$ una famiglia di Ω-algebre indicizzata da un insieme I: è data, cioè, un'applicazione $\alpha \mapsto A_\alpha$ di I in $\{A_\alpha\}$. Ammettiamo che possa essere $A_\alpha = A_\beta$ anche quando $\alpha \neq \beta$. In particolare, tutte le A_α possono coincidere con una stessa A. Conviene supporre che tutte le A_α siano sottoinsiemi di uno stesso insieme A. Ricordiamo che l'insieme prodotto $\prod_I A_\alpha$ è l'insieme delle applicazioni $a\colon \alpha \mapsto a_\alpha$ di I in A tali che $a_\alpha \in A_\alpha$ per ogni α. Definiamo ora su $\prod_I A_\alpha$ una struttura di Ω-algebra definendo i prodotti componente per componente. Se $\omega \in \Omega(0)$, prendiamo come elemento corrispondente di $\prod A_\alpha$ l'applicazione $\alpha \mapsto \omega_{A_\alpha}$, dove ω_{A_α} è l'elemento di A_α individuato da ω. Se $\omega \in \Omega(n)$ con $n \geq 1$, e $a^{(1)}, \ldots, a^{(n)} \in \prod A_\alpha$, definiamo $\omega a^{(1)} \cdots a^{(n)}$ come l'applicazione

$$\alpha \longmapsto \omega a_\alpha^{(1)} a_\alpha^{(2)} \cdots a_\alpha^{(n)},$$

che è evidentemente un elemento di $\prod A_\alpha$. Procedendo così per ogni ω si ottiene una struttura di Ω-algebra su $\prod A_\alpha$. L'insieme $\prod A_\alpha$ munito di questa struttura si chiama *prodotto della famiglia indicizzata di Ω-algebre $\{A_\alpha \mid \alpha \in I\}$*.

Se $I = \{1, 2, \ldots, r\}$, scriviamo $A_1 \times A_2 \times \cdots \times A_r$ al posto di $\prod_I A_\alpha$. Gli elementi di questa algebra sono le r-uple $(a_1, a_2, \ldots, a_r)$, $a_i \in A_i$. Se ω è nullario, l'elemento associato in $A_1 \times \cdots \times A_r$ è $(\omega_{A_1}, \omega_{A_2}, \ldots, \omega_{A_r})$. Se $n \geq 1$ e $a^{(i)} = (a_1^{(i)}, a_2^{(i)}, \ldots, a_r^{(i)})$, $1 \leq i \leq n$, allora $\omega a^{(1)} \cdots a^{(n)}$ è l'elemento di $A_1 \times \cdots \times A_r$ la cui i-esima componente è $\omega a_i^{(1)} a_i^{(2)} \cdots a_i^{(n)}$.

Esercizi

1. Sia G un gruppo. All'insieme dei simboli di operazione che definiscono G si aggiunga l'insieme G, facendolo agire secondo la regola $g(x) = g^{-1}xg$. Verificare che G è un gruppo con insieme di operatori G. Quali sono i G-sottogruppi?

2. Sia X un insieme di generatori di una Ω-algebra A (ossia $A = [X]$). Mostrare che A è l'unione delle sue sottoalgebre $[F]$, dove F percorre i sottoinsiemi finiti di X.

3. Mostrare che una Ω-algebra A è finitamente generata se e solo se possiede la seguente proprietà: l'unione di ogni insieme diretto di sottoalgebre proprie (diverse da A) è propria.

4. Dare esempi dei casi seguenti: (i) una Ω-algebra con due sottoalgebre a intersezione vuota; (ii) una Ω-algebra in cui l'intersezione di due sottoalgebre qualsiasi è una sottoalgebra, ma esistono insiemi infiniti di sottoalgebre a intersezione vuota.

2.3 Omomorfismi e congruenze

Definizione 2.2. *Se A e B sono Ω-algebre, un omomorfismo da A a B è un'applicazione f di A in B tale che, per ogni $\omega \in \Omega(n)$, $n = 0, 1, 2, \ldots$, e per ogni $(a_1, \ldots, a_n) \in A^{(n)}$, si abbia*

$$f(\omega a_1 a_2 \cdots a_n) = \omega f(a_1) f(a_2) \cdots f(a_n). \tag{6}$$

Nel caso $n = 0$ si intende che, se ω_A è l'elemento di A corrispondente a ω, allora $f(\omega_A) = \omega_B$.

È chiaro che il composto gf degli omomorfismi $f\colon A \to B$ e $g\colon B \to C$ è un omomorfismo da A a C, e che 1_A è un omomorfismo di A in sé. Otteniamo così una categoria, **Ω-alg**, i cui oggetti sono le Ω-algebre e i cui morfismi sono gli omomorfismi. È interessante vedere come si applichino a **Ω-alg** e alle sue principali sottocategorie le nozioni fondamentali della teoria delle categorie. Osserviamo fin d'ora che la costruzione del prodotto di Ω-algebre dà, in **Ω-alg**, un prodotto nel senso delle categorie. Sia $\{A_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di algebre e sia $\prod_I A_\alpha$ il loro prodotto, come definito nel ğ 2.2. Per ogni α abbiamo la proiezione $p_\alpha\colon a \mapsto a_\alpha$ di $P = \prod_I A_\alpha$ in A_α. Dalla definizione delle operazioni si vede subito che p_α è un omomorfismo di P in A_α. Affermiamo che $\{P, p_\alpha\}$ è un prodotto della famiglia $\{A_\alpha \mid \alpha \in I\}$ in **Ω-alg**. Per verificarlo, siano B una Ω-algebra e, per ogni $\alpha \in I$, $f_\alpha\colon B \to A_\alpha$ un omomorfismo. Se a ogni $b \in B$ associamo l'elemento di P la cui componente di indice α è $f_\alpha(b)$, otteniamo immediatamente un omomorfismo f di B in P. Inoltre $p_\alpha f = f_\alpha$, e f è l'unico omomorfismo di B in P che soddisfa questa condizione per ogni $\alpha \in I$. Pertanto $\{P, p_\alpha\}$ è effettivamente un prodotto delle A_α in **Ω-alg**.

Definizione 2.3. *Una congruenza su una Ω-algebra A è una relazione di equivalenza su A che sia una sottoalgebra di $A \times A$.*

Se Φ è una relazione di equivalenza sulla Ω-algebra A e $\omega \in \Omega(0)$, allora $(\omega_A, \omega_A) \in \Phi$, e questo è l'elemento $\omega_{A\times A}$ che corrisponde al simbolo nullario ω nell'algebra $A \times A$. Dunque una relazione di equivalenza Φ è una congruenza se e solo se per ogni $\omega \in \Omega(n)$, $n \geq 1$, e per ogni scelta di $(a_i, a_i') \in \Phi$, $i = 1, 2, \ldots, n$, si ha $\omega(a_1, a_1')(a_2, a_2') \cdots (a_n, a_n') \in \Phi$. Poiché

$$\omega(a_1, a_1')(a_2, a_2') \cdots (a_n, a_n') = (\omega a_1 a_2 \cdots a_n,\ \omega a_1' a_2' \cdots a_n'),$$

si richiede che $a_i\ \Phi\ a_i'$, $1 \leq i \leq n$, implichi $\omega a_1 \cdots a_n\ \Phi\ \omega a_1' \cdots a_n'$. La condizione affinché una relazione di equivalenza sia una congruenza è dunque che valga quest'ultima proprietà per ogni simbolo di operazione n-aria con $n \geq 1$. Sia A/Φ l'insieme quoziente di A determinato dalla congruenza Φ, e sia $\bar{a}$ l'elemento di A/Φ corrispondente all'elemento a di A. Poiché $a_i\ \Phi\ a_i'$, $1 \leq i \leq n$, implica $\omega a_1 \cdots a_n\ \Phi\ \omega a_1' \cdots a_n'$, risulta ben definita l'applicazione di $(A/\Phi)^{(n)}$ in A/Φ data da

$$(\bar{a}_1, \ldots, \bar{a}_n) \longmapsto \overline{\omega a_1 \cdots a_n}.$$

Possiamo dunque definire

$$\omega \bar{a}_1 \cdots \bar{a}_n = \overline{\omega a_1 \cdots a_n} \tag{7}$$

per ogni $\omega \in \Omega(n)$, $n \geq 1$. Per $\omega \in \Omega(0)$ definiamo inoltre

$$\omega_{A/\Phi} = \overline{\omega_A}. \tag{8}$$

In questo modo muniamo A/Φ di una struttura di Ω-algebra. Chiamiamo A/Φ, con questa struttura, *algebra quoziente di A rispetto alla congruenza Φ*. In termini dell'applicazione naturale $\nu\colon a \mapsto \bar{a}$ di A in A/Φ, le equazioni (7) e (8) si scrivono $\omega(\nu a_1) \cdots (\nu a_n) = \nu(\omega a_1 \cdots a_n)$ e $\omega_{A/\Phi} = \nu\omega_A$. Ciò significa precisamente che l'applicazione naturale ν è un omomorfismo di A in A/Φ.

Sia f un'applicazione di un insieme A in un insieme B. Allora $\Phi = f^{-1}f$ è una relazione su A. Infatti f è il sottoinsieme di $A \times B$ costituito dalle coppie $(a, f(a))$ con $a \in A$, e f^{-1} è il sottoinsieme di $B \times A$ costituito dalle coppie $(f(a), a)$; perciò $f^{-1}f$ è l'insieme delle coppie (a, a') di $A \times A$ tali che $f(a) = f(a')$. Si ha dunque $a \,\Phi\, a'$ se e solo se $f(a) = f(a')$, ed è chiaro che Φ è una relazione di equivalenza sull'insieme A (BAI, p. 17). D'ora in poi chiameremo questa relazione di equivalenza *nucleo* dell'applicazione f. Poiché $a \,\Phi\, a'$ implica $f(a) = f(a')$, è chiaro che $\bar{f}(\bar{a}) = f(a)$ definisce un'applicazione $\bar{f}$ di A/Φ in B che rende commutativo il diagramma

(9)
$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle \nu}\downarrow & \nearrow_{\bar{f}} & \\ A/\Phi & & \end{array} .$$

Qui $\nu = \nu_\Phi$ è l'applicazione $a \mapsto \bar{a} = \bar{a}_\Phi$. Inoltre $\bar{f}$ è determinata in modo univoco da questa proprietà ed è iniettiva. Chiaramente ν è suriettiva. Estendiamo ora il risultato alle Ω-algebre nel cosiddetto

Teorema fondamentale degli omomorfismi di Ω-algebre. *Siano A e B due Ω-algebre, e sia f un omomorfismo di A in B. Allora $\Phi = f^{-1}f$ è una congruenza su A e l'immagine $f(A)$ è una sottoalgebra di B. Esiste inoltre un unico omomorfismo $\bar{f}$ di A/Φ in B tale che $f = \bar{f}\nu$, dove ν è l'omomorfismo $a \mapsto \bar{a}$ di A in A/Φ. L'omomorfismo $\bar{f}$ è iniettivo e ν è suriettivo.*

Dimostrazione. Siano $\omega \in \Omega(n)$, $n \geq 1$, e $(a_i, a_i') \in \Phi$ per $1 \leq i \leq n$. Allora $f(a_i) = f(a_i')$ e

$$f(\omega a_1 \cdots a_n) = \omega f(a_1) \cdots f(a_n) = \omega f(a_1') \cdots f(a_n') = f(\omega a_1' \cdots a_n').$$

Pertanto $(\omega a_1 \cdots a_n, \omega a_1' \cdots a_n') \in \Phi$, ossia $\omega(a_1, a_1') \cdots (a_n, a_n') \in \Phi$. Poiché Φ è una relazione di equivalenza, ciò dimostra che Φ è una congruenza sull'algebra A. È immediato che $f(A)$ è una sottoalgebra di B. Consideriamo ora l'applicazione $\bar{f}$. Se $\omega \in \Omega(0)$, si ha $\bar{f}(\omega_{A/\Phi}) = \bar{f}(\overline{\omega_A}) = f(\omega_A) = \omega_B$. Se $\omega \in \Omega(n)$, $n \geq 1$, e $a_i \in A$, $1 \leq i \leq n$, si ha

$$\begin{aligned} \bar{f}(\omega \bar{a}_1 \cdots \bar{a}_n) &= \bar{f}(\overline{\omega a_1 \cdots a_n}) \\ &= f(\omega a_1 \cdots a_n) \\ &= \omega f(a_1) \cdots f(a_n) \\ &= \omega \bar{f}(\bar{a}_1) \cdots \bar{f}(\bar{a}_n). \end{aligned}$$

Dunque $\bar{f}$ è un omomorfismo. Le rimanenti asserzioni seguono dai risultati sulle applicazioni richiamati sopra. □

Consideriamo ora l'estensione alle Ω-algebre delle idee che si raccolgono attorno alla corrispondenza tra i sottogruppi di un gruppo e quelli di una sua immagine omomorfa (BAI, pp. 64–67). Sia f un omomorfismo suriettivo di una Ω-algebra A su una Ω-algebra B. Se A_1 è una sottoalgebra di A, la restrizione $f|_{A_1}$ è un omomorfismo di A_1; quindi $f(A_1)$ è una sottoalgebra di B. Sia ora B_1 una sottoalgebra di B e sia $A_1 = f^{-1}(B_1)$ la sua immagine inversa. Allora $\omega_A \in A_1$ per ogni ω nullario e, se $a_i \in A_1$ e $\omega \in \Omega(n)$ con $n \geq 1$, si ha

$$f(\omega a_1 \cdots a_n) = \omega f(a_1) \cdots f(a_n) \in B_1,$$

per cui $\omega a_1 \cdots a_n \in A_1$. Dunque $A_1 = f^{-1}(B_1)$ è una sottoalgebra di A. Inoltre $f(A_1) = B_1$ e A_1 è una sottoalgebra *satura* di A, nel senso che, se $a_1 \in A_1$, ogni a_1' tale che $f(a_1') = f(a_1)$ appartiene ad A_1. È anche chiaro che, se A_1 è una qualunque sottoalgebra satura di A, si ha $A_1 = f^{-1}(f(A_1))$. Ne segue che l'applicazione

$$A_1 \longmapsto f(A_1)$$

dall'insieme delle sottoalgebre sature di A all'insieme delle sottoalgebre di B è una biiezione, con inversa $B_1 \mapsto f^{-1}(B_1)$.

Ciò vale in particolare se è data una congruenza Φ su A e si prendono $B = A/\Phi$ e $f = \nu$, l'omomorfismo naturale $a \mapsto \bar{a} = \bar{a}_\Phi$ di A su A/Φ. In questo caso, per ogni sottoalgebra A_1 di A, $\nu^{-1}(\nu(A_1))$ è l'unione delle classi di congruenza di A (determinate da Φ) che incontrano A_1, che hanno cioè un elemento in comune con A_1. L'applicazione $\nu_1 = \nu|_{A_1}$ è un omomorfismo di A_1 in A/Φ. Si vede che la sua immagine è A_1'/Φ_1', dove $A_1' = \nu^{-1}(\nu(A_1))$ e Φ_1' è la congruenza $\Phi \cap (A_1' \times A_1')$ su A_1'. D'altra parte il nucleo di ν_1 è $\Phi_1 = \Phi \cap (A_1 \times A_1)$. Possiamo quindi applicare il teorema fondamentale degli omomorfismi per concludere che l'applicazione

$$\overline{a_1}_{\Phi_1} \longmapsto \overline{a_1}_{\Phi_1'}, \qquad a_1 \in A_1, \tag{10}$$

è un isomorfismo di A_1/Φ_1 su A_1'/Φ_1'. Enunciamo questo risultato come

Primo teorema di isomorfismo. *Sia Φ una congruenza su una Ω-algebra A e sia A_1 una sottoalgebra di A. Sia A_1' l'unione delle classi di equivalenza rispetto a Φ che incontrano A_1. Allora A_1' è una sottoalgebra di A contenente A_1, $\Phi_1' = \Phi \cap (A_1' \times A_1')$ e $\Phi_1 = \Phi \cap (A_1 \times A_1)$ sono congruenze rispettivamente su A_1' e su A_1, e la (10) è un isomorfismo di A_1/Φ_1 su A_1'/Φ_1'.*

Consideriamo ora le congruenze sull'algebra quoziente A/Φ, dove Φ è una congruenza assegnata su A. Osserviamo anzitutto che, se Θ è una seconda congruenza, abbiamo la corrispondenza

$$\nu_{\Theta/\Phi} = \{(\bar{a}_\Phi, \bar{a}_\Theta) \mid a \in A\} \tag{11}$$

da A/Φ ad A/Θ. Questa è un'applicazione di A/Φ in A/Θ se e solo se $a\ \Phi\ b$ implica $a\ \Theta\ b$, ossia se e solo se $\Phi \subseteq \Theta$. In tal caso $\nu_{\Theta/\Phi}\colon \bar{a}_\Phi \mapsto \bar{a}_\Theta$ è l'unica applicazione di A/Φ in A/Θ che renda commutativo il diagramma

(12)
$$\begin{array}{ccc} A & \xrightarrow{\nu_\Theta} & A/\Theta \\ {\scriptstyle \nu_\Phi}\downarrow & \nearrow_{\nu_{\Theta/\Phi}} & \\ A/\Phi & & \end{array} .$$

Una verifica diretta, che lasciamo al lettore, mostra che $\nu_{\Theta/\Phi}$ è un omomorfismo di algebre. È chiaro che $\nu_{\Theta/\Phi}$ è suriettivo, ed è iniettivo se e solo se $\Theta = \Phi$.

Indichiamo ora con Θ/Φ il nucleo dell'omomorfismo $\nu_{\Theta/\Phi}$ di A/Φ in A/Θ. Si tratta della congruenza su A/Φ costituita dalle coppie $(\bar{a}_\Phi, \bar{b}_\Phi)$ tali che $\bar{a}_\Theta = \bar{b}_\Theta$. Ne segue che, se Θ_1 e Θ_2 sono due congruenze su A tali che $\Theta_i \supseteq \Phi$, allora $\Theta_1 \supseteq \Theta_2$ se e solo se $\Theta_1/\Phi \supseteq \Theta_2/\Phi$. In particolare, $\Theta_1/\Phi = \Theta_2/\Phi$ implica $\Theta_1 = \Theta_2$.

Mostriamo ora che ogni congruenza $\bar{\Theta}$ su A/Φ è della forma Θ/Φ, dove Θ è una congruenza su A contenente Φ. Sia $\bar{\nu}$ l'omomorfismo canonico di A/Φ su $(A/\Phi)/\bar{\Theta}$. Allora $\bar{\nu}\nu_\Phi$ è un omomorfismo suriettivo di A su $(A/\Phi)/\bar{\Theta}$. Se Θ ne è il nucleo, il teorema fondamentale degli omomorfismi dà un unico isomorfismo $\nu'\colon A/\Theta \to (A/\Phi)/\bar{\Theta}$ che rende commutativo il diagramma

(13)
$$\begin{array}{ccc} A & \xrightarrow{\bar{\nu}\nu_\Phi} & (A/\Phi)/\bar{\Theta} \\ {\scriptstyle \nu_\Theta}\downarrow & \nearrow_{\nu'} & \\ A/\Theta & & \end{array} .$$

Allora $\nu_\Theta = (\nu')^{-1}\bar{\nu}\nu_\Phi$. Ciò implica $\Theta \supseteq \Phi$ e dà l'omomorfismo $\nu_{\Theta/\Phi}$ del diagramma commutativo (12). Poiché ν_Φ è suriettivo sull'algebra A/Φ e

$$\nu_\Theta = (\nu')^{-1}\bar{\nu}\nu_\Phi = \nu_{\Theta/\Phi}\nu_\Phi,$$

i due omomorfismi $(\nu')^{-1}\bar{\nu}$ e $\nu_{\Theta/\Phi}$ di A/Φ coincidono. Poiché ν' è un isomorfismo, il nucleo di $(\nu')^{-1}\bar{\nu}$ coincide con quello di $\bar{\nu}$. Gli omomorfismi $\bar{\nu}$ e $\nu_{\Theta/\Phi}$ di A/Φ hanno dunque lo stesso nucleo. Per $\bar{\nu}$ esso è $\bar{\Theta}$, per $\nu_{\Theta/\Phi}$ è Θ/Φ. Ne segue $\bar{\Theta} = \Theta/\Phi$, come affermato.

I risultati ottenuti si possono enunciare nel modo seguente.

Teorema 2.3. *Siano A una Ω-algebra, Φ una congruenza su A e A/Φ l'algebra quoziente corrispondente. Sia Θ una congruenza su A tale che $\Theta \supseteq \Phi$. Allora esiste un unico omomorfismo $\nu_{\Theta/\Phi}\colon A/\Phi \to A/\Theta$ che rende commutativo il diagramma (12). Se Θ/Φ denota il nucleo di $\nu_{\Theta/\Phi}$, allora Θ/Φ è una congruenza su A/Φ. L'applicazione $\Theta \mapsto \Theta/\Phi$ è una biiezione dall'insieme delle congruenze su A contenenti Φ all'insieme delle congruenze su A/Φ. Inoltre, per due congruenze su A contenenti Φ, si ha $\Theta_1 \supseteq \Theta_2$ se e solo se $\Theta_1/\Phi \supseteq \Theta_2/\Phi$.*

Abbiamo anche il

Secondo teorema di isomorfismo. *Siano Θ e Φ congruenze sulla Ω-algebra A tali che $\Theta \supseteq \Phi$, e sia Θ/Φ la corrispondente congruenza su A/Φ del teorema 2.3. Allora*

$$\overline{(\bar{a}_\Phi)}_{\Theta/\Phi} \longmapsto \bar{a}_\Theta, \qquad a \in A, \tag{14}$$

è un isomorfismo di $(A/\Phi)/(\Theta/\Phi)$ su A/Θ.

Dimostrazione. L'omomorfismo $\nu_{\Theta/\Phi}$ di A/Φ su A/Θ manda $\bar{a}_\Phi$ in $\bar{a}_\Theta$ e ha per nucleo Θ/Φ. Per il teorema fondamentale, la (14) è quindi un isomorfismo di $(A/\Phi)/(\Theta/\Phi)$ su A/Θ. □

Nel caso della categoria **Grp**, i risultati sugli omomorfismi di Ω-algebre si riducono a risultati ben noti (si veda BAI, pp. 61–66). Se f è un omomorfismo di un gruppo G in un gruppo H, allora $K = f^{-1}(1)$ è un sottogruppo normale di G. Il nucleo $\Phi = f^{-1}f$ è l'insieme delle coppie (a, b), $a, b \in G$, tali che $a^{-1}b \in K$. Ne segue che $\bar{a}_\Phi = aK = Ka$ e che G/Φ è l'usuale gruppo quoziente G/K. Per i gruppi, il teorema fondamentale degli omomorfismi, così come lo abbiamo enunciato, equivale al teorema che porta abitualmente questo nome nella teoria dei gruppi. Anche gli altri risultati ottenuti danno luogo a casi particolari ben noti (si veda l'esercizio 1 qui sotto). Analogamente, se R e S sono anelli e f è un omomorfismo di R in S, allora $K = f^{-1}(0)$ è un ideale di R e $R/\Phi = R/K$. Ritroviamo così i risultati classici sugli anelli (si veda l'esercizio 2).

Esercizi

1. Siano G e H due gruppi, f un omomorfismo di G in H e $K = f^{-1}(1)$. Nella terminologia usuale K si chiama *nucleo* di f. La formulazione consueta del *teorema fondamentale degli omomorfismi per i gruppi* afferma che $\bar{f}\colon aK \mapsto f(a)$ è un monomorfismo di G/K in H e che f si fattorizza nella forma $f = \bar{f}\nu$, dove ν è l'epimorfismo $a \mapsto aK$. Il *primo teorema di isomorfismo per i gruppi* afferma che, se H è un sottogruppo di un gruppo G e K è un sottogruppo normale di G, allora il sottogruppo generato da H e K è $HK = \{hk \mid h \in H,\ k \in K\}$, K è normale in HK, $K \cap H$ è normale in H e si ha l'isomorfismo

   $$hK \longmapsto h(H \cap K) \tag{15}$$

   di HK/K su $H/(H \cap K)$. Il *secondo teorema di isomorfismo* afferma che, se H e K sono normali in G e $H \supseteq K$, allora H/K è normale in G/K e

   $$gH \longmapsto (gK)(H/K) \tag{16}$$

   è un isomorfismo di G/H su $(G/K)/(H/K)$. Dedurre il teorema fondamentale degli omomorfismi e gli isomorfismi (15) e (16) dai risultati sulle congruenze delle Ω-algebre.

Enunciare i risultati corrispondenti per i Λ-gruppi (gruppi con operatori). Fare altrettanto per i moduli su un anello R.

2. Dedurre dai teoremi sulle congruenze delle Ω-algebre i risultati sugli omomorfismi di anelli analoghi a quelli precedenti sui gruppi.

3. Sia A una Ω-algebra e sia X un insieme di generatori di A (ossia sia $[X] = A$). Mostrare che, se f e g sono omomorfismi di A in una seconda Ω-algebra B tali che $f|_X = g|_X$, allora $f = g$.

2.4 Il reticolo delle congruenze. Prodotti sottodiretti

Studieremo dapprima alcune altre proprietà dell'insieme delle congruenze su una Ω-algebra A. Le applicheremo poi allo studio dell'importante nozione di prodotto sottodiretto di algebre.

Consideriamo anzitutto l'insieme $\Gamma(A)$ delle congruenze su A come insieme parzialmente ordinato, in cui l'ordine $\geq$ è dato dall'inclusione usuale $\Phi \supset \Theta$. Ciò significa, naturalmente, che $a\Theta b$ implica $a\Phi b$ o, equivalentemente, che $\bar{a}_\Theta = \bar{b}_\Theta$ implica $\bar{a}_\Phi = \bar{b}_\Phi$.

Teorema 2.4. *Se $\{\Phi_\alpha\}$ è un insieme di congruenze sulla Ω-algebra A, allora $\bigcap \Phi_\alpha$ è una congruenza. Inoltre, se $\{\Phi_\alpha\}$ è diretto, anche $\bigcup \Phi_\alpha$ è una congruenza.*

Dimostrazione. Osserviamo anzitutto che, se $\{\Phi_\alpha\}$ è un insieme di relazioni di equivalenza su A, allora $\bigcap \Phi_\alpha$ è una relazione di equivalenza e, se $\{\Phi_\alpha\}$ è diretto, anche $\bigcup \Phi_\alpha$ è una relazione di equivalenza. Infatti, poiché ogni Φ_α contiene 1_A, si ha $\bigcap \Phi_\alpha \supset 1_A$. Se $(x, y) \in \Phi_\alpha$, allora $(y, x) \in \Phi_\alpha$. Quindi, se $(x, y) \in \bigcap \Phi_\alpha$, anche $(y, x) \in \bigcap \Phi_\alpha$. Siano ora (x, y) e (y, z) in Φ_α. Allora $(x, z) \in \Phi_\alpha$. Pertanto, se (x, y) e (y, z) appartengono a $\bigcap \Phi_\alpha$, vi appartiene anche (x, z). Dunque $\bigcap \Phi_\alpha$ è una relazione di equivalenza. Supponiamo ora che $\{\Phi_\alpha\}$ sia diretto. È chiaro che $\bigcup \Phi_\alpha \supset 1_A$ e che $(\bigcup \Phi_\alpha)^{-1} = \bigcup \Phi_\alpha$. Siano (x, y) e (y, z) in $\bigcup \Phi_\alpha$. Poiché $\{\Phi_\alpha\}$ è diretto, esiste $\Phi_\delta \in \{\Phi_\alpha\}$ a cui appartengono sia (x, y) sia (y, z). Allora $(x, z) \in \Phi_\delta$, e quindi $(x, z) \in \bigcup \Phi_\alpha$. Anche $\bigcup \Phi_\alpha$ è dunque una relazione di equivalenza.

Supponiamo ora che le Φ_α siano congruenze, sicché sono, oltre che relazioni di equivalenza, sottoalgebre di $A \times A$. Allora $\bigcap \Phi_\alpha$ è una relazione di equivalenza e quindi non è vuota. Di conseguenza $\bigcap \Phi_\alpha$ è anche una sottoalgebra e perciò una congruenza. Analogamente, se $\{\Phi_\alpha\}$ è diretto, $\bigcup \Phi_\alpha$ è una sottoalgebra. □

È chiaro che $\bigcap \Phi_\alpha$ è l'estremo inferiore dell'insieme di congruenze $\{\Phi_\alpha\}$. È evidente anche che l'intero insieme $A \times A$, come sottoinsieme di $A \times A$, è una congruenza ed è il massimo nell'insieme parzialmente ordinato delle congruenze. L'algebra quoziente corrispondente $A/(A \times A)$ è l'*algebra banale*, ossia un'algebra con un solo elemento (nella quale l'azione di ogni $\omega \in \Omega$ è univocamente determinata). È chiaro inoltre che la diagonale 1_A è una congruenza e che $A/1_A$ si può identificare con A, poiché l'omomorfismo ν_{1_A} è un isomorfismo. L'insieme $\Gamma(A)$ delle congruenze su A possiede quindi un massimo e ogni suo sottoinsieme non vuoto ammette estremo inferiore. Per il teorema 2.1 (p. 57 dell'originale), $\Gamma(A)$ è dunque un reticolo completo. In particolare, due congruenze qualsiasi Φ e Θ hanno un estremo superiore $\Phi \vee \Theta$ in $\Gamma(A)$. Nell'esercizio 3 in fondo al paragrafo indicheremo un'altra dimostrazione, più costruttiva, di questo fatto.

Data una relazione binaria R sull'algebra A, possiamo definire la *congruenza* $[R]$ *generata da* R come l'estremo inferiore (o intersezione) di tutte le congruenze su A che contengono R. Essa è caratterizzata dalle consuete proprietà: (1) $[R]$ è una congruenza contenente R e (2) $[R]$ è contenuta in ogni congruenza contenente R.

Ricordiamo che un *elemento massimale* di un sottoinsieme S di un insieme parzialmente ordinato A è un elemento $m \in S$ per il quale non esiste alcun $s \in S$ tale che $s \neq m$ e $s \geq m$. Un teorema fondamentale di esistenza per le congruenze massimali è il seguente.

Teorema 2.5. *Siano a e b elementi distinti di una Ω-algebra A e sia $D(a,b)$ l'insieme delle congruenze Φ su A tali che $(a,b) \notin \Phi$. Allora $D(a,b)$ non è vuoto e contiene un elemento massimale.*

Dimostrazione. Si ha evidentemente $1_A \in D(a,b)$, sicché $D(a,b) \neq \varnothing$. Sia ora $\{\Phi_\alpha\}$ un sottoinsieme totalmente ordinato di $D(a,b)$, ossia per ogni $\Phi_\beta, \Phi_\gamma \in \{\Phi_\alpha\}$ si abbia $\Phi_\beta \supset \Phi_\gamma$ oppure $\Phi_\gamma \supset \Phi_\beta$. Allora $\{\Phi_\alpha\}$ è diretto, e quindi $\bigcup \Phi_\alpha$ è una congruenza. È evidente che $\bigcup \Phi_\alpha \in D(a,b)$ e che $\bigcup \Phi_\alpha \supset \Phi_\alpha$. Ogni sottoinsieme totalmente ordinato di $D(a,b)$ ha dunque un maggiorante in $D(a,b)$. Possiamo perciò applicare il lemma di Zorn e concludere che $D(a,b)$ contiene elementi massimali. □

Un'utile estensione del teorema 2.5 è la seguente.

Corollario 1. *Sia Θ una congruenza su A e siano a, b elementi tali che $\bar{a}_\Theta \neq \bar{b}_\Theta$. Allora l'insieme delle congruenze Φ tali che $\Phi \supset \Theta$ e $\bar{a}_\Phi \neq \bar{b}_\Phi$ contiene un elemento massimale.*

Dimostrazione. Applichiamo il teorema 2.5 all'algebra A/Θ e alla coppia $(\bar{a}_\Theta, \bar{b}_\Theta)$ di suoi elementi. In quest'algebra esiste una congruenza massimale fra le congruenze che non contengono $(\bar{a}_\Theta, \bar{b}_\Theta)$. Per il teorema 2.3, una tale congruenza ha la forma Φ/Θ, dove Φ è una congruenza su A contenente Θ. Poiché $(\bar{a}_\Theta, \bar{b}_\Theta) \notin \Phi/\Theta$, si ha $\nu_{\Phi/\Theta}\bar{a}_\Theta \neq \nu_{\Phi/\Theta}\bar{b}_\Theta$, il che significa che $\bar{a}_\Phi \neq \bar{b}_\Phi$. Inoltre Φ è massimale fra le congruenze che contengono Θ e hanno questa proprietà. □

Questo risultato ammette molti casi particolari importanti. Uno di essi, che consideriamo ora, riguarda l'esistenza di ideali massimali in un anello. Un ideale B (rispettivamente, un ideale sinistro o destro) di un anello R si chiama *massimale* se $B \neq R$ e non esiste alcun ideale B' (rispettivamente, sinistro o destro) tale che $R \supsetneq B' \supsetneq B$. Osserviamo che un ideale B, bilatero, sinistro o destro, è proprio ($B \neq R$) se e solo se $1 \notin B$. Abbiamo ora il seguente risultato.

Corollario 2. *In un anello $R \neq 0$, ogni ideale proprio è contenuto in un ideale massimale. Lo stesso vale per gli ideali unilateri, a sinistra o a destra.*

Dimostrazione. Per ottenere il risultato sugli ideali ci serviamo del fatto che ogni congruenza su un anello R è determinata da un ideale B come insieme delle coppie (a, a'), con $a, a' \in R$, tali che $a - a' \in B$. Viceversa, ogni ideale è determinato in questo modo da una congruenza, e, se Φ_B è la congruenza associata all'ideale B, si ha $\Phi_B \supset \Phi_{B'}$ per l'ideale B' se e solo se $B \supset B'$. Ora, se B è proprio, Φ_B non contiene $(1,0)$. Il corollario 1 dà allora una congruenza Φ_M, con M ideale, tale che $\Phi_M \supset \Phi_B$, $(1,0) \notin \Phi_M$ e Φ_M sia massimale fra le congruenze di questo tipo. Pertanto $M \supset B$ e $1 \notin M$, sicché M è proprio ed è massimale nell'insieme degli ideali con questa proprietà. Ne segue che M è un ideale massimale nel senso definito sopra. La dimostrazione per gli ideali unilateri si ottiene allo stesso modo considerando R come una Ω-algebra costituita da un gruppo (il gruppo additivo) con operatori. L'insieme R degli operatori agisce mediante moltiplicazioni a sinistra nel caso degli ideali sinistri, e mediante moltiplicazioni a destra per gli ideali destri. □

Naturalmente, questi risultati si possono anche ottenere applicando il lemma di Zorn direttamente agli insiemi di ideali (si veda l'esercizio 1 più avanti). Ci è parso tuttavia istruttivo dedurli dal teorema generale sulle congruenze.

Consideriamo di nuovo una Ω-algebra arbitraria A e sia $\{\Theta_\alpha \mid \alpha \in I\}$ una famiglia indicizzata di congruenze su A tale che $\bigcap \Theta_\alpha = 1_A$. Per ogni $\alpha \in I$ abbiamo il quoziente $A_\alpha = A/\Theta_\alpha$ e possiamo formare l'algebra prodotto $P = \prod_{\alpha \in I} A_\alpha$. Abbiamo l'omomorfismo $\nu_\alpha \colon a \mapsto \bar{a}_{\Theta_\alpha}$ di A su A_α e l'omomorfismo $\nu \colon a \mapsto \bar{a}$ di A in P, dove la componente di indice α di $\bar{a}$ è $\bar{a}_{\Theta_\alpha}$. Il nucleo di ν è l'insieme delle coppie (a,b) tali che $\bar{a}_{\Theta_\alpha} = \bar{b}_{\Theta_\alpha}$ per ogni $\alpha \in I$. Esso è dunque l'intersezione dei nuclei Θ_α dei ν_α. Poiché $\bigcap \Theta_\alpha = 1_A$, il nucleo di ν è 1_A, e quindi ν è un monomorfismo. Dalla definizione è chiaro anche che, per ogni α, l'immagine $p_\alpha \nu(A)$ di $\nu(A)$ mediante la proiezione p_α di P su A_α è tutto A_α.

Se $\{A_\alpha \mid \alpha \in I\}$ è una famiglia indicizzata arbitraria di algebre e $P = \prod A_\alpha$, diciamo che un'algebra A è un *prodotto sottodiretto* delle A_α se esiste un monomorfismo i di A in P tale che, per ogni α, $i_\alpha = p_\alpha i$ è suriettivo su A_α. Abbiamo dunque mostrato che, se un'algebra A possiede una famiglia di congruenze $\{\Theta_\alpha \mid \alpha \in I\}$ tale che $\bigcap \Theta_\alpha = 1_A$, allora A è un prodotto sottodiretto delle algebre $A_\alpha = A/\Theta_\alpha$. Viceversa, sia A un prodotto sottodiretto delle A_α mediante il monomorfismo i. Se Θ_α è il nucleo di $i_\alpha = p_\alpha i$, si vede immediatamente che $\bigcap \Theta_\alpha = 1_A$ e che l'immagine $i_\alpha(A)$ è isomorfa ad A/Θ_α.

Definizione 2.4. *Una Ω-algebra A si dice sottodirettamente irriducibile se l'intersezione di tutte le sue congruenze diverse da 1_A è diversa da 1_A.*

In virtù dei risultati appena osservati, ciò significa che, se A è sottodirettamente irriducibile ed è un prodotto sottodiretto di algebre A_α, uno degli omomorfismi $i_\alpha = p_\alpha i$ è un isomorfismo. Se $a \neq b$ in un'algebra A, nel teorema 2.5 abbiamo provato l'esistenza di una congruenza $\Phi_{a,b}$ massimale nell'insieme delle congruenze che non contengono (a, b). Affermiamo che $A/\Phi_{a,b}$ è sottodirettamente irriducibile. Per il teorema 2.3, ogni congruenza su $A/\Phi_{a,b}$ è della forma $\Theta_\alpha/\Phi_{a,b}$, con Θ_α congruenza su A contenente $\Phi_{a,b}$. Se essa è diversa dalla diagonale, allora $\Theta_\alpha \supsetneq \Phi_{a,b}$ e, per la massimalità di $\Phi_{a,b}$, si ha $(a, b) \in \Theta_\alpha$. Pertanto

$$(\bar{a}_{\Phi_{a,b}}, \bar{b}_{\Phi_{a,b}}) \in \Theta_\alpha/\Phi_{a,b}$$

per ogni congruenza $\Theta_\alpha/\Phi_{a,b}$ su $A/\Phi_{a,b}$ diversa dalla diagonale. Ciò significa, evidentemente, che $A/\Phi_{a,b}$ è sottodirettamente irriducibile. Ce ne serviamo per dimostrare il seguente teorema.

Teorema 2.6 (Birkhoff). *Ogni Ω-algebra A è un prodotto sottodiretto di algebre sottodirettamente irriducibili.*

Dimostrazione. Possiamo supporre che A contenga più di un elemento. Per ogni coppia (a, b), con $a \neq b$, sia $\Phi_{a,b}$ una congruenza massimale fra quelle tali che $(a, b) \notin \Phi_{a,b}$. Allora $A/\Phi_{a,b}$ è sottodirettamente irriducibile. Inoltre $\bigcap \Phi_{a,b} = 1_A$. Altrimenti esisterebbe $(c, d) \in \bigcap \Phi_{a,b}$ con $c \neq d$. Allora $(c, d) \in \Phi_{c,d}$, assurdo. Si ha dunque $\bigcap \Phi_{a,b} = 1_A$, e perciò A è un prodotto sottodiretto delle algebre sottodirettamente irriducibili $A/\Phi_{a,b}$. □

Esercizi

1. Dare una dimostrazione diretta del corollario 2 al teorema 2.5.
2. Mostrare che $\mathbb{Z}$ è un prodotto sottodiretto dei campi $\mathbb{Z}/(p)$, al variare di p fra i numeri primi.
3. Siano Θ e Φ congruenze su A. Mostrare che $\Theta\Phi \subset (\Theta\Phi)^2 \subset (\Theta\Phi)^3 \subset \cdots$ e che $\bigcup_k (\Theta\Phi)^k$ è una congruenza che è l'estremo superiore di Θ e Φ. Ne segue che ogni insieme finito di congruenze ha un estremo superiore. Servirsi di questo fatto e della seconda affermazione del teorema 2.4 per mostrare che ogni insieme di congruenze ha un estremo superiore.
4. Sia $\{\Theta_\alpha\}$ un insieme arbitrario di congruenze su un'algebra A e sia $\Theta = \bigcap \Theta_\alpha$. Mostrare che A/Θ è un prodotto sottodiretto delle algebre A/Θ_α.

2.5 Limiti diretti e inversi

Considereremo ora due costruzioni di Ω-algebre: i limiti diretti e i limiti inversi. Le definizioni si possono dare per categorie arbitrarie ed è interessante collocarle in quest'ambito, poiché vi sono altri esempi importanti di questi concetti, oltre a quello delle Ω-algebre che qui ci interessa. Cominciamo con la definizione di limite diretto in una categoria $\mathbf{C}$.

Sia I un insieme preordinato (l'insieme degli indici) e sia $\mathbf{I}$ la categoria definita da I come nell'esempio 12 a p. 13 dell'originale: $\operatorname{ob}\mathbf{I} = I$ e, per $\alpha, \beta \in I$, $\hom(\alpha, \beta)$ è vuoto a meno che $\alpha \leq \beta$, nel qual caso contiene un solo elemento. Se $\mathbf{C}$ è una categoria, un funtore F da $\mathbf{I}$ a $\mathbf{C}$ consiste di un'applicazione $\alpha \mapsto A_\alpha$ di I in $\operatorname{ob}\mathbf{C}$ e di un'applicazione $(\alpha, \beta) \mapsto \varphi_{\alpha\beta} \in \hom_{\mathbf{C}}(A_\alpha, A_\beta)$ definita per tutte le coppie (α, β) con $\alpha \leq \beta$, tali che

1. $\varphi_{\alpha\gamma} = \varphi_{\beta\gamma}\varphi_{\alpha\beta}$ se $\alpha \leq \beta \leq \gamma$;
2. $\varphi_{\alpha\alpha} = 1_{A_\alpha}$.

Dati questi elementi, definiamo un *limite diretto* (o *induttivo*) $\varinjlim(A_\alpha, \varphi_{\alpha\beta})$ come una coppia $(A, \{\eta_\alpha\})$ in cui $A \in \operatorname{ob}\mathbf{C}$, i morfismi $\eta_\alpha \colon A_\alpha \to A$, $\alpha \in I$, soddisfano $\eta_\alpha = \eta_\beta\varphi_{\alpha\beta}$, e $(A, \{\eta_\alpha\})$ è universale per questa proprietà nel senso seguente. Se $(B, \{\zeta_\alpha\})$ è un'altra coppia siffatta, esiste un unico morfismo $\theta \colon A \to B$ tale che $\zeta_\alpha = \theta\eta_\alpha$ per ogni $\alpha \in I$. (Questo si può interpretare come un universale da un oggetto a un funtore per categorie opportunamente definite. Si veda l'esercizio 1 in fondo al paragrafo.) È chiaro che, se un limite diretto esiste, esso è unico a meno di isomorfismo, nel senso che, se $(A', \{\eta'_\alpha\})$ è un secondo limite diretto, esiste un unico isomorfismo $\theta \colon A \to A'$ tale che $\eta'_\alpha = \theta\eta_\alpha$ per ogni $\alpha \in I$.

Un semplice esempio di limite diretto si ottiene considerando le sottoalgebre finitamente generate di una Ω-algebra. Sia A una Ω-algebra qualsiasi e sia I l'insieme dei sottoinsiemi finiti di A, ordinato per inclusione. Se $F \in I$, sia A_F la sottoalgebra di A generata da F e, se $F \subset G$, sia φ_{FG} l'omomorfismo di inclusione di A_F in $A_G \supset A_F$. Si ha evidentemente $\varphi_{FF} = 1_{A_F}$ e, per $F \subset G \subset H$, $\varphi_{GH}\varphi_{FG} = \varphi_{FH}$. Inoltre, se η_F indica l'omomorfismo di inclusione di A_F in A, allora $\eta_G\varphi_{FG} = \eta_F$. Siano ora B una Ω-algebra e $\{\zeta_F \mid F \in I\}$ una famiglia di omomorfismi $\zeta_F \colon A_F \to B$ tali che $\zeta_G\varphi_{FG} = \zeta_F$ per $F \subset G$. Poiché φ_{FG} è l'inclusione di A_F in A_G, ciò significa che l'omomorfismo ζ_G su A_G è un prolungamento di ζ_F su A_F. Essendo $\bigcup A_F = A$, esiste un unico omomorfismo θ di A in B tale che $\zeta_F = \theta\eta_F$ per ogni $F \in I$. Ne segue che A e $\{\eta_F\}$ costituiscono $\varinjlim(A_F, \varphi_{FG})$. Il risultato appena provato si può enunciare in forma leggermente imprecisa come segue.

Teorema 2.7. *Ogni Ω-algebra è isomorfa a un limite diretto di algebre finitamente generate.*

Mostreremo ora che, se l'insieme degli indici I è *diretto*, nel senso che per ogni $\alpha, \beta \in I$ esiste $\gamma \in I$ tale che $\gamma \geq \alpha$ e $\gamma \geq \beta$, allora il limite diretto esiste nella categoria $\mathbf{C} = \Omega\textbf{-alg}$ per ogni funtore F da $\mathbf{I}$ a $\mathbf{C}$.

Con le notazioni precedenti, siano le A_α delle Ω-algebre e sia $\varphi_{\alpha\beta}$, per $\alpha \leq \beta$, un omomorfismo di algebre da A_α ad A_β. Per costruire un limite diretto consideriamo l'unione disgiunta $\bigsqcup A_\alpha$ degli insiemi A_α. Vi introduciamo una relazione $\sim$ ponendo, per $a \in A_\alpha$ e $b \in A_\beta$, $a \sim b$ se esiste $\rho \geq \alpha, \beta$ tale che $\varphi_{\alpha\rho}(a) = \varphi_{\beta\rho}(b)$. (Ammettiamo anche $\alpha = \beta$.) La relazione è evidentemente riflessiva e simmetrica. Inoltre, se $\varphi_{\alpha\rho}(a) = \varphi_{\beta\rho}(b)$ e $\varphi_{\beta\sigma}(b) = \varphi_{\gamma\sigma}(c)$ per $\rho \geq \alpha, \beta$ e $\sigma \geq \beta, \gamma$, esiste un $\tau \geq \rho, \sigma$. Allora

$$\begin{aligned}\varphi_{\alpha\tau}(a) &= \varphi_{\rho\tau}\varphi_{\alpha\rho}(a) = \varphi_{\rho\tau}\varphi_{\beta\rho}(b) = \varphi_{\beta\tau}(b)\\ &= \varphi_{\sigma\tau}\varphi_{\beta\sigma}(b) = \varphi_{\sigma\tau}\varphi_{\gamma\sigma}(c) = \varphi_{\gamma\tau}(c).\end{aligned}$$

Quindi $a \sim b$ e $b \sim c$ implicano $a \sim c$. La nostra relazione è dunque una relazione di equivalenza.

Sia A il corrispondente insieme quoziente delle classi di equivalenza $\bar{a}$, con $a \in \bigsqcup A_\alpha$. Se $\omega \in \Omega(0)$, allora $\overline{\omega_{A_\alpha}} = \overline{\omega_{A_\beta}}$, poiché esiste $\rho \geq \alpha, \beta$ e $\varphi_{\alpha\rho}(\omega_{A_\alpha}) = \omega_{A_\rho} = \varphi_{\beta\rho}(\omega_{A_\beta})$. Definiamo $\omega_A = \overline{\omega_{A_\alpha}}$. Sia ora $n \geq 1$ e sia $a_i \in A_{\alpha_i}$ per $1 \leq i \leq n$. Scegliamo $\rho \geq \alpha_i$ per $1 \leq i \leq n$, cosa possibile poiché I è diretto. Definiamo ora

$$\omega\bar{a}_1\bar{a}_2\cdots\bar{a}_n = \overline{\omega\varphi_{\alpha_1\rho}(a_1)\varphi_{\alpha_2\rho}(a_2)\cdots\varphi_{\alpha_n\rho}(a_n)}. \tag{17}$$

Questa definizione è evidentemente indipendente dalla scelta degli a_i in $\bar{a}_i$. Dobbiamo anche mostrare che è indipendente dalla scelta di ρ. Sia dunque $\sigma \geq \alpha_i$ per $1 \leq i \leq n$ e scegliamo $\tau \geq \rho, \sigma$. Allora

$$\begin{aligned}\varphi_{\rho\tau}(\omega\varphi_{\alpha_1\rho}(a_1)\cdots\varphi_{\alpha_n\rho}(a_n)) &= \omega\,\varphi_{\rho\tau}\varphi_{\alpha_1\rho}(a_1)\cdots\varphi_{\rho\tau}\varphi_{\alpha_n\rho}(a_n)\\ &= \omega\,\varphi_{\alpha_1\tau}(a_1)\cdots\varphi_{\alpha_n\tau}(a_n).\end{aligned}$$

Analogamente,

$$\varphi_{\sigma\tau}(\omega\varphi_{\alpha_1\sigma}(a_1)\cdots\varphi_{\alpha_n\sigma}(a_n)) = \omega\,\varphi_{\alpha_1\tau}(a_1)\cdots\varphi_{\alpha_n\tau}(a_n),$$

e così la (17) è indipendente dalla scelta di $\rho \geq \alpha_i$, $1 \leq i \leq n$. La definizione dell'azione di ogni $\omega \in \Omega(n)$ per $n \geq 1$, insieme alla precedente definizione delle operazioni nullarie in A, dota A di una struttura di Ω-algebra.

Fissiamo ora α e consideriamo l'applicazione $\eta_\alpha\colon a_\alpha \mapsto \bar{a}_\alpha$ di A_α in A. Se $\omega \in \Omega(0)$, allora $\eta_\alpha\omega_{A_\alpha} = \overline{\omega_{A_\alpha}} = \omega_A$. Se $n \geq 1$ e $a_\alpha^{(1)}, \ldots, a_\alpha^{(n)} \in A_\alpha$, ponendo $\rho = \alpha$ nella (17) si ottiene

$$\omega\,\overline{a_\alpha^{(1)}}\cdots\overline{a_\alpha^{(n)}} = \overline{\omega a_\alpha^{(1)}\cdots a_\alpha^{(n)}}.$$

Dunque η_α è un omomorfismo. Per $\alpha \leq \beta$ si ha $\overline{\varphi_{\alpha\beta}(a_\alpha)} = \bar{a}_\alpha$, poiché $\varphi_{\alpha\beta}(a_\alpha) = \varphi_{\beta\beta}\varphi_{\alpha\beta}(a_\alpha)$. Ciò mostra che $\eta_\beta\varphi_{\alpha\beta}(a_\alpha) = \eta_\alpha(a_\alpha)$. Si ha quindi $\eta_\beta\varphi_{\alpha\beta} = \eta_\alpha$ per $\alpha \leq \beta$.

Supponiamo ora assegnati una Ω-algebra B e omomorfismi $\zeta_\alpha\colon A_\alpha \to B$ tali che $\zeta_\beta\varphi_{\alpha\beta} = \zeta_\alpha$ per $\alpha \leq \beta$ in I. Supponiamo che $\bar{a}_\alpha = \bar{a}_\beta$, cosicché esiste $\rho \geq \alpha, \beta$ tale che $\varphi_{\alpha\rho}(a_\alpha) = \varphi_{\beta\rho}(a_\beta)$. Allora

$$\zeta_\alpha(a_\alpha) = \zeta_\rho\varphi_{\alpha\rho}(a_\alpha) = \zeta_\rho\varphi_{\beta\rho}(a_\beta) = \zeta_\beta(a_\beta).$$

Abbiamo quindi l'applicazione $\theta\colon \bar{a}_\alpha \mapsto \zeta_\alpha(a_\alpha)$ con dominio $A = \bigcup_\alpha \eta_\alpha(A_\alpha)$ e codominio B. Essa soddisfa $\zeta_\alpha = \theta\eta_\alpha$, poiché $\theta\eta_\alpha(a_\alpha) = \theta(\bar{a}_\alpha) = \zeta_\alpha(a_\alpha)$ per ogni $a_\alpha \in A_\alpha$ e $\alpha \in I$. Essendo A l'unione degli $\eta_\alpha(A_\alpha)$, è chiaro che θ è determinata da questa condizione. Inoltre, poiché $\varphi_{\alpha\beta}(a_\alpha) \sim a_\alpha$ per $\beta \geq \alpha$, ogni insieme finito di classi rispetto a $\sim$ ammette rappresentanti in un medesimo A_ρ. Ne segue che θ è un omomorfismo di Ω-algebre. Abbiamo così l'universalità di $(A, \{\eta_\alpha\})$ richiesta nella definizione di limite diretto. Possiamo pertanto enunciare il seguente teorema.

Teorema 2.8. *Per ogni insieme diretto di indici I, nella categoria delle Ω-algebre esistono i limiti diretti.*

La nozione di limite inverso è duale a quella di limite diretto. Partiamo ancora da un insieme preordinato $I = \{\alpha\}$ e da una categoria $\mathbf{C}$, ma prendiamo ora un funtore controvariante F dalla categoria $\mathbf{I}$ definita da I a $\mathbf{C}$. Abbiamo dunque un'applicazione $\alpha \mapsto A_\alpha \in \operatorname{ob}\mathbf{C}$, $\alpha \in I$, e per ogni α, β con $\alpha \leq \beta$ un morfismo $\varphi_{\beta\alpha}\colon A_\beta \to A_\alpha$, tali che

$1'.$ $\varphi_{\gamma\alpha} = \varphi_{\beta\alpha}\varphi_{\gamma\beta}$ se $\alpha \leq \beta \leq \gamma$;

$2'.$ $\varphi_{\alpha\alpha} = 1_{A_\alpha}$.

Un *limite inverso* (o *proiettivo*) è allora una coppia $(A, \{\eta_\alpha\})$ con $A \in \operatorname{ob}\mathbf{C}$ e $\eta_\alpha\colon A \to A_\alpha$, tale che $\varphi_{\beta\alpha}\eta_\beta = \eta_\alpha$ per $\alpha \leq \beta$ e con la seguente proprietà: se $(B, \{\zeta_\alpha\})$ è una coppia con $B \in \operatorname{ob}\mathbf{C}$, $\zeta_\alpha\colon B \to A_\alpha$ e $\varphi_{\beta\alpha}\zeta_\beta = \zeta_\alpha$ per $\alpha \leq \beta$, allora esiste un unico morfismo $\theta\colon B \to A$ tale che $\eta_\alpha\theta = \zeta_\alpha$ per ogni $\alpha \in I$. Indichiamo $(A, \{\eta_\alpha\})$ con $\varprojlim(A_\alpha, \varphi_{\alpha\beta})$. Vale la consueta unicità a meno di isomorfismo: se $(A', \{\eta'_\alpha\})$ è un secondo limite inverso, allora esiste un unico isomorfismo $\theta\colon A' \to A$ tale che $\eta_\alpha\theta = \eta'_\alpha$.

Supponiamo ora $\mathbf{C} = \Omega$-**alg**, cosicché le A_α sono Ω-algebre e, per $\alpha \leq \beta$, $\varphi_{\beta\alpha}$ è un omomorfismo di A_β in A_α. Per cercare di costruire un'algebra limite inverso, partiamo dall'algebra

prodotto $\prod A_\alpha$ e dalle proiezioni $p_\alpha\colon \prod A_\alpha \to A_\alpha$ definite da $p_\alpha(a) = a_\alpha$, dove a è l'applicazione $\alpha \mapsto a_\alpha \in A_\alpha$. Poniamo

$$A = \left\{ a \in \prod A_\alpha \,\middle|\, p_\alpha(a) = \varphi_{\beta\alpha} p_\beta(a) \text{ per } \alpha \leq \beta \right\}, \tag{18}$$

con $\alpha, \beta \in I$. Può accadere, come si vedrà nell'esercizio 2, che A sia vuoto. In tal caso il nostro problema non ammette soluzione. Infatti, se B è un'algebra e per ogni $\alpha \in I$ si ha un omomorfismo $\zeta_\alpha\colon B \to A_\alpha$ tale che $\zeta_\alpha = \varphi_{\beta\alpha}\zeta_\beta$, allora, per ogni $b \in B$, l'elemento $a \in \prod A_\alpha$ le cui componenti sono $a_\alpha = \zeta_\alpha(b)$ soddisfa la condizione (18).

Supponiamo ora che A definito dalla (18) non sia vuoto. Affermiamo che A è una sottoalgebra di $\prod A_\alpha$. Se $\omega \in \Omega(0)$, si ha $p_\alpha(\omega_{\prod A_\alpha}) = \omega_{A_\alpha}$, sicché, per $\alpha \leq \beta$, dalla relazione $\varphi_{\beta\alpha}(\omega_{A_\beta}) = \omega_{A_\alpha}$ segue $p_\alpha(\omega_{\prod A_\alpha}) = \varphi_{\beta\alpha} p_\beta(\omega_{\prod A_\alpha})$. Pertanto $\omega_{\prod A_\alpha} \in A$. (Ciò mostra che $A \neq \varnothing$ se Ω contiene simboli di operazioni nullarie.) Sia ora $\omega \in \Omega(n)$, con $n \geq 1$, e siano $a^{(1)}, \ldots, a^{(n)} \in A$. Allora

$$\begin{aligned} p_\alpha(\omega a^{(1)} \cdots a^{(n)}) &= \omega a_\alpha^{(1)} \cdots a_\alpha^{(n)} = \omega p_\alpha(a^{(1)}) \cdots p_\alpha(a^{(n)}) \\ &= \omega \varphi_{\beta\alpha} p_\beta(a^{(1)}) \cdots \varphi_{\beta\alpha} p_\beta(a^{(n)}) \\ &= \varphi_{\beta\alpha} p_\beta(\omega a^{(1)} \cdots a^{(n)}). \end{aligned}$$

Quindi $\omega a^{(1)} \cdots a^{(n)} \in A$ e A è una sottoalgebra. Se A non è vuoto, affermiamo che questa sottoalgebra di $\prod A_\alpha$, insieme con gli omomorfismi $\eta_\alpha = p_\alpha|_A$, è un limite inverso $\varprojlim(A_\alpha, \varphi_{\alpha\beta})$ in Ω-**alg**. Per definizione di A si ha $\eta_\alpha = \varphi_{\beta\alpha}\eta_\beta$ per $\alpha \leq \beta$. Supponiamo di avere una Ω-algebra B e omomorfismi $\zeta_\alpha\colon B \to A_\alpha$, $\alpha \in I$, tali che $\zeta_\alpha = \varphi_{\beta\alpha}\zeta_\beta$ per $\alpha \leq \beta$. Abbiamo un unico omomorfismo $\theta'\colon B \to \prod A_\alpha$ dato da $b \mapsto a$, dove $a_\alpha = \zeta_\alpha(b)$. Allora, come abbiamo visto, $a \in A$, sicché θ' definisce un omomorfismo θ di B in A tale che $\theta(b) = \theta'(b)$. Si ha $\eta_\alpha\theta(b) = \zeta_\alpha(b)$ e θ è univocamente determinato da questa proprietà. È così completata la verifica che $(A, \{\eta_\alpha\}) = \varprojlim(A_\alpha, \varphi_{\alpha\beta})$.

Un caso particolare importante di limite inverso si ottiene quando sia assegnata una famiglia di congruenze $\{\Phi_\alpha\}$ su un'algebra B. Preordiniamo l'insieme $I = \{\alpha\}$ convenendo che $\alpha \leq \beta$ se $\Phi_\alpha \supset \Phi_\beta$. Poniamo $A_\alpha = B/\Phi_\alpha$ e, per $\alpha \leq \beta$, sia $\varphi_{\beta\alpha}$ l'omomorfismo $\bar{b}_{\Phi_\beta} \mapsto \bar{b}_{\Phi_\alpha}$ di A_β in A_α. Allora $\varphi_{\alpha\alpha} = 1_{A_\alpha}$ e $\varphi_{\beta\alpha}\varphi_{\gamma\beta} = \varphi_{\gamma\alpha}$ per $\alpha \leq \beta \leq \gamma$. Sia ν_α l'omomorfismo $b \mapsto \bar{b}_{\Phi_\alpha}$ di B su A_α. Si ha $\varphi_{\beta\alpha}\nu_\beta = \nu_\alpha$ per $\alpha \leq \beta$. Ciò implica che esiste $\varprojlim(A_\alpha, \varphi_{\alpha\beta}) = (A, \{\eta_\alpha\})$. Inoltre abbiamo l'omomorfismo $\theta\colon B \to A$ tale che $\eta_\alpha\theta = \nu_\alpha$. Supponiamo ora che $\bigcap \Phi_\alpha = 1_B$. Siano $b, c \in B$ tali che $\theta b = \theta c$. Allora $\nu_\alpha b = \nu_\alpha c$, ossia $\bar{b}_{\Phi_\alpha} = \bar{c}_{\Phi_\alpha}$ per ogni α. Essendo $\bigcap \Phi_\alpha = 1_B$, otteniamo $b = c$. In questo caso l'omomorfismo θ di B in A è dunque un monomorfismo.

Esempio *Anello degli interi p-adici.* Come esempio dell'ultima costruzione, per ogni primo p definiremo l'importante anello degli interi p-adici come un limite inverso. Si osservi che questa costruzione è essenzialmente quella originaria di Hensel, anteriore al metodo basato sulle valutazioni oggi divenuto abituale (si veda il capitolo 9, p. 548 dell'originale).

Sia p un primo in $\mathbb{Z}$ e sia (p^k) l'ideale principale dei multipli di p^k per $k = 1, 2, \ldots$. Sia Φ_k la congruenza determinata da p^k: $a\Phi_k b$ significa $a \equiv b \pmod{p^k}$. Allora $\mathbb{Z}/\Phi_k = \mathbb{Z}/(p^k)$ è l'anello dei resti modulo p^k. Abbiamo $\Phi_l \subset \Phi_k$ per $l \geq k$ e $\bigcap \Phi_k = 1_\mathbb{Z}$. Possiamo formare il limite inverso degli anelli finiti $\mathbb{Z}/(p^k)$, che chiamiamo *anello $\mathbb{Z}_p$ degli interi p-adici*. Un elemento di $\mathbb{Z}_p$ è una successione di classi di resti (o classi laterali)

$$(a_1 + (p),\ a_2 + (p^2),\ a_3 + (p^3), \ldots)$$

in cui gli a_i sono interi e $a_k \equiv a_l \pmod{p^k}$ per $l \geq k$. Possiamo rappresentare questo elemento con la successione di interi $(a_1, a_2, \ldots)$ in cui $a_k \equiv a_l \pmod{p^k}$ per $k \leq l$. Due successioni siffatte

$(a_1, a_2, \ldots)$ e $(b_1, b_2, \ldots)$ rappresentano allora lo stesso elemento se e solo se $a_k \equiv b_k \pmod{p^k}$ per $k = 1, 2, \ldots$. L'addizione e la moltiplicazione di tali successioni si eseguono componente per componente. Per un rappresentante intero non negativo a possiamo scrivere $a = r_0 + r_1 p + \cdots + r_n p^n$, con $0 \leq r_i < p$. Possiamo quindi sostituire il rappresentante $(a_1, a_2, \ldots)$, in cui $a_k \equiv a_l \pmod{p^k}$ per $k \leq l$, con un rappresentante della forma $(r_0, r_0 + r_1 p, r_0 + r_1 p + r_2 p^2, \ldots)$, dove $0 \leq r_i < p$. In questo modo a ogni elemento di $\mathbb{Z}_p$ possiamo associare un *numero p-adico* univocamente determinato

$$r_0 + r_1 p + r_2 p^2 + \cdots , \tag{19}$$

con $0 \leq r_i < p$. L'addizione e la moltiplicazione di queste serie, corrispondenti alle operazioni in $\mathbb{Z}_p$, si ottengono eseguendo le operazioni sulle cifre r_i con i «riporti». Ad esempio, per $p = 5$ si ha

$$\begin{aligned}(1 + 2 \cdot 5 + 3 \cdot 5^2 + \cdots) + (3 + 3 \cdot 5 + 2 \cdot 5^2 + \cdots) \\ = 4 + 0 \cdot 5 + 1 \cdot 5^2 + \cdots , \\ (1 + 2 \cdot 5 + 3 \cdot 5^2 + \cdots)(3 + 3 \cdot 5 + 2 \cdot 5^2 + \cdots) \\ = 3 + 4 \cdot 5 + 3 \cdot 5^2 + \cdots .\end{aligned}$$

Esercizi

1. Sia I un insieme preordinato e sia $\mathbf{I}$ la categoria associata, definita nel modo consueto. Siano $\alpha \mapsto A_\alpha$, $\varphi_{\alpha\beta} \colon A_\alpha \to A_\beta$ per $\alpha \leq \beta$, e $\alpha \mapsto B_\alpha$, $\psi_{\alpha\beta} \colon B_\alpha \to B_\beta$, due funtori da $\mathbf{I}$ a una categoria $\mathbf{C}$ (come all'inizio del paragrafo). Denotiamoli rispettivamente con F e G. Una trasformazione naturale λ di F in G è un'applicazione $\alpha \mapsto \lambda_\alpha$, dove $\lambda_\alpha \colon A_\alpha \to B_\alpha$ e, per $\alpha \leq \beta$, $\psi_{\alpha\beta}\lambda_\alpha = \lambda_\beta \varphi_{\alpha\beta}$. Verificare che si ottiene una categoria $\mathbf{C}^\mathbf{I}$ prendendo come oggetti i funtori da $\mathbf{I}$ a $\mathbf{C}$ e, per ogni coppia F, G di tali funtori, definendo $\hom(F, G)$ come la classe delle trasformazioni naturali di F in G (che è un insieme). Definire inoltre 1_F e il prodotto delle trasformazioni naturali come a p. 25 dell'originale. (È così completata la definizione di $\mathbf{C}^\mathbf{I}$.) Se $A \in \operatorname{ob} \mathbf{C}$, si definisca $F_A \in \mathbf{C}^\mathbf{I}$ ponendo $\alpha \mapsto A$ e $\varphi_{\alpha\beta} = 1_A$ per $\alpha \leq \beta$. Si definisca un funtore da $\mathbf{C}$ a $\mathbf{C}^\mathbf{I}$ mandando A in F_A e ogni $f \colon A \to B$ nella trasformazione naturale dal funtore F_A al funtore F_B la cui componente, per ogni $\alpha \in I$, è il morfismo f da $A_\alpha = A$ a $B_\alpha = B$. Mostrare che un limite diretto $\varinjlim(A_\alpha, \varphi_{\alpha\beta})$ si può definire come un universale da F (quale oggetto di $\mathbf{C}^\mathbf{I}$) al funtore da $\mathbf{C}$ a $\mathbf{C}^\mathbf{I}$ che abbiamo appena definito.

2. Sia I l'insieme ordinato degli interi positivi (con l'ordine naturale) e, per $k \in I$, sia $A_k = I$ considerato come semigruppo rispetto all'addizione. Per $k \leq l$, sia φ_{lk} l'applicazione $x \mapsto 2^{l-k}x$ di A_l in A_k. Osservare che si tratta di un omomorfismo di semigruppi e che $\varphi_{mk} = \varphi_{lk}\varphi_{ml}$ e $\varphi_{ll} = 1_{A_l}$. Mostrare che, per questo funtore da $\mathbf{I}$ alla categoria dei semigruppi, il limite inverso non esiste in tale categoria.

3. Sia $\mathbb{Z}_p$ l'anello degli interi p-adici e si rappresentino i suoi elementi mediante successioni $a = (a_1, a_2, a_3, \ldots)$, con $a_k \in \mathbb{Z}$ e $a_k \equiv a_l \pmod{p^k}$ per $k \leq l$, come sopra. Mostrare che $a \mapsto (a, a, a, \ldots)$ è un monomorfismo di $\mathbb{Z}$ in $\mathbb{Z}_p$. In questo modo $\mathbb{Z}$ è immerso in $\mathbb{Z}_p$ e si può identificare a con $(a, a, a, \ldots)$. Mostrare che $\mathbb{Z}_p$ non ha divisori dello zero. Esso ammette quindi un campo delle frazioni $\mathbb{Q}_p$, detto *campo dei numeri p-adici*.

4. Sia $p \neq 2$ e sia a un intero (un elemento di $\mathbb{Z}$) tale che $a \not\equiv 0 \pmod{p}$ e la congruenza $x^2 \equiv a \pmod{p}$ ammetta soluzione. Mostrare che $x^2 = a$ ammette una soluzione in $\mathbb{Z}_p$.

5. Mostrare che gli elementi invertibili di $\mathbb{Z}_p$ sono quelli rappresentati da successioni $(a_1, a_2, \ldots)$ con $a_k \equiv a_l \pmod{p^k}$ per $k \leq l$, tali che $a_1 \not\equiv 0 \pmod{p}$.

6. Sia $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$, e si ponga $u = (a, a^p, a^{p^2}, \ldots)$. Mostrare che questa successione rappresenta un elemento di $\mathbb{Z}_p$ e che $u^{p-1} = 1$ in $\mathbb{Z}_p$. Dedurne che $\mathbb{Z}_p$ contiene $p-1$ radici distinte dell'unità.

2.6 Ultraprodotti

Il concetto di ultraprodotto di algebre e, più in generale, di strutture provviste sia di relazioni sia di operazioni ha un ruolo importante nella logica matematica, dove fu introdotto. Si è rivelato uno strumento utile anche in algebra. Per semplicità ci limiteremo agli ultraprodotti di Ω-algebre. Dobbiamo richiamare alcuni risultati sui filtri nelle algebre di Boole esposti in BAI. Benché ci occorrano soltanto per l'algebra di Boole dei sottoinsiemi di un insieme dato, conviene enunciarli per un'algebra di Boole qualunque, tanto più che il caso generale risulta concettualmente più semplice.

Ricordiamo che un'algebra di Boole è un reticolo con minimo 0 e massimo 1, distributivo e complementato. La prima di queste condizioni significa che $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, la seconda che per ogni a esiste nel reticolo un elemento a' tale che $a \vee a' = 1$ e $a \wedge a' = 0$. Per i risultati sulle algebre di Boole di cui avremo bisogno, rinviamo a BAI, pp. 474–480. Nell'algebra di Boole $\mathcal{P}(S)$ dei sottoinsiemi di un insieme S, $A \vee B$ e $A \wedge B$ sono rispettivamente l'unione e l'intersezione dei sottoinsiemi A, B di S. Inoltre $1 = S$, $0 = \varnothing$ e A' è il complementare di A in S.

Ricordiamo che un *filtro* in un'algebra di Boole B è un sottoinsieme non vuoto F chiuso rispetto a $\wedge$ e contenente, per ogni $u \in F$, tutti i $b \geq u$. Un filtro è *proprio* se e solo se $F \neq B$, ossia se e solo se $0 \notin F$. Un *ultrafiltro* è un filtro proprio F massimale, nel senso che nessun altro filtro proprio di B lo contiene strettamente. Un filtro F è un ultrafiltro se e solo se è proprio e, per ogni $a \in B$, contiene a oppure il suo complemento a' (che è unico).

Un'algebra di Boole si può trasformare in un anello in due modi. Nel primo si pone

$$a + b = (a \wedge b') \vee (a' \wedge b), \qquad ab = a \wedge b,$$

prendendo per zero e unità gli elementi 0 e 1 dati (BAI, p. 478). Nel secondo si passa per dualità alle operazioni

$$a +' b = (a \vee b') \wedge (a' \vee b), \qquad a \cdot' b = a \vee b.$$

L'elemento zero è $0' = 1$ e l'unità è $1' = 0$. Con questa scelta un filtro in B è semplicemente un ideale dell'anello booleano $(B, +', \cdot', 0', 1')$. Si ottiene così il seguente caso particolare del corollario 2 al teorema 2.5.

Corollario 3 (al teorema 2.5). *Ogni filtro proprio F in un'algebra di Boole è contenuto in un ultrafiltro.*

Siano ora $\{A_\alpha\}$ una famiglia di Ω-algebre indicizzata da un insieme I e F un filtro nell'insieme delle parti $\mathcal{P}(I)$. Se $S_1, S_2 \in F$, allora $S_1 \cap S_2 \in F$, e se $S \in F$ e $T \supseteq S$, allora $T \in F$. Nell'algebra $\prod A_\alpha$ definiamo una relazione $\sim_F$ ponendo $a \sim_F b$ quando l'insieme di indici

$$I_{a,b} = \{\alpha \in I \mid a_\alpha = b_\alpha\} \tag{20}$$

appartiene a F.

Affermiamo che si tratta di una congruenza su $\prod A_\alpha$. La relazione è evidentemente simmetrica, ed è riflessiva perché $I \in F$. Supponiamo che $a \sim_F b$ e $b \sim_F c$, cosicché $I_{a,b}$ e $I_{b,c}$ appartengono a F. Poiché $I_{a,b} \cap I_{b,c} \subseteq I_{a,c}$ e F è un filtro, si ha $I_{a,c} \in F$, quindi $a \sim_F c$. Pertanto $\sim_F$ è una relazione di equivalenza su $\prod A_\alpha$. Per mostrare che è una congruenza, occorre provare che, se

$\omega \in \Omega(n)$, $n \geq 1$, e gli elementi $a^{(1)}, \ldots, a^{(n)}, b^{(1)}, \ldots, b^{(n)} \in \prod A_\alpha$ soddisfano $a^{(i)} \sim_F b^{(i)}$ per $1 \leq i \leq n$, allora

$$\omega a^{(1)} \cdots a^{(n)} \sim_F \omega b^{(1)} \cdots b^{(n)}.$$

Per ipotesi $I_{a^{(i)},b^{(i)}} \in F$ per $1 \leq i \leq n$, dunque $\bigcap_{i=1}^n I_{a^{(i)},b^{(i)}} \in F$. Per ogni α appartenente a questa intersezione vale

$$\omega a_\alpha^{(1)} \cdots a_\alpha^{(n)} = \omega b_\alpha^{(1)} \cdots b_\alpha^{(n)}.$$

Pertanto

$$\bigcap_{i=1}^n I_{a^{(i)},b^{(i)}} \subseteq I_{\omega a^{(1)} \cdots a^{(n)},\, \omega b^{(1)} \cdots b^{(n)}}.$$

L'insieme a destra appartiene quindi a F, e $\mathcal{F} = \sim_F$ è una congruenza sull'algebra $\prod A_\alpha$. L'algebra quoziente $(\prod A_\alpha)/\mathcal{F}$ si chiama *prodotto ridotto modulo* F delle Ω-algebre A_α. Se F è un ultrafiltro, $(\prod A_\alpha)/\mathcal{F}$ si chiama un *ultraprodotto* degli A_α. Se inoltre tutti gli A_α coincidono con una stessa algebra A, si parla di un'*ultrapotenza* di A.

Gli ultraprodotti devono la loro importanza al fatto che ogni enunciato «elementare» valido in tutti gli A_α vale anche in ogni loro ultraprodotto. Per la formulazione precisa e la dimostrazione di questo risultato rinviamo ai testi di teoria dei modelli. Un ottimo riferimento è il capitolo «Ultraproducts for Algebraists» di Paul Eklof nel volume *Handbook of Mathematical Logic*, a cura di Jon Barwise, North Holland Company, 1977. La proposizione che segue illustra il risultato.

Proposizione 2.1. *Ogni ultraprodotto di anelli di divisione è un anello di divisione.*

Dimostrazione. Dire che D è un anello di divisione significa dire che D è un anello nel quale $1 \neq 0$ e ogni $a \neq 0$ ammette un inverso moltiplicativo bilatero. (È questo un esempio di enunciato elementare.) Supponiamo che i D_α, $\alpha \in I$, siano anelli di divisione. Vogliamo mostrare che ogni ultraprodotto $D = (\prod D_\alpha)/\mathcal{F}$ determinato da un ultrafiltro F è un anello di divisione. Sia $a \in \prod D_\alpha$ tale che $\bar{a} = \bar{a}_{\mathcal{F}} \neq 0$. Allora

$$I_a = I_{a,0} = \{\alpha \in I \mid a_\alpha = 0_{D_\alpha}\} \notin F.$$

Poiché F è un ultrafiltro, l'insieme complementare $I'_a = \{\alpha \in I \mid a_\alpha \neq 0_{D_\alpha}\}$ appartiene a F. Definiamo b ponendo $b_\alpha = a_\alpha^{-1}$ per $\alpha \in I'_a$ e $b_\alpha = 0$ altrimenti. L'insieme degli α tali che $a_\alpha b_\alpha = 1_{D_\alpha} = b_\alpha a_\alpha$ è proprio I'_a, dunque appartiene a F. Pertanto $\overline{ab} = 1 = \overline{ba}$ in $(\prod D_\alpha)/\mathcal{F}$, e D è un anello di divisione. □

Lo stesso ragionamento mostra che ogni ultraprodotto di campi è un campo. Si osservi che la dimostrazione sfrutta in modo essenziale l'ipotesi che F sia un ultrafiltro. Essa mostra infatti che, per un filtro F, $(\prod D_\alpha)/\mathcal{F}$ è un anello di divisione se e solo se il complementare di ogni insieme di indici S che non appartiene a F appartiene a F, dunque se e solo se F è un ultrafiltro.

Un altro risultato che si può dimostrare servendosi degli ultraprodotti è il seguente.

Proposizione 2.2 (A. Robinson). *Sia R un anello senza divisori dello zero che sia sottoanello di un prodotto diretto $\prod D_\alpha$ di anelli di divisione D_α. Allora R si può immergere in un anello di divisione.*

Dimostrazione (M. Rabin). Sia I l'insieme degli indici. Per ogni $a \in R \subseteq \prod D_\alpha$, sia $I'_a = \{\alpha \in I \mid a_\alpha \neq 0_{D_\alpha}\}$. Se $a \neq 0$, allora $I'_a \neq \varnothing$. Poniamo $B = \{I'_a \mid a \neq 0\}$. Se $a_1, \ldots, a_n$ sono elementi non nulli di R, allora $a_1 a_2 \cdots a_n \neq 0$, sicché $I'_{a_1 \cdots a_n} \in B$. Evidentemente $I'_{a_1 \cdots a_n} \subseteq \bigcap_{i=1}^n I'_{a_i}$. Pertanto B è una *base di filtro* in $\mathcal{P}(I)$, nel senso che $\varnothing \notin B$ e l'intersezione di ogni famiglia finita di elementi di B contiene un elemento di B. L'insieme G dei sottoinsiemi di I che contengono almeno uno degli insiemi I'_a di B è dunque un filtro in $\mathcal{P}(I)$ che non contiene $\varnothing$. Per il corollario 3 al teorema 2.5, G è contenuto in un ultrafiltro F di $\mathcal{P}(I)$. Poniamo

$D = (\prod D_\alpha)/\mathcal{F}$. Per la proposizione 2.1 è un anello di divisione. Abbiamo l'omomorfismo $a \mapsto \bar{a}_\mathcal{F}$ di R in D. Affermiamo che è un monomorfismo. Altrimenti esisterebbe un $a \neq 0$ in R tale che $I_a = \{\alpha \in I \mid a_\alpha = 0_{D_\alpha}\} \in F$. D'altra parte $I'_a = \{\alpha \in I \mid a_\alpha \neq 0_{D_\alpha}\} \in B \subseteq F$ è il complementare di I_a in I. Essendo un filtro, F conterrebbe $\varnothing = I_a \cap I'_a$, il che contraddice il fatto che F è un ultrafiltro. Dunque $a \mapsto \bar{a}_\mathcal{F}$ è un monomorfismo e dà un'immersione di R in un anello di divisione. □

Esercizi.

1. Usare l'esercizio 2 del § 2.4 e la proposizione 2.2 per dimostrare che $\mathbb{Z}$ si può immergere in un campo.

2. Se a è un elemento di un'algebra di Boole, il sottoinsieme $F_a = \{x \mid x \geq a\}$ è un filtro, detto *filtro principale determinato da* a. Siano I un insieme, S un suo sottoinsieme e F_S il filtro principale determinato da S. Mostrare che, se $\mathcal{F}_S$ è la congruenza in $\prod_{\alpha\in I} A_\alpha$ determinata da F_S, allora
$$\left(\prod_{\alpha\in I} A_\alpha\right)/\mathcal{F}_S \cong \prod_{\beta\in S} A_\beta.$$

3. Mostrare che, se I è un insieme infinito, un ultrafiltro in $\mathcal{P}(I)$ è non principale se e solo se contiene il filtro costituito dai complementari dei sottoinsiemi finiti di I.

2.7 Le Ω-algebre libere

Sia $\Omega = \bigcup_{n=0}^{\infty} \Omega(n)$ un insieme di simboli di operazione, dove $\Omega(n)$ è l'insieme dei simboli n-ari, e sia X un insieme non vuoto. Sia Y l'unione disgiunta di Ω e X. Formiamo l'unione disgiunta $W(\Omega, X)$ degli insiemi $Y^{(m)}$, $m \geq 1$, dove $Y^{(m)}$ è l'insieme delle m-uple $(y_1, y_2, \ldots, y_m)$, $y_i \in Y$. Per semplicità scriviamo $y_1 y_2 \cdots y_m$ per $(y_1, y_2, \ldots, y_m)$. Questa notazione suggerisce di chiamare gli elementi di $W(\Omega, X)$ *parole* nell'alfabeto Y. Definiamo *grado* della parola $w = y_1 y_2 \cdots y_m$ il numero m. È utile introdurre anche la *valenza* di una parola. Poniamo $v(x) = 1$ per $x \in X$, $v(\omega) = 1 - n$ per $\omega \in \Omega(n)$, e

$$v(y_1 \cdots y_m) = \sum_{i=1}^{m} v(y_i), \qquad y_i \in Y.$$

Per esempio, la parola
$$w = \omega_1^{(1)} \omega_2^{(1)} x_1 \omega_3^{(2)} x_2 x_3 \omega_4^{(5)},$$
dove gli apici dei simboli di operazione ne indicano l'arità, ha grado 7 e valenza -2.

Introduciamo in $W(\Omega, X)$ la moltiplicazione per giustapposizione ponendo

$$(y_1 \cdots y_m)(y'_1 \cdots y'_r) = y_1 \cdots y_m y'_1 \cdots y'_r.$$

Il prodotto è evidentemente associativo, sicché per indicare prodotti di più di due parole non occorrono parentesi.

Usiamo questo prodotto associativo per definire una struttura di Ω-algebra su $W(\Omega, X)$. A ogni $\omega \in \Omega(0)$ facciamo corrispondere come elemento di $W(\Omega, X)$ la lettera di Y che rappresenta ω. Per $\omega \in \Omega(n)$, $n \geq 1$, e $w_1, w_2, \ldots, w_n \in W(\Omega, X)$, definiamo il risultato dell'azione di ω sulla n-upla $(w_1, w_2, \ldots, w_n)$ come la parola $\omega w_1 w_2 \cdots w_n$. In tal modo $W(\Omega, X)$ diventa una Ω-algebra. Sia ora $F(\Omega, X)$ la sottoalgebra della Ω-algebra $W(\Omega, X)$ generata dal sottoinsieme X. Mostreremo che si tratta di una Ω-algebra libera generata da X, nel senso che ogni applicazione da X in una Ω-algebra A si estende in modo unico a un omomorfismo da $F(\Omega, X)$ in A.

Stabiliamo dapprima un criterio di appartenenza a $F(\Omega, X)$ e una proprietà di fattorizzazione unica.

Lemma. *Una parola w appartiene a $F(\Omega, X)$ se e solo se ha valenza 1 e ogni suo fattore destro w' (cioè $w = w''w'$ oppure $w' = w$) ha valenza positiva. Gli elementi di grado 1 di $F(\Omega, X)$ formano l'insieme $X \cup \Omega(0)$. Se $w \in F(\Omega, X)$ ha grado maggiore di 1, allora w comincia con un simbolo $\omega \in \Omega(n)$, $n \geq 1$, e si può scrivere in uno e un solo modo come $\omega w_1 w_2 \cdots w_n$, con $w_i \in F(\Omega, X)$.*

Dimostrazione. L'affermazione riguardante gli elementi di grado 1 di $F(\Omega, X)$ è chiara. Per ciascuno di tali elementi w si ha $v(w) = 1$ e w stesso è il suo unico fattore destro, dunque le condizioni sulle valenze sono soddisfatte. Sia ora $w \in F(\Omega, X)$ di grado maggiore di 1. Dal procedimento induttivo del § 2.2 per costruire gli elementi della sottoalgebra di una Ω-algebra generata da un sottoinsieme, risulta che $w = \omega w_1 w_2 \cdots w_n$, con $\omega \in \Omega(n)$ e $w_i \in F(\Omega, X)$ per ogni i. Per induzione sul grado possiamo supporre che tutti i w_i soddisfino le condizioni sulle valenze. Ne segue che anche $w = \omega w_1 w_2 \cdots w_n$ le soddisfa.

Viceversa, sia w una parola che soddisfi tali condizioni. Se ha grado 1, allora w è un elemento $x \in X$ oppure un simbolo $\omega \in \Omega(0)$. In entrambi i casi $w \in F(\Omega, X)$. Supponiamo che w abbia grado maggiore di 1. Le condizioni sulle valenze implicano che w comincia con un simbolo $\omega \in \Omega(n)$, $n \geq 1$. Quindi $w = \omega y_1 y_2 \cdots y_m$, con $y_i \in Y$. Per $1 \leq i \leq n$, sia u_i il fattore destro di $u = y_1 y_2 \cdots y_m$ di grado massimo fra quelli che hanno valenza i. Per esempio, sia

$$w = \omega_1^{(4)} x_1 x_2 x_3 \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)},$$

dove gli apici indicano le arità dei simboli di operazione. Allora

$$u = x_1 x_2 x_3 \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}.$$

Scrivendo sopra ciascun simbolo la valenza del fattore destro che comincia con esso, otteniamo

$$u = \overset{4}{x_1}\overset{3}{x_2}\overset{2}{x_3}\overset{1}{\omega_2^{(2)}}\overset{2}{x_4}\overset{1}{\omega_3^{(4)}}\overset{4}{x_5}\overset{3}{x_6}\overset{2}{\omega_4^{(0)}}\overset{1}{\omega_5^{(0)}}.$$

In questo esempio $u_1 = \omega_2^{(2)} x_4 \omega_3^{(4)} x_5 x_6 \omega_4^{(0)} \omega_5^{(0)}$, $u_2 = x_3 u_1$, $u_3 = x_2 u_2$, $u = u_4 = x_1 u_3$. In generale $u_n = u = y_1 y_2 \cdots y_m$ e u_{i-1} è un fattore destro di u_i per $2 \leq i \leq n$. Possiamo dunque scrivere $u_1 = w_n$, $u_2 = w_{n-1} u_1$, $u_3 = w_{n-2} u_2$, e così via, dove i w_i soddisfano le condizioni sulle valenze. Si ha quindi

$$w = \omega y_1 y_2 \cdots y_m = \omega w_1 w_2 \cdots w_n.$$

Poiché ciascun w_i ha grado minore di w, per induzione sul grado possiamo supporre $w_i \in F(\Omega, X)$. Allora $w = \omega w_1 w_2 \cdots w_n \in F(\Omega, X)$. Abbiamo così provato la sufficienza delle condizioni sulle valenze.

Supponiamo ora di avere una seconda fattorizzazione $w = \omega w'_1 w'_2 \cdots w'_n$, con $w'_i \in F(\Omega, X)$. La valenza di w'_n è 1, quella di $w'_{n-1} w'_n$ è 2, quella di $w'_{n-2} w'_{n-1} w'_n$ è 3, e così via. Per la definizione degli u_i,

$$\deg(w'_i w'_{i+1} \cdots w'_n) \leq \deg(w_i w_{i+1} \cdots w_n), \qquad 1 \leq i \leq n.$$

Se vale l'uguaglianza per ogni i, allora $w'_1 = w_1$, $w'_2 = w_2, \ldots, w'_n = w_n$. Supponiamo dunque che per qualche i si abbia $\deg(w'_i \cdots w'_n) < \deg(w_i \cdots w_n)$, e scegliamo minimo un tale i. Chiaramente $i > 1$ e $\deg(w'_{i-1} \cdots w'_n) = \deg(w_{i-1} \cdots w_n)$, sicché $w'_{i-1} \cdots w'_n = w_{i-1} \cdots w_n$. Allora $\deg(w'_1 \cdots w'_{i-1}) > \deg(w_1 \cdots w_{i-1})$ e $w'_{i-1} = w_{i-1} z$ per una parola z. Poiché $v(w'_{i-1}) = 1 = v(w_{i-1})$, si ottiene $v(z) = 0$, in contraddizione con le condizioni sulle valenze che $w'_{i-1} \in F(\Omega, X)$ deve soddisfare. □

Possiamo ora dimostrare la proprietà che esprime il carattere libero di $F(\Omega, X)$.

Teorema 2.9. *Ogni applicazione f da X in una Ω-algebra A si estende in modo unico a un omomorfismo $\bar{f}$ da $F(\Omega, X)$ in A.*

Dimostrazione. Per $x \in X$ poniamo $\bar{f}(x) = f(x)$, e per $\omega \in \Omega(0)$, che è un elemento di $F(\Omega, X)$, poniamo $\bar{f}(\omega) = \omega_A$. I rimanenti elementi di $F(\Omega, X)$ hanno la forma $\omega w_1 w_2 \cdots w_n$, con $w_i \in F(\Omega, X)$, $\omega \in \Omega(n)$, $n \geq 1$. Supponiamo di aver già definito $\bar{f}(w')$ per tutte le parole w' di grado minore di $\deg(\omega w_1 \cdots w_n)$. Allora $\bar{f}(w_i)$ è definito per ogni i, ed estendiamo la definizione ponendo

$$\bar{f}(\omega w_1 \cdots w_n) = \omega \bar{f}(w_1) \cdots \bar{f}(w_n).$$

Questo procedimento induttivo definisce $\bar{f}$ su tutta $F(\Omega, X)$. È chiaro che $\bar{f}$ è un omomorfismo. Poiché X genera $F(\Omega, X)$, $\bar{f}$ è unico (si veda l'esercizio 3 del § 2.3). □

Il teorema 2.9 si può anche esprimere in termini categoriali. Consideriamo il funtore dimenticante F dalla categoria Ω-**alg** a **Set**, che associa a ogni Ω-algebra il suo insieme sostegno e a ogni omomorfismo di algebre la corrispondente applicazione fra insiemi. Dalla definizione di universale (§ 1.7) risulta allora che, per un insieme non vuoto X, la coppia $(F(\Omega, X), i)$, dove i è l'iniezione di X in $F(\Omega, X)$, è un universale da X al funtore F. Il fatto che $(F(\Omega, X), i)$ sia un universale ne implica l'unicità nel senso consueto.

2.8 Varietà

Il concetto di Ω-algebra libera $F(\Omega, X)$ permette di definire le identità per le Ω-algebre. Sia (w_1, w_2) una coppia di elementi di $F(\Omega, X)$ per un certo insieme X. Diciamo che una Ω-algebra A *soddisfa l'identità* $w_1 = w_2$ (ovvero che $w_1 = w_2$ è una *legge* in A) se $f(w_1) = f(w_2)$ per ogni omomorfismo f di $F(\Omega, X)$ in A. Sia S un sottoinsieme di $F(\Omega, X) \times F(\Omega, X)$. La classe delle Ω-algebre che soddisfano le identità $w_1 = w_2$ per ogni $(w_1, w_2) \in S$ si chiama *varietà di Ω-algebre $V(S)$ definita da S*, o anche *classe equazionale definita da S*. Per esempio, siano $\omega^{(2)}, \omega^{(1)}, \omega^{(0)}$ simboli di operazione rispettivamente binaria, unaria e nullaria, e si ponga $\Omega = \{\omega^{(2)}, \omega^{(1)}, \omega^{(0)}\}$ e $X = \{x_1, x_2, x_3\}$. La classe dei gruppi è definita dal seguente sottoinsieme di $F(\Omega, X) \times F(\Omega, X)$:

$$\begin{gathered}(\omega^{(2)}\omega^{(2)}x_1x_2x_3,\ \omega^{(2)}x_1\omega^{(2)}x_2x_3),\\ (\omega^{(2)}\omega^{(0)}x_1,\ x_1),\\ (\omega^{(2)}x_1\omega^{(0)},\ x_1),\\ (\omega^{(2)}x_1\omega^{(1)}x_1,\ \omega^{(0)}),\\ (\omega^{(2)}\omega^{(1)}x_1x_1,\ \omega^{(0)}).\end{gathered}$$

Infatti, dire che A è una Ω-algebra per l'Ω indicato significa che A è munita di una composizione binaria, una unaria e una nullaria. Se denotiamo il loro effetto in A rispettivamente con ab, a^{-1} e 1, dire che A appartiene a $V(S)$, per l'insieme S delle cinque coppie elencate, equivale ad affermare che in A valgono le leggi

$$(ab)c = a(bc), \quad 1a = a, \quad a1 = a, \quad aa^{-1} = 1, \quad a^{-1}a = 1.$$

Ciò significa semplicemente che A è un gruppo. Dunque $V(S)$ è la varietà dei gruppi. In modo analogo si vede che le classi dei monoidi, dei reticoli, degli anelli, degli anelli commutativi e delle algebre di Boole sono varietà.

Si vede facilmente che nella definizione delle varietà si può supporre, senza perdita di generalità, che X sia un insieme infinito numerabile $X_0 = \{x_1, x_2, \ldots\}$. D'ora in avanti faremo questa scelta. Sia $V(S)$ la varietà di Ω-algebre definita dal sottoinsieme S di $F(\Omega, X_0) \times F(\Omega, X_0)$. Se

$A \in V(S)$, è chiaro che ogni sottoalgebra di A appartiene a $V(S)$. Inoltre appartiene a $V(S)$ ogni immagine omomorfa $\overline{A}$ di A. Per vederlo osserviamo che ogni omomorfismo $\bar{f}$ di $F(\Omega, X_0)$ in $\overline{A}$ si può sollevare a un omomorfismo f di $F(\Omega, X_0)$ in A, nel senso seguente. Dato un omomorfismo suriettivo λ di A su $\overline{A}$, esiste un omomorfismo $f\colon F(\Omega, X_0) \to A$ tale che $\bar{f} = \lambda f$. Per definirlo scegliamo, per ogni $i = 1, 2, \ldots$, un elemento $a_i \in A$ tale che $\lambda(a_i) = \bar{f}(x_i)$, e prendiamo per f l'omomorfismo di $F(\Omega, X_0)$ in A che estende l'applicazione $x_i \mapsto a_i$ da X_0 in A. Allora $\lambda f(x_i) = \lambda(a_i) = \bar{f}(x_i)$. Poiché X_0 genera $F(\Omega, X_0)$, gli omomorfismi λf e $\bar{f}$ di $F(\Omega, X_0)$ in $\overline{A}$ coincidono. Sia ora $(w_1, w_2) \in S$, sia $\bar{f}$ un qualsiasi omomorfismo di $F(\Omega, X_0)$ in $\overline{A}$ e sia f un omomorfismo di $F(\Omega, X_0)$ in A tale che $\lambda f = \bar{f}$. Allora

$$\bar{f}(w_1) = \lambda f(w_1) = \lambda f(w_2) = \bar{f}(w_2).$$

Dunque $\overline{A}$ soddisfa l'identità $w_1 = w_2$ per ogni $(w_1, w_2) \in S$, e pertanto $\overline{A} \in V(S)$.

Osserviamo poi che se $\{A_\alpha \mid \alpha \in I\}$ è una famiglia indicizzata di algebre in $V(S)$, allora $\prod A_\alpha \in V(S)$. Infatti, indichiamo con p_α la proiezione di $A = \prod A_\alpha$ su A_α. Per ogni omomorfismo f di $F(\Omega, X_0)$ in A si ha $p_\alpha f(w_1) = p_\alpha f(w_2)$ per ogni $(w_1, w_2) \in S$. Segue $f(w_1) = f(w_2)$, quindi $A \in V(S)$.

Ogni varietà $V(S)$ definisce una sottocategoria piena $\mathbf{V}(S)$ di Ω-**alg**. Consideriamo ora alcune proprietà importanti di queste categorie, cominciando dalla seguente.

Proposizione 2.3. *Un morfismo in $\mathbf{V}(S)$ è un monomorfismo se e solo se è un'applicazione iniettiva.*

Dimostrazione. La dimostrazione generalizza immediatamente quella data a p. 17 dell'originale nel caso particolare della categoria degli anelli. Se f è un omomorfismo iniettivo di A in B, con $A, B \in V(S)$, allora f è un monomorfismo. Supponiamo ora che $f\colon A \to B$ non sia iniettivo. Consideriamo la sottoalgebra $\Phi = f^{-1}f$ di $A \times A$, ossia il nucleo di f. Si ha $\Phi \in V(S)$. Siano p e p' le restrizioni a Φ delle proiezioni $(a, a') \mapsto a$ e $(a, a') \mapsto a'$. Poiché $(a, a') \in \Phi$ equivale a $f(a) = f(a')$, abbiamo $fp = fp'$. D'altra parte, poiché f non è iniettivo, esiste una coppia (a, a') tale che $f(a) = f(a')$ e $a \neq a'$. Allora $(a, a') \in \Phi$ e $p(a, a') \neq p'(a, a')$. Poiché $fp = fp'$, questo mostra che f non è un monomorfismo in $\mathbf{V}(S)$. □

Ricordiamo che nella categoria degli anelli gli epimorfismi possono non essere suriettivi. L'analogo della proposizione 2.3 per gli epimorfismi non vale dunque in generale.

Sia $\mathbf{C}$ una sottocategoria di Ω-**alg** e sia X un insieme. Chiamiamo *algebra libera per $\mathbf{C}$ determinata da X* un universale da X al funtore dimenticante da $\mathbf{C}$ a **Set**. Si ha la seguente estensione del teorema 2.9 alle varietà.

Teorema 2.10. *Sia $\mathbf{V}(S)$ la categoria definita da una varietà $V(S)$ e sia X un insieme non vuoto. Esiste un'algebra libera per $\mathbf{V}(S)$ determinata da X.*

Dimostrazione. Consideriamo le algebre libere $F(\Omega, X)$ e $F(\Omega, X_0)$, dove $X_0 = \{x_1, x_2, \ldots\}$. Allora S è un sottoinsieme di $F(\Omega, X_0) \times F(\Omega, X_0)$. Se φ è un omomorfismo di $F(\Omega, X_0)$ in $F(\Omega, X)$ e $(w_1, w_2) \in S$, allora

$$(\varphi(w_1), \varphi(w_2)) \in F(\Omega, X) \times F(\Omega, X).$$

Indichiamo con $\Phi(S)$ la congruenza su $F(\Omega, X)$ generata da tutti gli elementi $(\varphi(w_1), \varphi(w_2))$ ottenuti facendo variare φ fra tutti questi omomorfismi e (w_1, w_2) fra tutte le coppie di S. Poniamo $F_{V(S)}(\Omega, X) = F(\Omega, X)/\Phi(S)$ e sia ν l'omomorfismo canonico $a \mapsto a^{\Phi(S)}$ di $F(\Omega, X)$ su $F_{V(S)}(\Omega, X)$. Affermiamo che $F_{V(S)}(\Omega, X)$, insieme con la restrizione i di ν a X, costituisce una $\mathbf{V}(S)$-algebra libera per l'insieme X.

Mostriamo anzitutto che $F_{V(S)}(\Omega, X) \in V(S)$. Sia $\bar{\varphi}$ un omomorfismo di $F(\Omega, X_0)$ in $F_{V(S)}(\Omega, X)$. Per quanto dimostrato sopra, esiste un omomorfismo $\varphi\colon F(\Omega, X_0) \to F(\Omega, X)$ tale

che $\bar{\varphi} = \nu\varphi$. Se $(w_1, w_2) \in S$, allora $(\varphi(w_1), \varphi(w_2)) \in \Phi(S)$, perciò $\nu\varphi(w_1) = \nu\varphi(w_2)$. Dunque $\bar{\varphi}(w_1) = \bar{\varphi}(w_2)$. Poiché ciò vale per ogni $(w_1, w_2) \in S$ e per ogni omomorfismo $\bar{\varphi}$ di $F(\Omega, X_0)$ in $F_{V(S)}(\Omega, X)$, segue che $F_{V(S)}(\Omega, X) \in V(S)$.

Supponiamo ora che g sia un'applicazione di X in un'algebra $A \in V(S)$. Allora g si estende a un omomorfismo $\bar{g}$ di $F(\Omega, X)$ in A. Se φ è un omomorfismo di $F(\Omega, X_0)$ in $F(\Omega, X)$, allora $\bar{g}\varphi$ è un omomorfismo di $F(\Omega, X_0)$ in A. Quindi, se $(w_1, w_2) \in S$, si ha $\bar{g}\varphi(w_1) = \bar{g}\varphi(w_2)$. La coppia $(\varphi(w_1), \varphi(w_2))$ appartiene dunque al nucleo $\ker \bar{g}$. Questo vale per ogni $(w_1, w_2) \in S$ e ogni omomorfismo φ di $F(\Omega, X_0)$ in $F(\Omega, X)$, perciò $\Phi(S) \subseteq \ker \bar{g}$. Esiste quindi un unico omomorfismo f di $F_{V(S)}(\Omega, X) = F(\Omega, X)/\Phi(S)$ in A che rende commutativo il primo dei diagrammi seguenti. Per $i = \nu|_X$ si ottiene allora il secondo diagramma commutativo:

$$\begin{array}{ccc} F(\Omega, X) & \xrightarrow{\ \nu\ } & F_{V(S)}(\Omega, X) \\ {\scriptstyle \bar{g}}\downarrow & \swarrow_{f} & \\ A & & \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\ i\ } & F_{V(S)}(\Omega, X) \\ {\scriptstyle g}\downarrow & \swarrow_{f} & \\ A & & \end{array}$$

Poiché X genera $F(\Omega, X)$, la sua immagine $i(X)$ genera $F_{V(S)}(\Omega, X)$. Pertanto f è unico e $(F_{V(S)}(\Omega, X), i)$ è un'algebra libera per $\mathbf{V}(S)$ determinata da X. □

Corollario. *Ogni algebra di una varietà è immagine omomorfa di un'algebra libera.*

Dimostrazione. Sia X un insieme di generatori dell'algebra data $A \in V(S)$. Per esempio, si può prendere $X = A$. Si ha allora un omomorfismo di $F_{V(S)}(\Omega, X)$ in A la cui immagine contiene X. Poiché X genera A, l'immagine è A. Abbiamo dunque un omomorfismo suriettivo di $F_{V(S)}(\Omega, X)$ su A. □

Abbiamo osservato che, data una famiglia indicizzata $\{A_\alpha \mid \alpha \in I\}$ di algebre in una varietà $V(S)$, si ha $\prod A_\alpha \in V(S)$. Ne segue che in $\mathbf{V}(S)$ esiste il prodotto di qualsiasi famiglia indicizzata di oggetti. Questo vale anche per i coprodotti.

Teorema 2.11. *In $\mathbf{V}(S)$ esiste il coprodotto di ogni famiglia indicizzata $\{A_\alpha \mid \alpha \in I\}$ di algebre appartenenti a $V(S)$.*

Dimostrazione. Riduciamo la dimostrazione al caso delle algebre libere in $\mathbf{V}(S)$. Mostreremo che, se il coprodotto esiste per una famiglia $\{A_\alpha \mid \alpha \in I\}$ di algebre di $V(S)$, allora esiste anche per ogni famiglia $\{\overline{A}_\alpha \mid \alpha \in I\}$ in cui $\overline{A}_\alpha$ sia immagine omomorfa di A_α. Sia $\{A, i_\alpha\} = \coprod A_\alpha$ in $\mathbf{V}(S)$ e sia η_α un omomorfismo suriettivo di A_α su $\overline{A}_\alpha$ per ogni $\alpha \in I$. Sia Θ_α il nucleo di η_α e indichiamo con $i_\alpha\Theta_\alpha$ il sottoinsieme di $A \times A$ costituito dalle coppie $(i_\alpha(a_\alpha), i_\alpha(b_\alpha))$ per $(a_\alpha, b_\alpha) \in \Theta_\alpha$. Sia Θ la congruenza su A generata da $\bigcup_\alpha i_\alpha\Theta_\alpha$ e poniamo $\overline{A} = A/\Theta$ e $i'_\alpha = \nu i_\alpha$, dove ν è l'omomorfismo canonico di A su $\overline{A} = A/\Theta$. Allora i'_α è un omomorfismo di A_α in $\overline{A}$. Se $(a_\alpha, b_\alpha) \in \Theta_\alpha$, si ha $(i_\alpha(a_\alpha), i_\alpha(b_\alpha)) \in \Theta$, dunque $\nu i_\alpha(a_\alpha) = \nu i_\alpha(b_\alpha)$. Pertanto Θ_α è contenuta nel nucleo di $i'_\alpha = \nu i_\alpha$. Esiste quindi un unico omomorfismo $\bar{i}_\alpha \colon \overline{A}_\alpha \to \overline{A}$ che rende commutativo il diagramma

$$\begin{array}{ccc} A_\alpha & \xrightarrow{\ i_\alpha\ } & A \\ {\scriptstyle \eta_\alpha}\downarrow & & \downarrow{\scriptstyle \nu} \\ \overline{A}_\alpha & \xrightarrow[\ \bar{i}_\alpha\ ]{} & \overline{A} \end{array}$$

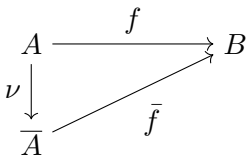
Si ha $\overline{A} \in V(S)$ poiché $\overline{A}$ è un'immagine omomorfa di $A \in V(S)$.

Affermiamo che $\{\overline{A}, \bar{i}_\alpha\} = \coprod \overline{A}_\alpha$. Sia $B \in V(S)$ e, per ogni $\alpha \in I$, sia $\bar{f}_\alpha$ un omomorfismo di $\overline{A}_\alpha$ in B. Allora $f_\alpha = \bar{f}_\alpha\eta_\alpha$ è un omomorfismo di A_α in B il cui nucleo contiene Θ_α. Poiché $\{A, i_\alpha\} = \coprod A_\alpha$, esiste un unico omomorfismo $f \colon A \to B$ tale che $fi_\alpha = f_\alpha$ per ogni $\alpha \in I$. Se

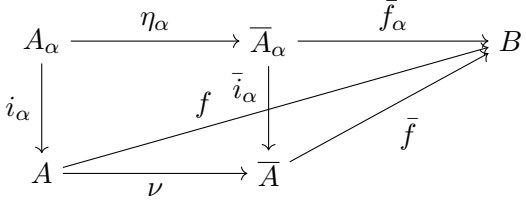
$(a_\alpha, b_\alpha) \in \Theta_\alpha$, allora $\eta_\alpha(a_\alpha) = \eta_\alpha(b_\alpha)$ e

$$f_\alpha(a_\alpha) = \bar{f}_\alpha\eta_\alpha(a_\alpha) = \bar{f}_\alpha\eta_\alpha(b_\alpha) = f_\alpha(b_\alpha).$$

Quindi $fi_\alpha(a_\alpha) = fi_\alpha(b_\alpha)$ e $i_\alpha\Theta_\alpha$ è contenuto nel nucleo di f. Ciò vale per ogni α, e Θ è la congruenza su A generata da $\bigcup_\alpha i_\alpha\Theta_\alpha$. Ne segue che Θ è contenuta nel nucleo di f. Esiste pertanto un unico omomorfismo $\bar{f}\colon \overline{A} \to B$ che rende commutativo il diagramma



Abbiamo ora il diagramma



nel quale sono commutativi il rettangolo e i triangoli $A\overline{A}B$ e $A_\alpha AB$. Seguendo i due cammini nel diagramma troviamo

$$\bar{f}\bar{i}_\alpha\eta_\alpha = \bar{f}\nu i_\alpha = fi_\alpha = f_\alpha = \bar{f}_\alpha\eta_\alpha.$$

Poiché η_α è suriettivo, e dunque un epimorfismo, segue $\bar{f}\bar{i}_\alpha = \bar{f}_\alpha$ per ogni $\alpha \in I$. Per dimostrare l'unicità di $\bar{f}$, osserviamo che, se $\bar{f}\colon \overline{A} \to B$ soddisfa $\bar{f}_\alpha = \bar{f}\bar{i}_\alpha$ per ogni α e poniamo $f = \bar{f}\nu$, nel diagramma precedente commutano il rettangolo e i triangoli $A\overline{A}B$ e $\overline{A}_\alpha\overline{A}B$. Anche il triangolo $A_\alpha AB$ è commutativo, poiché

$$f_\alpha = \bar{f}_\alpha\eta_\alpha = \bar{f}\bar{i}_\alpha\eta_\alpha = \bar{f}\nu i_\alpha = fi_\alpha.$$

Poiché $\{A, i_\alpha\} = \coprod A_\alpha$, ne segue l'unicità di f. Dalla suriettività di ν segue l'unicità di $\bar{f}$. Pertanto $\{\overline{A}, \bar{i}_\alpha\} = \coprod \overline{A}_\alpha$.

Il risultato appena dimostrato, insieme con il fatto che ogni $A_\alpha \in V(S)$ è immagine omomorfa di un'algebra libera in $\mathbf{V}(S)$, mostra che basta dimostrare il teorema per algebre libere $A_\alpha = F_{V(S)}(\Omega, X_\alpha)$. Formiamo a questo scopo $A = F_{V(S)}(\Omega, X)$, dove $X = \bigsqcup_\alpha X_\alpha$ è l'unione disgiunta degli X_α. Indichiamo con la stessa lettera i le applicazioni $X \to A$ e $X_\alpha \to A_\alpha$ che figurano nella definizione delle algebre libere in $\mathbf{V}(S)$, e sia i_α l'omomorfismo $A_\alpha \to A$ corrispondente all'inclusione di X_α in X. Dunque $i_\alpha i(x_\alpha) = i(x_\alpha)$. Siano ora dati omomorfismi $f_\alpha\colon A_\alpha \to B$, con $B \in \mathbf{V}(S)$. Sia g l'applicazione di X in B tale che $g(x_\alpha) = f_\alpha i(x_\alpha)$, $\alpha \in I$. Si ha allora un omomorfismo f di A in B tale che $fi(x) = g(x)$ per $x \in X$. Quindi

$$fi(x_\alpha) = g(x_\alpha) = f_\alpha i(x_\alpha) = fi_\alpha i(x_\alpha).$$

Poiché gli elementi $i(x_\alpha)$ generano A_α, abbiamo $fi_\alpha = f_\alpha$ per ogni $\alpha \in I$. Poiché gli elementi $i(x_\alpha)$, per $x_\alpha \in X_\alpha$ e $\alpha \in I$, generano A, l'omomorfismo f è unico. Dunque $\{A, i_\alpha\} = \coprod A_\alpha$. □

La costruzione precedente del coprodotto $\coprod A_\alpha = \{A, i_\alpha\}$ in una varietà mostra che A è generata dalle immagini $i_\alpha(A_\alpha)$. Lo si può vedere anche direttamente dalla definizione di coprodotto di algebre. È di particolare interesse il caso in cui gli i_α sono iniettivi. In tal caso chiameremo

$\coprod A_\alpha$ il *prodotto libero*. Un'utile condizione sufficiente affinché il coprodotto sia un prodotto libero è fornita dalla proposizione seguente.

Proposizione 2.4. *Sia $\coprod A_\alpha$ un coprodotto di Ω-algebre in una categoria $\mathbf{C}$. Se ogni A_α ha una sottoalgebra $\{\varepsilon_\alpha\}$ costituita da un solo elemento, allora $\coprod A_\alpha$ è un prodotto libero.*

Si osservi che la proposizione si applica alle categorie dei monoidi e dei gruppi, ma non a quella degli anelli.

Dimostrazione. Per ogni Ω-algebra A, l'applicazione di A in A_β che manda ogni elemento di A in ε_β è un omomorfismo. Se $\alpha \neq \beta$, sia $f_{\alpha\beta}$ questo omomorfismo da $A = A_\alpha$ in A_β, e si ponga $f_{\beta\beta} = 1_{A_\beta}$. Applicando la definizione di coprodotto si ottiene un omomorfismo $f_\beta \colon A = \coprod A_\alpha \to A_\beta$ tale che $f_{\alpha\beta} = f_\beta i_\alpha$ per ogni $\alpha \in I$. Poiché $f_{\beta\beta}$ è iniettivo, anche i_β è iniettivo. Dunque ogni i_β è iniettivo e $\coprod A_\alpha$ è un prodotto libero. □

Esercizi

1. Dare un esempio nella categoria degli anelli in cui il coprodotto non sia un prodotto libero.

2. Sia $F_{\mathbf{C}}(\Omega, X)$ un'algebra libera per una categoria $\mathbf{C}$ di Ω-algebre, determinata da un insieme X. Mostrare che, se λ è un omomorfismo suriettivo da A su $\overline{A}$, con $A \in \operatorname{ob}\mathbf{C}$, e $\bar{f}$ è un omomorfismo di $F_{\mathbf{C}}(\Omega, X)$ in $\overline{A}$, allora esiste un omomorfismo f di $F_{\mathbf{C}}(\Omega, X)$ in A tale che $\bar{f} = \lambda f$.

3. Sia $F_{\mathbf{C}}(\Omega, X)$ come nell'esercizio 2. Provare quanto segue.

   (i) $F_{\mathbf{C}}(\Omega, X)$ è generata da $i(X)$, dove i è l'applicazione canonica di X in $F_{\mathbf{C}}(\Omega, X)$.

   (ii) Se Y è un sottoinsieme non vuoto di X, la sottoalgebra di $F_{\mathbf{C}}(\Omega, X)$ generata da $i(Y)$, insieme con la restrizione di i a Y, considerata come applicazione nella sottoalgebra indicata, costituisce una $\mathbf{C}$-algebra libera determinata da Y.

   (iii) Sia X' un secondo insieme e sia $F_{\mathbf{C}}(\Omega, X')$ una $\mathbf{C}$-algebra libera per X'. Mostrare che se $|X| = |X'|$, allora $F_{\mathbf{C}}(\Omega, X)$ e $F_{\mathbf{C}}(\Omega, X')$ sono isomorfe.

4. Mostrare che, se $V(S)$ contiene un'algebra A con $|A| > 1$, contiene algebre di cardinalità maggiore di qualsiasi cardinale assegnato. Servirsene per dimostrare che, per ogni X, l'applicazione i di X in $F_{V(S)}(\Omega, X)$ è iniettiva se $V(S)$ contiene algebre non banali.

5. Siano $A_\alpha \in V(S)$ per $\alpha \in I$, dove I è un insieme preordinato. Mostrare che, se esiste $\varprojlim A_\alpha$, si ha $\varprojlim A_\alpha \in V(S)$. Mostrare inoltre che, se I è diretto, $\varinjlim A_\alpha \in V(S)$. Mostrare che ogni ultraprodotto di algebre $A_\alpha \in V(S)$ appartiene a $V(S)$.

6. Sia $FM^{(r)}$ il monoide libero determinato da $X = \{x_1, x_2, \ldots, x_r\}$ come in BAI, p. 67. I suoi elementi sono 1 e i monomi, o successioni, $x_{i_1} x_{i_2} \cdots x_{i_k}$ con $1 \leq i_j \leq r$. Il prodotto è definito per giustapposizione e dalla condizione che 1 sia l'unità. Formare il $\mathbb{Z}$-modulo libero di base $FM^{(r)}$ e definirvi un prodotto ponendo

$$\left(\sum_i r_i w_i\right)\left(\sum_j r'_j w'_j\right) = \sum_{i,j} r_i r'_j w_i w'_j$$

   per $r_i, r'_j \in \mathbb{Z}$, $w_i, w'_j \in FM^{(r)}$. Si ottiene così un anello $\mathbb{Z}\{X\} = \mathbb{Z}[FM^{(r)}]$ (BAI, p. 127, esercizio 8). Mostrare che $\mathbb{Z}\{X\}$, insieme con l'inclusione di X in $\mathbb{Z}\{X\}$, costituisce un anello libero determinato da X.

2.9 Prodotti liberi di gruppi

Esaminiamo più da vicino il coprodotto di una famiglia indicizzata $\{G_\alpha \mid \alpha \in I\}$ di gruppi. Per la proposizione 2.4, $\coprod G_\alpha$ è un prodotto libero. Nella teoria dei gruppi si usa indicarlo con $\prod^* G_\alpha$ e identificare G_α con la sua immagine $i_\alpha(G_\alpha)$ in $\prod^* G_\alpha$. Con questa identificazione, $\prod^* G_\alpha$ contiene i G_α come sottogruppi ed è generato da $\bigcup G_\alpha$. Inoltre, se H è un gruppo qualsiasi e per ogni $\alpha \in I$ è dato un omomorfismo f_α di G_α in H, esiste un unico omomorfismo f di $\prod^* G_\alpha$ in H tale che $f|_{G_\alpha} = f_\alpha$ per ogni $\alpha \in I$.

Se G è un gruppo che contiene dei sottogruppi G_α, $\alpha \in I$, ed è generato da $\bigcup G_\alpha$, allora ogni elemento di G è un prodotto di elementi dei G_α. Infatti, l'insieme G' di questi prodotti contiene $\bigcup G_\alpha$ e quindi contiene 1. Inoltre G' è chiuso rispetto alla moltiplicazione e al passaggio all'inverso. Dunque G' è un sottogruppo e $G' = G$. In un prodotto di elementi dei G_α possiamo sopprimere i fattori uguali a 1 e sostituire un prodotto di fattori consecutivi appartenenti allo stesso G_α con un unico elemento di G_α. In tal modo ogni prodotto è riconducibile a 1 oppure alla forma $x_1 x_2 \cdots x_n$, dove $x_i \neq 1$ e, se $x_i \in G_\alpha$, allora $x_{i+1} \notin G_\alpha$. I prodotti di questa forma si dicono *ridotti*. Mostreremo ora che, nel prodotto libero $\prod^* G_\alpha$, due prodotti ridotti che si scrivono in modo diverso sono distinti. A tal fine daremo una costruzione alternativa, più diretta, di $\prod^* G_\alpha$. Fra i diversi procedimenti possibili ne abbiamo scelto uno particolarmente semplice, dovuto a van der Waerden.

Ripartiamo da capo. Data una famiglia di gruppi $\{G_\alpha \mid \alpha \in I\}$, sia G'_α il sottoinsieme degli elementi di G_α diversi da 1. Formiamo l'unione disgiunta S degli insiemi G'_α e di $\{1\}$. In questo insieme possiamo identificare G_α con $G'_\alpha \cup \{1\}$. Otteniamo così un insieme che è l'unione dei G_α, con $G_\alpha \cap G_\beta = \{1\}$ per $\alpha \neq \beta$. Sia ora G l'insieme delle *parole ridotte* costruite sui G_α. Con ciò intendiamo 1 e le parole $x_1 x_2 \cdots x_n$ in cui $x_i \neq 1$ e, se $x_i \in G_\alpha$, allora $x_{i+1} \notin G_\alpha$, per $1 \leq i \leq n-1$. Definiamo un'azione di G_α su G (cfr. BAI, pp. 71–73) con le regole seguenti:

$$1w = w \qquad \text{per ogni } w \in G. \tag{21}$$

Se $x \neq 1$ in G_α, allora $x1 = x$. Se $x_1 \cdots x_n$ è una parola ridotta diversa da 1, poniamo

$$x(x_1 \cdots x_n) = \begin{cases} x x_1 \cdots x_n, & x_1 \notin G_\alpha, \\ (x x_1) x_2 \cdots x_n, & x_1 \in G_\alpha, \quad x x_1 \neq 1, \\ x_2 \cdots x_n, & x_1 \in G_\alpha, \quad x x_1 = 1. \end{cases} \tag{22}$$

Nell'ultima riga si intende che, se $n = 1$ e si ottiene quindi la parola vuota, essa si interpreta come 1.

Le definizioni danno $xw \in G$ per $x \in G_\alpha$ e $w \in G$. Verifichiamo gli assiomi di un'azione: $1w = w$ e $(xy)w = x(yw)$ per $x, y \in G_\alpha$, $w \in G$. Il primo è la definizione (21). Il secondo è chiaro se uno fra x, y, w è 1, oppure se $x_1 \notin G_\alpha$. Rimane il caso $x, y, x_1 \in G_\alpha$, $x \neq 1$, $y \neq 1$. Distinguiamo tre possibilità: (α) $yx_1 \neq 1$, $xyx_1 \neq 1$; (β) $yx_1 \neq 1$, $xyx_1 = 1$; (γ) $yx_1 = 1$, $xyx_1 \neq 1$. Il caso $yx_1 = 1$, $xyx_1 = 1$ è escluso, poiché implicherebbe $x = 1$.

(α) Qui $(xy)(x_1 \cdots x_n) = (xyx_1)x_2 \cdots x_n$ e

$$x\big(y(x_1 \cdots x_n)\big) = x\big((yx_1)x_2 \cdots x_n\big) = (xyx_1)x_2 \cdots x_n.$$

Quindi $(xy)(x_1 \cdots x_n) = x\big(y(x_1 \cdots x_n)\big)$.

(β) Qui $(xy)(x_1 \cdots x_n) = x_2 \cdots x_n$ e

$$x\big(y(x_1 \cdots x_n)\big) = x\big((yx_1)x_2 \cdots x_n\big) = x_2 \cdots x_n.$$

Dunque $(xy)(x_1 \cdots x_n) = x\big(y(x_1 \cdots x_n)\big)$.

(γ) Qui $(xy)(x_1 \cdots x_n) = (xyx_1)x_2 \cdots x_n = xx_2 \cdots x_n$ e

$$x(y(x_1 \cdots x_n)) = x(x_2 \cdots x_n) = xx_2 \cdots x_n.$$

Anche in questo caso $(xy)(x_1 \cdots x_n) = x(y(x_1 \cdots x_n))$.

Se T_x indica l'applicazione $w \mapsto xw$ per $w \in G$, $x \in G_\alpha$, si ha $T_x T_y = T_{xy}$ e $T_1 = 1$. Pertanto T_x è biiettiva, con inversa $T_{x^{-1}}$, e $x \mapsto T_x$ è un omomorfismo di G_α nel gruppo $\operatorname{Sym} G$ delle trasformazioni biiettive dell'insieme G. Poiché $T_x 1 = x$, l'applicazione $x \mapsto T_x$ è iniettiva, sicché G_α è isomorfo alla sua immagine $T(G_\alpha)$, sottogruppo di $\operatorname{Sym} G$. Sia G^* il sottogruppo di $\operatorname{Sym} G$ generato da $\bigcup_\alpha T(G_\alpha)$. Sia $T_{x_1} \cdots T_{x_n}$ un prodotto ridotto di elementi di $\bigcup_\alpha T(G_\alpha)$, con $x_i \neq 1$ per ogni i. Le formule (21) e (22) danno $T_{x_1} \cdots T_{x_n} 1 = x_1 \cdots x_n$. Allora $T_{x_1} \cdots T_{x_n} \neq 1$ e, se $T_{y_1} \cdots T_{y_m}$ è un secondo prodotto di questo tipo, l'uguaglianza $T_{x_1} \cdots T_{x_n} = T_{y_1} \cdots T_{y_m}$ implica $m = n$ e $x_i = y_i$ per $1 \leq i \leq n$. Possiamo identificare $T(G_\alpha)$ con G_α. Abbiamo così dimostrato la prima affermazione del teorema seguente.

Teorema 2.12. *Sia $\{G_\alpha \mid \alpha \in I\}$ una famiglia di gruppi. Esiste un gruppo G^* che contiene i G_α come sottogruppi, è generato da $\bigcup G_\alpha$ e gode della seguente proprietà. Se $x_1 \cdots x_n$ e $y_1 \cdots y_m$, con $x_i, y_j \in \bigcup G_\alpha$, sono prodotti ridotti rispetto ai G_α, l'uguaglianza $x_1 \cdots x_n = y_1 \cdots y_m$ implica $m = n$ e $x_i = y_i$ per $1 \leq i \leq n$. Inoltre, se G^* è un gruppo qualsiasi con questa proprietà e i_α è l'inclusione di G_α in G^*, allora $\{G^*, i_\alpha\}$ è un prodotto libero dei G_α.*

Dimostrazione. Per provare l'ultima affermazione ricorriamo all'esistenza del prodotto libero $\prod^* G_\alpha$, che segue dal teorema 2.11 e dalla proposizione 2.4. Per la proprietà che definisce $\prod^* G_\alpha$ abbiamo un omomorfismo η di $\prod^* G_\alpha$ in G^* che è l'identità su ciascun G_α. Affermiamo che η è un isomorfismo, da cui seguirà che $\{G^*, i_\alpha\}$ è un prodotto libero dei G_α. Poiché i G_α generano G^*, η è suriettivo. Sia ora a un elemento di $\prod^* G_\alpha$ diverso da 1. Possiamo scriverlo nella forma ridotta $a = x_1 \cdots x_n$, dove gli x_i sono diversi da 1 e due x_i consecutivi appartengono a G_α diversi. Allora $\eta(a) = x_1 \cdots x_n \neq 1$ in G^*. Il nucleo di η (nel senso consueto) è dunque 1 e η è iniettivo. □

Il prodotto libero permette di dare un'altra costruzione del gruppo libero $FG(X)$ determinato da un insieme non vuoto X, più esplicita di quelle considerate finora (in BAI o nel paragrafo precedente). A ogni $x \in X$ associamo il gruppo ciclico infinito $\langle x \rangle$ delle potenze x^k, $k = 0, \pm 1, \pm 2, \ldots$, e costruiamo, come sopra, il prodotto libero $\prod^*_{x \in X} \langle x \rangle$ dei gruppi $\langle x \rangle$. Esso contiene i sottogruppi $\langle x \rangle$ e gode delle proprietà enunciate per i G_α nel teorema 2.12. Pertanto $\prod^*_{x \in X} \langle x \rangle$ consiste di 1 e dei prodotti $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, dove $x_i \in X$, $k_i = \pm 1, \pm 2, \ldots$ e $x_i \neq x_{i+1}$ per $1 \leq i \leq n-1$. Questi prodotti sono tutti diversi da 1 e due di essi sono uguali soltanto se sono scritti allo stesso modo. Evidentemente $\prod^*_{x \in X} \langle x \rangle$ contiene il sottoinsieme degli elementi x^1, che possiamo identificare con X. Sia ora f un'applicazione di X in un gruppo H. Per ogni $x \in X$ abbiamo l'omomorfismo f_x di $\langle x \rangle$ in H che manda x in $f(x)$. Per la proprietà di $\prod^*_{x \in X} \langle x \rangle$ come prodotto libero dei suoi sottogruppi $\langle x \rangle$, vi è allora un unico omomorfismo $\bar{f}$ di $\prod^*_{x \in X} \langle x \rangle$ in H la cui restrizione a $\langle x \rangle$ sia f_x per ogni x. Ciò significa che $\bar{f}(x) = f(x)$, ossia che abbiamo un omomorfismo di $\prod^*_{x \in X} \langle x \rangle$ in H che prolunga l'applicazione data f di X in H. È chiaro anche che esiste un solo omomorfismo $\bar{f}$ con questa proprietà. Dunque $\prod^*_{x \in X} \langle x \rangle$ è un gruppo libero determinato dall'insieme X. L'unicità dei gruppi liberi in senso categoriale permette di formulare il risultato ottenuto da questa costruzione come segue.

Teorema 2.13. *Siano X un insieme non vuoto e $(FG(X), i)$ un gruppo libero determinato da X, dove i indica l'applicazione data di X in $FG(X)$. Allora i è iniettiva e possiamo quindi identificare X con $i(X)$. Con questa identificazione ogni elemento di $FG(X)$ diverso da 1 si può scrivere nella forma ridotta $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, dove $k_i = \pm 1, \pm 2, \ldots$ e due x_i consecutivi sono distinti. Inoltre ogni elemento della forma indicata è diverso da 1 e, se $y_1^{l_1} y_2^{l_2} \cdots y_m^{l_m}$ è un secondo*

elemento in forma ridotta, allora

$$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} = y_1^{l_1} y_2^{l_2} \cdots y_m^{l_m}$$

implica $m = n$, $y_i = x_i$ *e* $k_i = l_i$ *per* $1 \leq i \leq n$.

Gli esercizi illustreranno l'utilità delle forme normali degli elementi dei prodotti liberi e dei gruppi liberi date nei teoremi 2.12 e 2.13.

Esercizi

1. Dimostrare che, se $G_\alpha \neq 1$ per ogni $\alpha \in I$ e $|I| > 1$, il centro di $\prod^* G_\alpha$ è 1.

2. Dimostrare che il gruppo libero $FG(X)$ non ha elementi di ordine finito diversi dall'identità.

3. Sia $\prod^* G_\alpha$ come nell'esercizio 1. Determinare gli elementi di ordine finito di $\prod^* G_\alpha$.

I prossimi due esercizi hanno lo scopo di dimostrare che il gruppo delle trasformazioni del piano complesso completato con ∞ della forma

$$z \longmapsto \frac{az+b}{cz+d}, \qquad a, b, c, d \in \mathbb{Z}, \quad ad - bc = 1,$$

è un prodotto libero di un gruppo ciclico di ordine due e di un gruppo ciclico di ordine tre. Osserviamo un fatto di facile verifica: questo gruppo è isomorfo a $\mathrm{SL}_2(\mathbb{Z})/\{1, -1\}$, dove $\mathrm{SL}_2(\mathbb{Z})$ è il gruppo delle matrici 2×2 a coefficienti interi di determinante 1 e

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

4. Dimostrare che $\mathrm{SL}_2(\mathbb{Z})$ è generato dalle matrici $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Siano

   $$S\colon z \mapsto -\frac{1}{z}, \qquad T\colon z \mapsto -\frac{1}{z+1}.$$

   Verificare che $S^2 = 1$, $T^3 = 1$, $ST\colon z \mapsto z+1$ e $ST^2\colon z \mapsto z/(z+1)$. Dedurne che il gruppo G delle trasformazioni $z \mapsto (az+b)/(cz+d)$ di $\mathbb{C} \cup \{\infty\}$, con $a, b, c, d \in \mathbb{Z}$ e $ad - bc = 1$, è generato da S e T.

5. Dimostrare che tutti i prodotti della forma

   $$(ST)^{k_1}(ST^2)^{k_2}(ST)^{k_3} \cdots \quad \text{oppure} \quad (ST^2)^{k_1}(ST)^{k_2}(ST^2)^{k_3} \cdots,$$

   con $k_i > 0$, si possono scrivere come $z \mapsto (az+b)/(cz+d)$, dove $a, b, c, d \geq 0$ e al più uno di questi coefficienti è nullo. Dedurne che nessun prodotto di questo tipo è 1 o S. Usare questo fatto per provare che G è un prodotto libero di un gruppo ciclico di ordine due e di un gruppo ciclico di ordine tre.

6. Sia $\mathbb{Z}\{X\}$ l'anello libero generato da $X = \{x_1, x_2, \ldots, x_n\}$, come nell'esercizio 6 del § 2.8 (p. 86 dell'originale), e sia B l'ideale di $\mathbb{Z}\{X\}$ generato da $x_1^2, x_2^2, \ldots, x_n^2$. Poniamo $A = \mathbb{Z}\{X\}/B$. Diciamo *standard* una parola nelle x_i in cui non compaia alcun x_i^2. Dimostrare che le classi di 1 e delle parole standard formano una $\mathbb{Z}$-base di A. Si identifichino 1 e le parole standard con le rispettive classi. Allora A ha una $\mathbb{Z}$-base costituita da 1 e dalle parole standard, con l'ovvia moltiplicazione che dà come risultato 1, una parola standard oppure 0 (per esempio $x_i^2 = 0$). Si ponga $y_i = 1 + x_i$, $1 \leq i \leq n$. Osservare che y_i ha inverso $1 - x_i$, sicché gli y_i generano un gruppo rispetto alla moltiplicazione in A. Dimostrare che si tratta del gruppo libero $FG(Y)$, con $Y = \{y_1, y_2, \ldots, y_n\}$.

7. Sia $FG(Y)$ come nell'esercizio 6 e sia $FG(Y)_k$, $k = 1, 2, 3, \ldots$, il sottoinsieme di $FG(Y)$ formato dagli $a \equiv 1 \pmod{(X)^k}$, dove (X) è l'ideale di A generato da $x_1, \ldots, x_n$. Dimostrare che $FG(Y)_k$ è un sottogruppo normale di $FG(Y)$ e che $\bigcap_{k=1}^{\infty} FG(Y)_k = 1$. Per un gruppo qualsiasi G, si definiscano induttivamente i $G^{(r)}$ ponendo $G^{(1)} = G$ e prendendo per $G^{(r)}$ il sottogruppo generato dai commutatori $xyx^{-1}y^{-1}$, con $x \in G^{(r-1)}$ e $y \in G$. Si ha $G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \cdots$, e questa catena si chiama *serie centrale discendente* di G. Dimostrare che $FG(Y)^{(k)} \subseteq FG(Y)_k$. Dedurne il *teorema di Magnus*: $\bigcap_k FG(Y)^{(k)} = 1$.

8. Siano B, A_α, $\alpha \in I$, algebre di una varietà $V(S)$ e $f_\alpha \colon B \to A_\alpha$ omomorfismi, per $\alpha \in I$. Dimostrare che esiste una *somma amalgamata* (o *pushout*) degli f_α nel senso seguente. Esistono un'algebra $A \in V(S)$ e omomorfismi $i_\alpha \colon A_\alpha \to A$, $\alpha \in I$, tali che $i_\alpha f_\alpha = i_\beta f_\beta$ per ogni α, β; inoltre, se $C \in V(S)$ e $g_\alpha \colon A_\alpha \to C$ soddisfano $g_\alpha f_\alpha = g_\beta f_\beta$ per ogni α, β, esiste un unico omomorfismo $g \colon A \to C$ tale che $g i_\alpha = g_\alpha$ per ogni $\alpha \in I$.

9. Sia $\{G_\alpha \mid \alpha \in I\}$ una famiglia di gruppi che contengono tutti lo stesso sottogruppo H. Costruire un gruppo G con le seguenti proprietà. (i) G contiene ciascun G_α come sottogruppo e $G_\alpha \cap G_\beta = H$ se $\alpha \neq \beta$. (ii) Per $\alpha \in I$, sia X_α un insieme di rappresentanti delle classi laterali destre di H in G_α, scegliendo 1 per la classe H, e sia $X = \bigcup X_\alpha$. Ogni elemento di G ha un'unica espressione come prodotto $hx_1x_2 \cdots x_n$, dove $h \in H$, $x_i \in X \setminus \{1\}$ e, se $x_i \in X_\alpha$, allora $x_{i+1} \notin X_\alpha$ per $1 \leq i \leq n-1$. (Si ammette $n = 0$, e in tal caso l'elemento è in H.) Si chiama G il *prodotto libero dei G_α con sottogruppo amalgamato* H e lo si indica con $\prod_H^* G_\alpha$.

2.10 Caratterizzazione interna delle varietà

Sia $C = V(S)$ una varietà di Ω-algebre definita da un insieme di identità S. Qui S è un sottoinsieme di $F(\Omega, X_0) \times F(\Omega, X_0)$, dove $X_0 = \{x_1, x_2, x_3, \ldots\}$ e $F(\Omega, X_0)$ è la Ω-algebra libera determinata da X_0. Abbiamo visto che C gode delle seguenti proprietà di chiusura.

1. Se $A \in C$, ogni sottoalgebra di A appartiene a C.

2. Se $A \in C$, ogni immagine omomorfa di A appartiene a C.

3. Se $\{A_\alpha \mid \alpha \in I\} \subseteq C$, allora $\prod_\alpha A_\alpha \in C$.

Lo scopo principale di questa sezione è dimostrare il viceversa: se C è una classe di Ω-algebre che soddisfa le condizioni 1, 2 e 3, allora C è una varietà.

Come preliminare alla dimostrazione consideriamo le identità soddisfatte da una data Ω-algebra A. Per i nostri scopi occorre considerare identità in un insieme arbitrario di elementi, oltre che nell'insieme standard X_0. Sia dunque X un qualsiasi insieme non vuoto e sia $F(\Omega, X)$ la Ω-algebra libera determinata da X. Se η è un omomorfismo di $F(\Omega, X)$ in A, il nucleo $\ker \eta$ è una congruenza su $F(\Omega, X)$ e $F(\Omega, X)/\ker \eta$ è isomorfa a una sottoalgebra di A. Poniamo ora

$$\mathrm{Id}(X, A) = \bigcap_\eta \ker \eta,$$

dove l'intersezione è estesa a tutti gli omomorfismi η di $F(\Omega, X)$ in A. L'insieme $\mathrm{Id}(X, A)$ consiste allora delle coppie (w_1, w_2), con $w_i \in F(\Omega, X)$, tali che $\eta(w_1) = \eta(w_2)$ per ogni omomorfismo η di $F(\Omega, X)$ in A. Dunque $\mathrm{Id}(X, A)$ è il sottoinsieme di $F(\Omega, X) \times F(\Omega, X)$ delle identità nell'insieme X soddisfatte dall'algebra A. Evidentemente $\mathrm{Id}(X, A)$ è una congruenza su $F(\Omega, X)$. La chiamiamo *congruenza delle identità in X dell'algebra A*. Osserviamo che $F(\Omega, X)/\mathrm{Id}(X, A)$ è

un prodotto sottodiretto delle algebre $F(\Omega, X)/\ker\eta$ (esercizio 4 del ğ2.4), dunque è un prodotto sottodiretto di sottoalgebre di A.

Sia ora C una classe qualsiasi di Ω-algebre. Vogliamo considerare l'insieme delle identità in X soddisfatte da ogni $A \in C$. Evidentemente tale insieme è

$$\mathrm{Id}(X, C) = \bigcap_{A \in C} \mathrm{Id}(X, A).$$

Esso è una congruenza, che chiameremo *congruenza delle identità in X per la classe C*. È chiaro che $F(\Omega, X)/\mathrm{Id}(X, C)$ è un prodotto sottodiretto di sottoalgebre di algebre appartenenti alla classe C.

Supponiamo ora che C abbia le proprietà di chiusura 1, 2 e 3. Allora è chiaro che ogni prodotto sottodiretto di algebre della classe C appartiene a C. Ne segue che $F(\Omega, X)/\mathrm{Id}(X, C) \in C$. Sia ora $S = \mathrm{Id}(X_0, C)$ la congruenza delle identità nell'insieme standard X_0 per la classe C, e sia $V(S)$ la varietà definita da S. Mostreremo che $C = V(S)$. Ciò sarà conseguenza immediata del seguente teorema.

Teorema 2.14. *Se X è infinito, allora $F(\Omega, X)/\mathrm{Id}(X, C)$, insieme all'applicazione canonica $x \mapsto \bar{x}_{\mathrm{Id}(X,C)}$, costituisce un'algebra libera per $V(S)$ determinata da X.*

Dimostrazione. Ricordiamo la costruzione del ğ2.8 di un'algebra libera $F_{V(S)}(\Omega, X)$ per la varietà $V(S)$ e l'insieme X: si ha $F_{V(S)}(\Omega, X) = F(\Omega, X)/\Phi(S)$, dove $\Phi(S)$ è la congruenza su $F(\Omega, X)$ generata da tutte le coppie $(\varphi(w_1), \varphi(w_2))$ con $(w_1, w_2) \in S$ e φ omomorfismo da $F(\Omega, X_0)$ in $F(\Omega, X)$. Il risultato seguirà se dimostriamo che $\Phi(S) = \mathrm{Id}(X, C)$. Abbiamo visto che le proprietà di chiusura di C implicano $F(\Omega, X)/\mathrm{Id}(X, C) \in C$. Abbiamo quindi l'omomorfismo da $F(\Omega, X)/\Phi(S)$ in $F(\Omega, X)/\mathrm{Id}(X, C)$ che manda $\bar{x}_{\Phi(S)}$ in $\bar{x}_{\mathrm{Id}(X,C)}$. Perciò $\Phi(S) \subseteq \mathrm{Id}(X, C)$.

Sia ora $(z_1, z_2) \in \mathrm{Id}(X, C)$. Entrambi gli elementi appartengono a una sottoalgebra $F(\Omega, X')$ di $F(\Omega, X)$ generata da un sottoinsieme numerabile X' di X. Vi sono applicazioni $\zeta : X_0 \to X$ e $\lambda : X \to X_0$ tali che $\zeta(X_0) = X'$ e $\lambda\zeta = 1_{X_0}$. Esse si estendono univocamente a omomorfismi $\bar{\zeta} : F(\Omega, X_0) \to F(\Omega, X)$ e $\bar{\lambda} : F(\Omega, X) \to F(\Omega, X_0)$ tali che $\bar{\zeta}(F(\Omega, X_0)) = F(\Omega, X')$ e $\bar{\lambda}\bar{\zeta} = 1_{F(\Omega,X_0)}$. Scegliamo $w_i \in F(\Omega, X_0)$ tali che $\bar{\zeta}(w_i) = z_i$ per $i = 1, 2$. Sia f un omomorfismo di $F(\Omega, X_0)$ in un'algebra $A \in C$. Allora

$$f = f1_{F(\Omega,X_0)} = f\bar{\lambda}\bar{\zeta} = \bar{f}\bar{\zeta},$$

dove $\bar{f} = f\bar{\lambda}$ è un omomorfismo di $F(\Omega, X)$ in A. Poiché $(z_1, z_2) \in \mathrm{Id}(X, C)$, si ha $\bar{f}(z_1) = \bar{f}(z_2)$, e quindi $f(w_1) = \bar{f}\bar{\zeta}(w_1) = \bar{f}(z_1) = \bar{f}(z_2) = f(w_2)$. Si ha così $f(w_1) = f(w_2)$ per ogni omomorfismo f di $F(\Omega, X_0)$ in un'algebra $A \in C$. Ciò significa che $(w_1, w_2) \in S = \mathrm{Id}(X_0, C)$. Allora $(z_1, z_2) = (\bar{\zeta}(w_1), \bar{\zeta}(w_2)) \in \Phi(S)$. Dunque $\mathrm{Id}(X, C) \subseteq \Phi(S)$ e $\mathrm{Id}(X, C) = \Phi(S)$. □

Possiamo ora dimostrare il risultato principale.

Teorema 2.15 (Birkhoff). *Una classe C di Ω-algebre è una varietà se e solo se gode delle proprietà di chiusura 1, 2 e 3 elencate sopra.*

Dimostrazione. È chiaro che $C \subseteq V(S)$, dove S è l'insieme delle identità in X_0 soddisfatte da ogni $A \in C$. D'altra parte, se $A \in V(S)$, allora A è immagine omomorfa di un'algebra $F(\Omega, X)/\mathrm{Id}(X, C)$ per un opportuno insieme infinito X. Poiché $F(\Omega, X)/\mathrm{Id}(X, C) \in C$, ne segue che $A \in C$. Dunque $V(S) \subseteq C$ e pertanto $V(S) = C$. □

Riferimenti bibliografici

P. M. Cohn, *Universal Algebra*, Harper and Row, New York, 1965. Edizione riveduta, D. Reidel, 1981.

G. Grätzer, *Universal Algebra*, Van Nostrand-Reinhold, New York, 1967. Seconda edizione, Springer-Verlag, 1979.

3 Moduli

In questo capitolo riprendiamo lo studio dei moduli iniziato nel capitolo 3 di BAI. In precedenza ci siamo concentrati sulla struttura dei moduli finitamente generati su un dominio a ideali principali e sulle sue applicazioni alla teoria strutturale dei gruppi abeliani finitamente generati e alla teoria di una singola trasformazione lineare in uno spazio vettoriale di dimensione finita. Il presente capitolo non ha uno scopo altrettanto circoscritto né un obiettivo altrettanto immediato. Studieremo i moduli per il loro interesse intrinseco e in vista di applicazioni che incontreremo più avanti.

La teoria dei moduli ha importanza centrale in diversi campi dell'algebra, in particolare nella teoria strutturale degli anelli, nella teoria delle rappresentazioni di anelli e gruppi e nell'algebra omologica. A questi temi saranno dedicati i tre capitoli successivi.

Cominceremo mettendo in evidenza le caratteristiche peculiari delle categorie R-**mod** e **mod**-R dei moduli, rispettivamente sinistri e destri, sull'anello R. La più importante è che per ogni coppia di moduli (M, N) l'insieme $\hom_R(M, N)$ è un gruppo abeliano. Questa osservazione ha condotto a definire le categorie abeliane. Una parte considerevole della teoria dei moduli può essere incorporata nella teoria più generale delle categorie abeliane. Per alcune parti importanti della teoria dei moduli, tuttavia, ciò non è possibile. Per questa ragione, e per il vantaggio di una maggiore concretezza, in questo capitolo ci limiteremo al caso dei moduli.

Tratteremo le proprietà fondamentali delle categorie R-**mod** e **mod**-R (§ 1), la struttura dei moduli (§§ 2–5), i prodotti tensoriali di moduli e i bimoduli (§§ 6–8), i moduli proiettivi e iniettivi (§§ 10–11) e la teoria di Morita (§§ 12–15). Mediante i prodotti tensoriali definiremo le algebre e le coalgebre su anelli commutativi. A questo proposito isoleremo alcuni esempi importanti: le algebre tensoriali, le algebre simmetriche e le algebre esterne. Come applicazione della teoria di Morita daremo una dimostrazione del teorema di struttura di Wedderburn–Artin sugli anelli semplici. Rinunciamo a una descrizione più dettagliata degli argomenti: i titoli dei paragrafi basteranno forse a dare un'idea del loro contenuto.

3.1 Le categorie R-mod e mod-R

Iniziamo lo studio sistematico dei moduli adottando il punto di vista categoriale: considereremo anzitutto le peculiarità delle categorie R-**mod** e **mod**-R dei moduli sinistri e destri su un dato anello R. Abbiamo visto che si può passare liberamente dai moduli sinistri a quelli destri e viceversa sostituendo R con l'anello opposto R^{op}. Finché non avremo bisogno di considerare relazioni fra moduli sinistri e destri sul medesimo anello R, possiamo dunque limitarci agli uni o agli altri. Poiché presenta un piccolo vantaggio notazionale far agire l'anello R e gli R-omomorfismi da lati opposti, in questo capitolo daremo la preferenza ai moduli destri e alla categoria **mod**-R.

Il fatto forse più importante riguardo a **mod**-R, che finora abbiamo trascurato, è che i suoi insiemi di morfismi hanno una struttura naturale di gruppo abeliano. Se $M, N \in \mathrm{ob}(\textbf{mod}\text{-}R)$, vi è un modo naturale di introdurre una struttura di gruppo nell'insieme $\hom_R(M, N)$. Per $f, g \in \hom(M, N) = \hom_R(M, N)$ definiamo $f + g$ ponendo

$$(f + g)x = fx + gx, \qquad x \in M.$$

Qui abbiamo abbreviato $f(x)$ in fx, e così via. Definiamo l'applicazione 0 da M a N ponendo $0x = 0$, e l'applicazione $-f$ ponendo $(-f)x = -fx$, per $x \in M$. Una verifica diretta mostra che $f + g$, 0 e $-f$ appartengono a $\hom(M, N)$ e che $(\hom(M, N), +, 0)$ è un gruppo abeliano (BAI, pp. 168–169).

Osserviamo poi che nella nostra categoria il prodotto dei morfismi è distributivo da entrambi i lati rispetto all'addizione. Sia P un terzo modulo. Per $f, g \in \hom(M, N)$ e $h, k \in \hom(N, P)$ si ha

$$h(f+g) = hf + hg, \qquad (h+k)f = hf + kf.$$

In particolare, per $M = N = P$, in $\operatorname{End} M = \hom(M, M)$ sono definite l'addizione $+$ e la moltiplicazione, ossia la composizione delle applicazioni. Inoltre l'identità 1_M appartiene a $\operatorname{End} M$ ed è l'unità per la moltiplicazione. Dunque $(\operatorname{End} M, +, \cdot, 0, 1)$ è un anello, l'*anello degli endomorfismi* del modulo M.

Un importante concetto della teoria dei moduli, originato nella topologia algebrica, è quello di successione esatta di moduli e omomorfismi. Cominciamo col dire che il diagramma di omomorfismi di moduli

$$M \xrightarrow{f} N \xrightarrow{g} P$$

è *esatto* se $\operatorname{im} f = f(M) = \ker g$: in altre parole, per $y \in N$ si ha $gy = 0$ se e solo se esiste $x \in M$ tale che $fx = y$. Più in generale, una successione di moduli e omomorfismi

$$\cdots \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow \cdots,$$

finita o prolungata all'infinito in una o nell'altra direzione, si dice esatta se per ogni terna di termini consecutivi è esatta la sottosuccessione $M_i \to M_{i+1} \to M_{i+2}$. L'esattezza di $0 \to M \xrightarrow{f} N$ significa che $\ker f = 0$, ossia che f è iniettiva. È d'uso scrivere $M \xhookrightarrow{f} N$ per indicare questa esattezza. Analogamente, l'esattezza di $M \xrightarrow{f} N \to 0$ equivale alla suriettività di f e si può indicare con $M \overset{f}{\twoheadrightarrow} N$.

Una successione esatta della forma

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

si chiama *successione esatta corta*. Ciò significa che f è un monomorfismo, g è un epimorfismo e $\ker g = \operatorname{im} f$. Un caso particolare si ottiene considerando un sottomodulo N di un modulo M e il quoziente M/N. Si hanno l'inclusione i di N in M e l'omomorfismo canonico ν di M su M/N. Il primo è iniettivo, il secondo è suriettivo e $\ker \nu = N = \operatorname{im} i$. Si ha dunque la successione esatta corta

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\nu} M/N \longrightarrow 0.$$

Per $f\colon M \to N$ definiamo il *conucleo*, $\operatorname{coker} f$, come $N/\operatorname{im} f$. Evidentemente f è suriettivo se e solo se $\operatorname{coker} f = 0$. In ogni caso si ha

$$\ker f \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow \operatorname{coker} f,$$

ossia è esatta la successione $0 \to \ker f \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow \operatorname{coker} f \to 0$.

Nel capitolo 1, pp. 35–36 dell'originale, abbiamo visto che esistono prodotti e coprodotti per famiglie indicizzate arbitrarie di moduli. Se $\{M_\alpha \mid \alpha \in I\}$ è una famiglia di R-moduli destri, il prodotto in **mod**-R è $\{\prod M_\alpha, p_\alpha\}$, dove p_α è l'omomorfismo di proiezione di $\prod M_\alpha$ su M_α. Inoltre, sia $\bigoplus M_\alpha$ il sottomodulo di $\prod M_\alpha$ degli elementi (x_α) con un numero finito di componenti non nulle. Sia i_α l'omomorfismo di M_α in $\bigoplus M_\alpha$ che manda $x_\alpha \in M_\alpha$ nell'elemento avente componente α uguale a x_α e tutte le restanti componenti nulle. Allora $\{\bigoplus M_\alpha, i_\alpha\} = \coprod M_\alpha$ è il coprodotto degli M_α.

Sia ora I finito, $I = \{1, 2, \ldots, n\}$. Chiaramente $M = \prod_1^n M_i = \bigoplus_1^n M_i$. Dunque questo modulo, insieme con le applicazioni $i_1, \ldots, i_n$, costituisce un coprodotto degli M_i, mentre M, insieme

con $p_1, \dots, p_n$, ne costituisce un prodotto. Dalla definizione di i_j e p_j seguono immediatamente le relazioni

$$p_j i_j = 1_{M_j}, \qquad p_k i_j = 0 \ (j \neq k), \qquad i_1 p_1 + i_2 p_2 + \cdots + i_n p_n = 1_M. \tag{1}$$

Un'osservazione importante è che queste condizioni su una famiglia di omomorfismi caratterizzano il modulo M a meno di isomorfismo. Supponiamo precisamente che siano dati un modulo M' e omomorfismi $p'_j \colon M' \to M_j$ e $i'_j \colon M_j \to M'$, $1 \leq j \leq n$, tali che

$$p'_j i'_j = 1_{M_j}, \qquad p'_k i'_j = 0 \ (j \neq k), \qquad \sum_{j=1}^{n} i'_j p'_j = 1_{M'}. \tag{2}$$

Allora

$$\theta' = \sum_{j=1}^{n} i_j p'_j, \qquad \theta = \sum_{j=1}^{n} i'_j p_j \tag{3}$$

sono omomorfismi rispettivamente da M' a M e da M a M'. Per (1) e (2) si ha $\theta'\theta = 1_M$ e $\theta\theta' = 1_{M'}$, sicché θ e θ' sono isomorfismi e $\theta' = \theta^{-1}$. Inoltre $\theta i_j = i'_j \colon M_j \to M'$. Dalla definizione di coprodotto segue che M' e gli i'_j costituiscono un coprodotto degli M_j. Analogamente $p_j\theta' = p'_j$ e M' con i p'_j costituisce un prodotto degli M_j in **mod**-R.

Fra i funtori tra categorie di moduli, eventualmente su anelli diversi, ci interessano soprattutto quelli *additivi*, nel senso che per ogni coppia (M, N) l'applicazione $f \mapsto F(f)$ da $\hom(M, N)$ in $\hom(FM, FN)$ è un omomorfismo di gruppi. D'ora in poi, salvo esplicita indicazione contraria, supporremo sempre additivi i funtori fra categorie di moduli.

La caratterizzazione appena vista del prodotto e del coprodotto di $M_1, \dots, M_n$ mediante le relazioni (1) fra gli i_j e i p_j implica che ogni funtore F da una categoria **mod**-R a una categoria **mod**-S conserva i prodotti e i coprodotti finiti. Siano M, i_j e p_j come sopra. Applicando F alle relazioni (1) e usando le proprietà moltiplicative e additive di F, otteniamo

$$F(p_j)F(i_j) = 1_{FM_j}, \qquad F(p_k)F(i_j) = F(0) = 0 \quad (j \neq k),$$
$$\sum_j F(i_j)F(p_j) = 1_{FM}.$$

Dunque $\{FM, F(i_j)\} = \coprod FM_j$ e $\{FM, F(p_j)\} = \prod FM_j$.

Un funtore F da **mod**-R a **mod**-S si dice *esatto* se manda successioni esatte corte in successioni esatte corte. In altre parole, se $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ è esatta in **mod**-R, deve essere esatta $0 \to FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM'' \to 0$ in **mod**-S. Questo accade raramente. Più comuni sono i funtori *esatti a sinistra* o *esatti a destra*. Nel primo caso, dall'esattezza di $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ segue quella di $0 \to FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM''$; nel secondo, dall'esattezza di $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ segue quella di $FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM'' \to 0$.

Per i funtori controvarianti fra categorie di moduli valgono definizioni analoghe. Li supponiamo additivi nel senso che per ogni (M, N) l'applicazione da $\hom(M, N)$ a $\hom(FN, FM)$ è un omomorfismo di gruppi. Allora F è esatto a sinistra se dall'esattezza di $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ segue quella di $0 \to FM'' \xrightarrow{F(g)} FM \xrightarrow{F(f)} FM'$. È esatto a destra se dall'esattezza di $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ segue quella di $FM'' \xrightarrow{F(g)} FM \xrightarrow{F(f)} FM' \to 0$.

Abbiamo definito i funtori hom covarianti e controvarianti da una categoria arbitraria **C** in **Set** (p. 38 dell'originale). Se **C** = **mod**-R, è più naturale considerarli a valori in **mod**-$\mathbb{Z}$.

Ricordiamo che per $A \in \operatorname{ob}\mathbf{C}$ il funtore covariante $\hom(A,-)$ da $\mathbf{C}$ a **Set** manda un oggetto B in $\hom(A,B)$. Per $f\colon B \to B'$ l'applicazione $\hom(A,-)(f)$ da $\hom(A,B)$ a $\hom(A,B')$ moltiplica a sinistra per f gli elementi del primo insieme per ottenere i corrispondenti elementi del secondo. Sia ora $\mathbf{C} = \mathbf{mod}\text{-}R$ e siano M, N due suoi oggetti. Allora $\hom(M,N)$ è un gruppo abeliano, quindi uno $\mathbb{Z}$-modulo, e per $f\colon N \to N'$ e $g, h \in \hom(M,N)$ si ha $f(g+h) = fg + fh$. Dunque $\hom(M,-)(f)$ è un omomorfismo dello $\mathbb{Z}$-modulo $\hom(M,N)$ nello $\mathbb{Z}$-modulo $\hom(M,N')$. Se f' è un secondo elemento di $\hom(N,N')$, si ha inoltre $(f+f')g = fg + f'g$. Segue $\hom(M,-)(f+f') = \hom(M,-)(f) + \hom(M,-)(f')$. Possiamo dunque considerare $\hom(M,-)$ come funtore additivo da $\mathbf{mod}\text{-}R$ a $\mathbf{mod}\text{-}\mathbb{Z}$, e adotteremo d'ora in avanti questo punto di vista. Una proprietà fondamentale dei funtori hom è l'esattezza a sinistra.

Teorema 3.1. *Il funtore* $\hom(M,-)$ *da* $\mathbf{mod}\text{-}R$ *a* $\mathbf{mod}\text{-}\mathbb{Z}$ *è esatto a sinistra.*

Dimostrazione. Dobbiamo provare che se $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ è esatta, anche

$$0 \longrightarrow \hom(M,N') \xrightarrow{\hom(M,-)(f)} \hom(M,N) \xrightarrow{\hom(M,-)(g)} \hom(M,N'') \tag{4}$$

è esatta. Sappiamo che f è un monomorfismo e $\operatorname{im} f = \ker g$; dobbiamo provare che $\hom(M,-)(f)$ e $\hom(M,-)(g)$ godono delle proprietà corrispondenti. Sia $\varphi \in \hom(M,N')$ e supponiamo $(\hom(M,-)(f))(\varphi) = f\varphi = 0$. Per ogni $x \in M$ è allora $f\varphi x = 0$ e, per l'iniettività di f, segue $\varphi x = 0$. Dunque $\hom(M,-)(f)(\varphi) = 0$ implica $\varphi = 0$. Essendo un omomorfismo di gruppi, $\hom(M,-)(f)$ è pertanto un monomorfismo. Osserviamo poi che $gf\varphi = 0$, poiché $gf = 0$, onde $gf\varphi(x) = 0$ per ogni $x \in M$. Dunque $\hom(M,-)(g)\hom(M,-)(f)(\varphi) = 0$ per ogni $\varphi\colon M \to N'$ e il composto dei due omomorfismi è zero. Pertanto

$$\operatorname{im}\hom(M,-)(f) \subseteq \ker\hom(M,-)(g).$$

Per dimostrare l'inclusione opposta sia $\psi \in \ker\hom(M,-)(g)$, cioè $\psi \in \hom(M,N)$ e $g\psi = 0$, ossia $g\psi x = 0$ per ogni $x \in M$. Per ciascun $x \in M$, questa uguaglianza mostra che ψx, che è un elemento di N, appartiene a $\ker g$. Per ipotesi esiste dunque $y \in N'$ tale che $fy = \psi x$. Inoltre, essendo f un monomorfismo, y è univocamente determinato. Otteniamo un'applicazione $\varphi\colon x \mapsto y$ di M in N'. Dalla definizione segue direttamente che $\varphi \in \hom(M,N')$ e $f\varphi = \psi$. Si ha quindi $\ker\hom(M,-)(g) \subseteq \operatorname{im}\hom(M,-)(f)$ e i due insiemi sono uguali. Questo conclude la dimostrazione. □

Analogamente il funtore controvariante $\hom(-,M)$ determinato da $M \in \operatorname{ob}(\mathbf{mod}\text{-}R)$ si può considerare come funtore controvariante da $\mathbf{mod}\text{-}R$ a $\mathbf{mod}\text{-}\mathbb{Z}$. Qui $\hom(-,M)N = \hom(N,M)$ e, se $f\colon N \to N'$, $\hom(-,M)(f)$ moltiplica a destra per f gli elementi di $\hom(N',M)$, ottenendo elementi di $\hom(N,M)$. Si ha il risultato seguente.

Teorema 3.1′**.** *Il funtore* $\hom(-,M)$ *controvariante è esatto a sinistra.*

Lasciamo la dimostrazione al lettore.

Esercizi

1. Si consideri R come R-modulo destro nel modo consueto: l'azione di R su R è la moltiplicazione a destra nell'anello. Mostrare che il modulo destro M e $\hom_R(R,M)$ sono isomorfi come gruppi abeliani. Più precisamente, verificare che per ogni $x \in M$ l'applicazione $u_x\colon a \mapsto xa$, $a \in R$, appartiene a $\hom_R(R,M)$ e che $x \mapsto u_x$ è un isomorfismo da M, come gruppo abeliano, su $\hom_R(R,M)$. Usare questo fatto per provare che il funtore $\hom(R,-)$ da $\mathbf{mod}\text{-}R$ a $\mathbf{mod}\text{-}\mathbb{Z}$ è naturalmente isomorfo al funtore dimenticante che associa a un modulo il suo gruppo abeliano sottostante, e così via.

2. Siano $M = \mathbb{Z}$, $N = \mathbb{Z}/(m)$ con $m > 1$, e sia ν l'omomorfismo canonico di M su N. Mostrare che 1_N non si può scrivere come νf per alcun omomorfismo $f\colon N \to M$. Dedurne che l'immagine della successione esatta $M \to N \to 0$ mediante $\hom(N, -)$ non è esatta.

3. Siano $M = \mathbb{Z}$, $N = m\mathbb{Z}$ con $m > 1$, e sia i l'inclusione di N in M. Mostrare che l'omomorfismo $1/m\colon mx \mapsto x$ di N in M non si può scrivere come fi per alcun $f\colon M \to M$. Dedurne che l'immagine della successione esatta $0 \to N \to M$ mediante $\hom(-, M)$ non è esatta.

4. *Lemma dei cinque corto.* Si supponga che il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow u & & \downarrow v & & \downarrow w & & \\ 0 & \longrightarrow & N' & \xrightarrow[h]{} & N & \xrightarrow[k]{} & N'' & \longrightarrow & 0 \end{array}$$

sia commutativo e abbia righe esatte. Mostrare che, se due qualunque fra u, v, w sono isomorfismi, lo è anche il terzo.

3.2 Moduli artiniani e noetheriani

Dopo la veduta d'insieme della teoria dei moduli offerta dal paragrafo precedente, torniamo a terra per studiare i moduli uno per uno. Cominceremo con alcuni aspetti della loro teoria strutturale. Nei prossimi sei paragrafi le idee categoriali avranno soltanto una parte secondaria; torneranno in primo piano dal § 3.9 in avanti.

Raccogliamo anzitutto alcuni risultati sui moduli che ci serviranno come strumenti. Sono casi particolari di risultati già dimostrati per le Ω-algebre (pp. 63–65 dell'originale), precisamente della corrispondenza fra l'insieme delle sottoalgebre di un quoziente di una Ω-algebra e quello delle sottoalgebre sature dell'algebra, e dei due teoremi di isomorfismo. Per ottenere i risultati corrispondenti sui moduli, li si può considerare come gruppi con operatori, prendendo come insieme degli operatori l'anello dato. Si ottengono così i risultati seguenti. Se M è un modulo e P un suo sottomodulo, si ha una biiezione fra l'insieme dei sottomoduli del quoziente $\overline{M} = M/P$ e l'insieme dei sottomoduli di M contenenti P. A un sottomodulo N di M contenente P corrisponde il sottomodulo $\overline{N} = N/P = \{y + P \mid y \in N\}$ di $\overline{M}$. Se invece $\overline{N}$ è un sottomodulo di $\overline{M}$, poniamo $N = \{y \in M \mid y + P \in \overline{N}\}$. Allora N è un sottomodulo di M contenente P e $\overline{N} = N/P$. Si può verificare questo risultato anche direttamente, come nel caso dei gruppi (BAI, p. 64). I casi particolari dei teoremi di isomorfismo per le Ω-algebre sono i seguenti.

Primo teorema di isomorfismo per i moduli. *Se N_1 e N_2 sono sottomoduli di M, allora*

$$(y_1 + y_2) + N_2 \longmapsto y_1 + (N_1 \cap N_2), \qquad y_i \in N_i, \tag{5}$$

è un isomorfismo di $(N_1 + N_2)/N_2$ su $N_1/(N_1 \cap N_2)$.

Secondo teorema di isomorfismo per i moduli. *Se M è un modulo e N, P sono sottomoduli con $N \supseteq P$, allora*

$$(x + P) + N/P \longmapsto x + N, \qquad x \in M, \tag{6}$$

è un isomorfismo di $(M/P)/(N/P)$ su M/N.

Anche questi due risultati si possono dimostrare direttamente come per i gruppi (BAI, pp. 64–65). I risultati sui gruppi si estendono infatti immediatamente ai gruppi con operatori, di cui i

moduli sono un caso particolare. Nel paragrafo successivo avremo bisogno del fatto che valgono per i gruppi con operatori.

Un modulo M è detto *noetheriano* (rispettivamente *artiniano*) se soddisfa la seguente

Condizione delle catene ascendenti (discendenti). Non esiste in M una successione infinita strettamente crescente (decrescente) di sottomoduli,

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots \qquad (M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots).$$

In altri termini, se $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ è una successione crescente di sottomoduli, esiste n tale che $M_n = M_{n+1} = \cdots$. Formulazione analoga ha la condizione delle catene discendenti. Si vede facilmente che la condizione precedente equivale alla seguente

Condizione del massimo (minimo). Ogni insieme non vuoto S di sottomoduli di M contiene un elemento massimale (minimale) in S, ossia un modulo $P \in S$ tale che, se $N \in S$ e $N \supseteq P$ (rispettivamente $N \subseteq P$), allora $N = P$.

Esempi

1. L'anello $\mathbb{Z}$, considerato come $\mathbb{Z}$-modulo, soddisfa la condizione delle catene ascendenti ma non quella delle catene discendenti. Ricordiamo che ogni ideale di $\mathbb{Z}$ è principale (BAI, p. 143) e i sottomoduli di $\mathbb{Z}$ sono i suoi ideali. Se $I_1 \subseteq I_2 \subseteq \cdots$ è una successione crescente di ideali di $\mathbb{Z}$, allora $I = \bigcup_j I_j$ è un ideale. Esso è principale: $I = (m)$ con $m \in I$, dunque $m \in I_n$ per qualche n. Allora $I_n = I_{n+1} = \cdots$. Lo stesso ragionamento mostra che la condizione delle catene ascendenti vale per ogni dominio commutativo a ideali principali D, considerato come D-modulo (BAI, p. 147). D'altra parte, per $m \in \mathbb{Z}$ diverso da $0, \pm 1$, si ha $(m) \supsetneq (m^2) \supsetneq (m^3) \supsetneq \cdots$, dunque la condizione delle catene discendenti non vale in $\mathbb{Z}$.

2. Sia P il gruppo additivo dei razionali i cui denominatori sono potenze di un primo fissato p: i suoi elementi sono m/p^k, $m \in \mathbb{Z}$, $k = 0, 1, 2, \ldots$. Consideriamo P come $\mathbb{Z}$-modulo. Si ha la catena ascendente di sottomoduli

   $$\mathbb{Z} \subsetneq \mathbb{Z}(1/p) \subsetneq \mathbb{Z}(1/p^2) \subsetneq \mathbb{Z}(1/p^3) \subsetneq \cdots .$$

   Si vede facilmente che questi sono i soli sottomoduli propri di P contenenti $\mathbb{Z}$. Segue che $M = P/\mathbb{Z}$ è artiniano ma non noetheriano. Poiché $\mathbb{Z}$ è un sottomodulo di P, è chiaro d'altra parte che P non è né artiniano né noetheriano.

3. Un gruppo abeliano finito è artiniano e noetheriano come $\mathbb{Z}$-modulo.

Se M è artiniano o noetheriano, ogni suo sottomodulo ha evidentemente la stessa proprietà. Lo stesso vale per ogni quoziente M/N, dunque per ogni immagine omomorfa: la corrispondenza fra sottomoduli $P \mapsto \overline{P} = P/N$ ha infatti la proprietà che $P_1 \supseteq P_2$ se e solo se $\overline{P}_1 \supseteq \overline{P}_2$. Mostreremo ora che, viceversa, se M contiene un sottomodulo N tale che N e M/N sono artiniani (noetheriani), allora M è artiniano (noetheriano). Ci servirà il seguente lemma.

Lemma. *Siano N, P_1, P_2 sottomoduli di M tali che*

$$P_1 \supseteq P_2, \qquad N + P_1 = N + P_2, \qquad N \cap P_1 = N \cap P_2. \tag{7}$$

Allora $P_1 = P_2$.

Dimostrazione. Sia $z_1 \in P_1$. Allora $z_1 \in N + P_1 = N + P_2$, sicché $z_1 = y + z_2$ con $y \in N$, $z_2 \in P_2$. Si ha $y = z_1 - z_2 \in P_1$, perciò $y \in P_1 \cap N = P_2 \cap N$. Dunque $y \in P_2$ e $z_1 = y + z_2 \in P_2$. Segue $P_1 \subseteq P_2$ e quindi $P_1 = P_2$. □

Teorema 3.2. *Se M contiene un sottomodulo N tale che N e M/N sono artiniani (noetheriani), allora M è artiniano (noetheriano).*

Dimostrazione. Sia $P_1 \supseteq P_2 \supseteq P_3 \supseteq \cdots$ una catena discendente di sottomoduli di M. Allora $(N \cap P_1) \supseteq (N \cap P_2) \supseteq (N \cap P_3) \supseteq \cdots$ è una catena discendente di sottomoduli contenuti in N. Esiste quindi k tale che $N \cap P_k = N \cap P_{k+1} = \cdots$. Inoltre $(N + P_1)/N \supseteq (N + P_2)/N \supseteq \cdots$ è una catena discendente di sottomoduli di M/N. Esiste dunque l tale che $(N + P_l)/N = (N + P_{l+1})/N = \cdots$. Ne segue $N + P_l = N + P_{l+1} = \cdots$. Prendendo $n = \max(k, l)$ e applicando il lemma concludiamo che $P_n = P_{n+1} = \cdots$. Nel caso noetheriano basta sostituire ovunque $\supseteq$ con $\subseteq$. □

Teorema 3.3. *Sia $M = N + P$, dove N e P sono sottomoduli artiniani (noetheriani) di M. Allora M è artiniano (noetheriano).*

Dimostrazione. Abbiamo $M/N = (N + P)/N \cong P/(N \cap P)$, che è un'immagine omomorfa del modulo artiniano (noetheriano) P. Pertanto M/N e N sono artiniani (noetheriani), e per il teorema 3.2 lo è anche M. □

Un anello R si dice *noetheriano* o *artiniano a destra* (a sinistra) se R, come R-modulo destro (sinistro), è rispettivamente noetheriano o artiniano. Un modulo M si dice *finitamente generato* se è generato da un numero finito di elementi. Per un modulo destro ciò significa che esistono $x_1, \ldots, x_m \in M$ tali che $M = x_1R + x_2R + \cdots + x_mR$.

Teorema 3.4. *Se R è noetheriano (artiniano) a destra, ogni R-modulo destro finitamente generato M è noetheriano (artiniano).*

Dimostrazione. Abbiamo $M = x_1R + \cdots + x_mR$ e gli epimorfismi $a \mapsto x_ia$ da R su x_iR, $1 \leq i \leq m$. Quindi x_iR è noetheriano (artiniano). Per il teorema 3.3 e per induzione, anche M è noetheriano (artiniano). □

Se R è un anello di divisione, i suoi soli ideali sinistri o destri sono 0 e R. Quindi R è artiniano e noetheriano sia a destra sia a sinistra. Ne segue il corollario.

Corollario. *Uno spazio vettoriale finitamente generato su un anello di divisione è artiniano e noetheriano.*

Esercizi

1. Provare che M è noetheriano se e solo se ogni sottomodulo di M è finitamente generato.
2. Mostrare che se un endomorfismo di un modulo noetheriano (artiniano) è un epimorfismo (monomorfismo), allora è un isomorfismo.
3. Siano V uno spazio vettoriale su un campo F, T una trasformazione lineare di V su F e $F[\lambda]$ l'anello dei polinomi su F nell'indeterminata λ. Si dà a V una struttura di $F[\lambda]$-modulo ponendo
$$(a_0 + a_1\lambda + \cdots + a_m\lambda^m)x = a_0x + a_1(Tx) + a_2(T^2x) + \cdots + a_m(T^mx)$$
(BAI, p. 165). Sia $(x_1, x_2, \ldots)$ una base numerabile di V e sia T la trasformazione lineare tale che $Tx_1 = 0$ e $Tx_{i+1} = x_i$ per $i = 1, 2, 3, \ldots$. Mostrare che V, come $F[\lambda]$-modulo definito da T, è artiniano. Sia poi T' la trasformazione lineare di V tale che $T'x_i = x_{i+1}$ per $i = 1, 2, \ldots$. Mostrare che V, come $F[\lambda]$-modulo definito da T', è noetheriano.

3.3 Il teorema di raffinamento di Schreier e il teorema di Jordan–Hölder

I risultati che ora dimostreremo sono importanti anche per i gruppi non commutativi. Per comprendere insieme il caso dei gruppi e quello dei moduli considereremo i gruppi con operatori.

I risultati che otterremo si generalizzano anche alle Ω-algebre: per queste estensioni rinviamo al libro *Universal Algebra* di Cohn, pp. 91–93 (si vedano i riferimenti alla fine del capitolo 2).

Consideriamo la classe dei gruppi con un insieme fissato di operatori Λ. Si tratta di un insieme fissato di simboli di operazione unaria: per ogni $\lambda \in \Lambda$ e per ogni gruppo G della classe, $x \mapsto \lambda x$ è un'applicazione di G in sé. Richiediamo inoltre che

$$\lambda(xy) = (\lambda x)(\lambda y). \tag{8}$$

I moduli sinistri sono evidentemente un caso particolare: $G = M$ è un gruppo commutativo scritto additivamente e $\Lambda = R$ è un anello dato. Anche qui il passaggio dal punto di vista dei moduli a quello dei gruppi con operatori costituisce una generalizzazione, poiché si rinuncia agli assiomi dei moduli che coinvolgono la struttura di anello. Chiameremo Λ-*gruppi* i gruppi con insieme di operatori Λ. Per Λ-*sottogruppi* e Λ-*sottogruppi normali* intenderemo sottogruppi e sottogruppi normali stabili rispetto all'azione di Λ: se h appartiene al sottogruppo e $\lambda \in \Lambda$, anche λh appartiene al sottogruppo. Scriviamo $G \triangleright H$ o $H \triangleleft G$ per indicare che H è un Λ-sottogruppo normale di G. Un omomorfismo f da un Λ-gruppo G in un Λ-gruppo H è un omomorfismo di gruppi da G in H tale che

$$f(\lambda x) = \lambda f(x) \tag{9}$$

per ogni $x \in G$, $\lambda \in \Lambda$. L'immagine $f(G)$ è un Λ-sottogruppo di H e il nucleo $f^{-1}(1) = \{k \in G \mid f(k) = 1\}$ è un Λ-sottogruppo normale. Se $H \triangleleft G$, definiamo il Λ-*gruppo quoziente* G/H: i suoi elementi sono le classi laterali $xH = Hx$, con la consueta struttura di gruppo e con l'azione $\lambda(xH) = (\lambda x)H$, $\lambda \in \Lambda$. La stabilità di H garantisce che $\lambda(xH)$ sia ben definito. La (8) per G/H segue immediatamente dalla stessa proprietà per G.

Ricordiamo inoltre che, per due sottoinsiemi A, B di un gruppo G, si pone $AB = \{ab \mid a \in A,\ b \in B\}$. Se $K \triangleleft G$ e H è un sottogruppo, si ha $HK = KH$, poiché $HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$. Questo è un sottogruppo di G, ed è un Λ-sottogruppo quando G è un Λ-gruppo e H, K sono Λ-sottogruppi. In tal caso $H \cap K \triangleleft H$ e si ha l'isomorfismo di Λ-gruppi da $H/(H \cap K)$ su HK/K dato da

$$h(H \cap K) \longmapsto hK, \qquad h \in H. \tag{10}$$

La dimostrazione per gruppi privi di operatori si applica senza modifiche (BAI, p. 65). Lo stesso vale per gli altri risultati fondamentali, come quelli di BAI, pp. 64–65. Raccogliamo qui per comodità quelli di cui avremo bisogno.

L'applicazione $H \mapsto H/K$ è una biiezione fra l'insieme dei Λ-sottogruppi di G contenenti $K \triangleleft G$ e l'insieme dei Λ-sottogruppi di G/K. Inoltre $H \triangleleft G$ se e soltanto se $H/K \triangleleft G/K$. In tal caso si ha l'isomorfismo da $(G/K)/(H/K)$ su G/H dato da

$$(gK)(H/K) \longmapsto gH, \qquad g \in G. \tag{11}$$

Più in generale, supponiamo dato un epimorfismo f del Λ-gruppo G sul Λ-gruppo G' e sia H un Λ-sottogruppo normale di G contenente il nucleo K di f. Si ha allora l'isomorfismo di Λ-gruppi da G/H su $G'/f(H) = f(G)/f(H)$ dato da

$$gH \longmapsto f(g)f(H). \tag{12}$$

Il concetto di Λ-gruppo, oltre a riunire i casi dei gruppi e dei moduli, permette di trattare simultaneamente diverse classi interessanti di sottogruppi. Dato un gruppo G, prendiamo come Λ l'insieme dei suoi automorfismi interni. I Λ-sottogruppi di G sono allora i suoi sottogruppi

normali: lo studio di G come Λ-gruppo si concentra su questi, lasciando da parte i sottogruppi non normali. Analogamente, prendendo per Λ tutti gli automorfismi di G, si ottengono i sottogruppi mandati in sé da tutti gli automorfismi, detti *sottogruppi caratteristici*. Prendendo per Λ tutti gli endomorfismi di G, si ottengono i *sottogruppi pienamente invarianti*, ossia quelli mandati in sé da ogni endomorfismo di G.

Una *serie normale* del Λ-gruppo G è una catena discendente di Λ-sottogruppi

$$G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_{s+1} = 1, \tag{13}$$

nella quale ogni G_{i+1} è normale in G_i (anche se non necessariamente in G). La corrispondente successione di Λ-gruppi quoziente

$$G_1/G_2,\ G_2/G_3,\ \ldots,\ G_s/G_{s+1} = G_s \tag{14}$$

si chiama successione dei *fattori* della serie normale (13). L'intero s si chiama *lunghezza* della (13). La serie normale

$$G = H_1 \triangleright H_2 \triangleright H_3 \triangleright \cdots \triangleright H_{t+1} = 1 \tag{15}$$

è *equivalente* alla (13) se $t = s$ ed esiste una permutazione $i \mapsto i'$ di $\{1, 2, \ldots, s\}$ tale che $G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$ come Λ-gruppi. La serie (15) è un *raffinamento* della (13) se la successione dei G_i è una sottosuccessione di quella degli H_j. Vogliamo dimostrare il seguente risultato.

Teorema di raffinamento di Schreier. *Due serie normali di uno stesso Λ-gruppo ammettono raffinamenti equivalenti.*

La dimostrazione si basa sul lemma seguente.

Lemma di Zassenhaus. *Siano G_i, G_i', $i = 1, 2$, Λ-sottogruppi di un gruppo G con $G_i' \triangleleft G_i$. Allora*

$$(G_1 \cap G_2')G_1' \triangleleft (G_1 \cap G_2)G_1', \tag{16}$$

$$(G_1' \cap G_2)G_2' \triangleleft (G_1 \cap G_2)G_2', \tag{17}$$

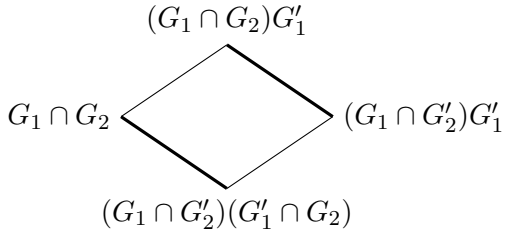
$$\frac{(G_1 \cap G_2)G_1'}{(G_1 \cap G_2')G_1'} \cong \frac{(G_1 \cap G_2)G_2'}{(G_1' \cap G_2)G_2'}. \tag{18}$$

Dimostrazione. Dimostreremo la (16) e le relazioni

$$(G_1' \cap G_2)(G_1 \cap G_2') = (G_1 \cap G_2')(G_1' \cap G_2) \triangleleft G_1 \cap G_2, \tag{19}$$

$$\frac{(G_1 \cap G_2)G_1'}{(G_1 \cap G_2')G_1'} \cong \frac{G_1 \cap G_2}{(G_1 \cap G_2')(G_1' \cap G_2)} = \frac{G_1 \cap G_2}{(G_1' \cap G_2)(G_1 \cap G_2')}. \tag{20}$$

Il seguente diagramma aiuta a visualizzare queste relazioni:



I tratti in grassetto rappresentano i gruppi quoziente dei quali vogliamo stabilire l'isomorfismo. Provate le relazioni indicate, per simmetria avremo la (17) e

$$\frac{(G_1 \cap G_2)G_2'}{(G_1' \cap G_2)G_2'} \cong \frac{G_1 \cap G_2}{(G_1 \cap G_2')(G_1' \cap G_2)},$$

da cui, insieme alla (20), seguirà la (18).

Consideriamo i Λ-sottogruppi $G_1 \cap G_2$ e G_1' di G_1. Poiché $G_1' \lhd G_1$, si ha $G_1' \cap G_2 = G_1' \cap (G_1 \cap G_2) \lhd G_1 \cap G_2$, il prodotto $(G_1 \cap G_2)G_1'$ è un Λ-sottogruppo e $G_1' \lhd (G_1 \cap G_2)G_1'$. Analogamente $G_1 \cap G_2' \lhd G_1 \cap G_2$. Segue la (19). Formiamo il Λ-gruppo quoziente $(G_1 \cap G_2)G_1'/G_1'$ e consideriamo l'omomorfismo $f\colon x \mapsto xG_1'$ di $G_1 \cap G_2$ in esso. Si tratta di un epimorfismo e

$$\begin{aligned} f\big((G_1 \cap G_2')(G_1' \cap G_2)\big) &= (G_1 \cap G_2')(G_1' \cap G_2)G_1'/G_1' \\ &= (G_1 \cap G_2')G_1'/G_1'. \end{aligned}$$

Il prodotto $(G_1 \cap G_2')(G_1' \cap G_2)$ è normale in $G_1 \cap G_2$ e f è un epimorfismo. Perciò

$$(G_1 \cap G_2')G_1'/G_1' \lhd (G_1 \cap G_2)G_1'/G_1'.$$

Ne segue $(G_1 \cap G_2')G_1' \lhd (G_1 \cap G_2)G_1'$, ossia la (16). Inoltre

$$\begin{aligned} \frac{G_1 \cap G_2}{(G_1 \cap G_2')(G_1' \cap G_2)} &\cong \frac{f(G_1 \cap G_2)}{f((G_1 \cap G_2')(G_1' \cap G_2))} \\ &= \frac{(G_1 \cap G_2)G_1'/G_1'}{(G_1 \cap G_2')G_1'/G_1'} \cong \frac{(G_1 \cap G_2)G_1'}{(G_1 \cap G_2')G_1'}, \end{aligned}$$

che dà la (20). □

Dimostrazione del teorema di raffinamento di Schreier. Siano (13) e (15) le serie normali assegnate. Poniamo

$$G_{ik} = (G_i \cap H_k)G_{i+1}, \qquad H_{ki} = (H_k \cap G_i)H_{k+1}. \tag{21}$$

Allora $G_{i1} = G_i$, $G_{i,t+1} = G_{i+1}$, $H_{k1} = H_k$, $H_{k,s+1} = H_{k+1}$. Per il lemma di Zassenhaus, $G_{i,k+1} \lhd G_{ik}$, $H_{k,i+1} \lhd H_{ki}$ e

$$G_{ik}/G_{i,k+1} \cong H_{ki}/H_{k,i+1}. \tag{22}$$

Abbiamo così le serie normali

$$\begin{aligned} (G =)\, & G_1 \supset G_{12} \supset \cdots \supset G_{1t} \\ & \supset G_2 \supset G_{22} \supset \cdots \supset G_{2t} \\ & \quad \vdots \\ & \supset G_s \supset G_{s2} \supset \cdots \supset G_{st} \supset G_{s,t+1}\ (= 1) \end{aligned} \tag{23}$$

e

$$\begin{aligned} (G =)\, & H_1 \supset H_{12} \supset \cdots \supset H_{1s} \\ & \supset H_2 \supset H_{22} \supset \cdots \supset H_{2s} \\ & \quad \vdots \\ & \supset H_t \supset H_{t2} \supset \cdots \supset H_{ts} \supset H_{t,s+1}\ (= 1). \end{aligned} \tag{24}$$

I fattori corrispondenti sono

$$\begin{array}{cccc} G_{11}/G_{12}, & G_{12}/G_{13}, & \ldots, & G_{1t}/G_{1,t+1}, \\ G_{21}/G_{22}, & G_{22}/G_{23}, & \ldots, & G_{2t}/G_{2,t+1}, \\ \vdots & \vdots & & \vdots \\ G_{s1}/G_{s2}, & G_{s2}/G_{s3}, & \ldots, & G_{st}/G_{s,t+1}, \end{array} \tag{25}$$

$$
\begin{array}{llll}
H_{11}/H_{12}, & H_{12}/H_{13}, & \dots, & H_{1s}/H_{1,s+1}, \\
H_{21}/H_{22}, & H_{22}/H_{23}, & \dots, & H_{2s}/H_{2,s+1}, \\
\vdots & \vdots & & \vdots \\
H_{t1}/H_{t2}, & H_{t2}/H_{t3}, & \dots, & H_{ts}/H_{t,s+1}.
\end{array} \tag{26}
$$

Il fattore nella riga i e nella colonna k della (25) è isomorfo, come Λ-gruppo, a quello nella riga k e nella colonna i della (26). Le serie (23) e (24) sono quindi equivalenti. È chiaro che la (23) raffina la (13) e la (24) raffina la (15); il teorema è dimostrato. □

Una serie normale (13) si dice *propria* se ogni inclusione è propria, ossia $G_i \neq G_{i+1}$. Una serie normale è una *serie di composizione* se è propria e non ammette alcun raffinamento proprio. Ciò significa che $G_i \neq G_{i+1}$ e che non esiste G' con $G_i \supsetneq G' \supsetneq G_{i+1}$, $G' \lhd G_i$ e $G_{i+1} \lhd G'$. Equivalentemente, G_i/G_{i+1} è *semplice* come Λ-gruppo: è diverso da 1 e non contiene alcun Λ-sottogruppo normale proprio diverso da 1. Un Λ-gruppo può non avere alcuna serie di composizione (per esempio, un gruppo ciclico infinito non ne ha). Quando ne ha una vale però il seguente risultato.

Teorema di Jordan–Hölder. *Due serie di composizione di uno stesso Λ-gruppo sono equivalenti.*

Dimostrazione. I fattori di una serie di composizione sono diversi da 1. I fattori di un suo raffinamento sono quelli della serie data, ai quali si aggiungono fattori uguali a 1. Due serie di composizione ammettono raffinamenti equivalenti. L'equivalenza mette in corrispondenza i fattori uguali a 1 e quindi anche quelli diversi da 1, ossia i fattori delle serie di composizione date. Le due serie sono dunque equivalenti. □

Prendendo come Λ gli automorfismi interni, i termini di una serie di composizione sono sottogruppi normali. Una serie siffatta si chiama *serie principale*. Il teorema di Jordan–Hölder mostra che due serie principali sono equivalenti. Il risultato si applica anche alle *serie caratteristiche*, definite come le serie di composizione ottenute prendendo per Λ tutti gli automorfismi, e alle *serie pienamente invarianti*, ottenute prendendo per Λ tutti gli endomorfismi.

Tutto ciò si applica anche ai moduli. Per questi si ha un importante criterio di esistenza delle serie di composizione.

Teorema 3.5. *Un modulo $M \neq 0$ ammette una serie di composizione se e soltanto se è al tempo stesso artiniano e noetheriano.*

Dimostrazione. Supponiamo che M abbia una serie di composizione $M = M_1 \supset M_2 \supset \cdots \supset M_{s+1} = 0$ (si ha necessariamente $M_i \rhd M_{i+1}$, poiché i gruppi sono abeliani). Siano $N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_t$ sottomoduli. La serie di composizione data e la serie normale $M \supset N_1 \supset N_2 \supset \cdots \supset N_t \supset N_{t+1} = 0$ ammettono allora raffinamenti equivalenti. Ne segue $t \leq s+1$, il che implica che M è artiniano e noetheriano. Supponiamo viceversa che $M \neq 0$ abbia queste proprietà. L'insieme dei sottomoduli propri di $M_1 = M$ ha un elemento massimale M_2, poiché M è noetheriano. Se $M_2 \neq 0$, si può ripetere il procedimento ottenendo un sottomodulo proprio massimale M_3 di M_2. Proseguendo si ha una successione discendente $M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots$ che, per la condizione della catena discendente, termina con $M_{t+1} = 0$. Allora $M = M_1 \supset M_2 \supset \cdots \supset M_{t+1} = 0$ è una serie di composizione. □

Esercizi

1. Sia G un gruppo con insieme di operatori Λ. Mostrare che G ammette una serie di composizione se e soltanto se valgono le due condizioni seguenti. (i) Se $G = G_1 \rhd G_2 \rhd \cdots$, esiste n tale che $G_n = G_{n+1} = \cdots$. (ii) Se H è un termine di una serie normale di G e $H_1 \subset H_2 \subset \cdots$ è una successione ascendente di Λ-sottogruppi normali di H, esiste n tale che $H_n = H_{n+1}$.

2. Sia G un Λ-gruppo con una serie di composizione e sia $H \lhd G$. Mostrare che esiste una serie di composizione avente H fra i suoi termini. Dedurne che H e G/H ammettono serie di composizione.

3. Siano G e H come nell'esercizio 2. Si chiami *lunghezza* $\ell(G)$ il numero dei fattori di composizione. Mostrare che $\ell(G) = \ell(H) + \ell(G/H)$. Mostrare inoltre che, se $H_i \lhd G$, $i = 1, 2$, si ha
$$\ell(H_1 H_2) = \ell(H_1) + \ell(H_2) - \ell(H_1 \cap H_2).$$

3.4 Il teorema di Krull–Schmidt

I risultati di questo paragrafo valgono anche per i gruppi con operatori e sono interessanti anche in quel contesto. Anzi, furono ottenuti dapprima per i gruppi senza operatori. Nel caso dei moduli, tuttavia, le dimostrazioni sono più semplici. Nel testo ci limiteremo perciò ai moduli e negli esercizi indicheremo come estendere la teoria ai gruppi con operatori.

Ricordiamo che, se $M = \bigoplus_{j=1}^{n} M_j$, si hanno gli omomorfismi $i_j \colon M_j \to M$, $p_j \colon M \to M_j$ che soddisfano le relazioni (1). Poniamo

$$e_j = i_j p_j. \tag{27}$$

Allora $e_j \in \operatorname{End} M$ $(= \hom_R(M, M))$ e dalle (1) si ricava

$$\begin{gathered} e_j^2 = e_j, \qquad e_j e_k = 0 \quad (j \neq k), \\ e_1 + e_2 + \cdots + e_n = 1. \end{gathered} \tag{28}$$

Ricordiamo che un elemento e di un anello si dice *idempotente* se $e^2 = e$. Due idempotenti e, f si dicono *ortogonali* se $ef = 0 = fe$. Pertanto gli e_j sono idempotenti a due a due ortogonali di $\operatorname{End} M$ e $\sum_1^n e_j = 1$. Poniamo $M_j' = i_j(M_j) = i_j p_j(M) = e_j(M)$. Per $x \in M$, si ha $x = 1x = \sum e_j x$, con $e_j x \in M_j'$. Dunque $M = M_1' + \cdots + M_n'$. Inoltre, se $x_j \in M_j'$, allora $x_j = e_j x$ per qualche $x \in M$. Quindi $e_j x_j = e_j^2 x = e_j x = x_j$, mentre $e_k x_j = e_k e_j x = 0$ per $j \neq k$. Ne segue che $M_j' \cap (M_1' + \cdots + M_{j-1}' + M_{j+1}' + \cdots + M_n') = 0$ per ogni j.

Viceversa, supponiamo che un modulo M contenga sottomoduli $M_1, \ldots, M_n$ che soddisfano le due condizioni

$$M = M_1 + M_2 + \cdots + M_n, \tag{29}$$

$$M_j \cap (M_1 + \cdots + M_{j-1} + M_{j+1} + \cdots + M_n) = 0, \qquad 1 \leq j \leq n. \tag{30}$$

Si ha allora l'omomorfismo di inclusione i_j di M_j in M e ogni $x \in M$ si scrive in modo unico come $x = x_1 + \cdots + x_n$, con $x_j \in M_j$. Si ottiene quindi un'applicazione $p_j \colon M \to M_j$ ponendo $p_j x = x_j$. È chiaro che le condizioni (1) per i_j e p_j sono soddisfatte. Come prima, si ha un isomorfismo di M su $\bigoplus M_j$. In virtù di questo risultato diremo che M è *somma diretta (interna)* dei sottomoduli $M_1, \ldots, M_n$ se valgono le (29) e (30). Scriveremo

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n. \tag{31}$$

Gli endomorfismi $e_j = i_j p_j$ si chiamano *proiezioni* determinate dalla decomposizione diretta (31).

È utile esprimere le condizioni (29) e (30) per mezzo degli elementi: ogni elemento di M si scrive in uno e un solo modo nella forma $x_1 + x_2 + \cdots + x_n$, con $x_j \in M_j$. Ne segue facilmente che, se M è somma diretta dei sottomoduli M_i e ciascun M_i è somma diretta di sottomoduli

M_{ij}, allora M è somma diretta dei sottomoduli M_{ij}. Ci serviremo all'occorrenza di altri fatti elementari di questo tipo (cfr. BAI, pp. 176–177).

Un modulo M si dice *decomponibile* se $M = M_1 \oplus M_2$ con entrambi gli M_i diversi da zero. Altrimenti si dice *indecomponibile*.

Proposizione 3.1. *Un modulo $M \neq 0$ è indecomponibile se e soltanto se* $\operatorname{End} M$ *non contiene idempotenti diversi da* 0 *e da* 1.

Dimostrazione. Se $M = M_1 \oplus \cdots \oplus M_n$ con $M_j \neq 0$ e $n > 1$, le proiezioni e_j sono idempotenti non nulli. Se $e_j = 1$, per ogni $i \neq j$ si avrebbe $e_i = e_i 1 = e_i e_j = 0$, dunque $e_j \neq 1$. Viceversa, supponiamo che $\operatorname{End} M$ contenga un idempotente $e \neq 0, 1$. Poniamo $e_1 = e$, $e_2 = 1 - e$. Allora $e_2^2 = (1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = e_2$ ed $e_1 e_2 = e(1-e) = 0 = e_2 e_1$. Si hanno così due idempotenti ortogonali non nulli. Ne segue $M = M_1 \oplus M_2$, con $M_j = e_j(M) \neq 0$. □

Ogni modulo è somma diretta di un numero finito di sottomoduli indecomponibili? È facile vedere che la risposta è negativa: basta prendere uno spazio vettoriale di dimensione infinita. Se M è somma diretta di un numero finito di sottomoduli indecomponibili, i suoi addendi sono univocamente determinati? Anche qui la risposta è negativa: basta considerare uno spazio vettoriale di dimensione finita maggiore di uno. Gli addendi indecomponibili sono determinati almeno a meno di isomorfismo? Si può mostrare che nemmeno questo vale in generale. Vi è però una condizione semplice che lo garantisce. Dapprima daremo la condizione, poi mostreremo che è soddisfatta per i moduli al tempo stesso artiniani e noetheriani o, equivalentemente, per quelli che ammettono serie di composizione. La condizione si basa su una nozione di notevole importanza nella teoria degli anelli.

Definizione 3.1. *Un anello R si dice locale se l'insieme I dei suoi elementi non invertibili è un ideale.*

Se R è locale, i suoi soli idempotenti sono 0 e 1. Infatti, se e è un idempotente diverso da 0 e da 1, la relazione $e(1-e) = 0$ implica che e non è invertibile. Nemmeno $1 - e$ è invertibile. Se R è locale, e e $1 - e$ appartengono dunque all'ideale I dei non invertibili. Ma allora $1 \in I$, il che è assurdo. Ne segue che, se $\operatorname{End} M$ è locale per un modulo $M \neq 0$, allora M è indecomponibile. Chiameremo M *fortemente indecomponibile* se $M \neq 0$ e $\operatorname{End} M$ è locale. Il principale teorema di unicità per le decomposizioni dirette in moduli indecomponibili che dimostreremo è il seguente.

Teorema 3.6. *Siano*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n, \tag{32}$$

$$N = N_1 \oplus N_2 \oplus \cdots \oplus N_m, \tag{33}$$

dove gli M_i sono fortemente indecomponibili, gli N_i sono indecomponibili e $M \cong N$. Allora $m = n$ ed esiste una permutazione $j \mapsto j'$ tale che $M_j \cong N_{j'}$ per $1 \leq j \leq n$.

Isoliamo dapprima il seguente lemma.

Lemma. *Siano M e N moduli con N indecomponibile e $M \neq 0$. Se $f\colon M \to N$ e $g\colon N \to M$ sono omomorfismi tali che gf è un automorfismo di M, allora f e g sono isomorfismi.*

Dimostrazione. Sia k l'inverso di gf, sicché $kgf = 1_M$. Poniamo $l = kg\colon N \to M$. Allora $lf = 1_M$ e, posto $e = fl\colon N \to N$, si ha $e^2 = flfl = f1_M l = fl = e$. Poiché N è indecomponibile, $e = 1$ oppure $e = 0$. Il secondo caso è escluso: implicherebbe $1_M = 1_M^2 = lflf = lef = 0$, contro l'ipotesi $M \neq 0$. Dunque $fl = e = 1_N$, perciò f è un isomorfismo e anche $g = k^{-1}f^{-1}$ è un isomorfismo. □

Dimostrazione del teorema 3.6. Procediamo per induzione su n. Il caso $n = 1$ è chiaro; supponiamo $n > 1$. Siano $e_1, \ldots, e_n$ le proiezioni determinate dalla decomposizione (32) di M e

$f_1, \dots, f_m$ quelle determinate dalla (33) di N. Sia g un isomorfismo di M su N e poniamo

$$h_j = f_j g e_1, \qquad k_j = e_1 g^{-1} f_j, \qquad 1 \le j \le m. \tag{34}$$

Allora

$$\sum_{j=1}^{m} k_j h_j = \sum_{j=1}^{m} e_1 g^{-1} f_j g e_1 = e_1 g^{-1} \Big(\sum_j f_j \Big) g e_1 = e_1 g^{-1} 1_N g e_1 = e_1.$$

Le restrizioni di e_1 e $k_j h_j$ a M_1 mandano M_1 in sé, e possiamo quindi considerarle come endomorfismi e_1' e $(k_j h_j)'$ di M_1. Poiché $M_1 = e_1(M)$ ed $e_1^2 = e_1$, si ha $e_1' = 1_{M_1}$. Pertanto $1_{M_1} = \sum_j (k_j h_j)'$. Essendo $\operatorname{End} M_1$ locale, almeno uno dei $(k_j h_j)'$ è invertibile, e quindi è un automorfismo di M_1. Riordinando gli N_j possiamo supporre che sia $j = 1$. La restrizione di h_1 a M_1 dà un omomorfismo h_1' da M_1 in N_1. Analogamente la restrizione di k_1 a N_1 dà un omomorfismo k_1' da N_1 in M_1 e $k_1' h_1' = (k_1 h_1)'$ è un automorfismo. Per il lemma, dunque, $h_1' = (f_1 g e_1)' \colon M_1 \to N_1$ e $k_1' = (e_1 g^{-1} f_1)' \colon N_1 \to M_1$ sono isomorfismi.

Dimostriamo ora che

$$M = g^{-1} N_1 \oplus (M_2 + \cdots + M_n). \tag{35}$$

Sia $x \in g^{-1}N_1 \cap (M_2 + \cdots + M_n)$. Allora $e_1 x = 0$ poiché $x \in M_2 + \cdots + M_n$, e $x = g^{-1} y$ con $y \in N_1$. Quindi $0 = e_1 x = e_1 g^{-1} y = e_1 g^{-1} f_1 y = k_1 y = k_1' y$. Segue $y = 0$, dunque $x = 0$, e $g^{-1}N_1 \cap (M_2 + \cdots + M_n) = 0$. Sia ora $x \in g^{-1}N_1 \subset M' = g^{-1}N_1 + M_2 + \cdots + M_n$. Poiché $x, e_2 x, \dots, e_n x \in M'$, anche $e_1 x \in M'$. Perciò $M' \supset e_1 g^{-1} N_1 = e_1 g^{-1} f_1 N_1 = k_1 N_1 = k_1' N_1 = M_1$. Dunque M' contiene ogni M_j, $1 \le j \le n$, cosicché $M' = M$. Abbiamo provato la (35).

L'isomorfismo g da M su N manda $g^{-1}N_1$ su N_1, inducendo un isomorfismo di $M/g^{-1}N_1$ su N/N_1. Per la (35), $M/g^{-1}N_1 \cong M_2 + \cdots + M_n = M_2 \oplus \cdots \oplus M_n$. Poiché $N/N_1 \cong N_2 \oplus \cdots \oplus N_m$, si ha un isomorfismo di $M_2 \oplus \cdots \oplus M_n$ su $N_2 \oplus \cdots \oplus N_m$. Il teorema segue per induzione. □

Mostreremo ora che questi risultati si applicano ai moduli che ammettono serie di composizione.

Dato un endomorfismo f di un modulo M, poniamo $f^\infty M = \bigcap_{n=0}^{\infty} f^n(M)$ e $f^{-\infty}0 = \bigcup_{n=0}^{\infty} \ker f^n$. Dunque $x \in f^\infty M$ se e soltanto se per ogni $n = 1, 2, \dots$ esiste y_n tale che $f^n y_n = x$, mentre $x \in f^{-\infty}0$ se e soltanto se $f^n x = 0$ per qualche $n = 1, 2, \dots$. Le immagini $f^n(M)$ formano la catena discendente

$$M \supset f(M) \supset f^2(M) \supset \cdots, \tag{36}$$

e, poiché da $f^n x = 0$ segue $f^{n+1} x = 0$, abbiamo la catena ascendente

$$0 \subset \ker f \subset \ker f^2 \subset \cdots. \tag{37}$$

I termini di entrambe sono sottomoduli stabili per f; lo stesso vale quindi per $f^\infty M$ e $f^{-\infty}0$. Si ha il seguente importante risultato.

Lemma di Fitting. *Sia f un endomorfismo di un modulo M artiniano e noetheriano (equivalentemente, che ammette una serie di composizione). Allora si ha la decomposizione di Fitting*

$$M = f^\infty M \oplus f^{-\infty}0. \tag{38}$$

La restrizione di f a $f^\infty M$ è un automorfismo e la restrizione di f a $f^{-\infty}0$ è nilpotente.

Dimostrazione. Poiché M è artiniano, esiste s tale che $f^s(M) = f^{s+1}(M) = \cdots = f^\infty M$. Poiché M è noetheriano, esiste t tale che $\ker f^t = \ker f^{t+1} = \cdots = f^{-\infty}0$. Sia $r = \max(s, t)$, cosicché $f^\infty M = f^r(M)$ e $f^{-\infty}0 = \ker f^r$. Se $z \in f^\infty M \cap f^{-\infty}0$, allora $z = f^r y$ con $y \in M$ e

$0 = f^r z = f^{2r} y$, per cui $y \in \ker f^{2r} = \ker f^r$. Ne segue $z = f^r y = 0$. Dunque $f^\infty M \cap f^{-\infty} 0 = 0$. Sia ora $x \in M$. Allora $f^r x \in f^r(M) = f^{2r}(M)$, ossia $f^r x = f^{2r} y$ per qualche $y \in M$. Ne segue $f^r(x - f^r y) = 0$ e quindi $z = x - f^r y \in f^{-\infty} 0$. Abbiamo $x = f^r y + z$ con $f^r y \in f^\infty M$. Pertanto $M = f^\infty M + f^{-\infty} 0$ e vale la decomposizione (38). Poiché $f^{-\infty} 0 = \ker f^r$, la restrizione di f a $f^{-\infty} 0$ è nilpotente. La restrizione a $f^\infty M = f^r(M) = f^{r+1}(M)$ è suriettiva; è anche iniettiva, poiché $f^\infty M \cap f^{-\infty} 0 = 0$ implica $f^\infty M \cap \ker f = 0$. □

Una conseguenza immediata del lemma è la seguente.

Teorema 3.7. *Sia M un modulo indecomponibile non nullo che soddisfa entrambe le condizioni di catena. Ogni endomorfismo f di M è nilpotente oppure è un automorfismo. Inoltre M è fortemente indecomponibile.*

Dimostrazione. Per il lemma di Fitting si ha $M = f^\infty M$ oppure $M = f^{-\infty} 0$. Nel primo caso f è un automorfismo, nel secondo è nilpotente. Per provare che M è fortemente indecomponibile, cioè che $\operatorname{End} M$ è locale, dobbiamo mostrare che l'insieme I degli endomorfismi che non sono automorfismi è un ideale. Basta vedere che, per $f \in I$ e $g \in \operatorname{End} M$, si ha $fg, gf \in I$, e che $f_1, f_2 \in I$ implica $f_1 + f_2 \in I$. La prima affermazione segue dal fatto che $f \in I$ è nilpotente: non è né suriettivo né iniettivo, perciò fg e gf non sono automorfismi. Supponiamo ora che $f_1 + f_2 \notin I$, cioè che $f_1 + f_2$ sia invertibile. Moltiplicando per $(f_1 + f_2)^{-1}$, si ottiene $h_1 + h_2 = 1$ con $h_i = f_i(f_1 + f_2)^{-1} \in I$. Ma $h_1 = 1 - h_2$ è invertibile: per qualche n si ha $h_2^n = 0$, dunque

$$(1 - h_2)(1 + h_2 + \cdots + h_2^{n-1}) = 1 = (1 + h_2 + \cdots + h_2^{n-1})(1 - h_2).$$

Ciò contraddice $h_1 \in I$. □

Dimostriamo ora l'esistenza di decomposizioni dirette in moduli indecomponibili per i moduli che soddisfano entrambe le condizioni di catena.

Teorema 3.8. *Se $M \neq 0$ è un modulo artiniano e noetheriano, esistono sottomoduli indecomponibili M_i, $1 \leq i \leq n$, tali che $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$.*

Dimostrazione. Definiamo la lunghezza di M come il numero dei fattori di composizione in una sua serie di composizione (esercizio 3, p. 110). Se N è un sottomodulo proprio, la serie normale $M \supset N \supset 0$ ammette un raffinamento che è una serie di composizione: ciò segue dal teorema di raffinamento di Schreier. La lunghezza di N è dunque minore di quella di M. Se M è indecomponibile la tesi è immediata. Altrimenti $M = M_1 \oplus M_2$ con $M_i \neq 0$. Si ha $\ell(M_i) < \ell(M)$ e per induzione sulla lunghezza possiamo supporre che

$$M_1 = M_{11} \oplus M_{12} \oplus \cdots \oplus M_{1n_1}, \qquad M_2 = M_{21} \oplus M_{22} \oplus \cdots \oplus M_{2n_2},$$

con gli M_{ij} indecomponibili. Per il criterio di decomposizione diretta espresso in termini di elementi si conclude che $M = M_{11} \oplus M_{12} \oplus \cdots \oplus M_{1n_1} \oplus M_{21} \oplus \cdots \oplus M_{2n_2}$. □

L'unicità, a meno di isomorfismi, degli addendi indecomponibili di M segue immediatamente dai teoremi 3.6 e 3.7. Più precisamente, abbiamo il risultato usualmente chiamato

Teorema di Krull–Schmidt. *Sia M un modulo artiniano e noetheriano e siano $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n = N_1 \oplus N_2 \oplus \cdots \oplus N_m$ due decomposizioni con gli M_i e gli N_j indecomponibili. Allora $m = n$ ed esiste una permutazione $i \mapsto i'$ tale che $M_i \cong N_{i'}$, $1 \leq i \leq n$.*

J. H. M. Wedderburn formulò per primo questo teorema per i gruppi finiti nel 1909. La sua dimostrazione conteneva una lacuna colmata da R. Remak nel 1911. L'estensione ai gruppi abeliani con operatori, quindi ai moduli, si deve a W. Krull (1925); quella ai gruppi arbitrari con operatori a O. Schmidt (1928). Per qualche tempo si parlò di «teorema di Wedderburn–Remak–Krull–Schmidt», poi il nome si ridusse a «teorema di Krull–Schmidt».

Esercizi

1. Sia $p \in \mathbb{Z}$ primo e sia R il sottoinsieme di $\mathbb{Q}$ formato dai razionali a/b con $(p, b) = 1$. Mostrare che R è un sottoanello locale di $\mathbb{Q}$.

2. Mostrare che l'anello $\mathbb{Z}_p$ degli interi p-adici (p. 74) è locale.

3. Sia A un'algebra su un campo generata da un solo elemento nilpotente ($z^n = 0$). Allora A è locale.

4. Sia F un campo e sia R l'insieme delle matrici triangolari di $M_n(F)$ della forma

$$\begin{pmatrix} a & & & 0 \\ & a & & \\ * & & \ddots & \\ & & & a \end{pmatrix}.$$

   Mostrare che R è un anello locale.

5. Siano M e f come nel lemma di Fitting e si abbia $M = M_0 \oplus M_1$, dove gli M_i sono sottomoduli stabili per f, $f|_{M_0}$ è nilpotente e $f|_{M_1}$ è un automorfismo. Mostrare che $M_0 = f^{-\infty}0$ e $M_1 = f^{\infty}M$.

6. Usare il teorema 3.6 per dimostrare che, se $R^{(1)}$ e $R^{(2)}$ sono anelli locali e n_1, n_2 sono interi positivi tali che $M_{n_1}(R^{(1)}) \cong M_{n_2}(R^{(2)})$, allora $n_1 = n_2$ e $R^{(1)} \cong R^{(2)}$.

7. Sia M uno spazio vettoriale di dimensione finita sul campo F e sia T una trasformazione lineare di M. Mediante T si introduca su M una struttura di $F[X]$-modulo come in BAI, p. 165, dove X è un'indeterminata. Usare il teorema di Krull–Schmidt per dimostrare l'unicità dei divisori elementari di T (BAI, p. 193).

8. Nelle ipotesi del teorema 3.6, dimostrare la seguente *proprietà di scambio*: per un opportuno ordinamento degli N_j si ha $N_j \cong M_j$ e

$$M = g^{-1}(N_1) \oplus \cdots \oplus g^{-1}(N_k) \oplus M_{k+1} \oplus \cdots \oplus M_n, \qquad 1 \leq k \leq n.$$

Gli esercizi rimanenti riguardano l'estensione dei risultati del paragrafo ai Λ-gruppi (gruppi con insieme di operatori Λ) e ulteriori risultati su questi gruppi.

9. Siano G e H due Λ-gruppi e sia $\hom(G, H)$ l'insieme degli omomorfismi da G in H come Λ-gruppi. Per $f, g \in \hom(G, H)$, si definisca $f + g$ mediante $(f + g)(x) = f(x)g(x)$. Dare un esempio in cui questa applicazione non è un omomorfismo. Mostrare che, se K è un terzo Λ-gruppo e $h, k \in \hom(H, K)$, allora $hf \in \hom(G, K)$ e $h(f + g) = hf + hg$, $(h + k)f = hf + kf$. Si definisca l'applicazione zero da G a H ponendo $x \mapsto 1$. Osservare che è un omomorfismo.

10. Siano G un Λ-gruppo e $G_1, \ldots, G_n$ suoi Λ-sottogruppi normali tali che

$$G = G_1 G_2 \cdots G_n, \tag{39}$$

$$G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = 1, \qquad 1 \leq i \leq n. \tag{40}$$

    Mostrare che, per $x_i \in G_i$, $x_j \in G_j$ e $i \neq j$, si ha $x_i x_j = x_j x_i$, e che ogni elemento di G si scrive in uno e un solo modo come $x_1 x_2 \cdots x_n$, $x_i \in G_i$. Quando valgono (39) e (40) si dice che G è un *prodotto diretto (interno)* dei G_i e si scrive $G = G_1 \times G_2 \times \cdots \times G_n$. Sia e_i

l'applicazione $x_1x_2\cdots x_n \mapsto x_i$. Verificare che $e_i \in \operatorname{End} G = \hom(G,G)$ e che e_i è *normale*, ossia commuta con ogni automorfismo interno di G. Verificare che $e_i^2 = e_i$, che $e_ie_j = 0$ per $i \neq j$, che $e_i + e_j = e_j + e_i$ per ogni i, j, e che $e_1 + e_2 + \cdots + e_n = 1$. (L'operazione $+$ è associativa, perciò non occorrono parentesi.) Mostrare che, per $i_1, \ldots, i_r$ distinti in $\{1, \ldots, n\}$, si ha $e_{i_1} + \cdots + e_{i_r} \in \operatorname{End} G$.

11. Si dica che G è *indecomponibile* se $G \neq G_1 \times G_2$ per ogni coppia di Λ-sottogruppi normali diversi da G e da 1. Si dica che G è *fortemente indecomponibile* se $G \neq 1$ e vale la seguente proprietà di $\operatorname{End} G$: se f e g sono endomorfismi normali di G e $f + g$ è un automorfismo, allora f oppure g è un automorfismo. Mostrare che ne segue l'indecomponibilità. Usare questa nozione per estendere il teorema 3.6 ai gruppi con operatori.

12. Estendere il lemma di Fitting agli endomorfismi normali di un Λ-gruppo che soddisfa entrambe le condizioni di catena sui Λ-sottogruppi normali.

13. Estendere il teorema di Krull–Schmidt ai Λ-gruppi che soddisfano la condizione dell'esercizio 12.

14. Mostrare che, se f è un endomorfismo normale suriettivo di G, allora $f = 1_G + g$ con $g(G) \subset C$, dove C è il centro di G.

15. Dimostrare che un gruppo finito G ha una sola decomposizione in prodotto diretto di sottogruppi normali indecomponibili se vale almeno una delle due condizioni: (i) $C = 1$; (ii) $G' = G$, dove G' è il gruppo derivato (BAI, p. 245).

3.5 Moduli completamente riducibili

Dal punto di vista strutturale il tipo più semplice di modulo è quello irriducibile. Un modulo M si dice *irriducibile* se $M \neq 0$ e non contiene alcun sottomodulo N con $M \neq N \neq 0$. È un caso particolare del concetto di Λ-gruppo semplice che abbiamo incontrato discutendo il teorema di Jordan–Hölder (p. 108). Supponendo $R \neq 0$, si hanno le seguenti caratterizzazioni.

Teorema 3.9. *Le seguenti condizioni su un modulo sono equivalenti: (1) M è irriducibile; (2) $M \neq 0$ e ogni $x \neq 0$ di M genera M; (3) $M \cong R/I$, dove I è un ideale destro massimale di R.*

Dimostrazione. (1) $\Leftrightarrow$ (2). Sia M irriducibile. Allora $M \neq 0$ e, per $x \neq 0$ in M, il sottomodulo ciclico xR è non nullo. Dunque $xR = M$. Viceversa, supponiamo $M \neq 0$ e $M = xR$ per ogni $x \neq 0$ di M. Sia N un sottomodulo non nullo di M e sia $0 \neq x \in N$. Allora $N \supseteq xR = M$. Quindi M è irriducibile.

(1) $\Leftrightarrow$ (3). Osserviamo anzitutto che M è ciclico ($M = xR$) se e soltanto se $M \cong R/I$ per un ideale destro I di R. Se $M = xR$, l'applicazione $a \mapsto xa$ è un omomorfismo suriettivo di moduli da R a M. Il nucleo è l'annullatore $I = \operatorname{ann} x$ di x in R (BAI, p. 163). Esso è un ideale destro e $M \cong R/I$. Viceversa, R/I è ciclico con generatore $1 + I$ e, se $M \cong R/I$, anche M è ciclico. Osserviamo ora che i sottomoduli di R/I sono della forma I'/I, dove I' è un ideale destro di R contenente I. Quindi R/I è irriducibile se e soltanto se I è un ideale destro massimale di R. Ora, se M è irriducibile, è ciclico, dunque $M \cong R/I$ e I è un ideale destro massimale. Il viceversa è chiaro. Pertanto (1) $\Leftrightarrow$ (3). □

Forse il fatto più importante sui moduli irriducibili è il seguente risultato fondamentale.

Lemma di Schur. *Siano M e N moduli irriducibili. Ogni omomorfismo da M in N è nullo oppure è un isomorfismo. Inoltre l'anello degli endomorfismi* $\operatorname{End} M$ *è un anello di divisione.*

Dimostrazione. Sia f un omomorfismo da M in N. Allora $\ker f$ è un sottomodulo di M e $\operatorname{im} f$ è un sottomodulo di N. Per l'irriducibilità di M e di N, si ha $\ker f = M$ oppure 0, e $\operatorname{im} f = N$

oppure 0. Se $f \neq 0$, allora $\ker f \neq M$ e $\operatorname{im} f \neq 0$. Quindi $\ker f = 0$ e $\operatorname{im} f = N$, ossia f è un isomorfismo. Nel caso $N = M$ si conclude che ogni endomorfismo $f \neq 0$ è un automorfismo. Allora $f^{-1} \in \operatorname{End} M$ e questo anello è un anello di divisione. □

I moduli che considereremo ora generalizzano direttamente i moduli irriducibili e gli spazi vettoriali su un anello di divisione. Come vedremo, esistono diverse definizioni equivalenti di questa classe più ampia. Forse la più naturale è in termini di somme dirette di insiemi arbitrari di sottomoduli, anche infiniti. Definiamo dunque tale concetto.

Sia $S = \{M_\alpha\}$ un insieme di sottomoduli di M. Il sottomodulo $\sum M_\alpha$ generato dagli M_α è l'insieme delle somme

$$x_{\alpha_1} + x_{\alpha_2} + \cdots + x_{\alpha_k}, \qquad x_{\alpha_i} \in M_{\alpha_i}.$$

L'insieme S si dice *indipendente* se per ogni $M_\alpha \in S$ si ha $M_\alpha \cap \sum_{M_\beta \neq M_\alpha} M_\beta = 0$. Altrimenti S si dice *dipendente*. Se N è un sottomodulo, $\{N\}$ è indipendente. Scrivendo la definizione di dipendenza in termini di elementi, vediamo che un insieme dipendente non vuoto di moduli contiene un sottoinsieme finito dipendente. Grazie al lemma di Zorn questa proprietà implica che, se S è un insieme non vuoto di sottomoduli e T è un suo sottoinsieme indipendente, allora T è contenuto in un sottoinsieme indipendente massimale di S. Se $M = \sum M_\alpha$ e $S = \{M_\alpha\}$ è indipendente, si dice che M è *somma diretta* (interna) dei sottomoduli M_α e si scrive $M = \bigoplus M_\alpha$. Si generalizza così direttamente il concetto considerato nel § 3.4 per insiemi finiti di sottomoduli.

Ci servirà il seguente lemma.

Lemma 1. *Sia $S = \{M_\alpha\}$ un insieme indipendente di sottomoduli di M e sia N un sottomodulo tale che $N \cap \sum M_\alpha = 0$. Allora $S \cup \{N\}$ è indipendente.*

Dimostrazione. In caso contrario esisterebbe $x_\alpha \in M_\alpha$, con $M_\alpha \in S$, tale che $x_\alpha = y + x_{\alpha_1} + \cdots + x_{\alpha_k} \neq 0$, dove $y \in N$, $x_{\alpha_i} \in M_{\alpha_i} \in S$ e $M_\alpha \neq M_{\alpha_i}$ per $1 \leq i \leq k$. Se $y = 0$, avremmo $x_\alpha = x_{\alpha_1} + \cdots + x_{\alpha_k}$, contro l'indipendenza di S. Dunque $y \neq 0$. Ma allora $y = x_\alpha - x_{\alpha_1} - \cdots - x_{\alpha_k} \in \sum M_\alpha$, contro l'ipotesi $N \cap \sum M_\alpha = 0$. □

Possiamo ora dare la seguente definizione.

Definizione 3.2. *Un modulo M è completamente riducibile se è somma diretta di sottomoduli irriducibili.*

Evidentemente ogni modulo irriducibile è completamente riducibile. Sia ora M uno spazio vettoriale destro su un anello di divisione Δ. Per $0 \neq x \in M$, $x\Delta$ è un sottomodulo irriducibile di M e $M = \sum_{x \neq 0} x\Delta$, dunque M è somma di sottomoduli irriducibili. In effetti, M è completamente riducibile. Ciò seguirà dal lemma seguente.

Lemma 2. *Sia $M = \sum M_\alpha$, con gli M_α irriducibili, e sia N un sottomodulo di M. Esiste un sottoinsieme $\{M_\beta\}$ di $\{M_\alpha\}$ tale che $\{N\} \cup \{M_\beta\}$ sia indipendente e $M = N + \sum M_\beta$.*

Dimostrazione. Consideriamo i sottoinsiemi di $\{M_\alpha\} \cup \{N\}$ che contengono N, e sia $\{M_\beta\} \cup \{N\}$ un sottoinsieme indipendente massimale fra questi, con N distinto dagli M_β. Poniamo $M' = N + \sum M_\beta$. Se $M' \neq M$, esiste M_α non contenuto in M'. Poiché M_α è irriducibile e $M_\alpha \cap M'$ è un suo sottomodulo, deve essere $M_\alpha \cap M' = 0$. Per il lemma 1, $\{M_\beta\} \cup \{N\} \cup \{M_\alpha\}$ sarebbe allora indipendente, contro la massimalità. Quindi $M = N + \sum M_\beta$. □

Questo lemma ha due conseguenze importanti. La prima è la seguente.

Corollario 1. *Se M è somma di moduli irriducibili, diciamo $M = \sum M_\alpha$, con gli M_α irriducibili, allora $M = \bigoplus M_\beta$ per un sottoinsieme $\{M_\beta\}$ di $\{M_\alpha\}$.*

Basta porre $N = 0$ nel lemma 2. Se M è uno spazio vettoriale destro su Δ, allora $M = \sum_{x \neq 0} x\Delta$ e ciascun $x\Delta$ è irriducibile. Per il corollario 1, M è dunque completamente riducibile. Abbiamo inoltre il seguente corollario.

Corollario 2. *Se M è completamente riducibile e N è un suo sottomodulo, esiste un sottomodulo N' di M tale che $M = N \oplus N'$.*

Dimostrazione. Sia $M = \sum M_\alpha$ con gli M_α irriducibili. Per il lemma 2 esiste un sottoinsieme $\{M_\beta\}$ di $\{M_\alpha\}$ tale che $M = \sum M_\beta + N$ e $\{N\} \cup \{M_\beta\}$ è indipendente. Posto $N' = \sum M_\beta$, abbiamo $M = N \oplus N'$. □

La proprietà enunciata nel corollario 2 dice che il reticolo $L(M)$ dei sottomoduli di un modulo completamente riducibile M è complementato (BAI, p. 469). Mostreremo che questa proprietà caratterizza i moduli completamente riducibili. Dimostriamo anzitutto il seguente lemma.

Lemma 3. *Sia M un modulo il cui reticolo $L(M)$ dei sottomoduli sia complementato. Anche $L(N)$ e $L(\bar{M})$ sono complementati per ogni sottomodulo N e per ogni immagine omomorfa $\bar{M}$ di M.*

Dimostrazione. Sia P un sottomodulo di N. Allora $M = P \oplus P'$ con P' sottomodulo di M. Poniamo $P'' = P' \cap N$. Per la modularità di $L(M)$ (BAI, p. 463), $N = N \cap M = N \cap (P + P') = P + P''$. Dunque $N = P \oplus P''$. Questo dimostra la prima asserzione. Per la seconda possiamo supporre che $\bar{M} = M/P$ con P sottomodulo di M. Allora $M = P \oplus P'$ per un sottomodulo P' e $\bar{M} \cong P'$. Poiché $L(P')$ è complementato per la prima parte, lo è anche $L(\bar{M})$. □

Per dimostrare che dalla complementazione di $L(M)$ segue la completa riducibilità, il risultato decisivo è il seguente.

Lemma 4. *Sia M un modulo non nullo con $L(M)$ complementato. Allora M contiene sottomoduli irriducibili.*

Dimostrazione. Sia $0 \neq x \in M$ e sia $\{N\}$ l'insieme dei sottomoduli di M che non contengono x. Tale insieme contiene 0 e quindi non è vuoto. Per il lemma di Zorn esiste un elemento massimale P in $\{N\}$. Chiaramente $P \neq M$, ma ogni sottomodulo strettamente maggiore di P contiene x. Dunque, se P_1 e P_2 contengono propriamente P, anche $P_1 \cap P_2$ contiene propriamente P. Ne segue che due sottomoduli non nulli di M/P hanno sempre intersezione non nulla. Sia ora P' un sottomodulo di M tale che $M = P \oplus P'$. Poiché $P' \cong M/P$, anche in P' due sottomoduli non nulli hanno sempre intersezione non nulla. Ne segue che P' è irriducibile. Infatti $P' \neq 0$ poiché $M \neq P$, e se P_1' fosse un sottomodulo di P' diverso da P' e da 0, il lemma 3 darebbe un sottomodulo P_2' con $P' = P_1' \oplus P_2'$. Si avrebbe allora $P_1' \cap P_2' = 0$ con entrambi i sottomoduli non nulli, contro la proprietà appena dimostrata per P'. □

Siamo ora in grado di stabilire le seguenti caratterizzazioni.

Teorema 3.10. *Le seguenti condizioni su un modulo sono equivalenti: (1) $M = \sum M_\alpha$ con gli M_α irriducibili; (2) M è completamente riducibile; (3) $M \neq 0$ e il reticolo $L(M)$ dei sottomoduli di M è complementato.*

Dimostrazione. L'implicazione (1) ⇒ (2) è stata dimostrata nel corollario 1 e (2) ⇒ (3) nel corollario 2. Supponiamo ora che valga (3). Per il lemma 4, M contiene sottomoduli irriducibili. Sia $\{M_\alpha\}$ il loro insieme e poniamo $M' = \sum M_\alpha$. Allora $M = M' \oplus M''$ con M'' sottomodulo. Per il lemma 3, $L(M'')$ è complementato. Dunque, se $M'' \neq 0$, esso contiene uno degli M_α, contro $M'' \cap M' = M'' \cap \sum M_\alpha = 0$. Pertanto $M'' = 0$ e $M = M' = \sum M_\alpha$. Questo dimostra (3) ⇒ (1). □

Sia N un sottomodulo irriducibile del modulo completamente riducibile M. Si chiama *componente omogenea* H_N di M determinata da N la somma $\sum N'$ estesa a tutti i sottomoduli $N' \cong N$. Mostreremo che M è somma diretta delle sue componenti omogenee. Vale anzi il seguente risultato più preciso.

Teorema 3.11. *Sia $M = \bigoplus M_{\alpha\beta}$ con gli $M_{\alpha\beta}$ irriducibili. Si scelgano gli indici in modo tale che $M_{\alpha\beta} \cong M_{\alpha'\beta'}$ se e soltanto se $\alpha = \alpha'$. Allora $H_\alpha = \sum_\beta M_{\alpha\beta}$ è una componente omogenea,*

$M = \bigoplus H_\alpha$ *e ogni componente omogenea coincide con uno degli* H_α.

Dimostrazione. Sia N un sottomodulo irriducibile di M. Poiché N è ciclico, è contenuto in una somma finita $M' = M_1 \oplus M_2 \oplus \cdots \oplus M_n$, con $M_i \in \{M_{\alpha\beta}\}$. Restringendo a N le proiezioni sugli M_i determinate dalla decomposizione di M', otteniamo omomorfismi da N negli M_i. Per il lemma di Schur sono nulli oppure isomorfismi. Quelli non nulli sono quindi isomorfismi su moduli M_i che, nella famiglia $\{M_{\alpha\beta}\}$, hanno tutti lo stesso primo indice. Pertanto $N \subseteq H_\alpha$ per un certo α. Per ogni sottomodulo $N' \cong N$ si ha del pari $N' \subseteq H_\alpha$. Quindi $H_N \subseteq H_\alpha$. Poiché è chiaro che $H_\alpha \subseteq H_N$, otteniamo $H_N = H_\alpha$. L'arbitrarietà del sottomodulo irriducibile N mostra che tutte le componenti omogenee si ottengono in questo modo. Infine $M = \bigoplus H_\alpha$ segue subito da $M = \bigoplus M_{\alpha\beta}$ e $H_\alpha = \sum_\beta M_{\alpha\beta}$. □

Esercizi

1. Sia M uno spazio vettoriale (sinistro) di dimensione finita su un campo F. Mostrare che M, considerato in modo naturale come modulo destro su $R = \mathrm{End}_F M$, è irriducibile. Vale ancora il risultato sostituendo a F un anello di divisione? E se si elimina l'ipotesi che la dimensione sia finita?

2. Sia M lo spazio vettoriale di base (e_1, e_2) su un campo F e sia R' l'insieme delle trasformazioni lineari a di M su F tali che $ae_1 = \alpha e_1$, $ae_2 = \beta e_1 + \gamma e_2$, dove $\alpha, \beta, \gamma \in F$. Mostrare che R' è un anello di endomorfismi e che M, considerato in modo naturale come R'-modulo destro, non è irriducibile. Mostrare che $\mathrm{End}_{R'} M$ è il campo delle moltiplicazioni scalari $x \mapsto \alpha x$. (Questo esempio mostra che il viceversa del lemma di Schur è falso.)

3. Esercizio 2, p. 193 di BAI.

4. Sia V il modulo su $F[\lambda]$ definito da una trasformazione lineare T come nell'esercizio 3, p. 103. Mostrare che V è completamente riducibile se e soltanto se il polinomio minimo $m(\lambda)$ di T è prodotto di fattori irriducibili distinti in $F[\lambda]$.

5. Mostrare che $\bigoplus M_\alpha$, con le iniezioni $i_\beta \colon M_\beta \to \bigoplus M_\alpha$, costituisce un coprodotto degli M_α.

6. Sia $\{M_\alpha\}$ un insieme di moduli irriducibili. Il prodotto $\prod M_\alpha$ è completamente riducibile?

7. Mostrare che un modulo completamente riducibile è artiniano se e soltanto se è noetheriano.

8. Sia M completamente riducibile. Mostrare che ogni sua componente omogenea H è un sottomodulo per l'azione naturale di $\mathrm{End}_R M$.

3.6 Relazioni astratte di dipendenza. Invarianza della dimensione

È ben noto che, in uno spazio vettoriale di dimensione finita, due basi qualsiasi hanno lo stesso numero di elementi. Dimostreremo ora una notevole generalizzazione di questo risultato: se M è un modulo completamente riducibile e $M = \bigoplus M_\alpha = \bigoplus M'_\beta$, con gli M_α e gli M'_β irriducibili, allora $|\{M_\alpha\}| = |\{M'_\beta\}|$. Per dimostrarlo svilupperemo alcuni risultati generali sulle relazioni astratte di dipendenza. Questo modo di procedere ha il vantaggio di fornire risultati applicabili in varie altre situazioni interessanti (per esempio, alla dipendenza algebrica nei campi).

Consideriamo un insieme non vuoto X e una corrispondenza Δ da X al suo insieme delle parti $\mathcal{P}(X)$. Scriviamo $x \prec S$ se $(x, S) \in \Delta$. Diremo che Δ è una *relazione di dipendenza* in X se sono soddisfatte le condizioni seguenti.

1. Se $x \in S$, allora $x \prec S$.

2. Se $x \prec S$, allora $x \prec F$ per un opportuno sottoinsieme finito F di S.

3. Se $x \prec S$ e $y \prec T$ per ogni $y \in S$, allora $x \prec T$.

4. Se $x \prec S$ ma $x \not\prec S \setminus \{y\}$ (il complementare di $\{y\}$ in S), allora $y \prec (S \setminus \{y\}) \cup \{x\}$. Questo è l'*assioma di scambio di Steinitz.*

Il caso che ci interessa direttamente è quello in cui X è l'insieme dei sottomoduli irriducibili di un modulo completamente riducibile M. Per $M_\alpha \in X$ e $S \subseteq X$, poniamo $M_\alpha \prec S$ se $M_\alpha \subseteq \sum_{M_\beta \in S} M_\beta$. La proprietà 1 è evidente. Supponiamo ora $M_\alpha \subseteq \sum_{M_\beta \in S} M_\beta$ e scegliamo $0 \neq x_\alpha \in M_\alpha$. Allora $x_\alpha \in \sum_{M_\gamma \in F} M_\gamma$ per un opportuno sottoinsieme finito F di S. Ne segue che $M_\alpha = x_\alpha R \subseteq \sum_{M_\gamma \in F} M_\gamma$. Ciò dimostra la proprietà 2. La proprietà 3 è chiara. Supponiamo ora che $M_\alpha \subseteq \sum_{M_\beta \in S} M_\beta$, ma che M_α non sia contenuto nella somma estesa agli $M_\gamma \in S$ diversi da un dato M_β. Come sopra, scegliamo $0 \neq x_\alpha \in M_\alpha$ e scriviamo

$$x_\alpha = x_{\beta_1} + x_{\beta_2} + \cdots + x_{\beta_m}, \qquad x_{\beta_i} \in M_{\beta_i} \in S.$$

Allora $M_\alpha \subseteq M_{\beta_1} + M_{\beta_2} + \cdots + M_{\beta_m}$. Possiamo supporre che tutti gli x_{β_i} siano non nulli e che $M_{\beta_i} \neq M_{\beta_j}$ per $i \neq j$. L'ipotesi sulla somma che esclude M_β implica inoltre che uno degli M_{β_i} coincida con M_β. Possiamo prendere $i = 1$. Quindi $0 \neq x_\beta = x_\alpha - x_{\beta_2} - \cdots - x_{\beta_m}$, da cui $M_\beta = x_\beta R \subseteq M_\alpha + M_{\beta_2} + \cdots + M_{\beta_m}$. Dunque $M_\beta \prec (S \setminus \{M_\beta\}) \cup \{M_\alpha\}$. È così dimostrato l'assioma di scambio.

Consideriamo ora una relazione di dipendenza qualsiasi su X. Un sottoinsieme S di X si dice *indipendente* (rispetto a Δ) se nessun $x \in S$ dipende da $S \setminus \{x\}$. Altrimenti S si dice *dipendente.* Dimostriamo l'analogo del lemma 1 del § 3.5.

Lemma 1. *Se S è indipendente e $x \not\prec S$, allora $S \cup \{x\}$ è indipendente.*[4]

Dimostrazione. Poiché $x \not\prec S$, si ha $x \notin S$. Se $S \cup \{x\}$ non fosse indipendente, esisterebbe $y \in S$ tale che $y \prec (S \setminus \{y\}) \cup \{x\}$. Per l'indipendenza di S si ha $y \not\prec S \setminus \{y\}$. L'assioma di scambio darebbe dunque $x \prec (S \setminus \{y\}) \cup \{y\} = S$, contro l'ipotesi. Pertanto $S \cup \{x\}$ è indipendente. □

Definizione 3.3. *Un sottoinsieme B di X si chiama base di X rispetto alla relazione di dipendenza Δ se (i) B è indipendente e (ii) ogni $x \in X$ dipende da B. (È ammesso $B = \varnothing$.)*

Teorema 3.12. *Esiste una base di X e due basi qualsiasi hanno lo stesso numero cardinale.*

Dimostrazione. La proprietà di finitezza 2 consente di applicare il lemma di Zorn per dimostrare che X contiene un sottoinsieme indipendente massimale. Essa implica infatti che l'unione di ogni catena di sottoinsiemi indipendenti di X è indipendente. Il lemma di Zorn dà quindi la conclusione voluta. Sia ora B un sottoinsieme indipendente massimale di X e sia $x \in X$. Allora $x \prec B$, altrimenti, per il lemma 1, $B \cup \{x\}$ sarebbe indipendente, contro la massimalità di B. Dunque ogni elemento di X dipende da B, che è quindi una base.

Siano B e C due basi. Se $B = \varnothing$, evidentemente anche $C = \varnothing$. Supponiamo dunque B, C non vuoti. Consideriamo dapprima il caso in cui B sia finito e scriviamo $B = \{x_1, \ldots, x_n\}$. Dimostriamo per induzione su k che per $1 \leq k \leq n+1$ esistono elementi $y_i \in C$ tali che $\{y_1, \ldots, y_{k-1}, x_k, \ldots, x_n\}$ sia una base. Per $k = 1$ ciò è vero perché B è una base. Supponiamo che valga per un certo $k \leq n$. Affermiamo che esiste $y \in C$ che non dipende da

$$D = \{y_1, \ldots, y_{k-1}, x_{k+1}, \ldots, x_n\}.$$

[4] Nell'enunciato e nella prima riga della dimostrazione, a p. 123 dell'originale, è caduta la negazione in $x \not\prec S$. Anche l'indipendenza di S, nella riga successiva, dà $y \not\prec S \setminus \{y\}$. [N.d.T.]

Altrimenti ogni $y \in C$ dipenderebbe da D e quindi ogni $x \in B$ dipenderebbe da D. Ciò contraddice l'indipendenza di $\{y_1, \dots, y_{k-1}, x_k, \dots, x_n\}$. Scegliamo $y_k = y$ con $y_k \not\prec D$. Per il lemma 1, $\{y_1, \dots, y_k, x_{k+1}, \dots, x_n\}$ è indipendente. Inoltre, poiché $y_k \prec \{y_1, \dots, y_{k-1}, x_k, \dots, x_n\}$, l'assioma di scambio dà $x_k \prec \{y_1, \dots, y_{k-1}, y_k, x_{k+1}, \dots, x_n\}$. Tutti gli elementi della precedente base dipendono quindi dal nuovo insieme, e di conseguenza ne dipende ogni $x \in X$. Pertanto $\{y_1, \dots, y_k, x_{k+1}, \dots, x_n\}$ è una base. Abbiamo dimostrato che a ogni passo k esiste una base di questa forma con gli y_i in C. Per $k = n$ otteniamo una base $\{y_1, \dots, y_n\}$ contenuta in C. Necessariamente $C = \{y_1, \dots, y_n\}$, e dunque $|C| = n = |B|$. Lo stesso argomento si applica se è C a essere finito.

Resta il caso in cui $|B|$ e $|C|$ sono entrambi infiniti. Per dimostrare il risultato useremo un argomento di conteggio dovuto a H. Löwig. Per ogni $y \in C$ scegliamo un sottoinsieme finito F_y di B tale che $y \prec F_y$. L'applicazione $y \mapsto F_y$ dà $|C| \geq |\{F_y\}|$. Poiché ogni F_y è finito, segue che $\aleph_0|C| \geq |\bigcup_y F_y|$. Essendo $|C|$ infinito, $\aleph_0|C| = |C|$, dunque $|C| \geq |\bigcup_y F_y|$. Ora $\bigcup_y F_y = B$: altrimenti ogni $y \in C$ dipenderebbe da uno stesso sottoinsieme proprio B' di B e, essendo C una base, ogni $x \in B$ dipenderebbe da B'. Ciò contraddice l'indipendenza di B. Pertanto $|C| \geq |\bigcup_y F_y| = |B|$. Per simmetria $|B| \geq |C|$. Dunque $|B| = |C|$. □

La prima parte della dimostrazione mostra che ogni sottoinsieme indipendente massimale di X è una base. Il viceversa è evidente. Ricordiamo anche due utili complementi al risultato sull'esistenza di una base:

(i) se ogni elemento di X dipende da un sottoinsieme S, allora S contiene una base;

(ii) se S è indipendente, esiste una base contenente S.

Applichiamo il teorema 3.12 ai moduli completamente riducibili prendendo per X l'insieme dei sottomoduli irriducibili di un modulo completamente riducibile M e ponendo $M_\alpha \prec \{M_\beta\}$ se $M_\alpha \subseteq \sum M_\beta$. Abbiamo visto che si tratta di una relazione di dipendenza. Inoltre l'indipendenza di un insieme di moduli irriducibili rispetto a $\prec$ coincide con l'indipendenza già definita per i sottomoduli di un modulo. Un insieme $B = \{M_\beta\}$ di moduli irriducibili è una base di X se è indipendente e ogni sottomodulo irriducibile M_α è contenuto in $\sum M_\beta$. Poiché M è somma di sottomoduli irriducibili, quest'ultima condizione equivale a $M = \sum M_\beta$. Dunque $B = \{M_\beta\}$ è una base se e soltanto se $M = \bigoplus M_\beta$. Il teorema sulle basi di un insieme X rispetto a una relazione di dipendenza dà allora il seguente risultato.

Teorema 3.13. *Sia $M = \bigoplus M_\beta = \bigoplus N_\gamma$ con gli M_β e gli N_γ irriducibili. Allora $|\{M_\beta\}| = |\{N_\gamma\}|$.*

Chiameremo $|\{M_\beta\}|$ la *dimensione* del modulo completamente riducibile M. Se M è uno spazio vettoriale destro su Δ di base (x_β), allora $M = \bigoplus x_\beta\Delta$ e ogni $x_\beta\Delta$ è irriducibile. La dimensione di M è dunque la cardinalità di (x_β). Perciò due basi qualsiasi hanno la stessa cardinalità. È questo il consueto «teorema di invarianza della dimensione».

Possiamo anche applicare il teorema 3.13 e la decomposizione in componenti omogenee per ottenere un teorema di Krull–Schmidt per i moduli completamente riducibili.

Teorema 3.14. *Sia $M = \bigoplus M_\beta = \bigoplus N_\gamma$ con gli M_β e gli N_γ irriducibili. Esiste una biiezione fra $\{M_\beta\}$ e $\{N_\gamma\}$ tale che i moduli corrispondenti siano isomorfi.*

Ciò è chiaro, poiché in ciascuna componente omogenea l'insieme degli M_β contenuti nella componente ha la stessa cardinalità dell'insieme degli N_γ in essa contenuti.

Esercizio

1. Mostrare che, se un modulo completamente riducibile M possiede una serie di composizione, la sua lunghezza, nel senso dell'esercizio 3 (p. 110), coincide con la dimensione.

3.7 Prodotti tensoriali di moduli

Il prodotto tensoriale di moduli generalizza una nozione classica per gli spazi vettoriali, che da lungo tempo svolge un ruolo importante in diversi rami della matematica, in particolare nella geometria differenziale e nella teoria delle rappresentazioni. Per gli spazi vettoriali lo si definiva originariamente servendosi di basi. La prima definizione indipendente dalle basi sembra dovuta a H. Whitney. Successivi perfezionamenti hanno condotto alla forma usuale che presenteremo. Prima di darla esaminiamo un esempio che conserva qualcosa dello spirito del punto di vista più antico.

Esempio. Sia R un anello. Vogliamo considerare insieme moduli liberi sinistri e destri su R. Indichiamo con $R^{(n)}$ il modulo libero destro con una base di n elementi e con ${}^{(n)}R$ il modulo libero sinistro con una base di n elementi. Conviene scrivere gli elementi di ${}^{(n)}R$ come righe $(x_1, \dots, x_n)$, $x_i \in R$, e quelli di $R^{(n)}$ come colonne,

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \tag{41}$$

Nel primo caso gli elementi di R agiscono per moltiplicazione a sinistra, nel secondo a destra. Consideriamo $R^{(m)}$, ${}^{(n)}R$ e il gruppo additivo $M_{m,n}(R)$ delle matrici $m \times n$ a coefficienti in R. Per $x \in R^{(m)}$ come in (41) e $y = (y_1, \dots, y_n) \in {}^{(n)}R$ formiamo il prodotto matriciale

$$xy = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} (y_1, \dots, y_n) = \begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & x_2y_2 & \cdots & x_2y_n \\ \vdots & \vdots & & \vdots \\ x_my_1 & x_my_2 & \cdots & x_my_n \end{pmatrix}. \tag{42}$$

Questo prodotto è distributivo da ambo i lati e soddisfa la condizione di associatività $(xa)y = x(ay)$, $a \in R$. È dunque un esempio di prodotto bilanciato nel senso che definiremo ora per una coppia costituita da un modulo destro e uno sinistro.

Siano M un modulo destro e N un modulo sinistro sull'anello R; scriveremo rispettivamente M_R e ${}_RN$. Un *prodotto bilanciato* di M e N è un gruppo abeliano P (in notazione additiva) con un'applicazione f dell'insieme prodotto $M \times N$ in P che soddisfi le condizioni

B1. $f(x + x', y) = f(x, y) + f(x', y)$,
B2. $f(x, y + y') = f(x, y) + f(x, y')$,
B3. $f(xa, y) = f(x, ay)$.

Qui $x, x' \in M$, $y, y' \in N$ e $a \in R$. Come per la somma e il prodotto in un anello, queste condizioni implicano $f(0, y) = 0 = f(x, 0)$ e $f(-x, y) = -f(x, y) = f(x, -y)$. Denotiamo il prodotto bilanciato con (P, f). Se (Q, g) ne è un secondo, un *morfismo da* (P, f) *a* (Q, g) è un omomorfismo η del gruppo additivo P nel gruppo additivo Q tale che per ogni $(x, y) \in M \times N$ si abbia

$$g(x, y) = \eta f(x, y). \tag{43}$$

Definizione 3.4. *Un prodotto tensoriale di M_R e ${}_RN$ è un prodotto bilanciato $(M \otimes_R N, \otimes)$ tale che per ogni prodotto bilanciato (P, f) di M_R e ${}_RN$ esista un unico morfismo da $(M \otimes_R N, \otimes)$ a (P, f). In altre parole, esiste un unico omomorfismo del gruppo abeliano $M \otimes_R N$ nel gruppo abeliano P che manda ogni $x \otimes y$, con $x \in M$, $y \in N$, in $f(x, y) \in P$.*

Dalla definizione risulta che, se $((M \otimes_R N)_1, \otimes_1)$ e $((M \otimes_R N)_2, \otimes_2)$ sono prodotti tensoriali, esiste un unico isomorfismo del primo gruppo sul secondo che manda $x \otimes_1 y$ in $x \otimes_2 y$. È chiaro inoltre che il gruppo $M \otimes_R N$ è generato dai prodotti $x \otimes y$. Anzi, poiché $-(x \otimes y) = (-x) \otimes y$, ogni suo elemento ha la forma $\sum x_i \otimes y_i$, con $x_i \in M$, $y_i \in N$.

Costruiamo un prodotto tensoriale per una coppia assegnata $(M_R, {}_RN)$. Partiamo dal gruppo abeliano libero F di base $M \times N$. I suoi elementi sono della forma

$$n_1(x_1, y_1) + n_2(x_2, y_2) + \cdots + n_r(x_r, y_r), \tag{44}$$

con $n_i \in \mathbb{Z}$, $x_i \in M$, $y_i \in N$. La somma è quella ovvia e, se le coppie (x_i, y_i) sono distinte, la (44) è zero se e soltanto se tutti gli n_i sono zero. Sia G il sottogruppo di F generato da tutti gli elementi

$$\begin{aligned} &(x + x', y) - (x, y) - (x', y), \\ &(x, y + y') - (x, y) - (x, y'), \\ &(xa, y) - (x, ay), \end{aligned} \tag{45}$$

per $x, x' \in M$, $y, y' \in N$, $a \in R$. Poniamo

$$M \otimes_R N = F/G, \qquad x \otimes y = (x, y) + G \in M \otimes_R N. \tag{46}$$

Affermiamo che $(M \otimes_R N, \otimes)$ è un prodotto tensoriale di M e N. Anzitutto,

$$\begin{aligned} (x + x') \otimes y - x \otimes y - x' \otimes y &= ((x + x', y) + G) - ((x, y) + G) - ((x', y) + G) \\ &= ((x + x', y) - (x, y) - (x', y)) + G = G = 0. \end{aligned}$$

Analogamente $x \otimes (y + y') = x \otimes y + x \otimes y'$ e $xa \otimes y = x \otimes ay$. Dunque il prodotto è bilanciato. Sia ora (P, f) un qualunque prodotto bilanciato. Poiché F è libero di base $M \times N$, esiste un unico omomorfismo di F in P che manda (x, y) in $f(x, y)$. Sia K il suo nucleo. Le condizioni B1, B2 e B3 implicano che tutti gli elementi $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$ e $(xa, y) - (x, ay)$ appartengono a K. Quindi $G \subseteq K$ e abbiamo un omomorfismo da $M \otimes_R N = F/G$ in P che manda $x \otimes y = (x, y) + G$ in $f(x, y)$. È unico perché le classi $x \otimes y$ generano $M \otimes_R N$. Abbiamo così verificato la proprietà richiesta.

Supponiamo d'ora in poi di avere scelto una determinazione di $(M \otimes_R N, \otimes)$. Scriveremo semplicemente $M \otimes N$, oppure $M \otimes_R N$ quando occorra specificare l'anello, e parleremo del prodotto tensoriale di M e N. Siano dati omomorfismi di moduli $f\colon M \to M'$ e $g\colon N \to N'$. L'applicazione $(x, y) \mapsto fx \otimes gy$ di $M \times N$ in $M' \otimes N'$ soddisfa le condizioni per un prodotto bilanciato poiché

$$\begin{aligned} f(x + x') \otimes gy &= fx \otimes gy + fx' \otimes gy, \\ fx \otimes g(y + y') &= fx \otimes gy + fx \otimes gy', \\ f(xa) \otimes gy &= fx \otimes g(ay). \end{aligned}$$

Vi è quindi un unico omomorfismo di $M \otimes N$ in $M' \otimes N'$ che manda $x \otimes y$ in $fx \otimes gy$. Lo denotiamo con $f \otimes g$; per definizione

$$(f \otimes g)(x \otimes y) = fx \otimes gy \tag{47}$$

per ogni $x \in M$, $y \in N$. Siano inoltre $f'\colon M' \to M''$, $g'\colon N' \to N''$ omomorfismi. Allora $f'f\colon M \to M''$, $g'g\colon N \to N''$ e

$$\begin{aligned}(f'f \otimes g'g)(x \otimes y) &= f'fx \otimes g'gy = (f' \otimes g')(fx \otimes gy)\\ &= (f' \otimes g')((f \otimes g)(x \otimes y)) = ((f' \otimes g')(f \otimes g))(x \otimes y).\end{aligned}$$

Poiché gli $x \otimes y$ generano $M \otimes N$, ne segue

$$(f' \otimes g')(f \otimes g) = f'f \otimes g'g. \tag{48}$$

Da $(1_M \otimes 1_N)(x \otimes y) = x \otimes y$ segue inoltre

$$1_M \otimes 1_N = 1_{M\otimes N}. \tag{49}$$

Questi risultati dicono che le corrispondenze $(M, N) \mapsto M \otimes N$, $(f, g) \mapsto f \otimes g$ definiscono un funtore dalla categoria **mod**-$R \times R$-**mod** alla categoria **Ab** (o $\mathbb{Z}$-**mod**). Lo indicheremo con $\otimes_R$.

Siano ancora $f\colon M \to M'$ in **mod**-R e $g\colon N \to N'$ in R-**mod**. Il diagramma

$$\begin{array}{ccc} M \otimes N & \xrightarrow{1_M \otimes g} & M \otimes N' \\ {\scriptstyle f\otimes 1_N}\downarrow & \searrow^{f\otimes g} & \downarrow{\scriptstyle f\otimes 1_{N'}} \\ M' \otimes N & \xrightarrow[1_{M'} \otimes g]{} & M' \otimes N' \end{array}$$

è commutativo; in altre parole,

$$(f \otimes 1_{N'})(1_M \otimes g) = f \otimes g = (1_{M'} \otimes g)(f \otimes 1_N). \tag{50}$$

Ciò segue subito dalla (48). Per $f_i\colon M \to M'$ e $g_i\colon N \to N'$ si hanno anche le leggi distributive

$$\begin{aligned}(f_1 + f_2) \otimes g &= f_1 \otimes g + f_2 \otimes g,\\ f \otimes (g_1 + g_2) &= f \otimes g_1 + f \otimes g_2.\end{aligned} \tag{51}$$

Basta applicare i due membri a $x \otimes y$, $x \in M$, $y \in N$.

Fissiamo uno degli argomenti di $\otimes_R$ e studiamo i funtori di una variabile che ne risultano. Fissato un R-modulo destro M, definiamo il funtore $M\otimes_R$ (o $M\otimes$) ponendo, per ogni R-modulo sinistro N e ogni omomorfismo $g\colon N \to N'$ di R-moduli sinistri,

$$(M\otimes_R)N = M \otimes_R N, \qquad (M\otimes_R)(g) = 1_M \otimes g.$$

Si ha $1_M \otimes g'g = (1_M \otimes g')(1_M \otimes g)$ per $g'\colon N' \to N''$, e $1_M \otimes 1_N = 1_{M\otimes N}$. Vale inoltre l'additività, poiché per la (51) si ha $1_M \otimes (g_1 + g_2) = 1_M \otimes g_1 + 1_M \otimes g_2$. Dunque $M\otimes_R$ è un funtore da R-**mod** a $\mathbb{Z}$-**mod** nel senso adottato in questo capitolo. Analogamente ogni modulo sinistro N definisce un funtore $\otimes_R N$ (o $\otimes N$) da **mod**-R a **mod**-$\mathbb{Z}$, ponendo

$$(\otimes_R N)M = M \otimes_R N, \qquad (\otimes_R N)(f) = f \otimes 1_N$$

per $f\colon M \to M'$ in **mod**-R. Prendiamo in particolare $M = R = R_R$, ossia R come modulo destro su se stesso.

Proposizione 3.2. *Sia N un R-modulo sinistro. L'applicazione*

$$\eta_N\colon y \longmapsto 1 \otimes y \tag{52}$$

*è un isomorfismo di N, considerato come $\mathbb{Z}$-modulo, su $R \otimes_R N$. Inoltre $N \mapsto \eta_N$ è un isomorfismo naturale fra il funtore dimenticante da R-**mod** a $\mathbb{Z}$-**mod** (o **Ab**) e il funtore $R\otimes_R$.*

Dimostrazione. La (52) è evidentemente uno $\mathbb{Z}$-omomorfismo. D'altra parte $f(r, y) = ry$, con $r \in R$, $y \in N$, è un prodotto bilanciato di R e N. Vi è dunque uno $\mathbb{Z}$-omomorfismo ζ_N di $R \otimes_R N$ in N tale che $\zeta_N(r \otimes y) = ry$. È chiaro che $\zeta_N\eta_N = 1_N$ e $\eta_N\zeta_N = 1_{R\otimes N}$. Ciò dimostra la prima affermazione. La seconda discende direttamente dalle definizioni. □

Analogamente, definendo $\eta'_M \colon M \to M \otimes_R R$ con $x \mapsto x \otimes 1$, si vede che η'_M è un isomorfismo e che $M \mapsto \eta'_M$ è un isomorfismo naturale dal funtore dimenticante **mod**-$R \to$ **mod**-$\mathbb{Z}$ al funtore $\otimes_R R$. Si noti che un risultato analogo per il funtore hom è stato proposto nell'esercizio 1 a p. 99.

Il risultato generale del § 3.1 (p. 98), secondo cui i funtori fra categorie di moduli rispettano i coprodotti finiti, si applica ai funtori $M\otimes_R$ e $\otimes_R N$. Otteniamo così isomorfismi canonici di $M \otimes (\bigoplus N_j)$ su $\bigoplus(M \otimes N_j)$ e di $(\bigoplus M_i) \otimes N$ su $\bigoplus(M_i \otimes N)$. Combinandoli si ottiene un isomorfismo

$$\left(\bigoplus_{i=1}^{m} M_i\right) \otimes \left(\bigoplus_{j=1}^{n} N_j\right) \;\simeq\; \bigoplus_{i,j}(M_i \otimes N_j).$$

La proposizione 3.2 fornisce un isomorfismo di $R \otimes_R R$ sul gruppo additivo di R, dato da $r \otimes s \mapsto rs$. Usando questo risultato e l'isomorfismo di $(\bigoplus M_i) \otimes (\bigoplus N_j)$ su $\bigoplus(M_i \otimes N_j)$, è facile vedere che il prodotto bilanciato di $R^{(m)}$ e ${}^{(n)}R$ in $M_{m,n}(R)$ dato all'inizio del paragrafo è il prodotto tensoriale.

Il risultato sull'isomorfismo del coprodotto finito $\bigoplus(M_i \otimes N)$ con $(\bigoplus M_i) \otimes N$ si estende a coprodotti arbitrari. Sia $\{M_\alpha \mid \alpha \in I\}$ una famiglia di R-moduli destri. Allora $\bigoplus M_\alpha$ è l'insieme delle funzioni $(x_\alpha)\colon \alpha \mapsto x_\alpha \in M_\alpha$ tali che $x_\beta = 0$ salvo che per un numero finito di indici β. Se N è un R-modulo sinistro, $(\bigoplus M_\alpha) \otimes N$ è l'insieme delle somme di elementi $(x_\alpha) \otimes y$, $y \in N$. Analogamente $\bigoplus(M_\alpha \otimes N)$ è l'insieme delle funzioni (z_α) con $z_\alpha \in M_\alpha \otimes N$ e $z_\beta = 0$ salvo che per un numero finito di indici. Ogni elemento di $M_\alpha \otimes N$ è una somma di elementi $x_\alpha \otimes y$ con $x_\alpha \in M_\alpha$, $y \in N$. Ogni elemento di $\bigoplus(M_\alpha \otimes N)$ è dunque una somma di elementi $(x_\alpha \otimes y)$, dove le parentesi indicano la funzione $\alpha \mapsto x_\alpha \otimes y$. Dimostriamo ora quanto segue.

Proposizione 3.3. *Se gli M_α, $\alpha \in I$, sono R-moduli destri e N è un R-modulo sinistro, vi è un isomorfismo*

$$\eta_N \colon \Big(\bigoplus M_\alpha\Big) \otimes N \longrightarrow \bigoplus(M_\alpha \otimes N)$$

tale che

$$(x_\alpha) \otimes y \longmapsto (x_\alpha \otimes y). \tag{53}$$

Dimostrazione. Siano $(x_\alpha) \in \bigoplus M_\alpha$ e $y \in N$. Allora $(x_\alpha \otimes y) \in \bigoplus(M_\alpha \otimes N)$ e la corrispondenza $((x_\alpha), y) \mapsto (x_\alpha \otimes y)$ definisce un prodotto bilanciato di $\bigoplus M_\alpha$ e N a valori in $\bigoplus(M_\alpha \otimes N)$. Dà dunque un omomorfismo da $(\bigoplus M_\alpha) \otimes N$ in $\bigoplus(M_\alpha \otimes N)$ con la proprietà (53). D'altra parte, se i_α è l'omomorfismo canonico di M_α in $\bigoplus M_\alpha$ (che manda x_α nella funzione di valore x_α in α e zero in ogni $\beta \neq \alpha$), abbiamo un omomorfismo $i_\alpha \otimes 1_N$ di $M_\alpha \otimes N$ in $(\bigoplus M_\alpha) \otimes N$. Per la proprietà che definisce il coprodotto $\bigoplus(M_\alpha \otimes N)$ otteniamo un omomorfismo

$$\zeta_N \colon \bigoplus(M_\alpha \otimes N) \longrightarrow \Big(\bigoplus M_\alpha\Big) \otimes N, \qquad (x_\alpha \otimes y) \longmapsto (x_\alpha) \otimes y.$$

Verificando sui generatori si vede che η_N e ζ_N sono inversi. La (53) è quindi un isomorfismo. □

Sia ora N' un secondo R-modulo sinistro e sia $f\colon N' \to N$. Gli omomorfismi $1_{M_\alpha} \otimes f$ di $M_\alpha \otimes N'$ in $M_\alpha \otimes N$ definiscono un omomorfismo f^* da $\bigoplus(M_\alpha \otimes N')$ in $\bigoplus(M_\alpha \otimes N)$ che manda $(x_\alpha \otimes y')$ in $(x_\alpha \otimes fy')$, per $x_\alpha \in M_\alpha$, $y' \in N'$. Abbiamo anche l'omomorfismo $1 \otimes f$

da $(\bigoplus M_\alpha) \otimes N'$ in $(\bigoplus M_\alpha) \otimes N$, dove $1 = 1_{\oplus M_\alpha}$. L'isomorfismo η_N della proposizione 3.3 è naturale, ossia il diagramma

$$\begin{array}{ccc} (\bigoplus M_\alpha) \otimes N' & \xrightarrow{\eta_{N'}} & \bigoplus(M_\alpha \otimes N') \\ {\scriptstyle 1\otimes f}\downarrow & & \downarrow{\scriptstyle f^*} \\ (\bigoplus M_\alpha) \otimes N & \xrightarrow[\eta_N]{} & \bigoplus(M_\alpha \otimes N) \end{array} \tag{54}$$

è commutativo, come si verifica direttamente sui generatori $(x_\alpha) \otimes y'$.

Stabiliamo ora la proprietà fondamentale di esattezza dei funtori tensoriali.

Teorema 3.15. *I funtori $M\otimes_R$ e $\otimes_R N$ sono esatti a destra.*

Dimostrazione. Sia $N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ esatta. Poiché g è suriettivo, ogni elemento di $M \otimes_R N''$ è della forma $\sum x_i \otimes g y_i$, $x_i \in M$, $y_i \in N$. Dunque $1 \otimes g$ manda $M \otimes N$ su $M \otimes N''$. Per provare l'esattezza di

$$M \otimes N' \xrightarrow{1\otimes f} M \otimes N \xrightarrow{1\otimes g} M \otimes N'' \longrightarrow 0$$

resta da mostrare che $\ker(1 \otimes g) = \operatorname{im}(1 \otimes f)$. Poiché $gf = 0$, si ha $(1 \otimes g)(1 \otimes f) = 0$ e $\operatorname{im}(1 \otimes f) \subseteq \ker(1 \otimes g)$. Vi è pertanto un omomorfismo θ da $(M \otimes N)/\operatorname{im}(1 \otimes f)$ in $M \otimes N''$ che manda $x \otimes y + \operatorname{im}(1 \otimes f)$ in $x \otimes gy$. Esso è un isomorfismo se e soltanto se $\operatorname{im}(1 \otimes f) = \ker(1 \otimes g)$, dunque basta provare che θ è un isomorfismo. Siano $x \in M$, $y'' \in N''$ e scegliamo $y \in N$ con $gy = y''$. La classe $x \otimes y + \operatorname{im}(1 \otimes f)$ è indipendente dalla scelta di y. Infatti, se $gy_1 = y'' = gy_2$, allora $g(y_1 - y_2) = 0$ e $y_1 - y_2 = fy'$ per qualche $y' \in N'$. Pertanto $x \otimes y_1 + \operatorname{im}(1 \otimes f) = x \otimes y_2 + \operatorname{im}(1 \otimes f)$. È quindi definita un'applicazione da $M \times N''$ in $(M \otimes N)/\operatorname{im}(1 \otimes f)$ che manda (x, y'') in $x \otimes y + \operatorname{im}(1 \otimes f)$ per $gy = y''$. Si tratta chiaramente di un prodotto bilanciato. Si ottiene così un omomorfismo θ' di $M \otimes N''$ in $(M \otimes N)/\operatorname{im}(1 \otimes f)$ tale che $\theta'(x \otimes y'') = x \otimes y + \operatorname{im}(1 \otimes f)$ quando $gy = y''$. Sui generatori si verifica che $\theta\theta' = 1_{M\otimes N''}$ e $\theta'\theta = 1_{(M\otimes N)/\operatorname{im}(1\otimes f)}$. Dunque θ è un isomorfismo. Ciò prova la prima affermazione; la seconda si dimostra in modo analogo. □

Esercizi

1. Sia R^{op} l'anello opposto di R, e si consideri come di consueto un R-modulo destro (sinistro) come un R^{op}-modulo sinistro (destro). Mostrare che esiste un isomorfismo di gruppi da $M \otimes_R N$ su $N \otimes_{R^{\mathrm{op}}} M$ che manda $x \otimes y$ in $y \otimes x$, $x \in M$, $y \in N$. Osservare che per R commutativo ciò si applica a $M \otimes_R N$ e $N \otimes_R M$.

2. Mostrare che, per un intero positivo m, si ha $(\mathbb{Z}/(m)) \otimes m\mathbb{Z} \simeq \mathbb{Z}/(m)$ $(\otimes = \otimes_{\mathbb{Z}})$. Dedurne che, per $m > 1$, la successione $0 \to m\mathbb{Z} \otimes (\mathbb{Z}/(m)) \xrightarrow{i\otimes 1} \mathbb{Z} \otimes (\mathbb{Z}/(m))$ non è esatta, dove i è l'inclusione di $m\mathbb{Z}$ in $\mathbb{Z}$. Ciò mostra che i funtori $M\otimes$ e $\otimes M$ possono non essere esatti.

3. Usare la proposizione 3.2 e il teorema 3.15 per mostrare che, se m, n sono interi positivi, $(\mathbb{Z}/(m)) \otimes (\mathbb{Z}/(n)) \simeq \mathbb{Z}/(d)$, dove $d = (m, n)$ è il massimo comune divisore di m e n.

4. Generalizzare l'esercizio 3 a un dominio a ideali principali R. Usare il risultato e il teorema di struttura dei gruppi abeliani finitamente generati (BAI, p. 195) per determinare la struttura del prodotto tensoriale di due moduli finitamente generati su un dominio a ideali principali.

5. Siano i_α, j_β, $k_{\alpha,\beta}$ i monomorfismi canonici di M_α in $\bigoplus M_\alpha$, di N_β in $\bigoplus N_\beta$ e di $M_\alpha \otimes N_\beta$ in $\bigoplus_{\alpha,\beta}(M_\alpha \otimes N_\beta)$. Mostrare che esiste un isomorfismo di $(\bigoplus M_\alpha)\otimes(\bigoplus N_\beta)$ su $\bigoplus_{\alpha,\beta}(M_\alpha \otimes N_\beta)$ che manda $i_\alpha x_\alpha \otimes j_\beta y_\beta$ in $k_{\alpha,\beta}(x_\alpha \otimes y_\beta)$.

3.8 Bimoduli

Sia M un R-modulo destro e sia $R' = \operatorname{End} M$. Possiamo considerare M come un R'-modulo sinistro definendo fx, per $f \in R'$ e $x \in M$, come l'immagine di x mediante f. Poiché f è un omomorfismo del gruppo additivo di M, si ha $f(x+y) = fx + fy$. Dalla definizione di somma e prodotto di omomorfismi seguono $(f+g)x = fx + gx$ e $(fg)x = f(gx)$ per $f, g \in R'$. Inoltre $1x = x$, per cui M è un R'-modulo sinistro. La definizione di omomorfismo di moduli dà anche la relazione

$$f(xa) = (fx)a, \qquad x \in M,\ a \in R,\ f \in R'. \tag{55}$$

Questa associatività collega la struttura data di R-modulo destro alla struttura di R'-modulo sinistro su M. Più in generale introduciamo la seguente definizione.

Definizione 3.5. *Siano R e S due anelli. Un S-R-bimodulo è un gruppo commutativo M (scritto additivamente) munito di azioni di S e di R tali che M, con l'azione di S (cioè con il prodotto sx, $s \in S$, $x \in M$), sia un S-modulo sinistro, che M, con l'azione di R, sia un R-modulo destro e che valga la condizione di associatività*

$$s(xr) = (sx)r \tag{56}$$

per ogni $s \in S$, $x \in M$, $r \in R$.

Le considerazioni precedenti mostrano che ogni R-modulo destro M si può considerare in modo naturale come un R'-R-bimodulo con $R' = \operatorname{End} M$.

Esempi

1. Sia R commutativo. Ogni R-modulo destro M si può considerare anche come un R-modulo sinistro ponendo $ax = xa$, $a \in R$, $x \in M$. Spesso conviene considerare M come un R-R-bimodulo con $ax = xa$. La condizione $a(xb) = (ax)b$ segue subito dalla commutatività di R.

2. Sia ancora R commutativo e sia η un automorfismo di R. Se M è un R-modulo destro, diventa un R-modulo sinistro ponendo $ax = x\eta(a)$. Questa azione e l'azione destra data fanno di M un R-R-bimodulo.

3. Ogni R-modulo destro si può considerare come uno $\mathbb{Z}$-R-bimodulo definendo mx, per $m \in \mathbb{Z}$, nel modo consueto. Analogamente ogni R-modulo sinistro diventa un R-$\mathbb{Z}$-bimodulo. La teoria dei moduli unilateri rientra così in quella dei bimoduli.

4. Per ogni anello R abbiamo il modulo sinistro ${}_RR$ e il modulo destro R_R. Grazie alla legge associativa $(ax)b = a(xb)$ possiamo riunire le due strutture di modulo in un bimodulo.

Scriviamo $M = {}_SM_R$ per indicare che M è un S-R-bimodulo. Un omomorfismo da ${}_SM_R$ in ${}_SN_R$ è un'applicazione da M in N che sia al tempo stesso un S-omomorfismo e un R-omomorfismo. Dalla (56) si vede che per ogni $s \in S$ l'applicazione $x \mapsto sx$ è un endomorfismo di M_R (M come R-modulo destro) e, per $r \in R$, l'applicazione $x \mapsto xr$ è un endomorfismo di ${}_SM$. Dati ${}_SM_R$ e ${}_TN_R$, interessano spesso gli omomorfismi di M in N come R-moduli destri. Il loro insieme si indica con $\hom_R({}_SM_R, {}_TN_R)$, che coincide con $\hom_R(M,N)$, ed è un gruppo abeliano. Poiché $x \mapsto sx$ è un endomorfismo di M_R, per $f \in \hom_R(M,N)$ la composizione

$$(fs)x = f(sx) \tag{57}$$

è un omomorfismo da M_R in N_R. Analogamente, facendo seguire a f l'applicazione $y \mapsto ty$, $t \in T$, $y \in N$, si ottiene un omomorfismo di M_R in N_R. Dunque tf, definito da

$$(tf)x = t(fx), \tag{58}$$

appartiene a $\hom_R(M_R, N_R)$. Dalle leggi associative e distributive per gli omomorfismi di moduli seguono le relazioni

$$\begin{aligned} t(f_1 + f_2) &= tf_1 + tf_2, \qquad (t_1 + t_2)f = t_1 f + t_2 f, \\ (t_1 t_2)f &= t_1(t_2 f), \qquad (f_1 + f_2)s = f_1 s + f_2 s, \\ f(s_1 + s_2) &= fs_1 + fs_2, \qquad f(s_1 s_2) = (fs_1)s_2, \end{aligned}$$

per $f, f_i \in \hom_R(M_R, N_R)$, $s, s_i \in S$, $t, t_i \in T$. Inoltre $1f = f = f1$ e $(tf)s = t(fs)$. Abbiamo quindi dimostrato la proposizione seguente.

Proposizione 3.4. *Il gruppo abeliano* $\hom_R({}_S M_R, {}_T N_R)$ *diventa un T-S-bimodulo ponendo, per* $f \in \hom_R({}_S M_R, {}_T N_R)$, $s \in S$, $t \in T$, $x \in M$,

$$(tf)x = t(fx), \qquad (fs)x = f(sx).$$

Analogamente, per ${}_R M_S$ e ${}_R N_T$ si ottiene la seguente proposizione.

Proposizione 3.5. *Il gruppo abeliano* $\hom_R({}_R M_S, {}_R N_T)$ *diventa un S-T-bimodulo ponendo*

$$(sf)x = f(xs), \qquad (ft)x = f(x)t. \tag{59}$$

Lasciamo la dimostrazione al lettore.

Un caso particolare importante della proposizione 3.4 si ottiene prendendo il modulo duale $M^* = \hom(M_R, R_R)$ di un R-modulo destro M. All'inizio del paragrafo abbiamo visto che M si considera in modo naturale come un R'-R-bimodulo con $R' = \operatorname{End} M$. Inoltre $R = {}_R R_R$. Per la proposizione 3.4, M^* è quindi un R-R'-bimodulo ponendo

$$(ry^*)x = r(y^* x), \qquad (y^* r')x = y^*(r'x), \tag{60}$$

per $r \in R$, $r' \in R'$, $y^* \in M^*$, $x \in M$.

Consideriamo ora i prodotti tensoriali di bimoduli. Dati ${}_S M_R$ e ${}_R N_T$, possiamo formare, rispetto a R, il prodotto tensoriale del modulo destro M e del modulo sinistro N. Vale allora la proposizione seguente.

Proposizione 3.6. *Il prodotto tensoriale* ${}_S M_R \otimes_R {}_R N_T$ *è un S-T-bimodulo se poniamo* $sz = (s \otimes 1)z$ *e* $zt = (1 \otimes t)(z)$, *per* $z \in {}_S M_R \otimes_R {}_R N_T$. *Qui s indica l'endomorfismo $x \mapsto sx$ di M_R e t l'endomorfismo $y \mapsto yt$ di ${}_R N$.*

La verifica è immediata e la lasciamo al lettore. Le proposizioni 3.4, 3.5 e 3.6 mostrano un vantaggio che si trae dall'uso dei bimoduli rispetto a quello dei moduli unilateri: prendendo il prodotto tensoriale, o applicando hom, a bimoduli che hanno un anello in comune nella posizione opportuna si ottengono ancora bimoduli. È interessante esaminare l'effetto di iterare questi procedimenti. Un primo risultato è la proprietà associativa del prodotto tensoriale.

Proposizione 3.7. *Esiste un isomorfismo di R-U-bimoduli da* $({}_R M_S \otimes_S {}_S N_T) \otimes_T {}_T P_U$ *su* ${}_R M_S \otimes_S ({}_S N_T \otimes_T {}_T P_U)$ *tale che*

$$(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z), \qquad x \in M,\ y \in N,\ z \in P.$$

Dimostrazione. Per $s \in S$ si ha

$$xs \otimes (y \otimes z) = x \otimes s(y \otimes z) = x \otimes (s \otimes 1)(y \otimes z) = x \otimes (sy \otimes z).$$

Dunque, fissato z, l'applicazione $f_z(x,y) = x \otimes (y \otimes z)$ è un prodotto bilanciato di M e N. Si ha perciò un omomorfismo di gruppi da $M \otimes N$ in $M \otimes (N \otimes P)$ che manda $x \otimes y$ in $x \otimes (y \otimes z)$, e dunque $\sum x_i \otimes y_i$ in $\sum x_i \otimes (y_i \otimes z)$. Poniamo

$$f\left(\sum x_i \otimes y_i, z\right) = \sum x_i \otimes (y_i \otimes z).$$

Si ottiene un prodotto bilanciato del T-modulo destro $M \otimes N$ e del T-modulo sinistro P. Abbiamo quindi un omomorfismo di gruppi da $(M \otimes N) \otimes P$ in $M \otimes (N \otimes P)$ che manda $(x \otimes y) \otimes z$ in $x \otimes (y \otimes z)$. È chiaro che esso è anzi un omomorfismo di R-U-bimoduli. Analogamente otteniamo un omomorfismo di bimoduli da $M \otimes (N \otimes P)$ in $(M \otimes N) \otimes P$ tale che $x \otimes (y \otimes z) \mapsto (x \otimes y) \otimes z$. Le composizioni, in entrambi gli ordini, sono le applicazioni identiche. Entrambi gli omomorfismi sono perciò isomorfismi. □

Consideriamo ora i bimoduli $M = {}_RM_S$, $N = {}_SN_T$, $P = {}_UP_T$. Allora $M \otimes N$ è un R-T-bimodulo e, poiché P è un U-T-bimodulo, $\hom_T(M \otimes N, P)$ è per la proposizione 3.4 un U-R-bimodulo. Osserviamo poi che $\hom_T(N,P)$ è un U-S-bimodulo e pertanto, ancora per la proposizione 3.4, $\hom_S(M, \hom_T(N,P))$ è un U-R-bimodulo. Sia $f \in \hom_T(M \otimes N, P)$. L'applicazione $f_x\colon y \mapsto f(x \otimes y)$ appartiene a $\hom_T(N,P)$ e $x \mapsto f_x$ appartiene a $\hom_S(M, \hom_T(N,P))$. Si ha il risultato seguente.

Proposizione 3.8. *Se $M = {}_RM_S$, $N = {}_SN_T$, $P = {}_UP_T$, l'applicazione $\varphi\colon f \mapsto \varphi(f)$, dove $\varphi(f)$ è l'applicazione $x \mapsto f_x$ per $x \in M$ e f_x è $y \mapsto f(x \otimes y)$ per $y \in N$, è un isomorfismo di U-R-bimoduli da $\hom_T(M \otimes N, P)$ su $\hom_S(M, \hom_T(N,P))$.*

Dimostrazione. Una verifica diretta mostra che φ è un omomorfismo di U-R-bimoduli. Viceversa, sia $g \in \hom_S(M, \hom_T(N,P))$. Per $x \in M$, $y \in N$ si ha $g(x)(y) \in P$. Per $s \in S$ risulta

$$g(xs)(y) = (g(x)s)(y) = g(x)(sy).$$

Poiché $g(x)(y)$ è additivo sia in x sia in y, esso definisce un prodotto bilanciato di M_S e ${}_SN$. Vi è quindi un omomorfismo di gruppi f da $M \otimes N$ in P tale che $f(x \otimes y) = g(x)(y)$. Sostituendo yt a y e servendoci dell'unicità del corrispondente f, vediamo che f è un T-omomorfismo. Poniamo $\psi(g) = f$. Dalle definizioni seguono $\varphi\psi(g) = g$ e $\psi\varphi(f) = f$. Pertanto φ è un isomorfismo. □

Esercizi

1. Sia M un R-R-bimodulo e sia $S = R \times M$ munito della struttura di gruppo abeliano indotta da quelle di R e di M, ossia $(r,x) + (r',x') = (r + r', x + x')$. Definire un prodotto in S ponendo
$$(r,x)(r',x') = (rr', rx' + xr').$$
Verificare che si ottiene un anello con unità $1 = (1,0)$, che contiene il sottoanello degli elementi della forma $(r,0)$ e l'ideale degli elementi della forma $(0,x)$. Identificandoli rispettivamente con R e con M si ha $S = R \oplus M$ e $M^2 = 0$.

2. Sia M un R-S-bimodulo per gli anelli R e S. Formare l'anello $T = R \oplus S$. Mostrare che M diventa un T-T-bimodulo ponendo, per $(r,s) \in R \oplus S$ e $x \in M$,
$$(r,s)x = rx, \qquad x(r,s) = xs.$$
Applicare la costruzione dell'esercizio 1 per definire un anello determinato da R, S e M come insieme di terne (r,s,x).

3. Specializzare la proposizione 3.8 ponendo $R = T = U = \mathbb{Z}$. Si ottiene così un isomorfismo da $\hom_{\mathbb{Z}}(M \otimes N, P)$ su $\hom_S(M, \hom_{\mathbb{Z}}(N, P))$ per $M = {}_{\mathbb{Z}}M_S$, $N = {}_S N_{\mathbb{Z}}$, $P = {}_{\mathbb{Z}}P_{\mathbb{Z}}$. Servirsi di questo risultato per mostrare che il funtore $M \otimes_R$ da R-**mod** a $\mathbb{Z}$-**mod** (o **Ab**) è aggiunto sinistro del funtore $\hom_{\mathbb{Z}}(M, -)$ da $\mathbb{Z}$-**mod** a R-**mod**.

4. Sia S un sottoanello di R. Restringendo l'azione a S, ogni R-modulo destro diventa un S-modulo destro. Gli omomorfismi di R-moduli destri sono anche omomorfismi dei corrispondenti S-moduli destri. Si ottiene così un funtore F da **mod**-R a **mod**-S («restrizione degli scalari a S»). Mostrare che F ha sia un aggiunto sinistro sia un aggiunto destro. *Suggerimento.* Dato un S-modulo destro M, considerare $M \otimes_S R$, dove R è un S-modulo sinistro nel modo ovvio. Considerare anche $\hom_S(R, M)$.

3.9 Algebre e coalgebre

Specializziamo ora la teoria dei prodotti tensoriali di moduli al caso in cui l'anello sia un anello commutativo K. In questo caso si può dire molto di più. In particolare, i prodotti tensoriali di moduli su K forniscono un'altra definizione di algebra, per molti aspetti preferibile alla prima (p. 44). Anzitutto la nuova definizione suggerisce la nozione duale di coalgebra. Essa rende inoltre più agevole definire il prodotto tensoriale di algebre. Entrambe le nozioni sono di notevole importanza. Daremo anche alcune importanti costruzioni di algebre, in particolare le algebre tensoriali, esterne e simmetriche definite a partire da K-moduli.

Un anello commutativo K è isomorfo al suo opposto K^{op}. Ogni K-modulo sinistro (destro) si può dunque considerare come K-modulo destro (sinistro) ponendo $kx = xk$ per $k \in K$. Possiamo perciò parlare semplicemente di moduli su K. Un'altra particolarità dei moduli su un anello commutativo è che, fissato $l \in K$, la moltiplicazione scalare $x \mapsto lx$ è un endomorfismo. Ciò segue immediatamente dalla commutatività.

È talvolta utile considerare un modulo M su K come un K-bimodulo nel quale le due azioni di ogni $k \in K$ coincidono, $kx = xk$. Anche qui la commutatività di K assicura che siano soddisfatte le condizioni che definiscono un bimodulo.

Dati due K-moduli M, N, possiamo considerarli come K-K-bimoduli e formare $M \otimes_K N$, ancora un K-K-bimodulo. Per $k \in K$, $x \in M$, $y \in N$ vale

$$k(x \otimes y) = kx \otimes y = x \otimes ky = (x \otimes y)k.$$

Possiamo dunque considerare $M \otimes_K N$ semplicemente come un K-modulo, sinistro o destro. L'applicazione $(x, y) \mapsto x \otimes y$ da $M \times N$ in $M \otimes N$ è K-bilineare: fissato x, l'applicazione $y \mapsto x \otimes y$ è un K-omomorfismo, e analogamente lo è $x \mapsto x \otimes y$ quando si fissa y (cfr. BAI, p. 344).

Sia ora $f\colon (x, y) \mapsto f(x, y)$ una qualsiasi applicazione K-bilineare da $M \times N$ in un K-modulo P. Si ha

$$\begin{aligned}
&\text{B1.} \quad f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y),\\
&\text{B2.} \quad f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2),\\
&\text{B3.} \quad f(kx, y) = kf(x, y) = f(x, ky)
\end{aligned}$$

per $k \in K$, $x \in M$, $y \in N$. Poiché $kx = xk$, B1, B2 e B3 implicano che (P, f) è un prodotto bilanciato di M e N. Esiste quindi un omomorfismo dei gruppi additivi da $M \otimes_K N$ in P tale che $x \otimes y \mapsto f(x, y)$. Per B3 si tratta di un omomorfismo di K-moduli. Viceversa, dato un K-omomorfismo π da $M \otimes_K N$ in un K-modulo P, la formula $f(x, y) = \pi(x \otimes y)$ definisce un'applicazione K-bilineare da $M \times N$ in P.

In particolare, $f(x,y) = y \otimes x$ definisce un'applicazione K-bilineare da $M \times N$ in $N \otimes M$. Si ha quindi un K-omomorfismo $\sigma\colon M \otimes N \to N \otimes M$ con $x \otimes y \mapsto y \otimes x$. Analogamente esiste un K-omomorfismo $\sigma'\colon N \otimes M \to M \otimes N$ tale che $y \otimes x \mapsto x \otimes y$. Allora $\sigma' = \sigma^{-1}$, sicché σ è un isomorfismo. Per $N = M$ si ottiene l'automorfismo $x \otimes y \mapsto y \otimes x$ di $M \otimes M$.

Ricordiamo inoltre l'associatività del prodotto tensoriale: se M, N, P sono K-moduli, esiste un K-isomorfismo da $(M \otimes N) \otimes P$ su $M \otimes (N \otimes P)$ che manda $(x \otimes y) \otimes z$ in $x \otimes (y \otimes z)$, con $x \in M$, $y \in N$, $z \in P$ (p. 135). Possiamo ora dare la nuova definizione di algebra su K.

Definizione 3.6. *Se K è un anello commutativo, un'algebra (associativa) su K, o K-algebra, è una terna (A, π, ε), dove A è un K-modulo, $\pi\colon A \otimes A \to A$ e $\varepsilon\colon K \to A$ sono K-omomorfismi e commutano i diagrammi seguenti.*

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\pi \otimes 1} & A \otimes A \\ {\scriptstyle 1 \otimes \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ A \otimes A & \xrightarrow[\pi]{} & A \end{array} \qquad \begin{array}{ccccc} & & A \otimes A & & \\ & {\scriptstyle \varepsilon \otimes 1}\nearrow & & \nwarrow{\scriptstyle 1 \otimes \varepsilon} & \\ K \otimes A & & {\scriptstyle \pi}\downarrow & & A \otimes K \\ & \searrow & & \swarrow & \\ & & A & & \end{array}$$

Qui $A \otimes A \otimes A$ indica indifferentemente $(A \otimes A) \otimes A$ e $A \otimes (A \otimes A)$, identificati mediante l'isomorfismo $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$, per $x, y, z \in A$. Il K-omomorfismo $\pi \otimes 1$ si applica al primo dei due moduli e $1 \otimes \pi$ al secondo. Le frecce senza etichetta sono gli isomorfismi canonici che mandano $k \otimes x$ in kx e $x \otimes k$ in $xk = kx$, per $k \in K$, $x \in A$.

Supponiamo data un'algebra nel senso appena definito. Introduciamo in A il prodotto

$$xy = \pi(x \otimes y) \tag{61}$$

e definiamo l'elemento 1 di A mediante

$$\varepsilon(1) = 1. \tag{62}$$

Per $x, y, z \in A$, la commutatività del primo diagramma, applicata a $(x \otimes y) \otimes z = x \otimes (y \otimes z)$, dà la legge associativa $(xy)z = x(yz)$. Applicando a $k \otimes x \in K \otimes A$ la commutatività del triangolo sinistro del secondo diagramma, si ottiene $kx = \pi(\varepsilon \otimes 1)(k \otimes x) = \pi(k1 \otimes x) = (k1)x$. Il triangolo destro dà analogamente $x(k1) = kx$. Segue che $1x = x = x1$ e, applicando la legge associativa a $k1, x, y$, si ottiene la condizione di algebra $k(xy) = (kx)y = x(ky)$.

Viceversa, supponiamo che sia data un'algebra nel primo senso. Il prodotto xy è K-bilineare, quindi esiste un K-omomorfismo $\pi\colon A \otimes A \to A$ tale che $\pi(x \otimes y) = xy$. Definiamo $\varepsilon\colon K \to A$ ponendo $k \mapsto k1$. Il primo diagramma commuta per la legge associativa e il secondo per la relazione $kx = (k1)x = x(k1)$, che segue da $k(xy) = (kx)y = x(ky)$. Le due definizioni sono dunque equivalenti.

In BAI, pp. 406–409 e 411–414, abbiamo dato numerosi esempi di algebre su campi. Ne daremo ora alcuni su un anello commutativo arbitrario K.

Esempi

1. $\mathrm{End}_K M$**.** Sia M un K-modulo e sia $A = \mathrm{End}_K M$. Sappiamo che A è un anello con le definizioni naturali di addizione, zero, opposto, prodotto e unità. Inoltre A è un K-modulo e $k(fg) = (kf)g = f(kg)$ per $k \in K$, $f, g \in A$. Infatti, applicando questi tre elementi a $x \in M$, si ottengono $k((fg)x)$, $((kf)g)x$, $(f(kg))x$, tutti uguali per la definizione $(kf)x = f(kx) = k(fx)$. Si ha dunque un'algebra su K nel primo senso.

2. Algebre tensoriali. Prima della costruzione successiva occorre considerare una proprietà generale di associatività dei prodotti tensoriali di K-moduli. Siano $M_1, M_2, \dots, M_n$ dei K-moduli. Definiamo per induzione $M_1 \otimes \cdots \otimes M_n$ ponendo

$$M_1 \otimes \cdots \otimes M_i = (M_1 \otimes \cdots \otimes M_{i-1}) \otimes M_i.$$

Per $x_j \in M_j$ definiamo analogamente $x_1 \otimes \cdots \otimes x_i = (x_1 \otimes \cdots \otimes x_{i-1}) \otimes x_i$. Per $1 \leq m < n$ affermiamo che esiste un unico isomorfismo π_{mn} da $(M_1 \otimes \cdots \otimes M_m) \otimes (M_{m+1} \otimes \cdots \otimes M_n)$ su $M_1 \otimes \cdots \otimes M_n$ tale che

$$\pi_{mn}((x_1 \otimes \cdots \otimes x_m) \otimes (x_{m+1} \otimes \cdots \otimes x_n)) = x_1 \otimes \cdots \otimes x_n. \tag{63}$$

Lo si vede immediatamente per induzione su $n - m$, usando l'isomorfismo $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$ della proposizione 3.7.

Supponiamo ora che tutti gli M_i coincidano con un K-modulo M. Indichiamo con $M^{(i)}$ il prodotto tensoriale di i copie di M, per $i = 1, 2, 3, \dots$. Poniamo inoltre $M^{(0)} = K$ e definiamo $\pi_{0n} \colon K \otimes M^{(n)} \to M^{(n)}$, $n = 0, 1, \dots$, come l'isomorfismo canonico $k \otimes x \mapsto kx$; analogamente π_{nn} manda $x \otimes k$ in $kx = xk$. Formiamo il K-modulo

$$T(M) = \bigoplus_{i=0}^{\infty} M^{(i)} = K \oplus M^{(1)} \oplus M^{(2)} \oplus \cdots . \tag{64}$$

Possiamo considerare π_{mn}, $0 \leq m \leq n$, $n = 0, 1, 2, \dots$, come un K-omomorfismo a valori in $T(M)$. Poiché $\bigoplus_{i,j}(M^{(i)} \otimes M^{(j)})$ è il coprodotto dei moduli $M^{(i)} \otimes M^{(j)}$, otteniamo un omomorfismo π' da tale somma diretta in $T(M)$ che coincide con π_{mn} su $M^{(m)} \otimes M^{(n-m)}$, identificato con la sua immagine nella somma diretta. Abbiamo inoltre un isomorfismo da $T(M) \otimes T(M) = (\bigoplus_i M^{(i)}) \otimes (\bigoplus_j M^{(j)})$ su $\bigoplus_{i,j}(M^{(i)} \otimes M^{(j)})$ (esercizio 5, p. 133). Componendo questo isomorfismo con π' otteniamo un omomorfismo π di $T(M) \otimes T(M)$ in $T(M)$. Sia ε l'iniezione di K in $T(M) = \bigoplus M^{(i)}$. Affermiamo che $(T(M), \pi, \varepsilon)$ è un'algebra nel senso della definizione 3.6, ossia che, posto $xy = \pi(x \otimes y)$, il prodotto è associativo e $1x = x = x1$. La seconda asserzione è evidente. Per la prima, ogni elemento di $T(M)$ è somma di termini della forma $k1$ e di termini della forma $x_1 \otimes \cdots \otimes x_m$. Basta verificare l'associatività sui termini di queste forme, perché il caso generale seguirà per distributività. Se uno dei fattori ha la forma $k1$, l'associatività segue dalla definizione del prodotto, che dà $(k1)x = kx = x(k1)$. Poniamo ora $x = x_1 \otimes \cdots \otimes x_m$, $y = y_1 \otimes \cdots \otimes y_n$ e $z = z_1 \otimes \cdots \otimes z_p$, con $m, n, p > 0$. La definizione di π dà

$$\begin{aligned}(xy)z &= \big((x_1 \otimes \cdots \otimes x_m)(y_1 \otimes \cdots \otimes y_n)\big)(z_1 \otimes \cdots \otimes z_p) \\ &= (x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n)(z_1 \otimes \cdots \otimes z_p) \\ &= x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n \otimes z_1 \otimes \cdots \otimes z_p.\end{aligned}$$

Per $x(yz)$ si ottiene allo stesso modo il medesimo risultato. Le nostre definizioni danno pertanto una K-algebra, detta *algebra tensoriale* $T(M)$ del K-modulo M.

Consideriamo ora il funtore dimenticante F da K-**alg** a K-**mod**. Affermiamo che $(T(M), i)$, dove i è l'iniezione di M in $T(M)$, è un universale da M a F. Sia infatti f un omomorfismo di K-moduli da M in una K-algebra A. Definiamo K-omomorfismi $f^{(n)}$ da $M^{(n)}$ in A, per $n = 1, 2, \dots$, ponendo $f^{(1)} = f$ e prendendo per $f^{(i)}$ l'omomorfismo da $M^{(i)} = M^{(i-1)} \otimes M$ ottenuto componendo $f^{(i-1)} \otimes f$ con l'omomorfismo $A \otimes A \to A$, $x \otimes y \mapsto xy$. Allora, per $x_i \in M$,

$$f^{(n)}(x_1 \otimes \cdots \otimes x_n) = f(x_1) \cdots f(x_n). \tag{65}$$

Poniamo $f^{(0)}\colon K \to A$, $k \mapsto k1$, e sia f^* l'omomorfismo di K-moduli da $T(M)$ in A che coincide con $f^{(n)}$ su $M^{(n)}$ per $n = 0, 1, 2, \ldots$. Dalla (65) si vede subito che f^* è un omomorfismo di K-algebre. Dalla definizione risulta poi che M genera $T(M)$. Pertanto f^* è l'unico omomorfismo da $T(M)$ in A che coincide con f su M, e $(T(M), i)$ è un universale da M al funtore dimenticante da K-**alg** a K-**mod**.

Un'algebra A si dice *graduata* (sui numeri naturali $0, 1, \ldots$) se $A = \bigoplus_{i=0}^{\infty} A_i$, dove gli A_i sono sottomoduli di A e $A_i A_j \subseteq A_{i+j}$. Il sottomodulo A_i si chiama *componente omogenea di grado* i di A. Un esempio familiare al lettore si ottiene prendendo $A = K[\lambda_1, \ldots, \lambda_r]$, l'algebra dei polinomi su K nelle indeterminate $\lambda_1, \ldots, \lambda_r$ (BAI, pp. 124–126). L'insieme A_i dei polinomi omogenei di grado totale i (BAI, p. 138) fornisce, al variare di i, una graduazione di A. L'algebra tensoriale $T(M)$ è graduata mediante i sottomoduli $M^{(i)}$: infatti $T(M) = \bigoplus M^{(i)}$ e $M^{(i)}M^{(j)} = M^{(i)} \otimes M^{(j)} \subseteq M^{(i+j)}$ (con le identificazioni sopra descritte).

L'algebra tensoriale è il punto di partenza per definire diverse altre algebre. Le più importanti sono forse l'algebra esterna e l'algebra simmetrica, che ora definiremo.

3. Algebre esterne. Definiamo l'*algebra esterna* del K-modulo M ponendo

$$E(M) = T(M)/B, \tag{66}$$

dove B è l'ideale di $T(M)$ generato dagli elementi

$$x \otimes x, \qquad x \in M. \tag{67}$$

Dalla definizione risulta che $B \subseteq \sum_{i \geq 2} M^{(i)}$. Dunque $B \cap M = 0$ e la restrizione a M dell'omomorfismo canonico da $T(M)$ su $E(M) = T(M)/B$ è iniettiva. Identifichiamo M con la sua immagine e lo consideriamo come un sottoinsieme di $E(M)$. È chiaro che M genera $E(M)$. È chiaro inoltre che, essendo generato dagli elementi omogenei $x \otimes x$, l'ideale B è omogeneo: $B = \bigoplus B_i$, con $B_i = B \cap M^{(i)}$. Ne segue che $E(M)$ è graduata dai sottoinsiemi $E^{(i)} = (M^{(i)} + B)/B$, ossia $E(M) = \bigoplus E^{(i)}$ ed $E^{(i)}E^{(j)} \subseteq E^{(i+j)}$.

Sia ora A una K-algebra e sia f un omomorfismo di K-moduli da M in A tale che $f(x)^2 = 0$ per ogni $x \in M$. La proprietà universale di $T(M)$ dà un omomorfismo f^* da $T(M)$ in A che estende f. Poiché $f^*(x)^2 = f(x)^2 = 0$, il nucleo di f^* contiene ogni $x \otimes x$ e dunque l'ideale B che definisce $E(M)$. Abbiamo pertanto un omomorfismo $\bar{f}$ da $E(M)$ in A che manda x, considerato come elemento di $E(M)$, in $f(x)$. In altri termini, ogni omomorfismo di K-moduli f da M in un'algebra A tale che $f(x)^2 = 0$ per $x \in M$ si estende a un omomorfismo di K-algebre da $E(M)$ in A. L'estensione è unica perché M genera $E(M)$. Questa è la proprietà universale di $E(M)$: ogni omomorfismo di K-moduli f da M in una K-algebra tale che $f(x)^2 = 0$ per ogni $x \in M$ si estende in uno e un solo modo a un omomorfismo di algebre da $E(M)$ in A. Se M è uno spazio vettoriale di dimensione finita su un campo, dalla proprietà universale segue che l'algebra esterna così definita è quella costruita mediante basi in BAI, pp. 411–414.

4. Algebre simmetriche. Partiamo ancora da $T(M)$ e passiamo al quoziente rispetto all'ideale C generato dagli elementi della forma

$$x \otimes y - y \otimes x, \qquad x, y \in M. \tag{68}$$

L'algebra $S(M) = T(M)/C$ si chiama *algebra simmetrica* del K-modulo M. Con gli argomenti dell'esempio precedente si vede che M può essere considerato come un sottoinsieme che genera $S(M)$ e che $S(M)$ è graduata dai sottomoduli $S^{(i)} = (M^{(i)} + C)/C$. In $S(M)$ si ha $xy = yx$ per i generatori $x, y \in M$, e pertanto $S(M)$ è commutativa. Si vede facilmente, inoltre, che $S(M)$, insieme con l'iniezione di M in $S(M)$, costituisce un universale da M al funtore dimenticante dalla categoria **Comalg** delle algebre commutative alla categoria K-**mod**.

5. Algebra inviluppante universale di un'algebra di Lie. Ricordiamo che un'algebra di Lie L su un anello commutativo K è un K-modulo dotato di una composizione bilineare $(x, y) \mapsto [xy]$ che soddisfa le due condizioni

$$[xx] = 0, \qquad [[xy]z] + [[yz]x] + [[zx]y] = 0.$$

Ogni algebra associativa A definisce un'algebra di Lie A^- con la medesima struttura di K-modulo e con prodotto di Lie $[xy] = xy - yx$ (BAI, p. 432). Date due algebre associative A_1, A_2, ogni omomorfismo da A_1 in A_2 è anche un omomorfismo da A_1^- in A_2^-. Si ottiene così un funtore F dalla categoria K-**alg** delle algebre associative su K alla categoria K-**Lie** delle algebre di Lie su K. Mostreremo che, data un'algebra di Lie L, esiste un universale da L a F. Per costruirlo formiamo l'algebra tensoriale del K-modulo L,

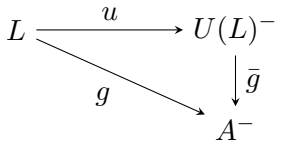
$$T(L) = K \oplus L^{(1)} \oplus L^{(2)} \oplus \cdots,$$

e prendiamo l'ideale B di $T(L)$ generato da tutti gli elementi della forma

$$[xy] - x \otimes y + y \otimes x, \qquad x, y \in L\ (= L^{(1)}).$$

Poniamo $U(L) = T(L)/B$ e sia u la restrizione a L dell'omomorfismo canonico da $T(L)$ su $U(L)$. Allora u è un omomorfismo dell'algebra di Lie L in $U(L)^-$. Chiamiamo $U(L)$ l'*algebra inviluppante (universale)* dell'algebra di Lie L. Affermiamo che $(U(L), u)$ è un universale da L al funtore F.

Occorre mostrare che, se A è associativa e g è un omomorfismo da L in A^-, allora esiste un unico omomorfismo di algebre associative $\bar{g}\colon U(L) \to A$ per il quale commuta il seguente diagramma di omomorfismi di algebre di Lie:



Abbiamo visto che esiste un unico omomorfismo $g^*\colon T(L) \to A$ che estende il K-omomorfismo g da L in A. Ora $g([xy]) = g(x)g(y) - g(y)g(x)$ per $x, y \in L$, perché g è un omomorfismo da L in A^-. Pertanto

$$g^*([xy] - x \otimes y + y \otimes x) = g([xy]) - g(x)g(y) + g(y)g(x) = 0,$$

da cui $B \subseteq \ker g^*$. Esiste dunque un omomorfismo $\bar{g}$ da $U(L) = T(L)/B$ in A tale che $\bar{g}(x+B) = g(x)$, ossia $\bar{g}u(x) = g(x)$. Il diagramma commuta. Poiché L genera $T(L)$, $u(L)$ genera $U(L)$ e $\bar{g}$ è unico.

Il risultato appena stabilito, ossia l'esistenza per ogni algebra di Lie di un universale a F, equivale ad affermare che il funtore F da K-**alg** a K-**Lie** ammette un aggiunto sinistro da K-**Lie** a K-**alg**. Un'osservazione analoga vale per le algebre simmetriche. L'algebra simmetrica di un K-modulo M si può anche considerare come l'algebra inviluppante dell'algebra di Lie M con prodotto banale $[xy] \equiv 0$.

Passiamo al prodotto tensoriale di algebre associative. Siano $(A_i, \pi_i, \varepsilon_i)$, $i = 1, 2$, algebre nel senso della definizione 3.6. Abbiamo dunque $\pi_i\colon A_i \otimes A_i \to A_i$, $\varepsilon_i\colon K \to A_i$, e commutano i diagrammi della definizione. Consideriamo i K-moduli $A_1 \otimes A_2$ e $(A_1 \otimes A_2) \otimes (A_1 \otimes A_2)$. Usando l'isomorfismo $A_2 \otimes A_1 \to A_1 \otimes A_2$ che manda $x_2 \otimes x_1$ in $x_1 \otimes x_2$, $x_i \in A_i$, e l'associatività dei prodotti tensoriali, si ottiene un isomorfismo da $(A_1 \otimes A_2) \otimes (A_1 \otimes A_2)$ su $(A_1 \otimes A_1) \otimes (A_2 \otimes A_2)$ tale che

$$(x_1 \otimes x_2) \otimes (y_1 \otimes y_2) \longmapsto (x_1 \otimes y_1) \otimes (x_2 \otimes y_2).$$

Componendolo con $\pi_1 \otimes \pi_2$ si ottiene un K-omomorfismo π da $(A_1 \otimes A_2) \otimes (A_1 \otimes A_2)$ in $A_1 \otimes A_2$ per il quale

$$(x_1 \otimes x_2) \otimes (y_1 \otimes y_2) \longmapsto \pi_1(x_1 \otimes y_1) \otimes \pi_2(x_2 \otimes y_2).$$

In altri termini, in $A_1 \otimes A_2$ abbiamo una moltiplicazione espressa, mediante quelle di A_1 e A_2, dalla formula

$$(x_1 \otimes x_2)(y_1 \otimes y_2) = x_1y_1 \otimes x_2y_2. \tag{69}$$

Poniamo inoltre

$$1 = 1_1 \otimes 1_2. \tag{70}$$

Allora per $x_i, y_i, z_i \in A_i$ si ha

$$\begin{aligned}((x_1 \otimes x_2)(y_1 \otimes y_2))(z_1 \otimes z_2) &= (x_1y_1)z_1 \otimes (x_2y_2)z_2,\\ (x_1 \otimes x_2)((y_1 \otimes y_2)(z_1 \otimes z_2)) &= x_1(y_1z_1) \otimes x_2(y_2z_2).\end{aligned}$$

Ne segue l'associatività della moltiplicazione in $A = A_1 \otimes A_2$. Vale inoltre

$$1(x_1 \otimes x_2) = x_1 \otimes x_2 = (x_1 \otimes x_2)1,$$

quindi 1 è l'elemento unità per la moltiplicazione. Abbiamo così una K-algebra $A = A_1 \otimes A_2$, che chiamiamo *prodotto tensoriale* di A_1 e A_2.

Il prodotto tensoriale di algebre è caratterizzato da una proprietà universale. Osserviamo anzitutto che $x_1 \mapsto x_1 \otimes 1_2$ e $x_2 \mapsto 1_1 \otimes x_2$ sono omomorfismi, rispettivamente da A_1 e A_2 in $A_1 \otimes A_2$; questi omomorfismi possono non essere iniettivi. Si ha

$$(x_1 \otimes 1_2)(1_1 \otimes x_2) = x_1 \otimes x_2 = (1_1 \otimes x_2)(x_1 \otimes 1_2). \tag{71}$$

In altri termini, se $e_1 \colon x_1 \mapsto x_1 \otimes 1_2$ ed $e_2 \colon x_2 \mapsto 1_1 \otimes x_2$, allora $e_1(x_1)e_2(x_2) = e_2(x_2)e_1(x_1)$ per ogni $x_i \in A_i$. Supponiamo ora dati omomorfismi $f_i \colon A_i \to B$, $i = 1, 2$, in un'algebra B, tali che $f_1(x_1)f_2(x_2) = f_2(x_2)f_1(x_1)$ per $x_i \in A_i$. Affermiamo che esiste un unico omomorfismo di algebre $f \colon A_1 \otimes A_2 \to B$ tale che $fe_i = f_i$. Infatti l'applicazione $(x_1, x_2) \mapsto f_1(x_1)f_2(x_2)$ da $A_1 \times A_2$ in B è K-bilineare e induce quindi un omomorfismo di K-moduli $f \colon A_1 \otimes A_2 \to B$ per cui $f(x_1 \otimes x_2) = f_1(x_1)f_2(x_2)$. Poiché $f(1) = f(1_1 \otimes 1_2) = f_1(1_1)f_2(1_2) = 1 \cdot 1 = 1$ e

$$\begin{aligned}f((x_1 \otimes x_2)(y_1 \otimes y_2)) &= f(x_1y_1 \otimes x_2y_2)\\ &= f_1(x_1y_1)f_2(x_2y_2) = f_1(x_1)f_1(y_1)f_2(x_2)f_2(y_2)\\ &= f_1(x_1)f_2(x_2)f_1(y_1)f_2(y_2) = f(x_1 \otimes x_2)f(y_1 \otimes y_2),\end{aligned}$$

f è un omomorfismo di K-algebre. Si ha $fe_1(x_1) = f(x_1 \otimes 1_2) = f_1(x_1)f_2(1_2) = f_1(x_1)$ e analogamente $fe_2(x_2) = f_2(x_2)$, dunque $fe_i = f_i$. La (71) e il fatto che ogni elemento di $A_1 \otimes A_2$ è una somma $\sum_j x_{1j} \otimes x_{2j}$ con $x_{ij} \in A_i$ implicano che f è il solo omomorfismo che soddisfi queste condizioni.

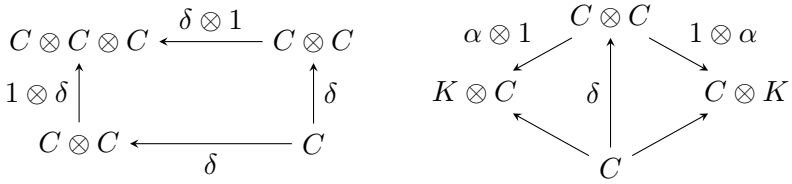
Il prodotto tensoriale di algebre è associativo e commutativo nel senso del teorema seguente.

Teorema 3.16. *Si ha un isomorfismo da $A_1 \otimes A_2$ su $A_2 \otimes A_1$ che manda $x_1 \otimes x_2$ in $x_2 \otimes x_1$, e un isomorfismo da $(A_1 \otimes A_2) \otimes A_3$ su $A_1 \otimes (A_2 \otimes A_3)$ che manda $(x_1 \otimes x_2) \otimes x_3$ in $x_1 \otimes (x_2 \otimes x_3)$, dove $x_i \in A_i$.*

Dimostrazione. Abbiamo già visto che esistono isomorfismi di moduli della forma indicata. Una verifica diretta mostra che sono omomorfismi di algebre. □

Abbiamo osservato diverse circostanze nelle quali è vantaggioso usare la definizione 3.6 di algebra. Forse il vantaggio principale è che essa suggerisce una nozione duale, che presentiamo nella forma seguente.

Definizione 3.7. *Una coalgebra su K (o K-coalgebra) è una terna (C, δ, α) dove C è un K-modulo, $\delta\colon C \to C \otimes_K C$ e $\alpha\colon C \to K$ sono K-omomorfismi e i diagrammi seguenti commutano:*



Qui le applicazioni $C \to C \otimes K$ e $C \to K \otimes C$ sono $x \mapsto x \otimes 1$ e $x \mapsto 1 \otimes x$. L'applicazione δ si chiama *diagonalizzazione* e α si chiama *aumentazione*.

È bello avere un'elegante definizione; è ancor più bello disporre di qualche bell'esempio. Eccone due per le coalgebre.

Esempi

1. Sia G un gruppo e sia $K[G]$ l'algebra del gruppo su K (si vedano BAI, p. 127, esercizio 8, e p. 408). Come K-modulo essa ha per base G e il suo prodotto è dato dalla formula

$$\left(\sum_i k_i s_i\right)\left(\sum_j l_j t_j\right) = \sum_{i,j} k_i l_j s_i t_j \qquad (k_i, l_j \in K,\ s_i, t_j \in G).$$

Come di consueto identifichiamo $1s$ con s e consideriamo così G immerso in $K[G]$. La proprietà fondamentale di $K[G]$ è che ogni omomorfismo g da G nel gruppo moltiplicativo degli elementi invertibili di un'algebra A si estende in modo unico a un omomorfismo da $K[G]$ in A. Prendiamo $A = K[G] \otimes_K K[G]$. L'applicazione $s \mapsto s \otimes s$ da G in A è un omomorfismo di gruppi e si estende quindi a un omomorfismo di algebre $\delta\colon K[G] \to K[G] \otimes K[G]$. Esiste inoltre un unico omomorfismo di algebre $\alpha\colon K[G] \to K$ che estende l'omomorfismo $s \mapsto 1$ da G nel gruppo moltiplicativo di K. Allora $(K[G], \delta, \alpha)$ è una coalgebra. Lasciamo al lettore la verifica delle condizioni della definizione.

2. Sia $U(L)$ l'algebra inviluppante di un'algebra di Lie L. Se u è l'applicazione di L in $U(L)$, allora $u([xy]) = [u(x), u(y)] = u(x)u(y) - u(y)u(x)$ per $x, y \in L$. Poniamo $u_2(x) = u(x) \otimes 1 + 1 \otimes u(x) \in U(L) \otimes U(L)$. Poiché $a \otimes 1$ e $1 \otimes b$ commutano per ogni $a, b \in U(L)$, si ha

$$[u_2(x), u_2(y)] = u_2([xy]).$$

Pertanto u_2 è un omomorfismo da L in $(U(L) \otimes U(L))^-$ e ha un'unica estensione a un omomorfismo δ da $U(L)$ in $U(L) \otimes U(L)$. Analogamente esiste un omomorfismo $\alpha\colon U(L) \to K$ che manda $u(x)$ in 0 per ogni $x \in L$. Lasciamo al lettore la verifica che $(U(L), \delta, \alpha)$ è una coalgebra.

I due esempi appena dati sono algebre oltre che coalgebre. Inoltre δ e α sono omomorfismi di algebre. In questa situazione la struttura complessiva $(C, \pi, \varepsilon, \delta, \alpha)$ prende il nome di *bialgebra*. Bialgebre di un tipo speciale, oggi dette *algebre di Hopf*, furono introdotte da Heinz Hopf nei suoi studi sulla topologia dei gruppi di Lie.

Esercizi

1. Siano M, N spazi vettoriali su un campo K e siano M^*, N^* i loro duali. Verificare che, dati $f \in M^*$, $g \in N^*$, l'applicazione $(x, y) \mapsto f(x)g(y)$ da $M \times N$ in K è bilineare. Esiste

dunque un unico $h \in (M \otimes N)^*$ tale che $h(x \otimes y) = f(x)g(y)$. Mostrare che esiste un monomorfismo di spazi vettoriali da $M^* \otimes N^*$ in $(M \otimes N)^*$ che manda $f \otimes g$ in h e che esso è un isomorfismo se M e N hanno dimensione finita.

2. Siano M, N spazi vettoriali di dimensione finita su un campo K. Mostrare che esiste un isomorfismo da $\mathrm{End}_K M \otimes_K \mathrm{End}_K N$ su $\mathrm{End}_K(M \otimes_K N)$ che manda $f \otimes g$, con $f \in \mathrm{End}_K M$ e $g \in \mathrm{End}_K N$, nella trasformazione lineare di $M \otimes N$ tale che $x \otimes y \mapsto f(x) \otimes g(y)$. Il risultato vale ancora se M oppure N ha dimensione infinita?

3. Siano $(A, \pi_A, \varepsilon_A)$ e $(B, \pi_B, \varepsilon_B)$ algebre su K. Mostrare che un K-omomorfismo $\theta\colon A \to B$ è un omomorfismo di algebre se e soltanto se commutano i diagrammi

$$\begin{array}{ccc} A & \xleftarrow{\pi_A} & A \otimes A \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta\otimes\theta} \\ B & \xleftarrow[\pi_B]{} & B \otimes B \end{array} \qquad \begin{array}{ccc} A & \overset{\varepsilon_A}{\nwarrow} & \\ {\scriptstyle\theta}\downarrow & & K \\ B & \underset{\varepsilon_B}{\swarrow} & \end{array}$$

Dualizzare i diagrammi per ottenere la definizione di omomorfismo di coalgebre.

4. Sia (C, π, ε) un'algebra e sia (C, δ, α) una coalgebra. Mostrare che $(C, \pi, \varepsilon, \delta, \alpha)$ è una bialgebra se e soltanto se π ed ε sono omomorfismi di coalgebre.

5. Sia (C, δ, α) una coalgebra su un campo K e sia ρ il monomorfismo di $C^* \otimes C^*$ in $(C \otimes C)^*$ dell'esercizio 1. Poniamo $\pi = \delta^* \rho$, dove $\delta^*\colon (C \otimes C)^* \to C^*$ è la trasposta di $\delta\colon C \to C \otimes C$ (p. 21). Sia $\varepsilon = \alpha^* \iota$, con ι l'isomorfismo canonico di K su $K^* = \hom_K(K, K)$ e α^* la trasposta di α. Verificare che (C^*, π, ε) è un'algebra. Essa si chiama *algebra duale* di (C, δ, α).

6. Sia (A, π, ε) un'algebra di dimensione finita su un campo K. Sia τ l'isomorfismo di $(A \otimes A)^*$ su $A^* \otimes A^*$ dato dall'esercizio 1. Poniamo $\delta = \tau \pi^*$, dove $\pi^*\colon A^* \to (A \otimes A)^*$ è la trasposta di π, e $\alpha = \iota^{-1} \varepsilon^*$, dove ι è come nell'esercizio 5 ed ε^* è la trasposta di ε. Verificare che (A^*, δ, α) è una coalgebra, detta *coalgebra duale* di A.

7. Sia $C(n)$ lo spazio con base $\{x_{ij} \mid 1 \le i, j \le n\}$ su un campo K. Siano δ, α le applicazioni lineari tali che $\delta(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj}$ e $\alpha(x_{ij}) = \delta_{ij}$. Verificare che $(C(n), \delta, \alpha)$ è la coalgebra duale di $M_n(K)$.

8. Data un'algebra (A, π, ε), si definisce un A-modulo sinistro come un K-modulo M dotato di un'applicazione $\mu\colon A \otimes_K M \to M$ tale che commutino i diagrammi

$$\begin{array}{ccc} K \otimes M & & \\ {\scriptstyle\varepsilon\otimes 1}\downarrow & \searrow & \\ A \otimes M & \underset{\mu}{\nearrow} & M \end{array} \qquad \begin{array}{ccc} A \otimes A \otimes M & \xrightarrow{1\otimes\mu} & A \otimes M \\ {\scriptstyle\pi\otimes 1}\downarrow & & \downarrow{\scriptstyle\mu} \\ A \otimes M & \xrightarrow[\mu]{} & M \end{array}$$

Dualizzare per definire i comoduli su una coalgebra.

9. Un'algebra A si dice *filtrata* se per ogni $i = 0, 1, 2, \ldots$ è dato un sottospazio $A^{(i)}$ tale che (i) $A^{(i)} \subseteq A^{(j)}$ se $i < j$, (ii) $\bigcup_i A^{(i)} = A$, (iii) $A^{(i)} A^{(j)} \subseteq A^{(i+j)}$. Mostrare che, se X è un insieme di generatori di A, si ottiene una filtrazione ponendo $A^{(i)} = K1 + KX + KX^2 + \cdots + KX^i$, dove KY è il K-sottomodulo generato dall'insieme Y e X^j è l'insieme dei prodotti di j elementi di X.

10. Sia A un'algebra filtrata e si ponga $G(A) = \bigoplus_{i\geq 0} A_i$, con $A_i = A^{(i)}/A^{(i-1)}$ per $i > 0$ e $A_0 = A^{(0)}$. Mostrare che $G(A)$ ammette una struttura di algebra graduata per la quale

$$(a_i + A^{(i-1)})(a_j + A^{(j-1)}) = a_i a_j + A^{(i+j-1)}.$$

Si chiama $G(A)$ l'*algebra graduata associata* all'algebra filtrata A.

11. Sia K un anello commutativo e sia $\Delta = K[\lambda]/(\lambda^2)$, con λ indeterminata. Mostrare che 1 e la classe $d = \lambda + (\lambda^2)$ formano una K-base di Δ e che $d^2 = 0$. Si chiama Δ l'*algebra dei numeri duali* su K. Data una K-algebra A, si formi l'algebra $\Delta \otimes_K A$. Osservare che è un A-modulo destro in cui $(b \otimes x)y = b \otimes xy$ per $b \in \Delta$, $x, y \in A$. Mostrare che $1 = 1 \otimes 1$ e $d = d \otimes 1$ ne formano una base su A e che

$$(x_1 + dy_1)(x_2 + dy_2) = x_1x_2 + d(x_1y_2 + y_1x_2),$$

dove $x_i = 1 \cdot x_i$ e $x_i, y_i \in A$. Mostrare che un K-endomorfismo D di A è una *derivazione*, ossia soddisfa $D(xy) = (Dx)y + x(Dy)$ per $x, y \in A$, se e soltanto se il Δ-endomorfismo di $\Delta \otimes_K A$ tale che $x \mapsto x + d(Dx)$ per $x \in A$ è un automorfismo di algebre. Mostrare che, per $a \in A$, l'elemento $1 + da$ è invertibile in $\Delta \otimes_K A$, con inverso $1 - da$, e che $(1 + da)x(1 - da) = x + d(ax - xa)$. Dedurne che $x \mapsto [a, x] = ax - xa$ è una derivazione, detta *derivazione interna* determinata da a.

12. Generalizzare l'esercizio 11 sostituendo Δ con $\Delta^{(n)} = K[\lambda]/(\lambda^n)$, $n \geq 2$. Si ottiene $\Delta^{(n)} \otimes_K A$, che è un A-modulo destro con base $(1, d, d^2, \ldots, d^{n-1})$, dove $d = \lambda + (\lambda^n)$ si identifica con $d \otimes 1$. Una successione $D = (D_0 = 1, D_1, \ldots, D_{n-1})$ di K-endomorfismi di A si chiama *derivazione superiore di ordine* n se

$$D_i(xy) = \sum_{j+k=i} (D_j x)(D_k y) \qquad (x, y \in A,\ 0 \leq i \leq n-1).$$

Mostrare che $D = (1, D_1, \ldots, D_{n-1})$ è una derivazione superiore di ordine n se e soltanto se il $\Delta^{(n)}$-endomorfismo di $\Delta^{(n)} \otimes_K A$ tale che

$$x \longmapsto x + d(D_1x) + d^2(D_2x) + \cdots + d^{n-1}(D_{n-1}x)$$

è un automorfismo di algebre.

13. Siano M, N moduli su un anello commutativo K, A, B algebre su K, K' un'algebra commutativa su K e K'' un'algebra commutativa su K'. Scriviamo $M_{K'} = K' \otimes_K M$, e così via. Osservare che K'' è un'algebra su K in cui $kk'' = (k1)k''$ per $k \in K$, $k'' \in K''$, con 1 l'unità di K'. Dimostrare i seguenti isomorfismi:

(i)	$M_{K'} \otimes_{K'} N_{K'} \simeq (M \otimes_K N)_{K'}$	di K'-moduli,
(ii)	$A_{K'} \otimes_{K'} B_{K'} \simeq (A \otimes_K B)_{K'}$	di K'-algebre,
(iii)	$(M_{K'})_{K''} \simeq M_{K''}$	di K''-moduli,
(iv)	$(A_{K'})_{K''} \simeq A_{K''}$	di K''-algebre.

3.10 Moduli proiettivi

In questo paragrafo introdurremo una classe di moduli che generalizza quella dei moduli liberi e che, dal punto di vista categoriale, risulta più naturale. Ricordiamo una proprietà fondamentale di sollevamento degli omomorfismi per le Ω-algebre libere. Se F è una Ω-algebra libera e λ è un omomorfismo suriettivo della Ω-algebra A sulla Ω-algebra $\overline{A}$, ogni omomorfismo $\bar{f}$ di F in $\overline{A}$

si può «sollevare» a un omomorfismo f di F in A, ossia esiste f tale che $\bar{f} = \lambda f$ (p. 80). Un risultato analogo vale per i moduli liberi. Se abbiamo un diagramma

$$\begin{array}{ccc} & & F \\ & & \downarrow \bar{f} \\ M & \xrightarrow[\lambda]{} & \overline{M} \end{array}$$

con F libero, possiamo completarlo con un $f\colon F \to M$ in modo da ottenere un diagramma commutativo. La dimostrazione è la stessa che per le Ω-algebre. Sia X una base di F. Per ogni $x \in X$ scegliamo un elemento $u \in M$ tale che $\lambda u = \bar{f}x$ e sia f l'omomorfismo di F in M che manda x in u. Si ha allora $\lambda f x = \bar{f}x$ per ogni $x \in X$, dunque $\lambda f = \bar{f}$, come richiesto.

Isoliamo questa proprietà dei moduli liberi per farne il punto di partenza della seguente generalizzazione.

Definizione 3.8. *Un modulo P si dice proiettivo se, dato un diagramma come quello a sinistra, esiste un omomorfismo $g\colon P \to M$ che rende commutativo il diagramma a destra:*

$$\begin{array}{ccc} & & P \\ & & \downarrow f \\ M & \xrightarrow[p]{} & N \end{array} \qquad\qquad \begin{array}{ccc} & \overset{g}{\swarrow} & P \\ & & \downarrow f \\ M & \xrightarrow[p]{} & N \end{array}$$

In altri termini, dato un epimorfismo $p\colon M \to N$, ogni omomorfismo $f\colon P \to N$ si fattorizza nella forma $f = pg$ con $g\colon P \to M$.

Ricordiamo che, per ogni modulo M, il funtore $\hom(M, -)$ è esatto a sinistra. Se dunque è esatta la successione

$$0 \longrightarrow N' \xrightarrow{i} N \xrightarrow{p} N'' \longrightarrow 0, \tag{72}$$

è esatta anche

$$0 \longrightarrow \hom(M, N') \xrightarrow{\hom(M,i)} \hom(M, N) \xrightarrow{\hom(M,p)} \hom(M, N'').$$

Supponiamo ora che $M = P$ sia proiettivo. Dato $f \in \hom(P, N'')$, esiste $g \in \hom(P, N)$ tale che $\hom(P, p)(g) = pg = f$. Dunque $\hom(P, p)$ è suriettivo e dall'esattezza della (72) segue quella dell'intera successione

$$0 \longrightarrow \hom(P, N') \xrightarrow{\hom(P,i)} \hom(P, N) \xrightarrow{\hom(P,p)} \hom(P, N'') \longrightarrow 0.$$

Se P è proiettivo, $\hom(P, -)$ è pertanto un funtore esatto da mod-R a mod-$\mathbb{Z}$.

Vale anche il viceversa. Supponiamo che $\hom(P, -)$ sia esatto e sia $p\colon M \twoheadrightarrow N$. Posto $K = \ker p$, la successione $0 \to K \xrightarrow{i} M \xrightarrow{p} N \to 0$ è esatta, con i l'inclusione. L'esattezza di $\hom(P, -)$ ci dà la proprietà della definizione 3.8. Abbiamo così stabilito la seguente caratterizzazione categoriale.

Proposizione 3.9. *Un modulo P è proiettivo se e soltanto se $\hom(P, -)$ è un funtore esatto.*

Quanto si avvicinano i moduli proiettivi ai moduli liberi? Daremo alcune risposte a questa domanda. Occorre dapprima un semplice risultato sulle successioni esatte corte

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0. \tag{73}$$

Supponiamo che esista $i'\colon M'' \to M$ tale che $pi' = 1_{M''}$. Allora $p(1_M - i'p) = p - p = 0$. Ne segue che esiste $p'\colon M \to M'$ tale che $1_M - i'p = ip'$. Infatti, per $x \in M$ si ha $p(1_M - i'p)x = 0$,

dunque $(1_M - i'p)x$ è nel nucleo di p, cioè nell'immagine di i. Esiste allora $x' \in M'$ tale che $ix' = (1_M - i'p)x$, unico perché i è un monomorfismo. Si ottiene così un'applicazione $p' \colon x \mapsto x'$ da M a M'. Si verifica direttamente che p' è un omomorfismo di moduli e $ix' = ip'x$, dunque $ip' = 1_M - i'p$, ossia

$$i'p + ip' = 1_M. \tag{74}$$

Inoltre $i'pi'p = i'1_{M''}p = i'p$. Moltiplicando la (74) a destra per $i'p$ si ottiene quindi $ip'i'p = 0$. Per la suriettività di p e l'iniettività di i segue $p'i' = 0$ (su M''). Se $x' \in M'$, allora $ip'ix' = (1_M - i'p)ix' = ix'$, quindi $p'i = 1_{M'}$, ancora per l'iniettività di i. Poiché fin dall'inizio $pi = 0$ e $pi' = 1_{M''}$, abbiamo le quattro relazioni

$$\begin{aligned} pi' &= 1_{M''}, \quad p'i' = 0, \\ p'i &= 1_{M'}, \qquad pi = 0. \end{aligned} \tag{75}$$

Insieme alla (74), esse implicano che M è canonicamente isomorfo a $M' \oplus M''$ (p. 97).

Analogamente, supponiamo che esista $p' \colon M \to M'$ con $p'i = 1_{M'}$. Allora $(1_M - ip')i = i - i1_{M'} = 0$. Ne segue $1_M - ip' = i'p$ per un omomorfismo $i' \colon M'' \to M$. Infatti, se $f \colon M \to M$ è un omomorfismo con $fi = 0$, allora $\ker p = \operatorname{im} i \subset \ker f$. Perciò $px \mapsto fx$ è un'applicazione ben definita g da $pM = M''$ a M. Si verifica direttamente che è un omomorfismo di moduli e chiaramente $gp = f$. Applicando questo fatto a $f = 1_M - ip'$ otteniamo $i' \colon M'' \to M$ con $1_M = ip' + i'p$. Poiché $ip'ip' = i1_{M'}p' = ip'$, si ha $ip'i'p = 0$, quindi $p'i' = 0$. Inoltre $pi'p = p(1_M - ip') = p - pip' = p$, perché $pi = 0$. Siccome p è suriettivo, $pi' = 1_{M''}$. Ritroviamo le (74) e (75), quindi l'isomorfismo canonico $M \simeq M' \oplus M''$.

Diremo che la successione esatta (73) *si spezza* se esiste un $i' \colon M'' \to M$ tale che $pi' = 1_{M''}$ o, equivalentemente, se esiste un $p' \colon M \to M'$ tale che $p'i = 1_{M'}$. Possiamo ora dare due importanti caratterizzazioni dei moduli proiettivi.

Proposizione 3.10. *Per un modulo P sono equivalenti:*

1. *P è proiettivo.*
2. *Ogni successione esatta corta $0 \to M \to N \to P \to 0$ si spezza.*
3. *P è un addendo diretto di un modulo libero (cioè esiste un modulo libero F isomorfo a $P \oplus P'$ per qualche P').*

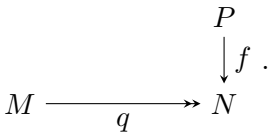
Dimostrazione. (1) $\Rightarrow$ (2). Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ esatta e consideriamo il diagramma

$$\begin{array}{ccc} & & P \\ & & \downarrow 1_P \\ N & \xrightarrow[g]{} & P \end{array}$$

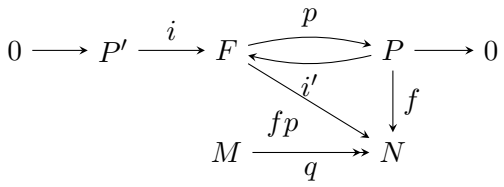
Per ipotesi possiamo completarlo con $g' \colon P \to N$ in modo da renderlo commutativo. Allora $gg' = 1_P$ e la successione si spezza.

(2) $\Rightarrow$ (3). Poiché ogni modulo è immagine omomorfa di un modulo libero, abbiamo una successione esatta corta $0 \to P' \xrightarrow{i} F \xrightarrow{p} P \to 0$, dove F è libero. Se P soddisfa la proprietà 2, questa successione si spezza e dunque $F \simeq P \oplus P'$.

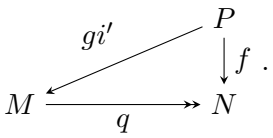
(3) $\Rightarrow$ (1). È data una successione esatta spezzata $0 \to P' \to F \xrightarrow{p} P \to 0$, con F libero. Supponiamo ora dato il diagramma



Combinandolo con il precedente otteniamo



dove $pi' = 1_P$ (la riga superiore si spezza). Poiché F è libero, quindi proiettivo, possiamo inserire $g\colon F \to M$ in modo che $fp = qg$. Allora $f = f1_P = fpi' = qgi'$, e $gi'\colon P \to M$ rende commutativo il diagramma



Pertanto P è proiettivo. □

Una prima conseguenza della proposizione 3.10 è l'esistenza di moduli proiettivi che non sono liberi. L'esempio più semplice è forse il seguente. Sia $F = \mathbb{Z}/(6)$, considerato come modulo su $R = \mathbb{Z}/(6)$, dunque libero. Ora $F \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$. Per la proposizione 3.10 i due addendi sono proiettivi e, evidentemente, nessuno dei due è libero su $\mathbb{Z}/(6)$.

Hanno particolare interesse i moduli proiettivi finitamente generati. La proposizione ne dà la caratterizzazione seguente.

Corollario. *Un modulo P è finitamente generato e proiettivo se e soltanto se è un addendo diretto di un modulo libero con base finita.*

Dimostrazione. Se P è addendo diretto di un modulo libero F con base finita, allora è proiettivo. Inoltre P è immagine omomorfa di F e ammette quindi un insieme finito di generatori, le immagini degli elementi della base mediante un epimorfismo di F su P. Viceversa, se P è finitamente generato e proiettivo, dalla prima condizione si ottiene una successione esatta $0 \to P' \to F \to P \to 0$ con F libero su una base finita. La dimostrazione della proposizione mostra che dalla proiettività di P segue $F \simeq P \oplus P'$, da cui la tesi. □

Alcuni anelli hanno la proprietà che tutti i loro moduli proiettivi sono liberi. È il caso dei domini commutativi a ideali principali. In BAI, pp. 179–180, abbiamo mostrato che ogni sottomodulo di un modulo libero con base finita su un tale dominio D è libero. La dimostrazione si estende a ogni sottomodulo di un modulo libero arbitrario su D. Per la proposizione 3.10(3), ne segue che ogni modulo proiettivo su un dominio a ideali principali è libero. Dimostreremo più avanti (p. 416) che ogni modulo proiettivo finitamente generato su un anello locale è libero. Un altro risultato dello stesso tipo, dimostrato indipendentemente da D. Quillen e A. Suslin, afferma che se $R = D[\lambda_1, \ldots, \lambda_n]$, dove D è un dominio a ideali principali, allora ogni R-modulo proiettivo finitamente generato è libero.[5] Con tale risultato essi risolsero una questione posta da J.-P. Serre nel 1955 e rimasta aperta per oltre vent'anni.

[5]Nell'enunciato dell'edizione inglese è omessa la parola «proiettivo». [N.d.T.]

Diamo ora un criterio «elementare» di proiettività di grandissima utilità.

Proposizione 3.11. *Un R-modulo destro P è proiettivo se e soltanto se esistono elementi $\{x_\alpha \mid \alpha \in I\}$ di P ed elementi $\{x^*_\alpha \mid \alpha \in I\}$ del modulo duale $P^* = \hom(P, R)$ tali che per ogni $x \in P$ si abbia $x^*_\alpha(x) = 0$ per tutti gli indici tranne un numero finito e*

$$x = \sum_{\alpha \in I} x_\alpha x^*_\alpha(x)$$

(con il significato evidente della somma). Se vale la condizione, gli x_α generano P; se P è proiettivo, si può scegliere come famiglia degli x_α una qualunque famiglia di generatori di P.

Dimostrazione. Supponiamo dapprima che P sia proiettivo e che $\{x_\alpha \mid \alpha \in I\}$ generi P. Esistono un modulo libero F con base $\{X_\alpha \mid \alpha \in I\}$ e un epimorfismo $p\colon F \to P$ tale che $p(X_\alpha) = x_\alpha$. La proiettività di P dà un omomorfismo $i'\colon P \to F$ con $pi' = 1_P$. Essendo gli X_α una base di F, ogni $X \in F$ si scrive come $X_{\alpha_1}a_{\alpha_1} + \cdots + X_{\alpha_r}a_{\alpha_r}$ con $a_{\alpha_j} \in R$, ovvero come $X = \sum_{\alpha \in I} X_\alpha a_\alpha$, dove solo un numero finito di coefficienti è diverso da zero e la somma è estesa a questi. Tutti i coefficienti, nulli o meno, sono univocamente determinati da X. Abbiamo così le applicazioni coordinate $X^*_\alpha\colon X \mapsto a_\alpha$; per ogni X tutti i valori $X^*_\alpha(X)$ tranne un numero finito sono nulli. Dalla definizione risulta subito che $X^*_\alpha \in F^* = \hom(F, R)$. Dunque $x^*_\alpha = X^*_\alpha i' \in P^*$ e, per $x \in P$, $x^*_\alpha(x) = X^*_\alpha(i'(x))$ si annulla salvo che per un numero finito di indici. Posto $X = i'(x)$, abbiamo $X = \sum X_\alpha X^*_\alpha(X)$ e, poiché $p(X_\alpha) = x_\alpha$,

$$x = pi'(x) = p(X) = \sum p(X_\alpha)X^*_\alpha(X) = \sum x_\alpha X^*_\alpha i'(x) = \sum x_\alpha x^*_\alpha(x).$$

Le due famiglie hanno quindi le proprietà richieste. Viceversa, siano date in P due famiglie $\{x_\alpha\}$ e $\{x^*_\alpha\}$ come nell'enunciato. Sia di nuovo F il modulo libero con base $\{X_\alpha\}$ e sia $p\colon F \to P$ definito da $p(X_\alpha) = x_\alpha$. Per ogni α abbiamo l'omomorfismo $x \mapsto X_\alpha x^*_\alpha(x)$ di P in F. Poiché per ogni x solo un numero finito di termini è diverso da zero, $i'(x) = \sum X_\alpha x^*_\alpha(x)$ definisce un omomorfismo $i'\colon P \to F$. Allora $pi'(x) = \sum p(X_\alpha)x^*_\alpha(x) = \sum x_\alpha x^*_\alpha(x) = x$. Dunque $pi' = 1_P$, e si ha una successione esatta spezzata $0 \to P' \to F \to P \to 0$. Ne segue che P è addendo diretto di F, dunque proiettivo. □

Il risultato della proposizione 3.11 è spesso detto «lemma della base duale» per i moduli proiettivi. Si osservi, tuttavia, che gli x_α dell'enunciato non formano necessariamente una base di P. Il lemma si usa di solito per caratterizzare i moduli proiettivi finitamente generati. Dalla proposizione 3.11 e dalla sua dimostrazione segue immediatamente il

Corollario. *Un modulo P è finitamente generato e proiettivo se e soltanto se esiste un insieme finito di coppie (x_i, x^*_i), con $x_i \in P$, $x^*_i \in P^*$, tale che per ogni $x \in P$ si abbia $x = \sum_i x_i x^*_i(x)$.*

Numerose proprietà importanti dei moduli liberi si estendono ai moduli proiettivi. Una di esse è la piattezza, che ora definiamo.

Definizione 3.9. *Un modulo destro $M = M_R$ si dice piatto se, per ogni monomorfismo $N' \xrightarrow{f} N$ di R-moduli sinistri, $1_M \otimes f\colon M \otimes_R N' \to M \otimes_R N$ è un monomorfismo di $\mathbb{Z}$-moduli.*

Ricordiamo che il funtore $M \otimes_R -$ da R-mod a $\mathbb{Z}$-mod è esatto a destra (teorema 3.15, p. 132). Come nella dimostrazione della proposizione 3.9, ne segue subito la

Proposizione 3.12. *Un modulo destro M è piatto se e soltanto se il funtore tensoriale $M \otimes_R -$ è esatto.*

Il principale risultato sulla piattezza che dimostreremo in questo paragrafo è che i moduli proiettivi sono piatti. La dimostrazione seguirà facilmente dalla

Proposizione 3.13. *$M = \bigoplus_\alpha M_\alpha$ è piatto se e soltanto se ogni M_α è piatto.*

Dimostrazione. Sia $f\colon N' \hookrightarrow N$ un monomorfismo di moduli sinistri. Basta mostrare che la corrispondente applicazione $M \otimes N' \to M \otimes N$ è iniettiva se e soltanto se lo è $M_\alpha \otimes N' \to M_\alpha \otimes N$

per ogni α. Grazie agli isomorfismi $\eta_{N'}$ e η_N della proposizione 3.3 e alla naturalità espressa dalla (54), basta mostrare che

$$f^*\colon \bigoplus_\alpha (M_\alpha \otimes N') \longrightarrow \bigoplus_\alpha (M_\alpha \otimes N)$$

è iniettiva se e soltanto se $1_{M_\alpha} \otimes f$ lo è per ogni α. Questo risulta dalla definizione di f^*. □

Possiamo ora dimostrare il

Teorema 3.17. *I moduli proiettivi sono piatti.*

Dimostrazione. Osserviamo dapprima che $R = R_R$ è piatto, perché l'applicazione $a \otimes y \mapsto ay$ è un isomorfismo di $R \otimes N$ su N. Dunque $f\colon N' \to N$ è iniettiva se e soltanto se $1_R \otimes f\colon R \otimes N' \to R \otimes N$ lo è. Dalla piattezza di R e dalla proposizione 3.13 segue che ogni R-modulo libero è piatto. Poiché ogni modulo proiettivo è addendo diretto di un modulo libero, una seconda applicazione della proposizione 3.13 conclude la dimostrazione. □

La tecnica di ricondursi a R mediante un risultato sulle somme dirette è abituale quando si tratta di stabilire proprietà dei moduli proiettivi. Per illustrarla ancora, abbozziamo la dimostrazione della

Proposizione 3.14. *Siano K un anello commutativo, P un K-modulo proiettivo finitamente generato e N un K-modulo arbitrario. L'omomorfismo da $\operatorname{End}_K P \otimes_K \operatorname{End}_K N$ a $\operatorname{End}_K(P \otimes_K N)$ che a $f \otimes g$, con $f \in \operatorname{End}_K P$ e $g \in \operatorname{End}_K N$, associa l'endomorfismo $f \otimes g$ dato da $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ è un isomorfismo di K-algebre.*

Dimostrazione. Si vede subito che l'omomorfismo è un omomorfismo di algebre e che è un isomorfismo per $P = K$. Sia ora $M \simeq \bigoplus_{j=1}^r M_j$. Abbiamo isomorfismi canonici da $\operatorname{End} M = \hom(M, M)$ su $\bigoplus_{j,k} \hom(M_j, M_k)$ e da $\operatorname{End} M \otimes \operatorname{End} N$ su $\bigoplus_{j,k}(\hom(M_j, M_k) \otimes \operatorname{End} N)$. Inoltre $\operatorname{End}(M \otimes N) = \hom(M \otimes N, M \otimes N)$ è canonicamente isomorfo a $\bigoplus_{j,k} \hom(M_j \otimes N, M_k \otimes N)$. Usando tali isomorfismi, si vede che l'omomorfismo $\operatorname{End} M \otimes \operatorname{End} N \to \operatorname{End}(M \otimes N)$ che manda $f \otimes g$ in $f \otimes g$, come nell'enunciato, è un isomorfismo se e soltanto se per ogni (j, k) l'analoga applicazione

$$\hom(M_j, M_k) \otimes \operatorname{End} N \longrightarrow \hom(M_j \otimes N, M_k \otimes N)$$

è un isomorfismo. Prendendo tutti gli $M_j = K$ si ottiene la tesi per un modulo libero P con base finita. Ne segue il caso di P proiettivo finitamente generato, poiché un tale P è addendo diretto di un modulo libero con base finita. □

Lasciamo al lettore il compito di completare i dettagli della dimostrazione.

Esercizi

1. Dato il diagramma

$$\begin{array}{ccccc} & \overset{k}{\swarrow} & P & & \\ & & \downarrow f & & \\ M & \xrightarrow[g]{} & N & \xrightarrow[h]{} & Q \end{array}$$

   con la riga esatta, P proiettivo e $hf = 0$, mostrare che esiste $k\colon P \to M$ tale che $f = gk$.

2. Mostrare che, se P_α è proiettivo per ogni $\alpha \in I$, allora $\bigoplus_\alpha P_\alpha$ è proiettivo.

3. Mostrare che, se e è un idempotente di un anello R, allora eR è proiettivo come modulo destro e Re come modulo sinistro.

4. Siano e_{ij} le usuali unità matriciali di $M_n(\Delta)$, con Δ anello di divisione. Mostrare che $e_{11}M_n(\Delta)$ è irriducibile come $M_n(\Delta)$-modulo destro. Concludere che, se $n > 1$, esso è proiettivo ma non libero.

5. Dimostrare che ogni sottomodulo di un modulo libero su un dominio a ideali principali D è libero. (*Suggerimento.* Estendere l'argomento di BAI, p. 179, mediante induzione transfinita oppure mediante il lemma di Zorn.)

6. Mostrare che il gruppo additivo di $\mathbb{Q}$, considerato come $\mathbb{Z}$-modulo, è piatto.

7. Siano R, S anelli, P un R-modulo sinistro proiettivo finitamente generato, M un R-S-bimodulo e N un S-modulo sinistro. Mostrare che esiste un isomorfismo di gruppi

$$\eta\colon \hom_R(P, M) \otimes_S N \longrightarrow \hom_R(P, M \otimes_S N)$$

tale che, per $f \in \hom_R(P, M)$ e $y \in N$, $\eta(f \otimes y)$ è l'omomorfismo $x \mapsto f(x) \otimes y$ da P in $M \otimes_S N$.

8. (*Lemma di Schanuel.*) Siano $0 \to N_i \to P_i \xrightarrow{g_i} M \to 0$, per $i = 1, 2$, successioni esatte corte con P_i proiettivo. Mostrare che $P_1 \oplus N_2 \simeq P_2 \oplus N_1$. (*Suggerimento.* Considerare il prodotto fibrato di g_1 e g_2 costruito nell'esercizio 6, p. 36.)

3.11 Moduli iniettivi. Inviluppo iniettivo

La nozione di modulo proiettivo ammette una nozione duale, ottenuta invertendo le frecce nella definizione. Si ottiene così la

Definizione 3.10. *Un modulo Q si dice iniettivo se, dato un diagramma di omomorfismi*

$$\begin{array}{ccc} N & \xrightarrow{\quad i \quad} & M \\ {\scriptstyle f}\downarrow & & \\ Q & & \end{array} \tag{76}$$

esiste un omomorfismo $g\colon M \to Q$ che rende commutativo il diagramma ottenuto inserendovi g. In altre parole, dati $f\colon N \to Q$ e un monomorfismo $i\colon N \to M$, esiste $g\colon M \to Q$ tale che $f = gi$.

Con un lieve cambiamento di notazione, la definizione equivale a dire che, data una successione esatta $0 \to N' \xrightarrow{i} N$, la successione

$$\hom(N, Q) \xrightarrow{\hom(i,Q)} \hom(N', Q) \longrightarrow 0$$

è esatta. Sappiamo inoltre che dall'esattezza di $N' \xrightarrow{i} N \xrightarrow{p} N'' \to 0$ segue quella di

$$0 \longrightarrow \hom(N'', M) \xrightarrow{\hom(p,M)} \hom(N, M) \xrightarrow{\hom(i,M)} \hom(N', M)$$

(teorema 3.1, p. 99). È quindi chiaro che Q è iniettivo se e soltanto se il funtore controvariante $\hom(-, Q)$ è esatto, nel senso che trasforma ogni successione esatta corta $0 \to N' \to N \to N'' \to 0$ in una successione esatta corta

$$0 \longrightarrow \hom(N'', Q) \longrightarrow \hom(N, Q) \longrightarrow \hom(N', Q) \longrightarrow 0.$$

È facile vedere che la definizione di iniettività equivale anche alla seguente condizione: per ogni sottomodulo N di un modulo M, ogni omomorfismo di N in Q si prolunga a un omomorfismo di

M in Q. Dualizzando la dimostrazione dell'analogo risultato sui proiettivi (cfr. proposizione 3.9, p. 149) si ottiene facilmente un altro risultato: se Q è iniettivo, ogni successione esatta corta $0 \to Q \to M \to N \to 0$ si spezza. Vale anche il viceversa, ma la sua dimostrazione richiede il duale del semplice fatto che ogni modulo è immagine omomorfa di un modulo proiettivo (anzi, libero). L'enunciato duale è che ogni modulo si può immergere in un modulo iniettivo. Vedremo che è effettivamente così, ma la dimostrazione risulterà piuttosto impegnativa.

Reinhold Baer introdusse nel 1940 il concetto di modulo iniettivo, prima ancora che si pensasse ai moduli proiettivi. A lui si deve la maggior parte dei risultati qui presentati, in particolare il criterio seguente.

Proposizione 3.15. *Un modulo destro Q è iniettivo se e soltanto se ogni omomorfismo da un ideale destro I di R in Q si può prolungare a un omomorfismo di R in Q.*

Dimostrazione. La condizione è evidentemente necessaria. Supponiamo ora che sia soddisfatta e sia f un omomorfismo in Q di un sottomodulo N di un modulo M. Consideriamo l'insieme delle coppie (g, M') dove M' è un sottomodulo di M contenente N e g un omomorfismo di M' in Q tale che $g|_N = f$. Introduciamo un ordine parziale ponendo $(g_1, M_1') \geq (g_2, M_2')$ se $M_1' \supseteq M_2'$ e $g_1|_{M_2'} = g_2$. Chiaramente ogni sottoinsieme totalmente ordinato ha un maggiorante in questo insieme. Per il lemma di Zorn esiste dunque una coppia massimale (g, M'). Abbiamo cioè un prolungamento di f a un omomorfismo g su $M' \supseteq N$ massimale nel senso che, se g_1 è definito su $M_1' \supseteq M'$ e $g_1|_{M'} = g$, si deve avere $M_1' = M'$. Affermiamo che $M' = M$. Altrimenti esisterebbe $x \in M \setminus M'$ e $xR + M'$ sarebbe un sottomodulo di M contenente propriamente M'. Poniamo

$$I = \{s \in R \mid xs \in M'\}. \tag{77}$$

Allora $I = \operatorname{ann}(x + M')$ nel modulo M/M', dunque I è un ideale destro di R. Per $s \in I$ si ha $xs \in M'$ e $g(xs) \in Q$. Si vede subito che $h\colon s \mapsto g(xs)$ è un omomorfismo di moduli da I in Q. Per ipotesi, h si prolunga a un omomorfismo k di R in Q. Ne faremo uso per prolungare g a un omomorfismo di $xR + M'$ in Q. Gli elementi di $xR + M'$ sono della forma $xr + y$, con $r \in R$, $y \in M'$. Se $xs + y' = 0$, $s \in R$, $y' \in M'$, la (77) dà $s \in I$ e quindi

$$k(s) = h(s) = g(xs) = -g(y').$$

Da $xs + y' = 0$ segue pertanto $k(s) + g(y') = 0$. L'applicazione

$$xr + y \longmapsto k(r) + g(y), \qquad r \in R,\ y \in M', \tag{78}$$

è dunque ben definita. Infatti, se $xr_1 + y_1 = xr_2 + y_2$, vale $xs + y' = 0$ per $s = r_1 - r_2$, $y' = y_1 - y_2$. Allora $k(s) + g(y') = 0$, ossia $k(r_1 - r_2) + g(y_1 - y_2) = 0$. Poiché k e g sono omomorfismi, $k(r_1) + g(y_1) = k(r_2) + g(y_2)$. La (78) è quindi univoca. Si verifica immediatamente che è un omomorfismo di moduli da $xR + M'$ in Q che prolunga g, in contraddizione con la massimalità di (g, M'). Pertanto $M' = M$: ogni omomorfismo da un sottomodulo N di M in Q si prolunga a M. Quindi Q è iniettivo. □

Per alcuni anelli particolarmente semplici, l'iniettività dei moduli è strettamente connessa alla nozione più elementare di divisibilità, che passiamo a definire. Se $a \in R$, diremo che un modulo M è *divisibile per a* se l'applicazione $x \mapsto xa$ di M in sé è suriettiva. Un modulo si dice *divisibile* se è divisibile per ogni $a \neq 0$. È chiaro che se M è divisibile per a, oppure se è divisibile, ogni sua immagine omomorfa ha la medesima proprietà. In un certo senso l'iniettività generalizza la divisibilità, come mostra la

Proposizione 3.16. *Se R non ha divisori dello zero non nulli, ogni R-modulo iniettivo è divisibile. Se ogni ideale destro di R è principale (cioè uguale ad aR per qualche $a \in R$), ogni R-modulo destro divisibile è iniettivo.*

Dimostrazione. Supponiamo che R non abbia divisori dello zero non nulli e sia Q un R-modulo iniettivo. Siano $x \in Q$ e $0 \neq r \in R$. Da $ra = rb$, con $a, b \in R$, segue $a = b$. Perciò $ra \mapsto xa$, $a \in R$, dà un'applicazione ben definita da rR in Q, evidentemente un omomorfismo di moduli. Poiché Q è iniettivo, si può prolungare tale omomorfismo a tutto R. Se il prolungamento manda 1 in y, manda $r = 1r$ in yr. Ma manda $r = r1$ in $x1 = x$, e dunque $x = yr$. Per l'arbitrarietà di x e di $r \neq 0$, Q è divisibile.

Supponiamo ora che ogni ideale destro di R sia principale. Sia M un R-modulo divisibile e sia f un omomorfismo di rR in M. Se $r = 0$, f è l'applicazione nulla, che si prolunga con l'applicazione nulla su R. Se $r \neq 0$ e $f(r) = x$, esiste $y \in M$ con $x = yr$. Allora $a \mapsto ya$ è un omomorfismo di moduli da R in M e, poiché $rb \mapsto yrb = xb = f(r)b = f(rb)$, prolunga f. Ogni omomorfismo di un ideale destro in M ammette quindi un prolungamento a R. Per il criterio di Baer, M è iniettivo. □

Se R soddisfa entrambe le condizioni della proposizione, un R-modulo è iniettivo se e soltanto se è divisibile. Ciò accade in particolare se R è un dominio a ideali principali. Possiamo servirci di questo fatto per costruire alcuni esempi di moduli iniettivi.

Esempi

1. Sia R un sottoanello di un campo F e consideriamo F come R-modulo nel modo naturale. Evidentemente F è divisibile su R. Se K è un qualunque R-sottomodulo di F, anche F/K è un R-modulo divisibile.

2. Sia D un dominio a ideali principali e sia F il suo campo delle frazioni. Per $r \in D$, il modulo $F/(r)$, dove $(r) = rD$, è divisibile e quindi iniettivo per la proposizione 3.16.

Il nostro prossimo obiettivo è dimostrare che ogni modulo si può immergere in un modulo iniettivo: dato M, esiste una successione esatta $0 \to M \xrightarrow{i} Q$ con Q iniettivo. Il primo passo della dimostrazione è il

Lemma 1. *Ogni gruppo abeliano si può immergere in un gruppo divisibile (come $\mathbb{Z}$-modulo).*

Dimostrazione. Sia dapprima F un gruppo abeliano libero con base $\{x_\alpha\}$ e sia F' lo spazio vettoriale su $\mathbb{Q}$ avente la stessa base. Allora F si immerge in F' ed è chiaro che F' è divisibile. Sia ora M un gruppo abeliano arbitrario. Esso è isomorfo a un quoziente F/K di un gruppo abeliano libero F. Il gruppo F'/K è divisibile e contiene il sottogruppo $F/K \simeq M$. □

Dal lemma e dalla proposizione 3.16 segue immediatamente il

Corollario. *Ogni $\mathbb{Z}$-modulo si può immergere in uno $\mathbb{Z}$-modulo iniettivo.*

Consideriamo ora un R-modulo destro arbitrario M. L'isomorfismo di M su $\hom_R(R, M)$ associa a $x \in M$ l'omomorfismo f_x che manda 1 in x. È un R-isomorfismo se si dà a $\hom_R(R, M)$ la struttura di R-modulo destro indicata nella proposizione 3.4, definendo fa, per $a \in R$, mediante $(fa)(b) = f(ab)$. La stessa definizione rende anche $\hom_{\mathbb{Z}}(R, M)$ un R-modulo destro, del quale $\hom_R(R, M)$ è evidentemente un sottomodulo. L'isomorfismo precedente ci dà così un'immersione di M in $\hom_{\mathbb{Z}}(R, M)$. Immergiamo ora M in uno $\mathbb{Z}$-modulo iniettivo Q, come permette il corollario. Ne risulta un'immersione di $\hom_{\mathbb{Z}}(R, M)$ in $\hom_{\mathbb{Z}}(R, Q)$ e quindi di M in $\hom_{\mathbb{Z}}(R, Q)$ come R-moduli. Abbiamo così immerso M in un R-modulo iniettivo in virtù del seguente lemma.

Lemma 2. *Se Q è iniettivo come $\mathbb{Z}$-modulo,* $\hom_{\mathbb{Z}}(R, Q)$ *è un R-modulo iniettivo.*

Dimostrazione. Dobbiamo mostrare che, se $0 \to N' \xrightarrow{f} N$ è una successione esatta di R-moduli,

allora è esatta

$$\hom_R(N, \hom_{\mathbb{Z}}(R, Q)) \xrightarrow{f^*} \hom_R(N', \hom_{\mathbb{Z}}(R, Q)) \longrightarrow 0, \tag{79}$$

dove $f^* = \hom_R(f, \hom_{\mathbb{Z}}(R, Q))$. Per la proposizione 3.8 abbiamo un isomorfismo

$$\varphi_N \colon \hom_{\mathbb{Z}}(N \otimes_R R, Q) \longrightarrow \hom_R(N, \hom_{\mathbb{Z}}(R, Q)),$$

naturale in N per definizione. Poiché anche l'isomorfismo $N \otimes_R R \to N$ che manda $y \otimes 1$ in y è naturale in N, abbiamo un isomorfismo naturale

$$\psi_N \colon \hom_{\mathbb{Z}}(N, Q) \longrightarrow \hom_R(N, \hom_{\mathbb{Z}}(R, Q)).$$

In altre parole è commutativo il diagramma

$$\begin{array}{ccc} \hom_{\mathbb{Z}}(N, Q) & \xrightarrow{\psi_N} & \hom_R(N, \hom_{\mathbb{Z}}(R, Q)) \\ \bar{f}\downarrow & & \downarrow f^* \\ \hom_{\mathbb{Z}}(N', Q) & \xrightarrow[\psi_{N'}]{} & \hom_R(N', \hom_{\mathbb{Z}}(R, Q)) \end{array}$$

con $\bar{f} = \hom_{\mathbb{Z}}(f, Q)$. Ora $\bar{f}$ è suriettivo perché Q è $\mathbb{Z}$-iniettivo. Dato che ψ_N e $\psi_{N'}$ sono isomorfismi, anche f^* è suriettivo. La (79) è dunque esatta. □

Il lemma completa la dimostrazione del teorema di immersione.

Teorema 3.18. *Ogni modulo si può immergere in un modulo iniettivo.*

La dimostrazione che abbiamo dato è dovuta a B. Eckmann e A. Schopf.

Possiamo ora applicare il teorema per completare la caratterizzazione dei moduli iniettivi cui si è accennato in precedenza.

Proposizione 3.17. *Un modulo Q è iniettivo se e soltanto se ogni successione esatta corta $0 \to Q \to M \to N \to 0$ si spezza. Equivalentemente, Q è iniettivo se e soltanto se è addendo diretto di ogni modulo che lo contiene come sottomodulo.*

Dimostrazione. Abbiamo visto che, se Q è iniettivo, ogni successione esatta $0 \to Q \to M \to N \to 0$ si spezza (p. 156). Viceversa, supponiamo che Q abbia questa proprietà. Per il teorema di immersione esiste una successione esatta $0 \to Q \xrightarrow{i} M$ in cui M è iniettivo. Abbiamo quindi la successione esatta corta $0 \to Q \xrightarrow{i} M \xrightarrow{p} M/Q \to 0$, dove si identifica Q con $i(Q)$ e p è l'omomorfismo canonico. Per ipotesi, esiste $p' \colon M \to Q$ tale che $p'i = 1_Q$. Supponiamo ora dato il diagramma

$$\begin{array}{ccc} N' & \xrightarrow{j} & N \\ f\downarrow & & \\ Q & & \end{array}.$$

L'iniettività di M permette di ampliarlo al diagramma commutativo

$$\begin{array}{ccc} N' & \xrightarrow{j} & N \\ f\downarrow & & \\ Q & \overset{g}{\cdots\cdots} & \\ i\big(\big\uparrow p' & & \\ M & & \end{array}$$

ossia esiste $g\colon N \to M$ con $if = gj$. Allora $f = 1_Q f = p'if = (p'g)j$. Quindi Q è iniettivo. □

Il teorema di immersione ammette un importante perfezionamento: esiste un'immersione in un modulo iniettivo che è in un certo senso minimale, e due estensioni iniettive minimali sono isomorfe. I concetti essenziali per ottenere questi risultati sono quelli di sottomodulo *grande* e di monomorfismo *essenziale*. Un sottomodulo M di un modulo N si dice *grande* (o *essenziale*) in N se $N' \cap M \neq 0$ per ogni sottomodulo $N' \neq 0$ di N. Un monomorfismo $i\colon M \to N$ si dice *essenziale* se $i(M)$ è grande in N. In questo caso N è detto *estensione essenziale* di M.

È chiaro che, se M è grande in N e N è grande in Q, allora M è grande in Q. Sia M un sottomodulo di un modulo N e sia E l'insieme dei sottomoduli S di N contenenti M come sottomodulo grande. Evidentemente $E \neq \varnothing$, poiché $M \in E$. Se $\{S_\alpha\}$ è una catena non vuota in E, allora $S' = \bigcup S_\alpha$ è un sottomodulo. Se N' è un suo sottomodulo non nullo, si ha $N' \cap S_\alpha \neq 0$ per qualche α e, poiché M è grande in S_α, $(N' \cap S_\alpha) \cap M \neq 0$, dunque $N' \cap M \neq 0$. Pertanto M è grande in $S' = \bigcup S_\alpha$. Per il lemma di Zorn, E contiene un elemento massimale S: abbiamo cioè un sottomodulo S di N che contiene M come sottomodulo grande, mentre M non è grande in alcun sottomodulo T che contenga propriamente S.

Possiamo caratterizzare i moduli iniettivi per mezzo dei monomorfismi essenziali.

Proposizione 3.18. *Un modulo Q è iniettivo se e soltanto se ogni monomorfismo essenziale di dominio Q è un isomorfismo.*

Dimostrazione. Supponiamo che Q sia iniettivo e sia $i\colon Q \to M$ un monomorfismo essenziale. La successione esatta $0 \to Q \xrightarrow{i} M \to M/i(Q) \to 0$ si spezza per la proposizione 3.17. Allora $M = i(Q) \oplus Q'$ per un sottomodulo Q'. Poiché $Q' \cap i(Q) = 0$ e i è essenziale, $Q' = 0$. Dunque $M = i(Q)$ e i è un isomorfismo. Viceversa, supponiamo che ogni monomorfismo essenziale di dominio Q sia un isomorfismo e sia $0 \to Q \xrightarrow{i} M \to N \to 0$ esatta. Per il lemma di Zorn esiste un sottomodulo S di M massimale fra quelli tali che $S \cap i(Q) = 0$. Consideriamo il modulo M/S. Poiché $S \cap i(Q) = 0$, l'applicazione $j\colon x \mapsto i(x) + S$ è un monomorfismo di Q in M/S di immagine $(i(Q) + S)/S$. Se un sottomodulo T/S di M/S, con $T \supseteq S$, soddisfa

$$(T/S) \cap ((i(Q) + S)/S) = S/S,$$

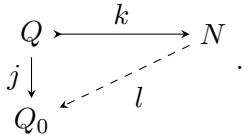
allora $T \cap (i(Q) + S) = S$, dunque $T \cap i(Q) \subseteq S \cap i(Q) = 0$. Per la massimalità di S, segue $T = S$. Questo mostra che j è essenziale, quindi un isomorfismo. Allora $M/S = (i(Q) + S)/S$ e $M = i(Q) + S$. Poiché $S \cap i(Q) = 0$, si ha $M = S \oplus i(Q)$. La successione esatta corta data si spezza e quindi, per la proposizione 3.17, Q è iniettivo. □

Il risultato principale sull'immersione in un modulo iniettivo è il seguente.

Teorema 3.19. *Per ogni modulo M esiste un monomorfismo essenziale i di M in un modulo iniettivo Q. Se i e i' sono monomorfismi essenziali di M nei moduli iniettivi Q e Q', rispettivamente, esiste un isomorfismo $l\colon Q \to Q'$ tale che $i' = li$.*

Per la dimostrazione ci occorre il seguente lemma.

Lemma. *Supponiamo dato il diagramma di monomorfismi*



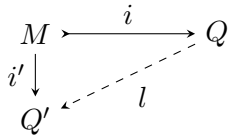
Se k è essenziale e Q_0 è iniettivo, esiste un monomorfismo $l\colon N \to Q_0$ che rende commutativo il triangolo.

Dimostrazione. Poiché Q_0 è iniettivo, esiste un omomorfismo $l\colon N \to Q_0$ che rende commutativo il triangolo. Sia $y \in \ker l \cap \operatorname{im} k$. Allora $y = kx$, con $x \in Q$, e $0 = ly = lkx = jx$. Ne segue $x = 0$

e $y = 0$. Dunque $\ker l \cap \operatorname{im} k = 0$. Poiché k è essenziale, $\ker l = 0$, sicché l è un monomorfismo. □

Possiamo ora dare la *dimostrazione del teorema 3.19.* Sia $i_0 \colon M \to Q_0$ un monomorfismo in un modulo iniettivo Q_0, la cui esistenza è assicurata dal teorema 3.18. Abbiamo visto che esiste un sottomodulo Q di Q_0 in cui $i_0(M)$ è grande e che è massimale rispetto a questa proprietà. Sia i il monomorfismo di M in Q ottenuto restringendo a Q il codominio di i_0. Sia j l'inclusione di Q in Q_0 e sia k un monomorfismo essenziale di Q in un modulo N. Ci troviamo nelle condizioni del lemma precedente. Esiste dunque un monomorfismo $l \colon N \to Q_0$ tale che $lk = j$. Ora $l(N)$ è un sottomodulo di Q_0 contenente $l(k(Q)) = j(Q) = Q$. Per l'essenzialità di k, $k(Q)$ è grande in N e, poiché l è un monomorfismo, $Q = l(k(Q))$ è grande in $l(N)$. Essendo $i(M)$ grande in Q, è grande anche in $l(N) \supseteq Q$. Per la massimalità di Q, $l(N) = Q$. Ne segue facilmente $k(Q) = N$ e quindi k è un isomorfismo. Abbiamo così mostrato che ogni monomorfismo essenziale di dominio Q è un isomorfismo. Per la proposizione 3.18, Q è iniettivo.

Sia ora i' un qualunque monomorfismo essenziale di M in un modulo iniettivo Q'. Applicando il lemma a



otteniamo un monomorfismo $l \colon Q \to Q'$ con $li = i'$. Poiché $l(Q)$ è un sottomodulo iniettivo di Q', esiste un sottomodulo Q'' di Q' con $Q' = l(Q) \oplus Q''$. Da $l(Q) \supseteq i'(M) = l(i(M))$ e $l(Q) \cap Q'' = 0$ segue $i'(M) \cap Q'' = 0$. Ma i' è essenziale, quindi $i'(M)$ è grande in Q' e $Q'' = 0$. Pertanto $Q' = l(Q)$ e l è un isomorfismo di Q su Q' tale che $li = i'$. □

Un modulo iniettivo Q per il quale esista un monomorfismo essenziale $i \colon M \to Q$ si chiama *inviluppo iniettivo* (o *involucro iniettivo*) di M. Il teorema 3.19 ne stabilisce l'esistenza e l'unicità a meno di isomorfismo. La dimostrazione mostra che, se Q' è un qualunque modulo iniettivo e $i' \colon M \to Q'$ è un monomorfismo, esiste un monomorfismo l di Q in Q' tale che $i' = li$. In questo senso un inviluppo iniettivo realizza un'immersione minimale di M in un modulo iniettivo.

Esercizi

1. Sia D un dominio (anello commutativo senza divisori dello zero non nulli) e sia F il suo campo delle frazioni ($F \supseteq D$). Mostrare che, per ogni D-modulo M, $M_F = F \otimes_D M$ è un D-modulo divisibile e che, se M è privo di torsione, $x \mapsto 1 \otimes x$ è un monomorfismo essenziale di M in M_F.

2. Mostrare che $\prod_\alpha Q_\alpha$ è iniettivo se e soltanto se ogni Q_α è iniettivo.

3. Mostrare che un sottomodulo M è grande nel modulo N se e soltanto se, per ogni $0 \neq x \in N$, esiste $r \in R$ tale che $xr \neq 0$ e $xr \in M$.

3.12 Contesti di Morita

Il resto di questo capitolo è dedicato alla teoria di Morita dell'equivalenza fra categorie di moduli. Quando sono equivalenti mod-R e mod-S? Come si realizzano tali equivalenze? Quali sono le autoequivalenze di mod-R? Nel capitolo 1, pp. 29–31, abbiamo dimostrato che mod-R e mod-$M_n(R)$ sono equivalenti per ogni anello R e ogni intero positivo n. Vedremo (§ 3.14) che questo caso è assai vicino a quello più generale in cui si abbia equivalenza fra mod-R e mod-S. Dal punto di vista delle applicazioni, gli strumenti con cui si ottengono questi risultati sono più

importanti dei risultati stessi. La nozione centrale è quella di *contesto di Morita* (o «insieme di dati di pre-equivalenza»). Cominciamo con un esempio.

Consideriamo una quaterna costituita da 1) un anello R, 2) un R-modulo destro M, 3) il duale $M^* = \hom(M, R)$ e 4) $R' = \operatorname{End} M_R$. Come abbiamo visto, M è in modo naturale un R'-R-bimodulo (p. 133): per $r' \in R'$ e $x \in M$, $r'x$ è l'immagine di x mediante r'. Inoltre M^* diventa un R-R'-bimodulo ponendo

$$(ry^*)x = r(y^*x), \qquad (y^*r')x = y^*(r'x) \tag{80}$$

per $r \in R$, $r' \in R'$, $y^* \in M^*$, $x \in M$ (p. 135). È opportuno trattare simmetricamente M e M^*. Scriviamo perciò (y^*, x) per $y^*x = y^*(x)$ e consideriamo l'applicazione da $M^* \times M$ in R che manda la coppia (y^*, x) nel valore (y^*, x). Ne elenchiamo le proprietà:

$$\begin{aligned} (y^*, x_1 + x_2) &= (y^*, x_1) + (y^*, x_2), \\ (y^*, xr) &= (y^*, x)r, \\ (y_1^* + y_2^*, x) &= (y_1^*, x) + (y_2^*, x), \\ (ry^*, x) &= r(y^*, x), \\ (y^*r', x) &= (y^*, r'x). \end{aligned} \tag{81}$$

Le prime due esprimono la definizione di omomorfismo da M_R in R_R, la terza la definizione di somma di omomorfismi; le ultime due sono le (80). La prima, la terza e la quinta mostrano che l'applicazione $(y^*, x) \mapsto (y^*, x)$ è un prodotto R'-bilanciato di M^* e M. Abbiamo dunque un omomorfismo τ da $M^* \otimes_{R'} M$ in R tale che $\tau(y^* \otimes x) = (y^*, x)$. La seconda e la quarta relazione diventano $\tau(y^* \otimes xr) = \tau(y^* \otimes x)r$ e $\tau(ry^* \otimes x) = r\tau(y^* \otimes x)$. Considerando $M^* = {}_R M^*_{R'}$ e $M = {}_{R'}M_R$, e di conseguenza $M^* \otimes_{R'} M$ come R-R-bimodulo, si vede che τ è un omomorfismo di bimoduli.

Definiamo ora un omomorfismo di bimoduli μ da $M \otimes_R M^*$ in R'. Un elemento (x, y^*) di $M \times M^*$ determina un'applicazione di M in sé,

$$[x, y^*] \colon y \longmapsto x(y^*, y). \tag{82}$$

Evidentemente $[x, y^*](y_1 + y_2) = [x, y^*]y_1 + [x, y^*]y_2$ e $[x, y^*](yr) = ([x, y^*]y)r$, sicché $[x, y^*] \in R' = \operatorname{End} M_R$. Inoltre dalla (82) e dalle (81) segue direttamente che

$$\begin{aligned} [x_1 + x_2, y^*] &= [x_1, y^*] + [x_2, y^*], \\ [x, y_1^* + y_2^*] &= [x, y_1^*] + [x, y_2^*], \\ [xr, y^*] &= [x, ry^*], \\ [r'x, y^*] &= r'[x, y^*], \\ [x, y^*r'] &= [x, y^*]r'. \end{aligned} \tag{83}$$

Dalle (83) si ottiene un omomorfismo di R'-R'-bimoduli $\mu \colon M \otimes_R M^* \to R'$ tale che $\mu(x \otimes y^*) = [x, y^*]$. La definizione (82) si può riscrivere

$$[x, y^*]y = x(y^*, y). \tag{84}$$

Si ha inoltre

$$x^*[x, y^*] = (x^*, x)y^*, \tag{85}$$

poiché

$$(x^*[x, y^*])y = x^*([x, y^*]y) = x^*(x(y^*, y)) = (x^*x)(y^*, y) = (x^*, x)(y^*, y)$$

e $\big((x^*,x)y^*\big)y = (x^*,x)(y^*y) = (x^*,x)(y^*,y)$.

Isoliamo gli elementi essenziali di questa situazione.

Definizione 3.11. *Un contesto di Morita è una sestupla (R,R',M,M',τ,μ), dove R,R' sono anelli, $M = {}_{R'}M_R$ è un R'-R-bimodulo, $M' = {}_R M'_{R'}$ un R-R'-bimodulo, $\tau\colon M'\otimes_{R'} M \to R$ un omomorfismo di R-R-bimoduli e $\mu\colon M\otimes_R M' \to R'$ un omomorfismo di R'-R'-bimoduli. Posto $\tau(x'\otimes x) = (x',x)$ e $\mu(x\otimes x') = [x,x']$, si richiede che*

$$\text{(i)}\quad [x,y']y = x(y',y), \qquad \text{(ii)}\quad x'[x,y'] = (x',x)y'.$$

Le condizioni (i) e (ii) equivalgono rispettivamente alla commutatività dei due diagrammi seguenti.

$$\begin{array}{ccc} M\otimes_R M'\otimes_{R'} M & \xrightarrow{1\otimes\tau} & M\otimes_R R \\ {\scriptstyle \mu\otimes 1}\big\downarrow & & \big\downarrow \\ R'\otimes_{R'} M & \longrightarrow & M \end{array}$$

$$\begin{array}{ccc} M'\otimes_{R'} M\otimes_R M' & \xrightarrow{1\otimes\mu} & M'\otimes_{R'} R' \\ {\scriptstyle \tau\otimes 1}\big\downarrow & & \big\downarrow \\ R\otimes_R M' & \longrightarrow & M' \end{array}$$

Le frecce senza etichetta sono gli isomorfismi canonici di $M\otimes_R R$ con M, di $R'\otimes_{R'} M$ con M, ecc.

Le considerazioni precedenti definiscono, a partire da un R-modulo destro M, un contesto di Morita $(R, R' = \operatorname{End} M_R, M, M^*, \tau, \mu)$. Lo chiameremo *contesto di Morita definito da M_R*. Eccone un esempio più semplice.

Esempio. Consideriamo il modulo libero sinistro ${}^{(n)}R$ e il modulo libero destro $R^{(n)}$ come a p. 126. Poniamo $M = R^{(n)}$, $M' = {}^{(n)}R$ e scriviamo gli elementi di M come colonne $x = (x_1,\dots,x_n)^{\mathsf t}$ e quelli di M' come righe $x' = (x'_1,\dots,x'_n)$. Sia $R' = M_n(R)$, l'anello delle matrici $n\times n$ a coefficienti in R. Definendo $r'x$ per $r'\in M_n(R)$ mediante il prodotto matriciale, otteniamo su M una struttura di R'-modulo sinistro e quindi un R'-R-bimodulo. Analogamente M' è un R-R'-bimodulo se r' agisce su x' mediante il prodotto matriciale $x'r'$. Poniamo inoltre $[x,y'] = xy'$, ancora il prodotto matriciale, come a p. 126. Abbiamo così un omomorfismo di R'-R'-bimoduli μ da $M\otimes_R M'$ in $R' = M_n(R)$ tale che $\mu(x\otimes y') = [x,y']$. Poniamo $(y',x) = y'x$. È una matrice 1×1, che possiamo considerare come un elemento di R. Si ha allora un omomorfismo di R-R-bimoduli $\tau\colon M'\otimes_{R'} M \to R$ con $\tau(y'\otimes x) = (y',x)$. Le relazioni (i) e (ii) seguono dall'associatività del prodotto di matrici. Dunque $(R, R' = M_n(R), R^{(n)}, {}^{(n)}R, \tau, \mu)$ è un contesto di Morita.

Se M è un R-modulo destro e $M^* = \hom(M,R)$, poniamo

$$T(M) = \left\{ \sum_{x,y^*} (y^*,x) \right\} \subset R. \tag{86}$$

È il sottogruppo del gruppo additivo di R generato dai valori $(y^*,x) = y^*(x)$, $y^*\in M^*$, $x\in M$. Questo sottogruppo $T(M)$, detto *traccia* di M, è un ideale di R: per $r\in R$ si ha infatti

$$(y^*,x)r = (y^*,xr)\in T(M), \qquad r(y^*,x) = (ry^*,x)\in T(M).$$

Siamo ora in grado di dimostrare il primo teorema fondamentale sui contesti di Morita. Dalla suriettività di τ e μ esso trae numerose conseguenze importanti. I risultati sono impliciti nel

lavoro fondamentale di K. Morita sulla dualità per i moduli. Più tardi H. Bass e altri ne migliorarono considerevolmente la formulazione e chiamarono il risultato «Morita I». Per brevità diremo *progeneratore* un modulo proiettivo finitamente generato il cui ideale traccia sia l'intero anello. La ragione di questo nome diventerà chiara trattando i generatori (§ 3.14).

Morita I. *Sia $(R, R', M, M', \tau, \mu)$ un contesto di Morita in cui τ e μ sono suriettivi. Allora:*

1. $M_R, {}_{R'}M, M'_{R'}, {}_RM'$ sono progeneratori.
2. τ e μ sono isomorfismi.
3. L'applicazione $l\colon x' \mapsto l(x')$, dove $l(x')\colon y \mapsto (x', y)$ manda M in R, è un isomorfismo di bimoduli da ${}_RM'_{R'}$ su ${}_RM^*_{R'}$, con $M^* = \hom(M_R, R_R)$. Analogamente si hanno isomorfismi di bimoduli fra ${}_RM'_{R'}$ e $\hom({}_{R'}M, {}_{R'}R')$, fra ${}_{R'}M_R$ e $\hom({}_RM', {}_RR)$ e fra ${}_{R'}M_R$ e $\hom(M'_{R'}, R'_{R'})$.
4. L'applicazione $\lambda\colon r' \mapsto \lambda(r')$, dove $\lambda(r')\colon y \mapsto r'y$, è un isomorfismo di anelli da R' su $\operatorname{End} M_R = \hom(M_R, M_R)$. Analogamente $\rho\colon r \mapsto \rho(r)$, dove $\rho(r)\colon y \mapsto yr$, è un anti-isomorfismo di anelli da R su $\operatorname{End}({}_{R'}M)$. Si hanno inoltre un isomorfismo λ' da R su $\operatorname{End} M'_{R'}$ e un anti-isomorfismo ρ' da R' su $\operatorname{End}({}_RM')$.
5. I funtori $- \otimes_R M'$ e $- \otimes_{R'} M$ definiscono un'equivalenza fra mod-R e mod-R'. Similmente $M \otimes_R -$ e $M' \otimes_{R'} -$ definiscono un'equivalenza fra R-mod e R'-mod.
6. Per ogni ideale destro I di R poniamo

$$\eta(I) = IM' = \left\{ \sum_i b_i x'_i \;\middle|\; b_i \in I,\ x'_i \in M' \right\}, \tag{87}$$

   e per ogni sottomodulo N' di $M'_{R'}$ poniamo

$$\zeta(N') = (N', M) = \left\{ \sum_i (y'_i, x_i) \;\middle|\; y'_i \in N',\ x_i \in M \right\}. \tag{88}$$

   Allora η e ζ sono inverse e danno isomorfismi fra il reticolo degli ideali destri di R e quello dei sottomoduli di $M'_{R'}$. Inducono inoltre isomorfismi fra il reticolo degli ideali bilateri di R e quello dei sottomoduli di ${}_RM'_{R'}$. Valgono enunciati analoghi per gli ideali sinistri di R, per gli ideali sinistri di R' e per gli ideali destri di R'. Ne segue che R e R' hanno reticoli degli ideali bilateri isomorfi.
7. I centri di R e R' sono isomorfi.

Dimostrazione. (1) Poiché μ è suriettivo, esistono $u_i \in M$, $v'_i \in M'$, $1 \le i \le m$, tali che $\sum_i [u_i, v'_i] = 1$ (l'unità di R'). Quindi, per $x \in M$, si ha

$$x = 1x = \sum_i [u_i, v'_i]x = \sum_i u_i(v'_i, x).$$

Ora l'applicazione $l(v'_i)\colon x \mapsto (v'_i, x)$ appartiene a $\hom(M_R, R)$. Per il lemma della base duale (proposizione 3.11, p. 152), M_R è proiettivo finitamente generato. La suriettività di τ significa che ogni $r \in R$ si scrive $r = \sum_i (y'_i, x_i)$, con $y'_i \in M'$ e $x_i \in M$. Allora $r = \sum_i l(y'_i)(x_i) \in T(M)$, dunque $T(M) = R$. Pertanto M_R è un progeneratore. Le altre tre affermazioni seguono per simmetria.

(2) Sia $\sum_i x'_i \otimes y_i \in \ker\tau$, ossia $\sum_i (x'_i, y_i) = 0$. Per la suriettività di τ esistono $w_j \in M$, $z'_j \in M'$ tali che $\sum_j (z'_j, w_j) = 1$ in R. Quindi

$$\begin{aligned}\sum_i x'_i \otimes y_i &= \sum_{i,j} x'_i \otimes y_i (z'_j, w_j) = \sum_{i,j} x'_i \otimes [y_i, z'_j] w_j \\ &= \sum_{i,j} x'_i [y_i, z'_j] \otimes w_j = \sum_{i,j} (x'_i, y_i) z'_j \otimes w_j = 0.\end{aligned}$$

Dunque $\ker\tau = 0$ e τ è un isomorfismo. Analogamente μ è un isomorfismo.

(3) Abbiamo osservato che $l(y')\colon x \mapsto (y', x)$ appartiene a $\hom(M_R, R)$. Una verifica diretta, usando la definizione delle azioni di R e R' su $\hom(M_R, R)$, mostra che $y' \mapsto l(y')$ è un omomorfismo di R-R'-bimoduli da M' in $\hom(M_R, R)$. Supponiamo $l(y') = 0$, ossia $(y', x) = 0$ per ogni x. Come sopra, scriviamo $1 = \sum_i [u_i, v'_i]$. Allora $y' = \sum_i y'[u_i, v'_i] = \sum_i (y', u_i) v'_i = 0$. Dunque l è iniettivo. Ora, dato $x^* \in \hom(M_R, R)$, poniamo $y' = \sum_i (x^* u_i) v'_i$ con gli stessi u_i, v'_i. Si ha

$$\begin{aligned}l(y')(x) = (y', x) &= \sum_i \left((x^* u_i) v'_i, x\right) = \sum_i (x^* u_i)(v'_i, x) \\ &= x^* \left(\sum_i u_i (v'_i, x)\right) = x^* \left(\sum_i [u_i, v'_i] x\right) = x^*(x).\end{aligned}$$

Quindi $x^* = l(y')$ e l è suriettivo. Le altre tre affermazioni seguono per simmetria.

(4) Poiché M è un R'-R-bimodulo, $\lambda(r')\colon x \mapsto r'x$ è un endomorfismo di M_R. È chiaro che λ è un omomorfismo di anelli da R' in $\operatorname{End} M_R$. Se $\lambda(r') = 0$, allora $r'x = 0$ per ogni $x \in M$. Scrivendo $1 = \sum_i [u_i, v'_i]$ in R' si ottiene

$$r' = r'1 = \sum_i r'[u_i, v'_i] = \sum_i [r' u_i, v'_i] = 0.$$

Quindi λ è iniettivo. Dato $f \in \operatorname{End} M_R$, poniamo $r' = \sum_i [f u_i, v'_i] \in R'$. Allora

$$r'x = \sum_i [f u_i, v'_i] x = \sum_i (f u_i)(v'_i, x) = f\left(\sum_i u_i (v'_i, x)\right) = f\left(\sum_i [u_i, v'_i] x\right) = f(x).$$

Perciò $f = \lambda(r')$ e λ è suriettivo, dunque un isomorfismo di anelli. Gli altri casi sono analoghi.

(5) Se N è un R-modulo destro, $N \otimes_R M'$ è un R'-modulo destro; se N' è un R'-modulo destro, $N' \otimes_{R'} M$ è un R-modulo destro. Si ottengono pertanto i funtori $- \otimes_R M'$ e $- \otimes_{R'} M$ rispettivamente da mod-R in mod-R' e viceversa. Componendoli otteniamo i funtori $- \otimes_R M' \otimes_{R'} M$ da mod-R in sé e $- \otimes_{R'} M \otimes_R M'$ da mod-R' in sé. L'isomorfismo di associatività identifica $(N \otimes_R M') \otimes_{R'} M$ con $N \otimes_R (M' \otimes_{R'} M)$. Applicando poi l'isomorfismo τ da $M' \otimes_{R'} M$ su R, si passa da quest'ultimo modulo a $N \otimes_R R$. Componendo infine con l'isomorfismo canonico da $N \otimes_R R$ a N, otteniamo un isomorfismo di R-moduli destri

$$(N \otimes_R M') \otimes_{R'} M \longrightarrow N. \tag{89}$$

Tutti gli isomorfismi intermedi sono naturali in N, dunque lo è la (89). Pertanto $- \otimes_R M' \otimes_{R'} M$ è naturalmente isomorfo al funtore identico di mod-R. Similmente $- \otimes_{R'} M \otimes_R M'$ è naturalmente isomorfo al funtore identico di mod-R'. Si ottiene così l'equivalenza fra le categorie mod-R e mod-R'; l'altra equivalenza del punto (5) segue per simmetria.

(6) Dalla definizione è chiaro che, se I è un ideale destro di R, $\eta(I)$ è un sottomodulo di $M'_{R'}$. Se poi I è un ideale bilatero, $\eta(I)$ è un sottomodulo di ${}_R M'_{R'}$. Analogamente, se N' è un sottomodulo di $M'_{R'}$, allora $\zeta(N')$ è un ideale destro di R; se è un sottomodulo di ${}_R M'_{R'}$,

allora $\zeta(N')$ è un ideale bilatero di R. Per un ideale destro I di R, $\zeta(\eta(I))$ è l'insieme delle somme di elementi $(by', x) = b(y', x)$, con $b \in I$, $y' \in M'$, $x \in M$. Per la suriettività di τ tale insieme è I. Dunque $\zeta\eta$ è l'identità sul reticolo degli ideali destri. Per un sottomodulo N' di $M'_{R'}$, $\eta(\zeta(N'))$ è l'insieme delle somme di elementi $(y', x)x'$, con $y' \in N'$, $x \in M$, $x' \in M'$. Poiché $(y', x)x' = y'[x, x']$ e μ è suriettivo, si ha $\eta(\zeta(N')) = N'$. È chiaro inoltre che η e ζ conservano l'ordine per inclusione. Sono perciò isomorfismi fra il reticolo degli ideali destri di R e quello dei sottomoduli di $M'_{R'}$ (BAI, p. 460). Evidentemente inducono isomorfismi fra i reticoli degli ideali bilateri di R e dei sottomoduli di ${}_RM'_{R'}$. Gli altri enunciati seguono per simmetria. In particolare, l'applicazione $I' \mapsto M'I' = \{\sum_i x'_i b'_i \mid b'_i \in I',\ x'_i \in M'\}$ è un isomorfismo dal reticolo degli ideali bilateri di R' su quello dei sottomoduli del bimodulo ${}_RM'_{R'}$. Componendo gli isomorfismi, vediamo che per ogni ideale bilatero I di R esiste un unico ideale bilatero I' di R' tale che $IM' = M'I'$, e che $I \mapsto I'$ è un isomorfismo dei reticoli degli ideali bilateri di R e R'.

(7) Per costruire un isomorfismo fra i centri $C(R)$ e $C(R')$, consideriamo gli anelli $\operatorname{End} M_R$ e $\operatorname{End}({}_{R'}M)$. Entrambi sono sottoanelli di $\operatorname{End} M$, l'anello degli endomorfismi del gruppo abeliano M. In quest'ultimo anello ciascuno è il centralizzante dell'altro. Infatti, per (4), $\operatorname{End} M_R$ è l'insieme delle applicazioni $y \mapsto r'y$, $r' \in R'$, e $\operatorname{End}({}_{R'}M)$ è l'insieme delle applicazioni $y \mapsto yr$, $r \in R$. D'altra parte, per definizione $\operatorname{End} M_R$ è il centralizzante del sottoanello costituito dalle applicazioni $y \mapsto yr$. Analogamente $\operatorname{End}({}_{R'}M)$ è il centralizzante in $\operatorname{End} M$ dell'insieme delle applicazioni $y \mapsto r'y$. Ne segue chiaramente che

$$C(\operatorname{End} M_R) = \operatorname{End} M_R \cap \operatorname{End}({}_{R'}M) = C(\operatorname{End}({}_{R'}M)).$$

Poiché $\operatorname{End} M_R$ è isomorfo a R' e $\operatorname{End}({}_{R'}M)$ è anti-isomorfo a R, si ottiene un isomorfismo di $C(R)$ con $C(R')$. □

Mostriamo ora che Morita I si applica a ogni contesto $(R, R' = \operatorname{End} P_R, P, P^* = \hom(P_R, R), \tau, \mu)$ determinato da un progeneratore $P = P_R$, dove τ, μ sono definiti come all'inizio del paragrafo. L'ipotesi che P sia un progeneratore comprende la condizione $T(P) = R$, ossia τ è suriettivo. Poiché P è proiettivo finitamente generato, per il lemma della base duale esistono $x_i \in P$, $x_i^* \in P^*$, $1 \le i \le m$, tali che $x = \sum_i x_i(x_i^* x)$ per ogni $x \in P$. Allora

$$x = \sum_i x_i(x_i^*, x) = \sum_i [x_i, x_i^*]x = \left(\sum_i [x_i, x_i^*]\right) x.$$

Dunque $\sum_i [x_i, x_i^*] = 1_P$, l'unità di $R' = \operatorname{End} P_R$. Ogni $r' \in \operatorname{End} P_R$ si scrive perciò $r' = r'1_P = \sum_i [r'x_i, x_i^*]$, sicché anche μ è suriettivo su R'. Abbiamo dunque il seguente risultato.

Teorema 3.20. *Se P è un progeneratore in* mod-R*, allora, nel contesto di Morita $(R, R' = \operatorname{End} P_R, P, P^* = \hom(P_R, R), \tau, \mu)$, μ e τ sono suriettivi. Si applica pertanto Morita I.*

Esercizi

1. Mostrare che Morita I si applica all'esempio delle pp. 166–167. Interpretare in questo caso i risultati del teorema come teoremi sulle matrici. In particolare, usare la corrispondenza fra i reticoli degli ideali di R e R' data nella dimostrazione di Morita I (6) per mostrare che $B \mapsto M_n(B)$ è un isomorfismo dal reticolo degli ideali di R su quello degli ideali di $M_n(R)$ (esercizio 8 a p. 103 di BAI).

2. Sia $(R, R', M, M', \tau, \mu)$ un contesto di Morita. Sia $\left(\begin{smallmatrix} R & M' \\ M & R' \end{smallmatrix}\right)$ l'insieme delle matrici $\left(\begin{smallmatrix} a & x' \\ y & b' \end{smallmatrix}\right)$, con $a \in R$, $b' \in R'$, $x' \in M'$, $y \in M$. Definire l'addizione componente per componente (usuale somma di matrici) e la moltiplicazione ponendo

$$\begin{pmatrix} a_1 & x'_1 \\ y_1 & b'_1 \end{pmatrix} \begin{pmatrix} a_2 & x'_2 \\ y_2 & b'_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + (x'_1, y_2) & a_1x'_2 + x'_1b'_2 \\ y_1a_2 + b'_1y_2 & [y_1, x'_2] + b'_1b'_2 \end{pmatrix}.$$

Verificare che l'addizione e la moltiplicazione così definite, con gli ovvi elementi 0 e 1, danno un anello. Lo chiameremo *anello del contesto di Morita* $(R, R', M, M', \tau, \mu)$. Siano B un ideale di R e B' un ideale di R'. Verificare che l'insieme delle matrici

$$\begin{pmatrix} B & BM' + M'B' \\ B'M + MB & B' \end{pmatrix}$$

è un ideale dell'anello precedente.[6]

3. Considerare il caso particolare dell'esercizio 2 in cui $M' = 0$, $\tau = 0$, $\mu = 0$. Mostrare che l'anello ottenuto è isomorfo a quello definito come nell'esercizio 1 di p. 136, considerando M come T-T-bimodulo per $T = R \times R'$, come nell'esercizio 2 della stessa pagina.

3.13 Il teorema di Wedderburn–Artin per gli anelli semplici

Applicheremo ora Morita I per dedurre un classico teorema di struttura per gli anelli semplici, il teorema di Wedderburn–Artin. Wedderburn lo dimostrò nel 1908 per le algebre di dimensione finita su un campo; Artin nel 1928 per gli anelli che soddisfano la condizione delle catene discendenti per gli ideali unilateri. Nel prossimo capitolo inseriremo questo teorema nella teoria generale della struttura degli anelli. Qui lo tratteremo separatamente e lo formuleremo nel modo seguente.

Teorema di Wedderburn–Artin per gli anelli semplici. *Per un anello R sono equivalenti le seguenti condizioni:*

1. *R è semplice e contiene un ideale destro (sinistro) minimale.*
2. *R è isomorfo all'anello delle trasformazioni lineari di uno spazio vettoriale di dimensione finita su un anello di divisione.*
3. *R è semplice, artiniano a sinistra e a destra e noetheriano a sinistra e a destra.*

Dimostrazione. (1) $\Rightarrow$ (2). Sia I un ideale destro minimale di R. Allora $I = I_R$ è un R-modulo destro irriducibile. Mostriamo anzitutto che I_R è proiettivo finitamente generato. Consideriamo $RI = \sum_{a \in R} aI$. È un ideale bilatero di R contenente I, quindi $RI = R$. Possiamo allora scrivere $1 = \sum_i a_i b_i$ con $a_i \in R$, $b_i \in I$. Ne segue che $R = \sum_i a_i I$. Osserviamo che, per $a \in R$, l'applicazione $x \mapsto ax$, $x \in I$, è un omomorfismo di moduli destri con dominio I. Per il lemma di Schur si ha $aI = 0$ oppure $aI \cong I$ come modulo destro. Dunque $R = \sum_i a_i I$ è somma di moduli destri irriducibili. Per il teorema 3.9 (p. 117), $R = I \oplus I'$, dove I' è un altro ideale destro. Ne segue che I è proiettivo e può essere generato da un solo elemento. Per il lemma della base duale l'ideale traccia $T(I)$ è diverso da zero; poiché R è semplice, $T(I) = R$ e I è un progeneratore. Morita I si applica perciò al contesto $(R, R' = \operatorname{End} I_R, I, I^* = \hom(I_R, R), \tau, \mu)$. Per il lemma di Schur, R' è un anello di divisione. Per Morita I, I^* è un modulo destro finitamente generato su R' e R è isomorfo a $\operatorname{End} I^*_{R'}$. Sostituendo nel modo consueto a R' il suo opposto $\Delta = (R')^{\mathrm{op}}$, I^* diventa uno spazio vettoriale sinistro di dimensione finita su Δ e R è isomorfo all'anello delle trasformazioni lineari di questo spazio. Per un ideale sinistro minimale I la dimostrazione è analoga.

(2) $\Rightarrow$ (3). Sia V uno spazio vettoriale di dimensione finita su un anello di divisione Δ e sia L il suo anello delle trasformazioni lineari. Poniamo $R = \Delta^{\mathrm{op}}$ e consideriamo V come modulo

[6] Quest'ultima affermazione dell'originale richiede condizioni di compatibilità: occorrono $(M'B', M) \subseteq B$ e $[MB, M'] \subseteq B'$. Per esempio, nel contesto matriciale con $n = 1$ su un campo, la scelta $B = R$, $B' = 0$ non dà un ideale dell'anello delle matrici 2×2. [N.d.T.]

destro su R. Allora V_R è libero con una base finita, dunque è proiettivo finitamente generato. Inoltre, dato $0 \neq x \in V$, esiste una funzione lineare f tale che $f(x) = 1$. Ne segue che $T(V_R) = R$ e quindi V_R è un progeneratore. Morita I si applica al contesto

$$(R, L = \operatorname{End} V_R = \operatorname{End}({}_\Delta V), V, V^* = \hom(V_R, R), \tau, \mu).$$

Il punto (6) di Morita I mostra che L e l'anello di divisione R hanno reticoli degli ideali bilateri isomorfi. Pertanto L è semplice. Lo stesso risultato mostra che il reticolo degli ideali sinistri di L è isomorfo al reticolo dei sottomoduli di V^* e quello degli ideali destri al reticolo dei sottomoduli di V. Poiché gli spazi vettoriali di dimensione finita soddisfano le condizioni delle catene discendenti e ascendenti per i sottospazi, L è artiniano e noetheriano sia a sinistra sia a destra.

L'implicazione (3) $\Rightarrow$ (1) è chiara. □

Esercizi

1. Usare Morita I (6) per dimostrare che, se L è l'anello delle trasformazioni lineari di uno spazio vettoriale V di dimensione finita su un anello di divisione, allora L agisce irriducibilmente su V (cioè V, considerato in modo naturale come L-modulo sinistro, è irriducibile).

2. Siano V uno spazio vettoriale di dimensione finita su un anello di divisione Δ e V^* lo spazio vettoriale destro delle funzioni lineari su V. Per $x \in V$, $f \in V^*$ scrivere $\langle x, f\rangle = f(x)$. Per un sottospazio U di V e un sottospazio U^* di V^* porre rispettivamente

$$U^\perp = \{f \in V^* \mid \langle y, f\rangle = 0 \text{ per ogni } y \in U\},$$
$$(U^*)^\perp = \{y \in V \mid \langle y, g\rangle = 0 \text{ per ogni } g \in U^*\}.$$

   Mostrare che le applicazioni $U \mapsto U^\perp$, $U^* \mapsto (U^*)^\perp$ sono inverse e quindi sono anti-isomorfismi fra i reticoli dei sottospazi di V e di V^*.

3. Siano V, L come nell'esercizio 1. Usare Morita I (6) e l'esercizio 2 per mostrare che l'applicazione

$$\alpha\colon U \longmapsto \alpha(U) = \{\ell \in L \mid \ell(U) = 0\}$$

   è un anti-isomorfismo dal reticolo dei sottospazi di V su quello degli ideali sinistri di L.

4. Mostrare che l'applicazione $J \mapsto \operatorname{ann}_L J = \{\ell \in L \mid \ell J = 0\}$ è un anti-isomorfismo dal reticolo degli ideali destri di L su quello degli ideali sinistri di L.

5. Mostrare che ogni ideale sinistro (destro) di L è un ideale sinistro (destro) principale generato da un idempotente, ossia è della forma Le, con $e^2 = e$ (rispettivamente eL, con $e^2 = e$).

6. Mostrare che per ogni $\ell \in L$ esiste $u \in L$ tale che $\ell u \ell = \ell$.

3.14 Generatori e progeneratori

Siano R un anello e M un R-modulo destro. Ogni $x \in M$ appartiene al sottomodulo xR, per cui $M = \sum_{x \in M} xR$, e xR è immagine omomorfa di R_R. Diremo che un R-modulo destro X è un *generatore* di mod-R se ogni modulo M è somma di sottomoduli che sono immagini omomorfe di X. Dunque R è un generatore. È chiaro che, se X è un generatore ed è immagine omomorfa di Y, anche Y è un generatore. Poiché un'immagine omomorfa di $X^{(n)}$ è somma di

immagini omomorfe di X, se $X^{(n)}$ è un generatore lo è anche X. I generatori avranno una parte centrale nello studio delle equivalenze fra categorie di moduli. Il prossimo teorema ne dà alcune importanti caratterizzazioni.

Teorema 3.21. *Per un modulo X le seguenti condizioni sono equivalenti.*

1. X è un generatore.
2. Il funtore $\hom(X, -)$ è fedele (si veda p. 22).
3. L'ideale traccia $T(X)$ coincide con R.
4. Esiste un intero n tale che R è immagine omomorfa di $X^{(n)}$.

Dimostrazione. (1) $\Rightarrow$ (2). Dati due R-moduli destri M, N, dobbiamo mostrare che $f \mapsto \hom(X, f)$ è iniettiva da $\hom(M_R, N_R)$ nell'insieme degli omomorfismi da $\hom(X, M)$ a $\hom(X, N)$. Qui $\hom(X, f)$ manda g in fg. Per additività basta mostrare che per ogni $f\colon M \to N$ diverso da zero esiste un $g \in \hom(X, M)$ con $fg \neq 0$. Supponiamo invece $fg = 0$ per ogni g. Poiché X è un generatore, $M = \sum_g gX$, dove la somma è estesa a tutti gli omomorfismi da X in M. Allora $fM = f(\sum_g gX) = \sum_g fgX = 0$, contro l'ipotesi.

(2) $\Rightarrow$ (3). Poniamo $M = R$, $N = R/T(X)$ e sia ν l'omomorfismo canonico da M in N. Se $g \in X^* = \hom(X, M)$, allora $g(x) \in T(X)$ per ogni $x \in X$ e quindi $\nu g(x) = 0$. Dunque $\nu g = 0$ per ogni g e, per ipotesi, $\nu = 0$. Ne segue $N = 0$, cioè $R = T(X)$.

(3) $\Rightarrow$ (4). Per la (3) possiamo scrivere $1 = \sum_{i=1}^{m} f_i(x_i)$, con $x_i \in X$, $f_i \in X^*$. Consideriamo l'applicazione $(y_1, \ldots, y_m) \mapsto \sum_i f_i(y_i)$ da $X^{(m)}$ a R. È un omomorfismo di R-moduli destri, dunque la sua immagine è un ideale destro di R. Poiché contiene 1, coincide con R e l'omomorfismo è suriettivo.

(4) $\Rightarrow$ (1). Poiché R è un generatore ed è immagine omomorfa di $X^{(n)}$, anche $X^{(n)}$ è un generatore. Lo è quindi X. □

Per la terza caratterizzazione, X è un progeneratore nel senso del ğ3.12 se e soltanto se è proiettivo, finitamente generato e generatore di mod-R.

Chiamiamo *fedele* un modulo M se $Ma = 0$ per $a \in R$ implica $a = 0$. Per ogni M poniamo $\operatorname{ann}_R M = \{b \in R \mid Mb = 0\}$. È un ideale di R, e M è fedele se e soltanto se $\operatorname{ann}_R M = 0$. Il modulo R_R è fedele e dalla condizione (4) del teorema 3.21 segue che ogni generatore X è fedele: se R è immagine omomorfa di $X^{(n)}$, allora $\operatorname{ann}_R X \subseteq \operatorname{ann}_R R = 0$.

Nel caso importante in cui R è commutativo, per i moduli proiettivi finitamente generati si può sostituire la condizione (3) del teorema 3.21 con la più semplice condizione di fedeltà. Per dimostrarlo ci serve il seguente lemma.

Lemma. *Siano R un anello commutativo e M un R-modulo finitamente generato. Per un ideale I di R vale $MI = M$ se e soltanto se $I + \operatorname{ann}_R M = R$.*

Dimostrazione. (1) Se $I + \operatorname{ann}_R M = R$, scriviamo $1 = b + c$, con $b \in I$ e $c \in \operatorname{ann}_R M$. Per $x \in M$ si ha $x = x1 = xb + xc = xb \in MI$. Dunque $MI = M$. Per questa parte non occorre che M sia finitamente generato.

(2) Siano $x_1, \ldots, x_n$ generatori di M. Se $MI = M$, ogni $x \in M$ ha la forma $\sum_i x_i b_i$, $b_i \in I$. In particolare $x_i = \sum_j x_j b_{ji}$ per $1 \leq i \leq n$, ossia $\sum_j x_j(\delta_{ji} - b_{ji}) = 0$. Ponendo $B = (b_{ij})$, ne segue $x_j \det(1 - B) = 0$ per ogni j. Evidentemente $c = \det(1 - B) = 1 - b$ con $b \in I$. Per commutatività, da $x_j c = 0$ per tutti i generatori segue $xc = 0$ per ogni $x \in M$. Dunque $c \in \operatorname{ann}_R M$ e $1 = b + c \in I + \operatorname{ann}_R M$, come volevamo. □

Teorema 3.22. *Ogni modulo fedele, finitamente generato e proiettivo su un anello commutativo è un generatore, e quindi un progeneratore.*

Dimostrazione. Se M è proiettivo finitamente generato, il lemma della base duale fornisce $x_1, \dots, x_n \in M$ e $f_1, \dots, f_n \in \hom_R(M, R)$ tali che $x = \sum_i x_i f_i(x)$. Poiché $f_i(x) \in T(M)$, si ha $M = MT(M)$. Dal lemma segue $R = \operatorname{ann}_R M + T(M)$. Se M è fedele, $R = T(M)$ e il teorema 3.21 conclude. □

Considerando equivalenze fra mod-R e mod-R' per un secondo anello R', supponiamo naturalmente additivi i funtori F, G che danno l'equivalenza. Ricordiamo che F è fedele e pieno (proposizione 1.3, p. 27). Per ogni coppia M, N di R-moduli, F induce dunque un isomorfismo fra $\hom_R(M, N)$ e $\hom_{R'}(FM, FN)$, e rispetta la composizione. Pertanto le proprietà di un modulo o di un omomorfismo che si esprimono in termini categoriali si trasportano alla categoria equivalente. Per esempio, $f\colon M \to N$ è iniettivo (suriettivo) se e soltanto se è un monomorfismo (epimorfismo) in mod-R. Ciò equivale all'iniettività (suriettività) di $F(f)\colon FM \to FN$.

La nozione di sottoggetto (p. 18) consente di trattare categorialmente i sottomoduli di N. Un sottoggetto di N è una classe $[f]$ di monomorfismi $f\colon M \to N$, dove $f'\colon M' \to N$ è equivalente a f quando esiste un isomorfismo $g\colon M' \to M$ tale che $f' = fg$. Allora $f'M' = fM$: tutti i rappresentanti hanno per immagine lo stesso sottomodulo. Viceversa, se M è un sottomodulo, l'inclusione $i\colon M \to N$ è un monomorfismo con immagine M. Si ha così una biiezione fra sottomoduli e sottoggetti di N. Essa conserva l'ordine se i sottomoduli sono ordinati per inclusione e si pone $[f'] \leq [f]$ quando $f' = fg$ per un monomorfismo g. Per una famiglia diretta $\{N_\alpha\}$ di sottomoduli, l'unione $\bigcup N_\alpha$ è un sottomodulo ed è l'estremo superiore della famiglia. Anche ogni famiglia diretta di sottoggetti ammette quindi un estremo superiore. Se (F, G) è un'equivalenza e $[f] = \sup_\alpha [f_\alpha]$, allora i $[F(f_\alpha)]$ formano una famiglia diretta di sottoggetti di FN con estremo superiore $[F(f)]$. Un sottoggetto $[f]$ si dice *proprio* quando f non è un isomorfismo, ossia quando fM è un sottomodulo proprio di N. Se $[f]$ è proprio, lo è $[F(f)]$.

Vogliamo mostrare che, se X è un progeneratore di mod-R, allora FX è un progeneratore di mod-R'. Ciò seguirà dalla proposizione seguente.

Proposizione 3.19. *Sia (F, G) un'equivalenza fra* mod-R *e* mod-R'. *(1) Se X è un generatore, FX è un generatore. (2) Se X è proiettivo, FX è proiettivo. (3) Se X è finitamente generato, FX è finitamente generato.*

Dimostrazione. (1) Per il teorema 3.21, condizione (2), X è un generatore se e soltanto se per ogni $f\colon M \to N$ diverso da zero esiste $g\colon X \to M$ con $fg \neq 0$. Sia $f'\colon M' \to N'$ diverso da zero in mod-R'. Allora $G(f') \neq 0$, per cui esiste $g\colon X \to GM'$ con $G(f')g \neq 0$. Si ha $FG(f')F(g) \neq 0$; poiché FG è naturalmente isomorfo all'identità, esiste $g'\colon FX \to M'$ tale che $f'g' \neq 0$ (si disegni un diagramma). Dunque FX è un generatore.

(2) Poiché la suriettività equivale all'essere un epimorfismo, X è proiettivo se e soltanto se per ogni epimorfismo $p\colon M \to N$ l'applicazione $g \mapsto pg$ da $\hom_R(X, M)$ a $\hom_R(X, N)$ è suriettiva. Se ne deduce facilmente che FX è proiettivo. Lasciamo al lettore i particolari.

(3) X è finitamente generato se e soltanto se non è unione di una famiglia diretta di sottomoduli propri (esercizio 3, p. 60). In termini categoriali l'estremo superiore di ogni famiglia diretta di sottoggetti propri di X è proprio. Per la simmetria dell'equivalenza basta mostrare che se $[f] = \sup_\alpha [f_\alpha]$ non è proprio, pur essendo propri i $[f_\alpha]$ del modulo N, lo stesso vale per i $[F(f_\alpha)]$ in FN. Ciò segue dall'osservazione precedente. □

Esercizi

1. Mostrare che la proposizione 3.19 vale anche per l'iniettività di un modulo.

2. Nelle ipotesi della proposizione 3.19, mostrare che, se M è noetheriano, lo è FM. Che cosa accade se N è artiniano?

3. Un modulo X si dice *cogeneratore* se per ogni M esiste un monomorfismo di M in un prodotto $\prod_I X$ di copie di X. Mostrare che ciò equivale alla fedeltà del funtore $\hom(-, X)$.

4. Determinare un cogeneratore per mod-$\mathbb{Z}$.

3.15 Equivalenza di categorie di moduli

Prima di passare al prossimo risultato fondamentale, che fornirà una condizione per l'equivalenza delle categorie **mod**-R e **mod**-R' di due anelli R e R' e descriverà la forma di tali equivalenze, stabiliremo un isomorfismo naturale fra due funtori che compaiono nella situazione del teorema Morita I.

Ricordiamo che, per $P = {}_{R'}P_R$ e $M = M_R$ (dunque $M = {}_{\mathbb{Z}}M_R$), si può considerare $\hom(P_R, M_R)$ come un R'-modulo destro, secondo la proposizione 3.4: per $f \in \hom(P_R, M_R)$ e $r' \in R'$ si pone $(fr')x = f(r'x)$ (p. 134). Si definisce così un funtore $\hom(P_R, -)$ da **mod**-R a **mod**-R'. Mostreremo ora che, dato un contesto di Morita $(R, R', P, P', \tau, \mu)$ con τ e μ suriettive, come in Morita I, i funtori $\hom(P_R, -)$ e $- \otimes_R P'$ sono naturalmente isomorfi. Per $u \in M$ e $z' \in P'$, definiamo l'applicazione da P in M

$$\{u, z'\}\colon z \longmapsto u(z', z), \qquad z \in P. \tag{90}$$

È chiaro che $\{u, z'\} \in \hom(P_R, M_R)$ e che $(u, z') \mapsto \{u, z'\}$ definisce un prodotto bilanciato di M_R e ${}_RP'$. Si ha dunque un omomorfismo da $M \otimes_R P'$ in $\hom(P_R, M_R)$ tale che $u \otimes z' \mapsto \{u, z'\}$. Per $r' \in R'$ si ha

$$(\{u, z'\}r')z = \{u, z'\}(r'z) = u(z', r'z) = u(z'r', z).$$

Dunque $\{u, z'\}r' = \{u, z'r'\}$ e l'omomorfismo $u \otimes z' \mapsto \{u, z'\}$ è un omomorfismo di R'-moduli destri. Affermiamo che è un isomorfismo. Come nella dimostrazione di Morita I, scriviamo $1 = \sum_j [u_j, v'_j]$ con $u_j \in P$, $v'_j \in P'$. Se $f \in \hom(P_R, M_R)$ e $z \in P$, si ha

$$\begin{aligned} fz = f(1z) &= f\Big(\sum_j [u_j, v'_j]z\Big) = f\Big(\sum_j u_j(v'_j, z)\Big) \\ &= \sum_j f(u_j)(v'_j, z) = \sum_j \{fu_j, v'_j\}z. \end{aligned}$$

Quindi $f = \sum_j \{fu_j, v'_j\}$ e l'omomorfismo è suriettivo. Supponiamo ora che $\sum_i \{w_i, w'_i\} = 0$, con $w_i \in M$, $w'_i \in P'$. Allora

$$\begin{aligned} \sum_i w_i \otimes w'_i &= \sum_i w_i \otimes w'_i 1 = \sum_{i,j} w_i \otimes w'_i [u_j, v'_j] \\ &= \sum_{i,j} w_i \otimes (w'_i, u_j)v'_j = \sum_{i,j} w_i(w'_i, u_j) \otimes v'_j \\ &= \sum_{i,j} \{w_i, w'_i\} u_j \otimes v'_j = 0. \end{aligned}$$

L'omomorfismo è quindi iniettivo. Abbiamo così un isomorfismo di R'-moduli destri

$$\eta_M\colon M \otimes_R P' \longrightarrow \hom(P_R, M_R) \tag{91}$$

tale che $\eta_M(u \otimes z') = \{u, z'\}$. Esso è naturale in M: per $f \in \hom(M_R, N_R)$ il diagramma

$$\begin{array}{ccc} M \otimes_R P' & \xrightarrow{\eta_M} & \hom(P_R, M_R) \\ {\scriptstyle f \otimes 1}\downarrow & & \downarrow{\scriptstyle \hom(P, f)} \\ N \otimes_R P' & \xrightarrow[\eta_N]{} & \hom(P_R, N_R) \end{array}$$

è commutativo. Infatti, per $u \otimes z' \in M \otimes_R P'$, la (90) dà $\hom(P,f)\eta_M(u \otimes z') = f\{u,z'\} = \{fu,z'\}$, e anche $\eta_N(f \otimes 1)(u \otimes z') = \{fu,z'\}$. Ciò prova la commutatività. I funtori $- \otimes_R P'$ e $\hom(P_R,-)$ sono quindi naturalmente isomorfi.

Possiamo ora dimostrare il secondo risultato fondamentale della teoria di Morita.

Morita II. *Siano R e R' anelli tali che le categorie* **mod**-R *e* **mod**-R' *siano equivalenti. Allora:*

1. *Esistono bimoduli ${}_{R'}P_R$, ${}_RP'_{R'}$ e un contesto di Morita (R,R',P,P',τ,μ) per il quale τ e μ sono suriettive e vale quindi Morita I. In particolare, R' è isomorfo a* $\operatorname{End} P_R$ *per un progeneratore P di* **mod**-R*, e R è isomorfo a* $\operatorname{End} P'_{R'}$ *per un progeneratore P' di* **mod**-R'*.*

2. *Se (F,G) è una coppia di funtori che dà un'equivalenza fra* **mod**-R *e* **mod**-R'*, allora F è naturalmente isomorfo a $- \otimes_R P'$ e G a $- \otimes_{R'} P$, con P, P' come in (1).*

Dimostrazione. (1) Sia (F,G) come in (2) e poniamo $P = GR'$, $P' = FR$. Poiché R è un progeneratore di **mod**-R, per la proposizione 3.19 P' è un progeneratore di **mod**-R'. Analogamente P è un progeneratore di **mod**-R. Essendo R' un anello, l'applicazione $\lambda\colon r' \mapsto \lambda(r')$, dove $\lambda(r')$ è la moltiplicazione a sinistra $x' \mapsto r'x'$, è un isomorfismo di R' su $\operatorname{End} R'_{R'}$. Applicando G a $\operatorname{End} R'_{R'} = \hom(R'_{R'}, R'_{R'})$ si ha un isomorfismo di questo anello su $\hom(P_R,P_R) = \operatorname{End} P_R$. Otteniamo dunque l'isomorfismo di anelli $r' \mapsto G\lambda(r')$ da R' su $\operatorname{End} P_R$. La formula $r'x = G\lambda(r')x$ fa di P un R'-R-bimodulo. Analogamente $r \mapsto F\lambda(r)$ è un isomorfismo di R su $\operatorname{End} P'_{R'}$ e P' è un R-R'-bimodulo con $rx' = F\lambda(r)x'$. Si ha la catena di isomorfismi di gruppi

$$\begin{aligned} P'_{R'} &\cong \hom(R', P'_{R'}) = \hom(R', FR) \\ &\cong \hom(P_R, GFR) \cong \hom(P_R, R) = P^*. \end{aligned} \tag{92}$$

Il primo è l'isomorfismo canonico (esercizio 1, p. 99), il secondo è dato da G e il terzo è $g \mapsto \zeta_{GFR}g$, dove ζ è l'isomorfismo naturale assegnato da GF al funtore identico di **mod**-R. Tutti i moduli $R', P'_{R'}, P_R, R, GFR$ della (92), salvo GFR, sono già bimoduli; GFR diventa un R-R-bimodulo ponendo $rx = GF\lambda(r)x$ per $r \in R$, $x \in GFR$. Con queste definizioni, la proposizione 3.4 (p. 134) munisce tutti i gruppi di omomorfismi della (92) di una struttura di R-R'-bimodulo. L'isomorfismo canonico fra $P'_{R'}$ e $\hom(R', P'_{R'})$ è evidentemente un isomorfismo di tali bimoduli. Su $\hom(R', FR)$ l'azione sinistra di R è data da $rf = F\lambda(r)f$ e l'azione destra di R' da $fr' = f\lambda(r')$. Applicando G si ottiene $G(rf) = GF\lambda(r)G(f)$ e $G(fr') = G(f)G\lambda(r')$. Considerate le azioni di R e R' su $\hom(P_R, GFR)$, si vede che anche il secondo isomorfismo della (92) è un isomorfismo di R-R'-bimoduli. Analogamente, usando la condizione di naturalità $\zeta_{GFR}GF\lambda(r) = \lambda(r)\zeta_{GFR}$, si vede che anche l'ultimo isomorfismo della (92) lo è. Si ottiene così un isomorfismo di R-R'-bimoduli fra ${}_RP'_{R'}$ e ${}_RP^*_{R'}$. Applicandolo al contesto di Morita $(R,R',P,P^*,-,-)$ determinato da P, si ha un contesto (R,R',P,P',τ,μ) nel quale τ e μ sono suriettive. Valgono pertanto Morita I e il risultato stabilito all'inizio del paragrafo.

(2) Se M è un R-modulo destro, si hanno gli isomorfismi

$$\begin{aligned} FM &\cong \hom(R'_{R'}, FM) \cong \hom(GR'_{R'}, GFM) \\ &\cong \hom(P, M) \cong M \otimes_R P'. \end{aligned}$$

Il secondo è dato da G, il terzo dall'isomorfismo naturale di GF col funtore identico di **mod**-R, l'ultimo dal risultato precedente. Tutti sono naturali in M. Dunque F è naturalmente isomorfo a $- \otimes_R P'$; analogamente G è naturalmente isomorfo a $- \otimes_{R'} P$. □

L'esistenza di un contesto di Morita (R,R',P,P',τ,μ) con τ e μ suriettive implica sia l'equivalenza di **mod**-R e **mod**-R', sia quella di R-**mod** e R'-**mod** (Morita I, (5)). Da questo fatto e da Morita II segue che le categorie dei moduli destri **mod**-R e **mod**-R' sono equivalenti se e

soltanto se lo sono le categorie R-**mod** e R'-**mod**. In questo caso diciamo che R e R' sono *simili (nel senso di Morita)*. Morita II e la caratterizzazione dei generatori data nel teorema 3.21 (p. 173) permettono di identificare con precisione gli anelli R' simili a un anello assegnato R. Si ha infatti il teorema seguente. **Teorema 3.23.** *Dato un anello R, sia e un idempotente di un anello di matrici $M_n(R)$, $n \geq 1$, tale che l'ideale $M_n(R)eM_n(R)$ generato da e sia tutto $M_n(R)$. Allora $R' = eM_n(R)e$ è simile a R. Inoltre ogni anello simile a R è isomorfo a un anello di questa forma.*

Ci occorrerà il seguente lemma, che raccoglie parecchie informazioni utili.

Lemma. *(1) Se e è un idempotente di R e N è un R-modulo destro, allora* $\hom_R(eR, N)$ *è l'insieme delle applicazioni $ea \mapsto uea$, $u \in N$. L'applicazione $f \mapsto f(e)$ è un isomorfismo di gruppi da* $\hom_R(eR, N)$ *su Ne e, nel caso $N = eR$, è un isomorfismo di anelli da* $\mathrm{End}_R(eR) = \hom_R(eR, eR)$ *su eRe. (2) L'ideale traccia $T(eR)$ è ReR. (3) Un R-modulo destro M è un progeneratore ciclico se e soltanto se $M \cong eR$ per un idempotente e di R tale che $ReR = R$. (4) Se $M = M_1 \oplus M_2$ è una somma diretta di moduli destri e gli e_i sono le proiezioni determinate da questa decomposizione, allora* $\mathrm{End}_R M_i \cong e_i(\mathrm{End}_R M)e_i$.

Dimostrazione. (1) Poiché e genera eR, un omomorfismo f da eR in N è determinato dall'immagine $f(e) \in N$. Ora $f(e) = f(e^2) = f(e)e$, dunque $f(e) = ue \in Ne$ e $f(ea) = uea$. Viceversa, per qualunque $u \in N$, l'applicazione $ea \mapsto uea$ è un omomorfismo di moduli da eR in N. Si verifica direttamente che $f \mapsto f(e) = ue$ è un isomorfismo di gruppi da $\hom_R(eR, N)$ su Ne e che, quando $N = eR$, è un isomorfismo di anelli (eRe è un sottoanello di R con unità e).

(2) La descrizione di $\hom_R(eR, N)$ nel caso $N = R$ mostra che $(eR)^* = \hom_R(eR, R)$ è l'insieme delle applicazioni $ea \mapsto bea$, con $a, b \in R$. Quindi $T(eR)$ è l'insieme delle somme $\sum b_i e a_i$, con $a_i, b_i \in R$. Dunque $T(eR) = ReR$.

(3) È chiaro che M è un R-modulo destro ciclico e proiettivo se e soltanto se è isomorfo a un addendo diretto di R, ossia se e soltanto se $M \cong eR$ con $e^2 = e \in R$. Per il teorema 3.21, eR è un generatore se e soltanto se $T(eR) = R$, il che, per (2), equivale a $ReR = R$. Combinando questi risultati, vediamo che M è un progeneratore ciclico se e soltanto se $M \cong eR$ con e idempotente di R e $ReR = R$.

(4) Sia $M = M_1 \oplus M_2$ e siano e_i, $i = 1, 2$, le proiezioni determinate da questa decomposizione. Allora $e_i \in \mathrm{End}_R M$, $e_1 + e_2 = 1$, $e_i^2 = e_i$ ed $e_1 e_2 = 0 = e_2 e_1$. L'anello $e_1(\mathrm{End}_R M)e_1$ ha unità e_1. Se $\eta \in \mathrm{End}_R M$, allora $e_1 \eta e_1$ manda M_1 in sé, dunque $(e_1 \eta e_1)|_{M_1} \in \mathrm{End}_R M_1$. Poiché $(e_1 \eta e_1)M_2 = 0$, l'omomorfismo di anelli $e_1 \eta e_1 \mapsto (e_1 \eta e_1)|_{M_1}$ è iniettivo. È anche suriettivo: se $\zeta \in \mathrm{End}_R M_1$, allora $e_1 \zeta e_1 \in \mathrm{End}_R M$ e $(e_1 \zeta e_1)|_{M_1} = \zeta$. Dunque la restrizione a M_1 è un isomorfismo di $e_1(\mathrm{End}_R M)e_1$ su $\mathrm{End}_R M_1$. Analogamente si ottiene un isomorfismo di $e_2(\mathrm{End}_R M)e_2$ su $\mathrm{End}_R M_2$. □

Possiamo ora dare la *dimostrazione del teorema 3.23.* Nella proposizione 1.4 (p. 29) abbiamo dimostrato direttamente l'equivalenza fra **mod**-R e **mod**-$M_n(R)$. Un modo migliore di ottenerla è applicare il teorema Morita I all'esempio del modulo sinistro $M' = {}^{(n)}R$ delle righe di n elementi di R e del modulo destro $R^{(n)}$ delle colonne di n elementi di R, come nell'esempio di p. 166. Si vede subito che gli accoppiamenti μ e τ sono suriettivi, perciò si può applicare Morita I. La parte (5) del teorema fornisce un'equivalenza fra le categorie dei moduli di R e di $M_n(R)$. Dunque R e $M_n(R)$ sono simili. Se e è un idempotente di $M_n(R)$ tale che $M_n(R)eM_n(R) = M_n(R)$, per la parte (3) del lemma $eM_n(R)$ è un progeneratore di **mod**-$M_n(R)$. Per il teorema 3.20, $M_n(R)$ e $\mathrm{End}_{M_n(R)}(eM_n(R))$ sono quindi simili. Per la parte (1) del lemma, il secondo anello è isomorfo a $eM_n(R)e$. Dunque $M_n(R)$ ed $eM_n(R)e$ sono simili e, perciò, lo sono anche R ed $eM_n(R)e$ se $M_n(R)eM_n(R) = M_n(R)$.

Viceversa, sia R' un qualunque anello simile a R. Per Morita II, $R' \cong \mathrm{End}_R P$ con P pro-

generatore di **mod**-R. Allora P è un addendo diretto di $R^{(n)}$ per un opportuno n e $T(P) = R$. Dunque $P = eR^{(n)}$ con $e^2 = e \in \mathrm{End}_R\, R^{(n)}$. Per la parte (4) del lemma,

$$\mathrm{End}_R\, P \cong e(\mathrm{End}_R\, R^{(n)})e.$$

D'altra parte, applicando Morita I all'esempio $(R, M_n(R), R^{(n)}, {}^{(n)}R, \tau, \mu)$, vediamo che gli endomorfismi di $R^{(n)}$ sono le moltiplicazioni a sinistra degli elementi di $R^{(n)}$ per matrici $n \times n$ a coefficienti in R e che $\mathrm{End}_R\, R^{(n)} \cong M_n(R)$. Identificando e con la matrice corrispondente otteniamo $R' \cong eM_n(R)e$. Poiché P è un generatore, $T(P) = R$. Essendo P un addendo diretto di $R^{(n)}$, gli elementi di $P^* = \hom_R(P, R)$ sono le restrizioni a P degli elementi di $\hom_R(R^{(n)}, R)$. Questi ultimi sono le moltiplicazioni a sinistra per righe $(a_1, a_2, \ldots, a_n)$, $a_i \in R$. Ora $P = eR^{(n)}$, sicché $T(P)$ è l'insieme delle somme di elementi della forma

$$(a_1, \ldots, a_n)e \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \qquad a_i, b_i \in R.$$

In particolare, 1 si può esprimere come una tale somma. Ne segue che $M_n(R)eM_n(R)$ contiene la matrice e_{11} che ha 1 al posto $(1,1)$ e zero altrove. Poiché $M_n(R)e_{11}M_n(R) = M_n(R)$, si ha $M_n(R)eM_n(R) = M_n(R)$. Risulta così $R' \cong eM_n(R)e$ con $e^2 = e$ e $M_n(R)eM_n(R) = M_n(R)$. □

Stabilita la forma degli anelli simili a un anello assegnato, studiamo più da vicino le equivalenze fra mod-R e mod-R' (e fra R-mod e R'-mod). Per Morita II esse si ottengono, a meno di isomorfismo naturale, tensorizzando con un R'-R-bimodulo P di un contesto di Morita $(R, R', P, P', \tau, \mu)$ nel quale τ e μ sono suriettivi, e quindi isomorfismi. Dunque μ è un isomorfismo di R'-R'-bimoduli da $P \otimes_R P'$ su R', e τ è un isomorfismo di R-R-bimoduli da $P' \otimes_{R'} P$ su R. Viceversa, siano R, R' due anelli e supponiamo di avere tali isomorfismi per un R'-R-bimodulo P e un R-R'-bimodulo P'. Allora, come nella dimostrazione di Morita I (5), i funtori $- \otimes_R P'$ e $- \otimes_{R'} P$ danno un'equivalenza fra mod-R e mod-R', e i funtori $P \otimes_R -$ e $P' \otimes_{R'} -$ un'equivalenza fra R'-mod e R-mod. Quindi R e R' sono simili. Inoltre, poiché un'equivalenza fra categorie di moduli manda progeneratori in progeneratori e $R \otimes_R P' \cong P'$, è chiaro che P' è un progeneratore di mod-R'. Analogamente è un progeneratore di R-mod, mentre P è un progeneratore di mod-R e di R'-mod.

Chiameremo *invertibile* un R'-R-bimodulo P se esiste un R-R'-bimodulo P' tale che $P' \otimes_{R'} P \cong R$ come R-R-bimoduli e $P \otimes_R P' \cong R'$ come R'-R'-bimoduli. Si possono moltiplicare tensorialmente moduli di questo tipo. Più precisamente, se R'' è un terzo anello e Q è un R''-R'-bimodulo invertibile (sicché R'' e R' sono simili), dall'associatività del prodotto tensoriale segue che $Q \otimes_{R'} P$ è invertibile. Possiamo ora mettere in relazione questo fatto con le classi di isomorfismo dei funtori che danno equivalenze fra le categorie dei moduli di due anelli. È quanto afferma il teorema seguente.

Morita III. *Siano $R, R', R'', \ldots$ anelli simili. L'applicazione $P \mapsto - \otimes_{R'} P$ dà una biiezione fra la classe delle classi di isomorfismo di R'-R-bimoduli invertibili e la classe delle classi di isomorfismo naturale dei funtori che danno equivalenze da* mod-R' *a* mod-R. *In tale corrispondenza, alla composizione di equivalenze corrisponde il prodotto tensoriale di bimoduli invertibili.*

Dimostrazione. La prima affermazione significa quanto segue. Se P è un R'-R-bimodulo invertibile, allora $- \otimes_{R'} P$ dà un'equivalenza fra mod-R' e mod-R, e ogni tale equivalenza è naturalmente isomorfa a una di questa forma. Inoltre, per due R'-R-bimoduli invertibili P_1, P_2, i funtori $- \otimes_{R'} P_1$ e $- \otimes_{R'} P_2$ sono naturalmente isomorfi se e soltanto se P_1 e P_2 sono isomorfi come bimoduli. Il primo fatto è stato dimostrato nei primi due teoremi di Morita. Supponiamo ora che P_1, P_2 siano R'-R-bimoduli invertibili isomorfi. Allora per ogni $N' = N'_{R'}$ i moduli $N' \otimes_{R'} P_1$ e $N' \otimes_{R'} P_2$ sono isomorfi mediante un isomorfismo naturale in N'. Dunque $- \otimes_{R'} P_1$

e $- \otimes_{R'} P_2$ sono naturalmente isomorfi. Viceversa, supponiamo che i due funtori siano naturalmente isomorfi. Esiste allora un R-isomorfismo η da $R' \otimes_{R'} P_1$ su $R' \otimes_{R'} P_2$ tale che per ogni $a' \in R'$ sia commutativo il diagramma

$$\begin{array}{ccc} R' \otimes_{R'} P_1 & \xrightarrow{l(a') \otimes 1_{P_1}} & R' \otimes_{R'} P_1 \\ \eta \downarrow & & \downarrow \eta \\ R' \otimes_{R'} P_2 & \xrightarrow[l(a') \otimes 1_{P_2}]{} & R' \otimes_{R'} P_2 \end{array}$$

Ciò significa che $R' \otimes_{R'} P_1$ e $R' \otimes_{R'} P_2$ sono isomorfi come R'-R-bimoduli. Anche P_1 e P_2 sono quindi isomorfi come R'-R-bimoduli. Sia ora Q un R''-R'-bimodulo invertibile. Abbiamo il funtore $- \otimes_{R''} Q$ da mod-R'' a mod-R' e il funtore $- \otimes_{R'} P$ da mod-R' a mod-R. Il composto è il funtore $(- \otimes_{R''} Q) \otimes_{R'} P$ da mod-R'' a mod-R. Per associatività si tratta del funtore $- \otimes_{R''} (Q \otimes_{R'} P)$. È questo il significato dell'ultima affermazione. □

Nel caso particolare $R' = R$, il teorema precedente mette in relazione le classi di isomorfismo dei bimoduli invertibili su R e le classi di isomorfismo naturale delle autoequivalenze di mod-R. È facile vedere che la prima di queste due collezioni è un insieme (lo si dimostri). Essa costituisce dunque un gruppo in cui la moltiplicazione è definita dal prodotto tensoriale. Il teorema dà un isomorfismo di questo gruppo con il gruppo delle classi di isomorfismo naturale delle autoequivalenze di mod-R. Il primo gruppo si indica con $\operatorname{Pic} R$. Di particolare interesse è il caso in cui R è commutativo. Studieremo questo gruppo più avanti (§§ 7.8 e 10.6).

Esercizi

1. Sia e un idempotente in un anello R tale che $ReR = R$. Mostrare che $B \mapsto eBe = B \cap eRe$ è un isomorfismo dal reticolo degli ideali di R su quello degli ideali di eRe. Vale lo stesso senza l'ipotesi $ReR = R$?

2. Definire una relazione $\sim$ fra anelli ponendo $R \sim R'$ se $R' \cong eM_n(R)e$ per qualche n e un idempotente e tale che $M_n(R)eM_n(R) = M_n(R)$. Per il teorema 3.23 è una relazione di equivalenza. Si può dimostrarlo direttamente, senza usare la teoria di Morita?

3. Mostrare che, se R è un dominio a ideali principali, ogni anello simile a R è isomorfo a un anello di matrici $M_n(R)$.

Riferimenti bibliografici

K. Morita, *Duality for modules and its application to the theory of rings with minimum condition*, Science Reports of the Tokyo Kyoiku Daigaku, vol. 6, sez. A (1958), pp. 83–142.

H. Bass, *The Morita Theorems*, appunti delle lezioni, University of Oregon, 1962, 21 pagine.

C. Faith, *Algebra: Rings, Modules and Categories I*, New York, Springer, 1973.

4 Fondamenti della teoria della struttura degli anelli

La teoria della struttura degli anelli, di cui ci occuperemo in questo capitolo, nasce dalla teoria della struttura delle algebre di dimensione finita su un campo, sviluppata nell'ultima parte dell'Ottocento e nei primi anni di questo secolo. La scoperta dei quaternioni da parte di Hamilton nel 1843 portò alla costruzione di altri «sistemi di numeri ipercomplessi», ossia di algebre di dimensione finita su $\mathbb{R}$ e su $\mathbb{C}$, alcune delle quali non associative (ad esempio gli ottonioni di Cayley e Graves). Nella seconda metà dell'Ottocento numerosi matematici, fra cui Molien, Frobenius e Cartan, studiarono intensamente il problema di classificare questi sistemi. I loro risultati costituirono una teoria assai soddisfacente per le algebre su $\mathbb{R}$ e su $\mathbb{C}$, che comprendeva la classificazione completa di un'importante sottoclasse, le algebre semisemplici. Nel 1908 Wedderburn estese questa teoria alle algebre di dimensione finita su un campo arbitrario. Nel 1927 Artin, stimolato dalla notevole semplificazione che Emmy Noether aveva ottenuto nella teoria degli ideali degli anelli commutativi introducendo le condizioni sulle catene, e mosso dalle esigenze dell'aritmetica nelle algebre di dimensione finita, estese la teoria di Wedderburn agli anelli che soddisfano condizioni sulle catene di ideali unilateri. Nel 1945 l'autore sviluppò una teoria della struttura degli anelli priva di ipotesi di finitezza. I suoi ingredienti principali erano una nuova definizione di radicale, le nozioni di primitività e di semiprimitività (allora chiamata semisemplicità) e un teorema di densità, ottenuto indipendentemente da Chevalley, che generalizzava ampiamente un teorema classico di Burnside.

In questo capitolo invertiremo l'ordine storico: esporremo dapprima la teoria generale e passeremo poi, per successive specializzazioni, alla teoria di Artin e a quella di Wedderburn delle algebre di dimensione finita su campi. Il teorema di struttura di Wedderburn per le algebre semplici ne riconduce la classificazione a quella delle algebre di divisione. Lo strumento adatto a studiarle è il gruppo di Brauer delle classi di algebre, in cui la composizione è definita mediante il prodotto tensoriale. Daremo un'introduzione allo studio di questi gruppi e ad alcuni risultati connessi sulle algebre semplici centrali. Alla fine del capitolo applicheremo i risultati allo studio delle algebre di Clifford, necessarie per completare la teoria della struttura dei gruppi ortogonali presentata nel capitolo 6 di BAI. Nel prossimo capitolo daremo ulteriori applicazioni alla teoria delle rappresentazioni dei gruppi finiti.

4.1 Primitività e semiprimitività

Nello sviluppo che daremo alla teoria degli anelli hanno un ruolo predominante gli anelli di endomorfismi di gruppi abeliani e le realizzazioni concrete degli anelli come anelli di endomorfismi. Ricordiamo che, se M è un gruppo abeliano (scritto additivamente), l'insieme dei suoi endomorfismi ha una struttura naturale di anello. Si ottiene così $\operatorname{End} M$ (o $\operatorname{End}_{\mathbb{Z}} M$), l'anello degli endomorfismi di M. Per *anello di endomorfismi* intendiamo un sottoanello di $\operatorname{End} M$ per qualche gruppo abeliano M.

Definiamo *rappresentazione* ρ di un anello R un omomorfismo di R nell'anello $\operatorname{End} M$ degli endomorfismi di un gruppo abeliano additivo M. Una rappresentazione ρ di R che agisca su M (cioè che abbia codominio $\operatorname{End} M$) definisce su M una struttura di R-modulo sinistro, facendo agire R su M tramite ρ:

$$ax = \rho(a)x \qquad (a \in R,\ x \in M). \tag{1}$$

La (1) definisce un'azione di modulo sinistro perché $\rho(a)$ è un endomorfismo e $a \mapsto \rho(a)$ è un omomorfismo di anelli. Viceversa, se M è un modulo sinistro sull'anello R, allora M è un gruppo abeliano e dà luogo a una rappresentazione $\rho = \rho_M$ di R: per $a \in R$ si definisce a_M come

l'endomorfismo $a_M\colon x \mapsto ax$. Allora $\rho\colon a \mapsto a_M$ è un omomorfismo di R in $\operatorname{End} M$ e dunque una rappresentazione di R.

Per *rappresentazione irriducibile* di un anello intenderemo una rappresentazione ρ il cui modulo associato M, ora definito, sia irriducibile: $M \neq 0$ e i suoi soli sottomoduli sono M e 0. La teoria della struttura che svilupperemo poggia su due articoli di fede: le rappresentazioni irriducibili sono il tipo migliore di rappresentazioni, e gli anelli meglio comportati sono quelli che hanno abbastanza rappresentazioni irriducibili da distinguerne gli elementi. Ciò significa che, dati due elementi distinti a, b di R, esiste una rappresentazione irriducibile ρ tale che $\rho(a) \neq \rho(b)$. Equivalentemente, per ogni $a \neq 0$ in R deve esistere una rappresentazione irriducibile ρ di R tale che $\rho(a) \neq 0$.

Prima di passare alle definizioni principali, raccogliamo alcuni fatti elementari sulle rappresentazioni e sui moduli. Per il legame indicato tra le rappresentazioni e i moduli sinistri, in questo capitolo daremo la preferenza a questi ultimi. Il termine «modulo», senza ulteriori qualificazioni, indicherà dunque sempre un modulo sinistro.

Se ρ è una rappresentazione dell'anello R su M, il suo nucleo è evidentemente l'ideale

$$\operatorname{ann}_R M = \{b \in R \mid bM = 0\}, \tag{2}$$

dove $bx = \rho(b)x$. Diremo *fedele* la rappresentazione ρ (e talvolta il modulo M) quando $\ker \rho = 0$. A ogni $x \in M$ è associato l'ideale d'ordine o annullatore di x, $\operatorname{ann}_R x = \{b \in R \mid bx = 0\}$. Questo è un ideale sinistro e il sottomodulo ciclico Rx generato da x è isomorfo a $R/\operatorname{ann}_R x$, dove R è considerato nel modo naturale come R-modulo sinistro. Evidentemente

$$\ker \rho = \operatorname{ann}_R M = \bigcap_{x \in M} \operatorname{ann}_R x. \tag{3}$$

Se f è un omomorfismo di un anello S in R e ρ è una rappresentazione di R su M, allora ρf è una rappresentazione di S su M. L'azione di S su M che ne risulta è data da

$$bx = f(b)x \qquad (b \in S). \tag{4}$$

Come nel capitolo precedente, le notazioni ${}_SM$ e ${}_RM$ distinguono M come S-modulo da M come R-modulo e indicano che l'azione è a sinistra. Il più delle volte il contesto basterà a chiarire il significato e scriveremo semplicemente M. È chiaro che

$$\operatorname{ann}_S M = f^{-1}(\operatorname{ann}_R M), \tag{5}$$

dove $f^{-1}(\ )$ indica naturalmente l'immagine inversa mediante f. Se la rappresentazione ρ di R è fedele, $\operatorname{ann}_S M = f^{-1}(0) = \ker f$.

Sia B un ideale di R contenuto in $\operatorname{ann}_R M$. Facciamo di M un modulo su $\bar{R} = R/B$ definendo l'azione della classe $a + B$ su $x \in M$ con la formula

$$(a + B)x = ax. \tag{6}$$

Poiché $bx = 0$ per ogni $b \in B$, $x \in M$, è chiaro che questa azione è ben definita. È immediato che essa dà una struttura di $\bar{R}$-modulo su M e che un sottoinsieme N di M è un R-sottomodulo se e solo se è un $\bar{R}$-sottomodulo. In altri termini, ${}_RM$ e ${}_{\bar{R}}M$ hanno lo stesso reticolo dei sottomoduli. La relazione tra i nuclei delle rappresentazioni di R e di $\bar{R}$ è

$$\operatorname{ann}_{\bar{R}} M = (\operatorname{ann}_R M)/B. \tag{7}$$

Introduciamo ora due delle nostre definizioni principali.

Definizione 4.1. *Un anello R si dice primitivo se possiede una rappresentazione irriducibile fedele. Si dice semiprimitivo se, per ogni $a \neq 0$ in R, esiste una rappresentazione irriducibile ρ tale che $\rho(a) \neq 0$.*

Ci interesseranno anche le rappresentazioni completamente riducibili, nel senso che il modulo corrispondente M è completamente riducibile: $M = \sum M_\alpha$, con le M_α sottomoduli irriducibili. Diamo anzitutto due caratterizzazioni della semiprimitività.

Proposizione 4.1. *Per un anello R sono equivalenti le condizioni seguenti: (1) R è semiprimitivo; (2) R ha una rappresentazione completamente riducibile fedele; (3) R è un prodotto sottodiretto di anelli primitivi (si veda p. 69).*

Dimostrazione. (1) $\Rightarrow$ (2). Per ogni $a \neq 0$ di R sia M_a un modulo irriducibile tale che $\rho_{M_a}(a) \neq 0$. Formiamo $M = \bigoplus_{a\neq 0} M_a$. Questo modulo è completamente riducibile ed è chiaro che

$$\operatorname{ann}_R M = \bigcap_{a\neq 0} \operatorname{ann}_R M_a = 0. \tag{8}$$

Dunque ρ_M è una rappresentazione completamente riducibile fedele di R.

(2) $\Rightarrow$ (3). Sia ρ una rappresentazione completamente riducibile fedele di R. Per il suo modulo M si ha $M = \sum M_\alpha$, con le M_α irriducibili. Vale $0 = \operatorname{ann}_R M = \bigcap_\alpha \operatorname{ann}_R M_\alpha$, e $\operatorname{ann}_R M_\alpha$ è un ideale di R. Dunque R è un prodotto sottodiretto degli anelli $R_\alpha = R/\operatorname{ann}_R M_\alpha$. D'altra parte, poiché $(\operatorname{ann}_R M_\alpha)M_\alpha = 0$, possiamo considerare M_α come un modulo irriducibile su R_α; la rappresentazione di R_α definita da M_α è fedele. Quindi R_α è primitivo e R è un prodotto sottodiretto di anelli primitivi.

(3) $\Rightarrow$ (1). Sia R un prodotto sottodiretto degli anelli primitivi R_α. Per ogni R_α sia ρ_α una sua rappresentazione irriducibile fedele. Abbiamo gli omomorfismi canonici π_α di R su R_α e $\bigcap_\alpha \ker \pi_\alpha = 0$. La rappresentazione irriducibile $\rho_\alpha\pi_\alpha$ di R ha nucleo $\ker \pi_\alpha$. Abbiamo dunque una famiglia di rappresentazioni irriducibili $\{\rho_\alpha\pi_\alpha\}$ di R con $\bigcap_\alpha \ker(\rho_\alpha\pi_\alpha) = 0$. Pertanto R è semiprimitivo. □

Le definizioni date finora fanno intervenire oggetti (rappresentazioni e moduli) esterni all'anello R. È facile e utile sostituirle con caratterizzazioni interne. Sia I un ideale sinistro di R. Definiamo

$$(I : R) = \{b \in R \mid bR \subseteq I\}. \tag{9}$$

Ponendo $M = R/I$ e considerandolo come R-modulo sinistro è chiaro che

$$(I : R) = \operatorname{ann}_R(R/I). \tag{10}$$

Ne segue, oppure lo si ricava direttamente dalla (9), che $(I : R)$ è un ideale. Per la (9), $(I : R) \subseteq I$ e $(I : R)$ contiene ogni ideale di R contenuto in I. In altri termini, $(I : R)$ è l'unico massimo ideale di R contenuto in I. Possiamo ora dare la seguente caratterizzazione della primitività e della semiprimitività.

Proposizione 4.2. *Un anello R è primitivo se e solo se contiene un ideale sinistro massimale I che non contiene alcun ideale non nullo di R. Un anello R è semiprimitivo se e solo se $R \neq 0$ e $\bigcap_I (I : R) = 0$, dove l'intersezione è estesa a tutti gli ideali sinistri massimali I di R.*

Dimostrazione. Se R è primitivo, esiste un modulo irriducibile M con $\operatorname{ann}_R M = 0$. Ora $M \cong R/I$ per un ideale sinistro massimale I (p. 117). Dunque $(I : R) = \operatorname{ann}_R(R/I) = \operatorname{ann}_R M = 0$. Quindi I è un ideale sinistro massimale che non contiene alcun ideale non nullo di R. Viceversa, se vale la condizione, esiste un ideale sinistro massimale I con $(I : R) = 0$. Allora $M = R/I$ fornisce una rappresentazione irriducibile fedele di R, onde R è primitivo.

Sia ora R semiprimitivo e sia $\{\rho_\alpha\}$ un insieme di rappresentazioni irriducibili sufficiente a distinguere gli elementi di R. Allora $\bigcap \ker \rho_\alpha = 0$. Se M_α è il modulo di ρ_α, si ha $M_\alpha \cong R/I_\alpha$, con I_α ideale sinistro massimale di R. Quindi $(I_\alpha : R) = \operatorname{ann}_R M_\alpha = \ker \rho_\alpha$ e $\bigcap_\alpha (I_\alpha : R) = 0$. A maggior ragione è zero l'intersezione $\bigcap (I : R)$ estesa a tutti gli ideali sinistri massimali di R. Il viceversa si ottiene ripercorrendo i passaggi in senso inverso. □

Registriamo alcune importanti conseguenze di queste caratterizzazioni interne.

Corollario 1. *Ogni anello semplice non nullo è primitivo.*

Dimostrazione. Ogni anello $R \neq 0$ contiene un ideale sinistro massimale I (p. 68). Se R è semplice, $(I : R) = 0$. Dunque R è primitivo. □

Otteniamo ora una caratterizzazione per gli anelli commutativi.

Corollario 2. *Un anello commutativo R è primitivo se e solo se è un campo, ed è semiprimitivo se e solo se è un prodotto sottodiretto di campi.*

Dimostrazione. Se R è commutativo e primitivo, contiene un ideale sinistro massimale I che non contiene alcun ideale non nullo di R. Essendo R commutativo, I è un ideale; dunque $I = 0$. Pertanto 0 è un ideale massimale, ossia $R \neq 0$ e gli unici ideali dell'anello commutativo R sono 0 e R. Quindi R è un campo. Viceversa, ogni campo soddisfa evidentemente la prima condizione della proposizione 4.2 ed è quindi primitivo. Dal punto (3) della proposizione 4.1 segue che R è semiprimitivo se e solo se è un prodotto sottodiretto di campi. □

Diamo ora esempi di anelli primitivi e semiprimitivi. Un modo comodo di costruire esempi di anelli è realizzarli come anelli di endomorfismi di gruppi abeliani. Se R è un anello di endomorfismi di un gruppo abeliano M, questo è un R-modulo in modo naturale: ax, per $a \in R$, $x \in M$, è l'immagine di x mediante a. La rappresentazione corrispondente è evidentemente l'inclusione di R in $\operatorname{End} M$ ed è quindi fedele. Se R agisce irriducibilmente su $M \neq 0$, nel senso che 0 e M sono gli unici sottogruppi di M stabili sotto R, allora R è un anello primitivo. A questo tipo appartengono parecchi degli esempi che seguono.

Esempi

1. L'anello L delle trasformazioni lineari di uno spazio vettoriale di dimensione finita su un corpo è semplice (p. 171). Dunque L è primitivo.

2. Sia V uno spazio vettoriale su un corpo Δ, non necessariamente di dimensione finita. Affermiamo che l'anello L delle trasformazioni Δ-lineari di V agisce irriducibilmente su V, e quindi è primitivo. Per dimostrare l'irriducibilità dobbiamo mostrare che, dati un vettore non nullo x e un vettore qualunque y, esiste $l \in L$ tale che $lx = y$. Ciò è chiaro, perché possiamo includere x in una base (e_α) di V su Δ e, per ogni base (e_α) e ogni scelta di un elemento f_α per ciascun e_α, esiste una trasformazione lineare l tale che $le_\alpha = f_\alpha$. Se V ha dimensione infinita, il sottoinsieme F delle trasformazioni l a immagine $l(V)$ di dimensione finita è un ideale non nullo di L. Poiché $1 \notin F$, $F \neq L$. Quindi L non è semplice e fornisce un esempio di anello primitivo non semplice. Se la dimensione di V è l'infinito numerabile, si vede facilmente che F è l'unico ideale proprio non nullo di L. Dunque L/F è semplice e pertanto primitivo.

3. Se $(x_1, x_2, x_3, \ldots)$ è una base di uno spazio vettoriale V sul corpo Δ, una trasformazione lineare l è determinata dalla sua azione sulla base. Possiamo scrivere

$$lx_i = \sum_j \lambda_{ij} x_j, \tag{11}$$

dove $\lambda_{ij} \in \Delta$ e, per ogni i fissato, soltanto un numero finito di coefficienti λ_{ij} è diverso da zero. Si può dunque descrivere l mediante una matrice $\Lambda = (\lambda_{ij})$ *finita per righe*, nel senso che ciascuna riga ha soltanto un numero finito di elementi non nulli. Le matrici finite per righe a coefficienti in Δ formano un anello rispetto alle usuali addizione e moltiplicazione, e l'applicazione $l \mapsto \Lambda$ che associa a l la sua matrice rispetto alla base (x_i) è un anti-isomorfismo. Sia ora R l'insieme delle trasformazioni lineari la cui matrice rispetto alla base data ha la forma

$$\begin{pmatrix} \Phi & & & 0 \\ & \lambda & & \\ & & \lambda & \\ 0 & & & \ddots \end{pmatrix}, \tag{12}$$

dove Φ è un blocco quadrato finito e $\lambda \in \Delta$. Le matrici della forma (12) costituiscono un sottoanello dell'anello delle matrici finite per righe. Quindi R è un sottoanello dell'anello L delle trasformazioni lineari. Mostriamo che R agisce irriducibilmente su V. Se x è un vettore non nullo e y un vettore qualunque, possiamo scrivere $x = \xi_1 x_1 + \cdots + \xi_n x_n$, $y = \eta_1 x_1 + \cdots + \eta_n x_n$ per qualche n, con $\xi_i, \eta_i \in \Delta$. I due vettori appartengono quindi a un sottospazio V' di dimensione finita. Esiste una trasformazione lineare l' di V' in sé tale che $l'x = y$; possiamo estenderla a una trasformazione lineare l di V appartenente a R, ad esempio imponendo $lx_i = 0$ per $i > n$. Allora $lx = y$. Pertanto V è irriducibile come R-modulo e R è primitivo.

4. Sia V come nell'esempio 3, con $\Delta = F$ un campo, e siano p, q le trasformazioni F-lineari di V definite da

$$\begin{aligned} &px_1 = 0, \qquad px_i = x_{i-1} \quad (i > 1), \\ &qx_i = x_{i+1} \qquad\qquad\quad (i = 1, 2, 3, \ldots). \end{aligned} \tag{13}$$

Si ha $pqx_i = x_i$ per ogni i, mentre $qpx_1 = 0$ e $qpx_i = x_i$ per $i > 1$. Dunque

$$pq = 1, \qquad qp \neq 1. \tag{14}$$

Sia R l'insieme delle trasformazioni lineari

$$\sum_{i,j=0}^{n} \alpha_{ij} q^i p^j, \qquad n = 0, 1, 2, \ldots, \quad \alpha_{ij} \in F. \tag{15}$$

La prima relazione della (14) implica che R è chiuso rispetto alla moltiplicazione, e dunque è un anello di endomorfismi di V. Poniamo ora

$$e_{ij} = q^{i-1} p^{j-1} - q^i p^j, \qquad i, j = 1, 2, \ldots. \tag{16}$$

La matrice di e_{ij} ha un 1 nella posizione (j, i) e zeri altrove. L'anello di matrici corrispondente a R contiene quindi tutte le matrici (12). Pertanto R contiene come sottoanello quello dell'esempio 3. Di conseguenza anche questo R agisce irriducibilmente su V ed è primitivo.

5. Per ogni anello R abbiamo la rappresentazione regolare ρ_R, il cui modulo è il gruppo additivo di R sul quale l'anello agisce per moltiplicazione a sinistra (si veda BAI, pp. 422–426). Questa rappresentazione è fedele e i sottomoduli di R sono gli ideali sinistri. Sia ora A un'algebra sul campo F. La sua rappresentazione regolare ρ_A fornisce un monomorfismo di A nell'algebra L delle trasformazioni lineari dello spazio vettoriale A/F. Ogni algebra su un

campo si può dunque immergere in un anello primitivo. Mostriamo che A è anche immagine omomorfa di un anello primitivo. Poiché A è un'algebra arbitraria su un campo, si vedrà che non si può dire molto delle immagini omomorfe degli anelli primitivi. Prendiamo $V = \bigoplus A$, somma diretta di un'infinità numerabile di copie dello spazio vettoriale A. Facciamo agire A su V nel modo evidente e identifichiamo A con la corrispondente algebra di trasformazioni lineari di V. Per $n = 1, 2, 3, \ldots$ sia V_n il sottospazio di V degli elementi della forma $(x_1, x_2, \ldots, x_n, 0, 0, \ldots)$, con $x_i \in A$, e sia L_n l'insieme delle trasformazioni lineari che mandano V_n in sé e annullano tutti gli elementi $(0, \ldots, 0, x_{n+1}, x_{n+2}, \ldots)$. Allora $L_1 \subseteq L_2 \subseteq \cdots$. Poniamo $L = \bigcup L_i$ e sia R l'anello di trasformazioni lineari generato da A e L. Allora R agisce irriducibilmente su V e quindi è primitivo. Inoltre $R = A + L$, $A \cap L = 0$ e L è un ideale di R. Pertanto $R/L \cong A$ e l'algebra data A è immagine omomorfa dell'algebra primitiva R.

6. L'anello $\mathbb{Z}$ è semiprimitivo: infatti $\bigcap_{p \text{ primo}}(p) = 0$ e $\mathbb{Z}/(p)$ è un campo. Quindi $\mathbb{Z}$ è un prodotto sottodiretto di campi ed è semiprimitivo. Lo stesso vale per ogni dominio a ideali principali con infiniti primi.

Esercizi

1. Sia $F\{x, y\}$ l'algebra libera generata da x, y e sia K il suo ideale generato da $xy - 1$. Mostrare che $F\{x, y\}/K$ è isomorfa all'algebra R dell'esempio 4.

2. (Samuel.) Siano V, F come nell'esempio 4 e sia S l'algebra delle trasformazioni lineari generata dal p di tale esempio e dalla trasformazione lineare r tale che $rx_i = x_{i^2+1}$. Mostrare che S è primitiva ed è isomorfa all'algebra libera $F\{x, y\}$.

3. Sia $F\{x, y\}$ come nell'esercizio 1 e sia K l'ideale generato da $xy - yx - x$. Supposto che F abbia caratteristica zero, mostrare che $R = F\{x, y\}/K$ è primitivo.

4. Sia R un anello contenente un ideale $N \neq 0$ nilpotente, nel senso che esiste un intero m tale che $N^m = 0$ (cioè il prodotto di m elementi qualunque di N è zero). Mostrare che R non è semiprimitivo.

5. Mostrare che, se R è primitivo, l'anello di matrici $M_n(R)$ è primitivo.

6. Mostrare che, se R è primitivo ed e è un idempotente non nullo di R, l'anello eRe (di unità e) è primitivo.

7. Mostrare che, se R e R' sono simili nel senso di Morita (p. 179), R è primitivo se e solo se lo è R'.

8. Siano F un campo e $P = F[t_1, \ldots, t_n]$ l'anello dei polinomi in n indeterminate a coefficienti in F. Mostrare che, per ogni $i = 1, \ldots, n$, esiste un'unica derivazione D_i di P tale che $D_i t_j = \delta_{ij}$ (si veda l'esercizio 11 a p. 147). Per $f \in P$ si indichi con $\bar{f}$ la moltiplicazione $g \mapsto fg$ in P. Mostrare che, se D è una derivazione di P e $f \in P$, allora $\bar{f}D$ è una derivazione di P. Mostrare che le derivazioni di P in P sono le applicazioni $\sum_{i=1}^{n} \bar{f}_i D_i$, con D_i come sopra e $f_i \in P$. Sia R l'anello degli endomorfismi del gruppo additivo di P generato dalle derivazioni e dalle moltiplicazioni di P. Mostrare che, se F ha caratteristica zero, R è un anello irriducibile di endomorfismi e pertanto è primitivo.

9. Sia F un campo di caratteristica zero e sia $F\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ l'algebra libera su F determinata dai $2n$ elementi $x_1, \ldots, x_n, y_1, \ldots, y_n$. Sia I l'ideale generato dagli elementi

$$[x_i, x_j], \qquad [y_i, y_j], \qquad [y_i, x_j] - \delta_{ij}1, \qquad 1 \leq i, j \leq n.$$

L'algebra $W_n = F\{x_1, \ldots, x_n, y_1, \ldots, y_n\}/I$ si chiama *algebra di Weyl*. Con P e R come nell'esercizio 8, mostrare che l'omomorfismo η di $F\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ in R tale che $x_i \mapsto \bar{t}_i$, $y_i \mapsto D_i$, $1 \leq i \leq n$, è suriettivo e ha nucleo I. Concludere che W_n è primitiva.

10. Mostrare che W_n è semplice. (*Suggerimento.* Trattare anzitutto il caso $n = 1$.)

4.2 Il radicale di un anello

Dal punto di vista adottato nel paragrafo precedente, lo scopo di definire il radicale di un anello è quello di isolare la parte dell'anello i cui elementi vengono mandati in zero da ogni rappresentazione irriducibile. Introduciamo perciò la seguente definizione.

Definizione 4.2. *Il radicale (di Jacobson) di un anello è l'intersezione dei nuclei delle rappresentazioni irriducibili dell'anello.*

Il radicale $\operatorname{rad} R$ dell'anello R è evidentemente un ideale di R.

Diremo che un ideale P di R è *primitivo* (in R) se R/P è un anello primitivo. Sia I un ideale sinistro massimale di R e poniamo $P = (I : R)$. Allora $M = R/I$ è un R-modulo irriducibile di annullatore P. Per la (6) possiamo considerare M come un modulo su $\bar{R} = R/P$, e come $\bar{R}$-modulo esso è irriducibile. Per la (7) si ha $\operatorname{ann}_{\bar{R}} M = (\operatorname{ann}_R M)/P = P/P = 0$. Dunque M è un $\bar{R}$-modulo fedele e irriducibile, sicché $\bar{R}$ è primitivo. Per definizione, P è quindi un ideale primitivo di R. Viceversa, sia P un ideale primitivo di R. Esiste allora un modulo irriducibile M su $\bar{R} = R/P$ la cui rappresentazione associata è fedele. Considerando M come R-modulo mediante la (4), vediamo che esso è irriducibile e che $\operatorname{ann}_R M = P$ (si veda la (5)). Ora $M \simeq R/I$, dove I è un ideale sinistro massimale di R, e quindi $\operatorname{ann}_R(R/I) = P$. Poiché $\operatorname{ann}_R(R/I) = (I : R)$, otteniamo $P = (I : R)$. Abbiamo così provato il lemma seguente.

Lemma 1. *Un ideale P di R è primitivo in R se e soltanto se $P = (I : R)$ per qualche ideale sinistro massimale I di R.*

Possiamo ora dare la prima caratterizzazione interna del radicale.

Proposizione 4.3. *(1)* $\operatorname{rad} R$ *è l'intersezione degli ideali primitivi di R. (2)* $\operatorname{rad} R$ *è l'intersezione degli ideali sinistri massimali di R.*

Dimostrazione. (1) Per definizione,

$$\operatorname{rad} R = \bigcap_M \operatorname{ann}_R M, \tag{17}$$

dove M percorre la classe dei moduli irriducibili su R. Poiché $M \simeq R/I$ e $\operatorname{ann}_R(R/I) = (I : R)$, si ha

$$\operatorname{rad} R = \bigcap_I (I : R), \tag{18}$$

dove I percorre gli ideali sinistri massimali di R. Per il lemma si può scrivere anche

$$\operatorname{rad} R = \bigcap_P P, \tag{18$'$}$$

dove P percorre gli ideali primitivi di R. Ciò dimostra (1). Per dimostrare (2), ricordiamo che per ogni modulo M si ha $\operatorname{ann}_R M = \bigcap_{x \in M} \operatorname{ann}_R x = \bigcap_{x \neq 0} \operatorname{ann}_R x$. Se M è irriducibile, questa espressione presenta $\operatorname{ann}_R M$ come intersezione di ideali sinistri massimali. Dunque, per la (17), $\operatorname{rad} R$ è intersezione di ideali sinistri massimali e pertanto $\operatorname{rad} R \supseteq \bigcap_I I$ se I li percorre tutti. D'altra parte, da $I \supseteq (I : R)$ segue $\bigcap_I I \supseteq \bigcap_I (I : R) = \operatorname{rad} R$. Otteniamo così

$$\operatorname{rad} R = \bigcap_I I, \tag{19}$$

con l'intersezione estesa all'insieme di tutti gli ideali sinistri massimali di R. □

Dimostriamo ora il seguente risultato.

Proposizione 4.4. *(1) R è semiprimitivo se e soltanto se* $\operatorname{rad} R = 0$. *(2) Se $R \neq 0$, allora $R/\operatorname{rad} R$ è semiprimitivo e* $\operatorname{rad} R$ *è contenuto in ogni ideale B di R tale che R/B sia semiprimitivo.*

Dimostrazione. (1) Se $\operatorname{rad} R = 0$, gli ideali primitivi P di R hanno intersezione zero. Allora R è un prodotto sottodiretto degli anelli primitivi R/P, quindi è semiprimitivo per la proposizione 4.1. Viceversa, se R è semiprimitivo, è un prodotto sottodiretto di anelli primitivi ed esiste perciò un insieme di ideali primitivi con intersezione zero. A maggior ragione $\operatorname{rad} R = \bigcap_P P = 0$ se P percorre tutti gli ideali primitivi di R.

(2) Se B è un ideale di R, ogni ideale di $\bar{R} = R/B$ ha la forma $\bar{P} = P/B$, con P ideale di R contenente B. Poiché $\bar{R}/\bar{P} \simeq R/P$, è chiaro che $\bar{P}$ è primitivo in $\bar{R}$ se e soltanto se P è primitivo in R. Ora $\bar{R}$ è semiprimitivo se e soltanto se $\bigcap_{\bar{P}} \bar{P} = 0$, dove $\bar{P}$ percorre gli ideali primitivi di $\bar{R}$. Dunque $\bar{R}$ è semiprimitivo se e soltanto se B è l'intersezione di tutti gli ideali primitivi di R che contengono B. In tal caso $B \supseteq \operatorname{rad} R$ per la (18′). Se $B = \operatorname{rad} R$, la (18′) mostra che B è un'intersezione di ideali primitivi. Allora $R/B = R/\operatorname{rad} R$ è semiprimitivo, come afferma (2). □

Daremo ora un'importante caratterizzazione del radicale in termini dei suoi elementi. Ci occorrono alcune definizioni. Un elemento z di un anello R si dice *quasiregolare a sinistra* (a destra) in R se $1 - z$ ammette in R un inverso sinistro (destro). La quasiregolarità a sinistra (a destra) equivale evidentemente a dire che l'ideale principale sinistro $R(1 - z)$ (destro $(1 - z)R$) coincide con R. Se z è quasiregolare sia a sinistra sia a destra, diremo che è *quasiregolare*. Un ideale sinistro (destro) I si dice quasiregolare se tutti i suoi elementi sono quasiregolari a sinistra (a destra).

Se z è quasiregolare a sinistra, $1 - z$ ammette un inverso sinistro che possiamo scrivere $1 - z'$. Allora $(1 - z')(1 - z) = 1$ dà la relazione

$$z' \circ z = z + z' - z'z = 0. \tag{20}$$

Il prodotto binario $z' \circ z = z + z' - z'z$ definisce in R la *composizione circolare* $\circ$. Sia σ l'applicazione $x \mapsto 1 - x$ su R. Allora $\sigma^2 = 1$, sicché σ è biiettiva. Vale

$$z' \circ z = 1 - (1 - z')(1 - z) = \sigma(\sigma(z')\sigma(z)) = \sigma^{-1}(\sigma(z')\sigma(z)).$$

Ne segue che la composizione circolare è associativa. Inoltre $\sigma(0) = 1$, perciò $0 \circ z = z = z \circ 0$. Dunque $(R, \circ, 0)$ è un monoide.

Lemma 2. *(1) Se I è un ideale sinistro (destro) quasiregolare, I è un sottogruppo di $(R, \circ, 0)$. (2) Gli elementi nilpotenti sono quasiregolari.*

Dimostrazione. (1) Sia $z \in I$. Esiste $z' \in R$ tale che $z' \circ z = 0$. Allora $z + z' - z'z = 0$ e $z' = z'z - z \in I$. Esiste quindi z'' con $z'' \circ z' = 0$. Poiché $(R, \circ, 0)$ è un monoide, dalle due equazioni $z' \circ z = 0 = z'' \circ z'$ si ricava $z'' = z$. Pertanto z' è l'inverso di z in $(R, \circ, 0)$ e appartiene a I. Poiché I è chiuso rispetto a $\circ$ e contiene 0, segue la (1).

(2) Se $z^n = 0$, si ha $(1 - z)(1 + z + z^2 + \cdots + z^{n-1}) = 1 = (1 + z + z^2 + \cdots + z^{n-1})(1 - z)$. Dunque z è quasiregolare. □

Un ideale (sinistro, destro o bilatero) si dice *nil* se tutti i suoi elementi sono nilpotenti. La seconda parte del lemma 2 mostra che ogni ideale sinistro (destro) nil è quasiregolare. Possiamo ora caratterizzare $\operatorname{rad} R$ in termini dei suoi elementi.

Proposizione 4.5. *(1)* $\operatorname{rad} R$ *è un ideale sinistro quasiregolare che contiene ogni ideale sinistro*

quasiregolare di R. (2) $\operatorname{rad} R$ *è l'insieme degli elementi z tali che az sia quasiregolare a sinistra per ogni $a \in R$.*

Dimostrazione. (1) Supponiamo che $z \in \operatorname{rad} R$ non sia quasiregolare a sinistra. Allora $R(1-z) \neq R$, sicché questo ideale sinistro è contenuto in un ideale sinistro massimale I. Poiché $\operatorname{rad} R$ è l'intersezione degli ideali sinistri massimali di R, si ha $z \in I$. Ma anche $1 - z \in R(1 - z) \subseteq I$, dunque $1 = 1 - z + z \in I$, contro $I \neq R$. Questa contraddizione dimostra che ogni elemento di $\operatorname{rad} R$ è quasiregolare a sinistra, e quindi che $\operatorname{rad} R$ è un ideale sinistro quasiregolare. Sia Z un qualunque ideale sinistro quasiregolare di R. Se $Z \nsubseteq \operatorname{rad} R$, esiste un ideale sinistro massimale I con $Z \nsubseteq I$. Allora $I + Z \neq I$ e quindi $I + Z = R$. Si ha $1 = b + z$ con $b \in I$, $z \in Z$, per cui $1 = (1 - z)^{-1}b \in I$, contro $I \neq R$. Dunque $Z \subseteq \operatorname{rad} R$ e la (1) è dimostrata.

(2) Se $z \in \operatorname{rad} R$, allora $az \in \operatorname{rad} R$ per ogni $a \in R$ e quindi az è quasiregolare a sinistra. Viceversa, supponiamo che z soddisfi tale condizione. Allora Rz è un ideale sinistro quasiregolare, dunque $Rz \subseteq \operatorname{rad} R$ per la (1), e $z \in \operatorname{rad} R$. □

La nozione di primitività, tanto per gli anelli quanto per i loro ideali, non è simmetrica rispetto alla sinistra e alla destra. Esistono infatti anelli primitivi che non sono primitivi a destra, nel senso che non possiedono alcun modulo destro irriducibile M' per cui l'antirappresentazione associata $\rho' \colon a \mapsto \rho'(a)$, con $\rho'(a)x = xa$, sia iniettiva. I primi esempi di tali anelli sono dovuti a George Bergman. Malgrado questa asimmetria della primitività, le nozioni di radicale e di semiprimitività sono simmetriche. Quanto si è fatto fin qui si può evidentemente trasportare alle antirappresentazioni, ai moduli destri e agli ideali destri. Indichiamo il radicale destro così ottenuto con $\operatorname{rad}' R$. Per $\operatorname{rad}' R$ vale l'analoga della proposizione 4.5. D'altra parte, per il lemma 2, gli elementi di $\operatorname{rad} R$ e di $\operatorname{rad}' R$ sono quasi-invertibili. La proposizione 4.5 e la proposizione analoga per gli ideali destri danno dunque $\operatorname{rad}' R \subseteq \operatorname{rad} R$ e $\operatorname{rad} R \subseteq \operatorname{rad}' R$, e pertanto $\operatorname{rad} R = \operatorname{rad}' R$. Ciò permette di dare altre caratterizzazioni del radicale. Le enunciamo insieme con quelle già ottenute.

Teorema 4.1. *Il radicale di un anello R ammette le seguenti caratterizzazioni. Esso è*

1. *l'intersezione degli ideali primitivi di R;*
2. *l'intersezione degli ideali sinistri massimali di R;*
3. *l'intersezione degli ideali primitivi a destra di R;*
4. *l'intersezione degli ideali destri massimali di R;*
5. *un ideale sinistro quasiregolare che contiene ogni ideale sinistro quasiregolare;*
6. *l'insieme degli elementi z tali che az sia quasiregolare a sinistra per ogni $a \in R$;*
7. *un ideale destro quasiregolare che contiene ogni ideale destro quasiregolare;*
8. *l'insieme degli elementi z tali che za sia quasiregolare a destra per ogni $a \in R$.*

È chiaro inoltre che $\operatorname{rad} R$ contiene ogni ideale destro nil, come pure ogni ideale sinistro nil, di R. Poiché la semiprimitività a destra, definita nel modo ovvio, equivale a $\operatorname{rad}' R = 0$, un anello è semiprimitivo se e soltanto se possiede un'antirappresentazione fedele completamente riducibile e se e soltanto se è un prodotto sottodiretto di anelli primitivi a destra. Si può anche esprimere questa simmetria dicendo che, se si identificano gli insiemi sottostanti a R e a R^{op}, allora $\operatorname{rad} R = \operatorname{rad} R^{\mathrm{op}}$, e che, se R è semiprimitivo, tale è anche R^{op}.

Esercizi

1. Mostrare che un anello R è locale (p. 111) se e soltanto se $R/\operatorname{rad} R$ è un anello di divisione e che in tal caso $\operatorname{rad} R$ è l'ideale degli elementi non invertibili di R.

2. Determinare il radicale di $\mathbb{Z}/(n)$, $n \neq 0$.

3. (McCrimmon.) Mostrare che $z \in \operatorname{rad} R$ se e soltanto se per ogni $a \in R$ esiste un w tale che $z + w = waz = zaw$.

4. Mostrare che ab è quasiregolare se e soltanto se ba è quasiregolare.

5. Un elemento a di un anello R si dice *regolare nel senso di von Neumann* se esiste un b tale che $aba = a$. Mostrare che il solo elemento di $\operatorname{rad} R$ con questa proprietà è 0. Un anello si dice regolare nel senso di von Neumann se tali sono tutti i suoi elementi. Segue dunque da questo esercizio che gli anelli regolari nel senso di von Neumann sono semiprimitivi.

6. Sia R un anello tale che per ogni $a \in R$ esista un intero $n(a) > 1$ con $a^{n(a)} = a$. Mostrare che R è semiprimitivo.

7. Sia e un idempotente non nullo di un anello R. Mostrare che

$$\operatorname{rad}(eRe) = e(\operatorname{rad} R)e = eRe \cap \operatorname{rad} R.$$

   (Traccia. Mostrare che ogni elemento di $e(\operatorname{rad} R)e$ è quasiregolare in eRe, sicché $e(\operatorname{rad} R)e \subseteq \operatorname{rad}(eRe)$. Siano ora $z \in \operatorname{rad}(eRe)$ e $a \in R$. Scrivere $a = eae + ea(1-e) + (1-e)ae + (1-e)a(1-e)$, la *decomposizione bilatera di Peirce*. Allora $za = zeae + zea(1-e)$ e $zeae$ ha un quasi-inverso z' in eRe. Si ha $(za) \circ z' = zea(1-e)$, che è nilpotente e dunque quasiregolare. Ne segue che za è quasiregolare a destra. Pertanto $z \in \operatorname{rad} R \cap eRe$ e $\operatorname{rad}(eRe) \subseteq e(\operatorname{rad} R)e$.)

8. Mostrare che, per ogni anello R, $\operatorname{rad} M_n(R) = M_n(\operatorname{rad} R)$. (Traccia. La corrispondenza $B \mapsto M_n(B)$ è una biiezione fra gli ideali di R e quelli di $M_n(R)$; si veda l'esercizio 1, p. 171. Sia $\{e_{ij} \mid 1 \leq i, j \leq n\}$ un sistema di unità matriciali di $M_n(R)$. Si ha l'isomorfismo $r \mapsto (r1_n)e_{11}$ di R su $e_{11}M_n(R)e_{11}$. Esso manda $\operatorname{rad} R$ in $\operatorname{rad}(e_{11}M_n(R)e_{11}) = e_{11}(\operatorname{rad} M_n(R))e_{11}$, per l'esercizio 7. Quest'ultimo è $e_{11}M_n(B)e_{11}$, dove B corrisponde a $\operatorname{rad} M_n(R)$. Ne segue che $B = \operatorname{rad} R$.)

9. Mostrare che, se R e R' sono simili nel senso di Morita, in ogni corrispondenza fra i loro ideali data dal teorema di Morita I i radicali di R e di R' si corrispondono.

10. Dimostrare che ogni ultraprodotto di anelli semiprimitivi (primitivi) è semiprimitivo (primitivo).

4.3 Teoremi di densità

Sia V uno spazio vettoriale su un anello di divisione Δ. Un insieme S di trasformazioni lineari di V si dice *denso* se, dati un insieme finito di vettori linearmente indipendenti $x_1, \ldots, x_n$ e vettori arbitrari $y_1, \ldots, y_n$, esiste $l \in S$ tale che $lx_i = y_i$ per $1 \leq i \leq n$. Se V ha dimensione finita, possiamo prendere per x_i gli elementi di una base e porre $y_i = ax_i$, dove a è una trasformazione lineare assegnata. Esiste allora $l \in S$ con $lx_i = ax_i$ per ogni i, da cui $l = a$. Pertanto l'unico insieme denso di trasformazioni lineari di uno spazio vettoriale di dimensione finita è l'insieme di tutte le sue trasformazioni lineari.

Dimostreremo un teorema fondamentale che consente di identificare ogni anello primitivo con un anello denso di trasformazioni lineari. Consideriamo dapprima una situazione più generale: siano R un anello arbitrario e M un R-modulo sinistro completamente riducibile. Poniamo $R' = \mathrm{End}_R M$, $R'' = \mathrm{End}_{R'} M$, considerando M nel modo naturale come R'-modulo sinistro. Dimostreremo anzitutto il seguente teorema.

Teorema di densità per i moduli completamente riducibili. *Sia M un modulo completamente riducibile su un anello R e siano $R' = \mathrm{End}_R M$, $R'' = \mathrm{End}_{R'} M$. Per ogni sottoinsieme finito $\{x_1, \ldots, x_n\}$ di M e ogni $a'' \in R''$ esiste $a \in R$ tale che $ax_i = a''x_i$ per $1 \leq i \leq n$.*

La dimostrazione che daremo è dovuta a Bourbaki e si basa sui due lemmi seguenti.

Lemma 1. *Ogni R-sottomodulo N di M è un R''-sottomodulo.*

Dimostrazione. Poiché M è completamente riducibile come R-modulo, si può scrivere $M = N \oplus P$, dove P è un secondo sottomodulo (p. 121). Sia e la proiezione su N determinata da questa decomposizione. Allora $e \in R'$ e $N = e(M)$. Per $a'' \in R''$ si ha dunque $a''(N) = a''e(M) = ea''(M) \subseteq N$. Pertanto N è un R''-sottomodulo di M. □

Lemma 2. *Sia M un modulo e sia $M^{(n)}$ la somma diretta di n copie di M, $n = 1, 2, \ldots$. Allora $\mathrm{End}_R M^{(n)}$ è l'insieme delle applicazioni $(u_1, u_2, \ldots, u_n) \mapsto (v_1, v_2, \ldots, v_n)$ dove $v_i = \sum_j a'_{ij} u_j$ e $a'_{ij} \in R' = \mathrm{End}_R M$. Inoltre, per ogni $a'' \in R'' = \mathrm{End}_{R'} M$, l'applicazione*

$$(u_1, u_2, \ldots, u_n) \longmapsto (a''u_1, a''u_2, \ldots, a''u_n)$$

appartiene all'anello degli endomorfismi di $M^{(n)}$ come modulo sinistro su $\mathrm{End}_R M^{(n)}$.

Dimostrazione. Sia $l \in \mathrm{End}_R M^{(n)}$ e consideriamone l'azione sull'elemento $(0, \ldots, 0, u_i, 0, \ldots, 0)$ con u_i al posto i-esimo. Scrivendo $l(0, \ldots, 0, u_i, 0, \ldots, 0) = (u_{1i}, u_{2i}, \ldots, u_{ni})$, si definisce per ogni j un'applicazione $u_i \mapsto u_{ji}$ che appartiene a $\mathrm{End}_R M$. Indicandola con a'_{ji} si ottiene

$$l(u_1, \ldots, u_n) = \Big(\sum_i a'_{1i} u_i,\ \sum_i a'_{2i} u_i, \ldots, \sum_i a'_{ni} u_i \Big).$$

È chiaro anche che ogni applicazione di questa forma appartiene a $\mathrm{End}_R M^{(n)}$. Questo dimostra la prima asserzione. La seconda segue dal fatto che, per ogni $a'' \in R''$, l'applicazione $(u_1, \ldots, u_n) \mapsto (a''u_1, \ldots, a''u_n)$ commuta con ogni applicazione della forma appena scritta, poiché gli a'_{ji} appartengono a R'. □

Possiamo ora dare la *dimostrazione del teorema.* Per $n = 1$, $N = Rx_1$ è un R-sottomodulo, dunque anche un R''-sottomodulo. Poiché $x_1 \in N$, abbiamo $a''x_1 \in N = Rx_1$, cioè esiste $a \in R$ tale che $ax_1 = a''x_1$. Sia ora n arbitrario. La somma diretta $M^{(n)}$ di n copie dell'R-modulo M è completamente riducibile perché lo è M. Per il lemma 2, dato $a'' \in R''$, l'applicazione $(u_1, \ldots, u_n) \mapsto (a''u_1, \ldots, a''u_n)$ è un endomorfismo di $M^{(n)}$ come modulo sinistro su $\mathrm{End}_R M^{(n)}$. Applichiamo il caso $n = 1$ a questo endomorfismo e all'elemento $x = (x_1, \ldots, x_n)$ di $M^{(n)}$. Esiste allora $a \in R$ con $ax = (a''x_1, \ldots, a''x_n)$, cioè $ax_i = a''x_i$ per ogni i, come richiesto. □

Si potrebbe dire ancora molto sui moduli completamente riducibili (si vedano gli esercizi). Per semplicità passiamo invece al caso che più interessa per la teoria della struttura: quello di una rappresentazione fedele e irriducibile di un anello. Vale allora il

Teorema di densità per gli anelli primitivi. *Un anello R è primitivo se e soltanto se è isomorfo a un anello denso di trasformazioni lineari di uno spazio vettoriale su un anello di divisione.*

Dimostrazione. Un anello primitivo R ammette una rappresentazione fedele e irriducibile ρ su M. Per il lemma di Schur, $\Delta = \mathrm{End}_R M$ è un anello di divisione. Poiché ρ è fedele, R è isomorfo a $\rho(R)$, un anello di trasformazioni lineari di M come spazio vettoriale su Δ. Siano $x_1, \ldots, x_n$

linearmente indipendenti e $y_1, \ldots, y_n$ vettori arbitrari di M. Essendo gli x_i parte di una base, esiste una trasformazione lineare l con $lx_i = y_i$ per $1 \leq i \leq n$. Da $l \in \mathrm{End}_\Delta M$ e $\Delta = \mathrm{End}_R M$ segue, per il teorema precedente, che esiste $a \in R$ con $ax_i = lx_i = y_i$ per ogni i. Quindi $\rho(R)$ è denso. Viceversa, supponiamo che R sia isomorfo a un anello denso di trasformazioni lineari di uno spazio vettoriale M su un anello di divisione Δ. Detto ρ l'isomorfismo, ponendo $ax = \rho(a)x$ per $a \in R$, $x \in M$, si rende M un R-modulo. Esso è irriducibile poiché, dati $x \neq 0$ e y arbitrario, esiste $a \in R$ con $ax = y$. Pertanto ρ è una rappresentazione fedele e irriducibile di R e R è primitivo. □

Per alcune applicazioni è importante disporre di una descrizione interna dell'anello di divisione Δ del teorema precedente. La si ottiene identificando un R-modulo irriducibile con un modulo isomorfo della forma R/I, con I ideale sinistro massimale di R. Occorre determinare $\mathrm{End}_R(R/I)$. Lo faremo per un ideale sinistro arbitrario I o, equivalentemente, per un modulo ciclico arbitrario. Definiamo l'*idealizzatore* di I in R ponendo

$$B = \{b \in R \mid Ib \subseteq I\}. \tag{21}$$

È chiaro che B è un sottoanello di R contenente I come ideale e che anzi contiene ogni sottoanello di R che abbia questa proprietà. Vale la

Proposizione 4.6. *Se I è un ideale sinistro di R, allora $\mathrm{End}_R(R/I)$ è anti-isomorfo a B/I, dove B è l'idealizzatore di I in R.*

Dimostrazione. Poiché $1 + I$ genera R/I, ogni $f \in \mathrm{End}_R(R/I)$ è determinato da $f(1 + I) = b + I = b(1 + I)$ ed è dato da

$$a + I = a(1 + I) \longmapsto a(b + I) = ab + I. \tag{22}$$

Se $a \in I$, allora $a+I = I = 0$ in R/I e quindi anche la sua immagine è $ab+I = I$. Ne segue $ab \in I$, dunque b appartiene all'idealizzatore B. Viceversa, per $b \in B$ consideriamo l'omomorfismo del modulo libero R in R/I che manda 1 in $b+I$. Esso manda ogni $d \in I$ in $db+I = I$. Si ha quindi un omomorfismo indotto di R/I in sé che manda $1 + I$ in $b + I$. Pertanto ogni $b \in B$ determina un endomorfismo di R/I dato dalla (22). Indichiamo con g la corrispondenza così definita fra elementi di B ed endomorfismi di R/I. Evidentemente g è additiva e $g(1) = 1$. Per $b_1, b_2 \in B$ abbiamo

$$g(b_1b_2)(1 + I) = b_1b_2 + I, \qquad g(b_2)g(b_1)(1 + I) = g(b_2)(b_1 + I) = b_1b_2 + I.$$

Dunque g è un antiomomorfismo di B su $\mathrm{End}_R(R/I)$. Gli elementi di B mandati in zero formano l'ideale I. Ne segue l'anti-isomorfismo fra B/I ed $\mathrm{End}_R(R/I)$. □

Il lettore tenga presente che, nonostante la bella determinazione di Δ data dalla proposizione 4.6, questo anello di divisione non è un invariante dell'anello primitivo. Uno stesso anello primitivo può ammettere moduli irriducibili non isomorfi che danno rappresentazioni fedeli e perfino moduli irriducibili i cui anelli di divisione degli endomorfismi non sono isomorfi. Vi sono però casi importanti in cui Δ è un invariante. Per esempio, come vedremo nel prossimo paragrafo, ciò accade per gli anelli primitivi artiniani. Il teorema seguente ne descrive la struttura.

Teorema 4.2. *Per un anello R sono equivalenti le condizioni:*

1. *R è semplice, artiniano a sinistra e non nullo.*
2. *R è primitivo e artiniano a sinistra.*
3. *R è isomorfo a un anello $\mathrm{End}_\Delta M$, dove M è uno spazio vettoriale di dimensione finita positiva su un anello di divisione Δ.*

Dimostrazione. (1) $\Rightarrow$ (2) è chiaro.

(2) $\Rightarrow$ (3). Sia M un R-modulo fedele e irriducibile, $\Delta = \operatorname{End}_R M$. Affermiamo che M ha dimensione finita su Δ. Altrimenti esisterebbe in M una famiglia infinita di elementi linearmente indipendenti $\{x_i \mid i = 1, 2, 3, \ldots\}$. Poniamo $I_j = \operatorname{ann}_R x_j$, un ideale sinistro. Evidentemente $I_1 \cap \cdots \cap I_n$ consiste negli elementi di R che annullano $x_1, \ldots, x_n$. Per il teorema di densità esiste $a \in R$ tale che $ax_1 = \cdots = ax_n = 0$ e $ax_{n+1} \neq 0$. Quindi $I_1 \cap \cdots \cap I_n \supsetneq I_1 \cap \cdots \cap I_{n+1}$. Si avrebbe una catena infinita strettamente decrescente di ideali sinistri

$$I_1 \supsetneq I_1 \cap I_2 \supsetneq I_1 \cap I_2 \cap I_3 \supsetneq \cdots,$$

in contrasto con l'ipotesi artiniana. Dunque M ha dimensione finita su Δ. Se $(x_1, \ldots, x_n)$ è una base di M, per la densità e per ogni $y_1, \ldots, y_n$ esiste $a \in R$ con $ax_i = y_i$ per ogni i. Pertanto, se ρ è la rappresentazione determinata da M, $\rho(R) = \operatorname{End}_\Delta M$ e R è isomorfo all'anello delle trasformazioni lineari dello spazio di dimensione finita M su Δ.

(3) $\Rightarrow$ (1). Lo abbiamo dimostrato nel corso della prova del teorema di Wedderburn–Artin (p. 171). Lo si può vedere anche direttamente dall'anti-isomorfismo di $\operatorname{End}_\Delta M$ con $M_n(\Delta)$ e ricordando che, per ogni anello R, l'applicazione $B \mapsto M_n(B)$ è un isomorfismo del reticolo degli ideali di R sul reticolo degli ideali di $M_n(R)$ (esercizio 8, p. 103 di BAI, oppure esercizio 1, p. 171). Il risultato segue allora dalla semplicità di Δ. □

Esercizi

1. Sia R un anello primitivo, M un R-modulo fedele e irriducibile, $\Delta = \operatorname{End}_R M$. Mostrare che o $R \simeq M_n(\Delta)$ per qualche n, oppure per ogni $k = 1, 2, 3, \ldots$ l'anello R contiene un sottoanello avente $M_k(\Delta)$ come immagine omomorfa.[7]

2. Usare l'esercizio 1 per mostrare che, se R è un anello primitivo tale che per ogni $a \in R$ esiste un intero $n(a) > 1$ con $a^{n(a)} = a$, allora R è un anello di divisione.

3. Si dica che un insieme S di trasformazioni lineari è k *volte transitivo* se, dati $l \leq k$ vettori linearmente indipendenti $x_1, \ldots, x_l$ e vettori arbitrari $y_1, \ldots, y_l$, esiste $a \in S$ tale che $ax_i = y_i$ per $1 \leq i \leq l$. Mostrare che un anello di trasformazioni lineari due volte transitivo è denso.

Nei tre esercizi seguenti M è un R-modulo sinistro completamente riducibile, $R' = \operatorname{End}_R M$ e $R'' = \operatorname{End}_{R'} M$.

4. Mostrare che ogni R-omomorfismo di un R-sottomodulo N di M in M si può prolungare a un R-endomorfismo di M (un elemento di R') e che, se N è irriducibile su R, ogni R-omomorfismo non nullo di N in M si può prolungare a un R-automorfismo di M.

5. Mostrare che, se $x \neq 0$ appartiene a un R-sottomodulo irriducibile N di M, allora $R'x$ è un R'-sottomodulo irriducibile di M. (*Suggerimento.* Sia $y = a'x \neq 0$, con $a' \in R'$, e si consideri l'applicazione $u \mapsto a'u$ da $N = Rx$ in M.)

6. Mostrare che M è completamente riducibile su R' e che la sua dimensione (definita a p. 125) è finita se R è artiniano a sinistra. Mostrare inoltre che in questo caso $R'' = \rho(R)$, dove ρ è la rappresentazione definita da M.

[7] Con la convenzione dei moduli sinistri usata nel testo, l'identificazione con le matrici su Δ è un anti-isomorfismo, come nella dimostrazione precedente; per avere un isomorfismo si prende l'anello opposto Δ^{op}. [N.d.T.]

7. Sia M un R-modulo completamente riducibile e sia B un ideale di R. Mostrare che sono equivalenti: (i) $BM = M$; (ii) se $x \in M$ soddisfa $Bx = 0$, allora $x = 0$; (iii) per ogni $x \in M$ si ha $x \in Bx$.

8. Dimostrare la seguente estensione del teorema di densità per i moduli completamente riducibili. Se R, M, B sono come nell'esercizio 7 e B soddisfa (i), (ii), (iii), allora, per ogni $a'' \in R''$ e $x_1, \ldots, x_n \in M$, esiste $b \in B$ tale che $bx_i = a''x_i$ per $1 \leq i \leq n$.

9. Usare l'esercizio 8 per dimostrare la semplicità dell'anello delle trasformazioni lineari di uno spazio vettoriale di dimensione finita positiva su un anello di divisione.

4.4 Anelli artiniani

In questo paragrafo ricaveremo i risultati classici sulla struttura e sulle rappresentazioni degli anelli artiniani (a sinistra). Mostreremo dapprima che il radicale di un tale anello è nilpotente. Ricordiamo che per due ideali B, C di un anello R si pone $BC = \{\sum b_i c_i \mid b_i \in B,\ c_i \in C\}$. Si ottiene un ideale di R. Inoltre, per un altro ideale D, $(BC)D = B(CD)$. Definiamo induttivamente $B^1 = B$, $B^i = B^{i-1}B$. L'ideale B si dice *nilpotente* se $B^k = 0$ per qualche k. Ciò equivale a dire che il prodotto di k elementi qualsiasi di B è zero. In particolare $b^k = 0$ per ogni $b \in B$. Quindi un ideale nilpotente è un ideale nil. È invece facile dare esempi di ideali nil che non sono nilpotenti (esercizio 1 alla fine del paragrafo).

Teorema 4.3. *Il radicale di un anello artiniano (a sinistra) è nilpotente.*

Dimostrazione. Sia $N = \operatorname{rad} R$ con R artiniano. Per induzione $N \supseteq N^2 \supseteq N^3 \supseteq \cdots$. Poiché si tratta di ideali sinistri, esiste k tale che $P = N^k = N^{k+1} = \cdots$. Quindi $P = P^2 = N^{2k}$. Ora N è nilpotente se e soltanto se $P = 0$. Supponiamo il contrario e consideriamo l'insieme S degli ideali sinistri I di R tali che (1) $I \subseteq P$ e (2) $PI \neq 0$. Poiché P possiede entrambe le proprietà, S non è vuoto e, poiché R è artiniano, S contiene un elemento minimale I. Evidentemente I contiene un elemento b tale che $Pb \neq 0$. Allora Pb è un ideale sinistro contenuto sia in I sia in P, e $P(Pb) = P^2b = Pb \neq 0$. Per la minimalità di I in S abbiamo quindi $Pb = I$. Poiché $b \in I$, esiste $z \in P$ con $zb = b$, ossia $(1 - z)b = 0$. Ma $z \in P \subseteq \operatorname{rad} R$, quindi z è quasi-regolare. Esiste pertanto $(1 - z)^{-1}$ e $b = (1 - z)^{-1}(1 - z)b = 0$. Ciò contraddice $Pb \neq 0$ e dimostra che $(\operatorname{rad} R)^k = P = 0$. □

Ricordiamo che il radicale di un anello contiene tutti gli ideali unilateri quasi-regolari e quindi tutti gli ideali unilateri nil. Il risultato precedente implica che in un anello artiniano tutti questi ideali sono nilpotenti. Ricaviamo ora il risultato principale sulla struttura degli anelli artiniani semiprimitivi. Per la dimostrazione ci occorre il seguente lemma.

Lemma. *Sia M un modulo artiniano che sia un prodotto sottodiretto di moduli irriducibili. Allora M è somma diretta di un numero finito di sottomoduli irriducibili.*

Dimostrazione. La seconda ipotesi equivale all'esistenza in M di un insieme di sottomoduli $\{N_\alpha\}$ tale che $\bigcap N_\alpha = 0$ e ciascun $M_\alpha = M/N_\alpha$ sia irriducibile. Consideriamo l'insieme delle intersezioni finite $N_{\alpha_1} \cap \cdots \cap N_{\alpha_k}$ di elementi di $\{N_\alpha\}$. Per la condizione artiniana su M questo insieme ha un elemento minimale, diciamo $N_1 \cap \cdots \cap N_m$. Per ogni N_α si ha allora $N_\alpha \cap (N_1 \cap \cdots \cap N_m) = N_1 \cap \cdots \cap N_m$, ossia $N_\alpha \supseteq N_1 \cap \cdots \cap N_m$. Poiché $\bigcap N_\alpha = 0$, risulta $N_1 \cap \cdots \cap N_m = 0$. Abbiamo così un monomorfismo di M in $\prod_{i=1}^m M_i = \bigoplus_{i=1}^m M_i$, con $M_i = M/N_i$. Pertanto M è isomorfo a un sottomodulo del modulo completamente riducibile $\bigoplus M_i$. Ne segue che M è completamente riducibile ed è somma diretta di irriducibili isomorfi ad alcuni degli M_i. □

Diremo che un anello è *semisemplice* se è un prodotto sottodiretto di anelli semplici. Dal lemma precedente segue facilmente la proposizione seguente.

Proposizione 4.7. *Se R è semisemplice e soddisfa la condizione del minimo per gli ideali bilateri, allora R è una somma diretta $\bigoplus_{i=1}^{n} R_i$ di anelli semplici R_i.*

Dimostrazione. Sia $M(R)$ l'anello degli endomorfismi del gruppo additivo di R generato dalle moltiplicazioni a sinistra e a destra $x \mapsto ax$ e $x \mapsto xa$. Questo anello si chiama *anello delle moltiplicazioni* di R. Il gruppo additivo di R si può considerare in modo naturale come $M(R)$-modulo, e i sottomoduli di ${}_{M(R)}R$ sono allora gli ideali dell'anello R. L'ipotesi che R sia semisemplice equivale a dire che R, come $M(R)$-modulo, è prodotto sottodiretto di $M(R)$-moduli irriducibili. Anche l'altra ipotesi del lemma è soddisfatta. La conclusione segue quindi dal lemma. □

Possiamo ora dimostrare il risultato principale.

Teorema di struttura degli anelli artiniani semiprimitivi. *Le seguenti condizioni su un anello R sono equivalenti.*

1. *R è artiniano e non contiene ideali nilpotenti non nulli.*
2. *R è semiprimitivo e artiniano.*
3. *R è semisemplice e artiniano.*
4. *${}_RR$ è un R-modulo completamente riducibile.*
5. *R è somma diretta di un numero finito di anelli R_i, ciascuno isomorfo all'anello delle trasformazioni lineari di uno spazio vettoriale di dimensione finita su un anello di divisione.*

L'implicazione (1) ⇒ (5) prende il nome di *teorema di Wedderburn–Artin*.

Dimostrazione. (1) ⇔ (2). Il radicale di un anello artiniano è un ideale nilpotente che contiene tutti gli ideali nilpotenti, e $\operatorname{rad} R = 0$ equivale alla semiprimitività.

(2) ⇔ (3) segue subito dal teorema 4.2, che per gli anelli artiniani stabilisce l'equivalenza fra semplicità e primitività.

(2) ⇒ (4). Poiché $\operatorname{rad} R$ è l'intersezione degli ideali sinistri massimali, dalla semiprimitività di R segue che ${}_RR$ è prodotto sottodiretto di moduli irriducibili. Il lemma dà allora (4).

(4) ⇒ (2). La semiprimitività è evidente, poiché la rappresentazione determinata da ${}_RR$ è fedele e completamente riducibile. Inoltre $R = \sum I_\alpha$, con gli I_α ideali sinistri minimali. Si ha dunque $1 = e_1 + \cdots + e_k$, con $e_i \in I_i \in \{I_\alpha\}$. Per $a \in R$, risulta $a = a1 = ae_1 + \cdots + ae_k \in I_1 + \cdots + I_k$. Quindi $R = I_1 + \cdots + I_k$ e, scegliendo un sottoinsieme fra gli I_j e rinumerandolo, $R = I_1 \oplus I_2 \oplus \cdots \oplus I_t$. È chiaro che

$$R \supset I_2 + \cdots + I_t \supset I_3 + \cdots + I_t \supset \cdots \supset I_t \supset 0$$

è una serie di composizione per ${}_RR$. L'esistenza di tale serie implica che R è artiniano e noetheriano. Vale quindi (2).

(3) ⇒ (5). La condizione artiniana implica quella del minimo per gli ideali bilateri. Per la proposizione 4.7, R è dunque somma diretta di anelli semplici. Scriviamo $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$, dove gli R_i sono ideali e sono anelli semplici. Per $i \neq j$ si ha $R_iR_j \subseteq R_i \cap R_j = 0$. Ne segue che ogni ideale sinistro di R_i è un ideale sinistro di R, perciò ogni R_i è artiniano. Allora R_i è isomorfo all'anello delle trasformazioni lineari di uno spazio vettoriale di dimensione finita su un anello di divisione. Vale quindi (5).

(5) ⇒ (2). Supponiamo $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$, con R_i ideali e $R_i \cong \operatorname{End}_{\Delta_i} M_i$, dove M_i è uno spazio vettoriale di dimensione finita sull'anello di divisione Δ_i. Per il teorema 4.2, R_i è primitivo e artiniano; R è un prodotto sottodiretto di anelli primitivi, dunque è semiprimitivo. Poiché R_i

è un sottomodulo di ${}_RR$ e i suoi R-sottomoduli sono gli ideali sinistri di R_i, il modulo ${}_RR_i$ è artiniano. Di conseguenza anche R è artiniano. Vale così (2) e la dimostrazione è completa. □

Sia R un anello qualsiasi e sia $R = R_1 \oplus \cdots \oplus R_s$ con gli R_i ideali indecomponibili, nel senso che, se $R_i = R_i' \oplus R_i''$ con R_i', R_i'' ideali, allora $R_i' = 0$ oppure $R_i'' = 0$. Sia B un qualunque ideale di R. Abbiamo $B = B1 = BR = BR_1 + \cdots + BR_s$ e, poiché $BR_i \subseteq R_i$, segue $B = BR_1 \oplus \cdots \oplus BR_s$. Inoltre BR_i è un ideale di R; perciò, se B è indecomponibile, $BR_i = B$ per qualche i. Analogamente $B = R_jB$ per qualche j e, poiché $R_i \cap R_j = 0$ per $i \neq j$, si ha $B = R_iB$. Ne segue che, se $R = R_1' \oplus \cdots \oplus R_t'$ è una seconda decomposizione in somma diretta di ideali indecomponibili, allora $s = t$ e gli R_j' coincidono, a meno dell'ordine, con gli R_i. Ciò si applica in particolare alla decomposizione di un anello artiniano semisemplice in somma diretta di ideali che sono anelli semplici. Tale decomposizione è quindi unica. Chiameremo perciò i suoi termini R_i *componenti semplici* di R.

Il teorema di struttura degli anelli artiniani semiprimitivi (o il teorema 4.2) mostra che, se R è semplice e artiniano, allora $R \cong \mathrm{End}_\Delta M$ dove M è uno spazio vettoriale di dimensione finita sull'anello di divisione Δ. Consideriamo ora l'unicità di M e di Δ. Se $\mathrm{End}_{\Delta_1} M_1$ ed $\mathrm{End}_{\Delta_2} M_2$ sono isomorfi per due spazi M_i di dimensione finita sui rispettivi Δ_i, che cosa si può dire della relazione fra i due spazi? Vedremo che essi sono *semilinearmente isomorfi*. Dato un isomorfismo σ da Δ_1 su Δ_2, un'applicazione $s\colon M_1 \to M_2$ si dice *σ-semilineare* se

$$s(x+y) = sx + sy, \qquad s(\delta x) = \sigma(\delta)(sx) \tag{23}$$

per $x, y \in M_1$, $\delta \in \Delta_1$ (BAI, p. 469). È immediato che, se s è biiettiva, s^{-1} è un'applicazione σ^{-1}-semilineare da M_2 su M_1. Diremo che M_1 e M_2 sono semilinearmente isomorfi se esiste un isomorfismo semilineare (ossia un'applicazione semilineare biiettiva) da M_1 su M_2. Ciò presuppone implicitamente che gli anelli di divisione sottostanti Δ_1 e Δ_2 siano isomorfi. Inoltre, se $\{x_\alpha\}$ è una base di M_1 su Δ_1 e s è un isomorfismo semilineare da M_1 su M_2, allora $\{sx_\alpha\}$ è una base di M_2 su Δ_2. Gli spazi hanno quindi la stessa dimensione. Viceversa, supponiamo che M_1 su Δ_1 e M_2 su Δ_2 abbiano la stessa dimensione e che Δ_1 e Δ_2 siano isomorfi. Siano $\{x_\alpha\}$ e $\{y_\alpha\}$ basi rispettivamente di M_1 e di M_2, indicizzate dallo stesso insieme, e sia σ un isomorfismo di Δ_1 su Δ_2. Definiamo l'applicazione s da M_1 in M_2 mediante

$$\sum \delta_\alpha x_\alpha \longmapsto \sum \sigma(\delta_\alpha) y_\alpha \qquad \text{(somme finite)}. \tag{24}$$

Si verifica direttamente che s è σ-semilineare e biiettiva. Dunque M_1 su Δ_1 e M_2 su Δ_2 sono semilinearmente isomorfi se e soltanto se hanno la stessa dimensione e Δ_1, Δ_2 sono isomorfi.

Per il teorema di isomorfismo, e anche per la teoria delle rappresentazioni, il risultato decisivo è il seguente.

Lemma 1. *Due moduli irriducibili qualsiasi su un anello semplice artiniano sono isomorfi.*

Dimostrazione. Scegliamo un ideale sinistro minimale I di R, che è dunque un R-modulo irriducibile. Basta mostrare che ogni R-modulo irriducibile M è isomorfo a I. Poiché R è semplice, la rappresentazione di R data da M è fedele. Dato che $I \neq 0$, esiste perciò $x \in M$ tale che $Ix \neq 0$. Abbiamo l'omomorfismo $b \mapsto bx$ di I in M. Essendo $Ix \neq 0$, l'omomorfismo è non nullo. Per il lemma di Schur è un isomorfismo. □

Ci occorre inoltre il seguente lemma.

Lemma 2. *Sia M uno spazio vettoriale su un anello di divisione Δ e sia $R = \mathrm{End}_\Delta M$ l'anello delle trasformazioni lineari di M su Δ. Il centralizzante di R nell'anello* $\mathrm{End}\, M$ *degli endomorfismi del gruppo abeliano M è l'insieme delle applicazioni $\delta'\colon u \mapsto \delta u$, $\delta \in \Delta$. Inoltre $\delta \mapsto \delta'$ è un isomorfismo di Δ su questo centralizzante.*

Dimostrazione. Poiché M è un Δ-modulo completamente riducibile, la prima asserzione è un caso particolare del teorema di densità. Possiamo anche darne una semplice dimostrazione

diretta. Sia d un endomorfismo di $(M, +, 0)$ che commuta con $\mathrm{End}_\Delta M$. Sia $0 \neq x \in M$. Allora $dx \in \Delta x$: in caso contrario x e dx sarebbero linearmente indipendenti e quindi esisterebbe $l \in \mathrm{End}_\Delta M$ con $lx = 0$ e $l(dx) \neq 0$, il che è impossibile perché $l(dx) = d(lx) = 0$. Dunque per ogni $x \neq 0$ esiste $\delta_x \in \Delta$ tale che $dx = \delta_x x$. Sia y un secondo elemento non nullo di M e scegliamo $l \in \mathrm{End}_\Delta M$ con $lx = y$. Allora $\delta_y y = dy = dlx = ldx = l(\delta_x x) = \delta_x lx = \delta_x y$. Quindi $\delta_x = \delta_y$ per ogni coppia x, y di elementi non nulli, e d ha la forma $\delta' \colon u \mapsto \delta u$. È chiaro che $\delta \mapsto \delta'$ è un isomorfismo. □

Teorema di isomorfismo per gli anelli semplici artiniani. *Sia M_i uno spazio vettoriale di dimensione finita su un anello di divisione Δ_i, $i = 1, 2$, e sia g un isomorfismo di $R_1 = \mathrm{End}_{\Delta_1} M_1$ su $R_2 = \mathrm{End}_{\Delta_2} M_2$. Esiste un isomorfismo semilineare s di M_1 su M_2 tale che*

$$g(a) = sas^{-1} \tag{25}$$

per ogni $a \in R_1$.

Dimostrazione. Consideriamo M_1 come R_1-modulo nel modo naturale e rendiamo M_2 un R_1-modulo ponendo $ay = g(a)y$ per $a \in R_1$, $y \in M_2$. Questi due moduli sull'anello semplice artiniano R_1 sono irriducibili, dunque isomorfi. Esiste quindi un isomorfismo di gruppi s di M_1 su M_2 tale che $s(ax) = a(sx)$ per ogni $x \in M_1$, $a \in R_1$. Poiché $ay = g(a)y$ per $y \in M_2$, si ricava l'identità di operatori $g(a) = sas^{-1}$, ossia la (25).

Poiché s è un isomorfismo di M_1 su M_2, l'applicazione $b \mapsto sbs^{-1}$ per $b \in \mathrm{End}\, M_1$ è un isomorfismo dall'anello degli endomorfismi del gruppo abeliano M_1 su quello del gruppo abeliano M_2. Essa manda $\mathrm{End}_{\Delta_1} M_1$ su $\mathrm{End}_{\Delta_2} M_2$ e perciò induce, per restrizione, un isomorfismo fra i rispettivi centralizzanti in $\mathrm{End}\, M_1$ e $\mathrm{End}\, M_2$. Per il lemma 2 i due centralizzanti sono rispettivamente isomorfi a Δ_1 e Δ_2 mediante le applicazioni che mandano $\delta_i \in \Delta_i$ nell'endomorfismo $\delta_i' \colon u_i \mapsto \delta_i u_i$. Otteniamo quindi un isomorfismo σ da Δ_1 su Δ_2 componendo $\delta_1 \mapsto \delta_1' \mapsto s\delta_1' s^{-1}$ con l'inversa di $\delta_2 \mapsto \delta_2'$. Allora $s\delta_1' s^{-1} = (\sigma\delta_1)'$ e per ogni $x \in M_1$ si ha

$$s(\delta_1 x) = s\delta_1' x = s\delta_1' s^{-1}(sx) = (\sigma\delta_1)'(sx) = (\sigma\delta_1)sx.$$

Questo mostra che s è un isomorfismo σ-semilineare di M_1 su M_2. □

Segue immediatamente che, se $\mathrm{End}_{\Delta_1} M_1$ ed $\mathrm{End}_{\Delta_2} M_2$ sono isomorfi, M_1 e M_2 sono semilinearmente isomorfi. Viceversa, se s è un isomorfismo semilineare di M_1 su M_2, allora $sas^{-1} \in \mathrm{End}_{\Delta_2} M_2$ per ogni $a \in \mathrm{End}_{\Delta_1} M_1$ ed è immediato che $a \mapsto sas^{-1}$ è un isomorfismo fra i due anelli. Abbiamo visto che M_1 e M_2 sono semilinearmente isomorfi esattamente quando hanno la stessa dimensione e Δ_1 e Δ_2 sono isomorfi. Un anello semplice artiniano è dunque determinato, a meno di isomorfismo, da un intero n, la dimensione di M, e dalla classe di isomorfismo di un anello di divisione Δ.

Il teorema di isomorfismo determina anche il gruppo degli automorfismi di un tale anello. Posto $R = \mathrm{End}_\Delta M$, con M di dimensione finita su Δ, applicando il teorema a $\mathrm{End}_\Delta M$ e a sé stesso si vede che gli automorfismi di R sono le applicazioni

$$a \longmapsto sas^{-1}, \tag{26}$$

dove s appartiene al gruppo G delle trasformazioni semilineari biiettive dello spazio vettoriale M. Indicando con I_s l'applicazione (26) si ottiene l'epimorfismo $s \mapsto I_s$ da G su $\mathrm{Aut}\, R$. Il nucleo è l'insieme delle trasformazioni semilineari biiettive s tali che $sas^{-1} = a$ per ogni $a \in R = \mathrm{End}_\Delta M$. Per il lemma 2 ogni tale applicazione ha la forma $\delta' \colon x \mapsto \delta x$, $\delta \in \Delta$. Osserviamo inoltre che per $\delta \neq 0$ l'applicazione δ' è un automorfismo semilineare di M cui è associato l'automorfismo interno $i_\delta \colon \alpha \mapsto \delta\alpha\delta^{-1}$ di Δ. Ciò segue da

$$\delta'(\alpha x) = \delta(\alpha x) = (\delta\alpha\delta^{-1})\delta x = (\delta\alpha\delta^{-1})\delta' x.$$

Il nucleo di $s \mapsto I_s$ è quindi il gruppo $\Delta^{*\prime}$ delle moltiplicazioni $x \mapsto \delta x$ determinate dagli elementi non nulli di Δ. I risultati sugli automorfismi si possono pertanto formulare come segue.

Corollario. *Si ha una successione esatta*

$$1 \longrightarrow \Delta^* \xrightarrow{i} G \xrightarrow{I} \operatorname{Aut} R \longrightarrow 1, \tag{27}$$

dove Δ^* è il gruppo moltiplicativo degli elementi non nulli di Δ, G è il gruppo moltiplicativo delle trasformazioni semilineari biiettive dello spazio vettoriale M, $\operatorname{Aut} R$ è il gruppo degli automorfismi di $R = \operatorname{End}_\Delta M$, i è l'applicazione $\delta \mapsto \delta'$ e I è l'applicazione $s \mapsto I_s$.

Naturalmente ciò implica $\operatorname{Aut} R \cong G/\Delta^{*\prime}$. Il lettore che conosca il teorema fondamentale della geometria proiettiva (BAI, pp. 468–473) confronti i risultati qui ottenuti sugli isomorfismi e sugli automorfismi degli anelli semplici artiniani con quel teorema e le sue conseguenze. I risultati presenti si potrebbero dedurre dal teorema geometrico, ma per una via piuttosto indiretta.

Ricaviamo ora il risultato principale sulle rappresentazioni degli anelli artiniani.

Teorema 4.4. *Ogni modulo su un anello artiniano semisemplice R è completamente riducibile e vi è una corrispondenza biunivoca fra le classi di isomorfismo dei moduli irriducibili su R e le componenti semplici dell'anello. Più precisamente, se $R = R_1 \oplus \cdots \oplus R_s$, dove gli R_j sono le componenti semplici, e I_j è un ideale sinistro minimale di R_j, allora $\{I_1, \ldots, I_s\}$ è un sistema di rappresentanti delle classi di isomorfismo degli R-moduli irriducibili.*

Dimostrazione. Scriviamo ogni componente semplice come somma di ideali sinistri minimali di R. Si ottiene $R = \sum I_k$, dove ciascun I_k è un ideale sinistro minimale di R contenuto in una componente semplice. Sia M un R-modulo e sia x un suo elemento non nullo. Allora $x = 1x \in Rx = \sum I_k x$. Per il lemma di Schur, $I_k x = 0$ oppure $I_k x$ è un modulo irriducibile isomorfo a I_k. Ora $M = \sum_{x \in M} Rx = \sum_{k,x} I_k x$; dunque M è somma di sottomoduli irriducibili isomorfi a ideali sinistri minimali delle componenti semplici di R. Pertanto M è completamente riducibile e, se irriducibile, è isomorfo a un ideale sinistro minimale I di una componente semplice di R. Resta da mostrare che un ideale sinistro minimale I di R_j e un ideale sinistro minimale I' di $R_{j'}$ sono isomorfi come R-moduli se e soltanto se $j = j'$. Quando $j = j'$, per il lemma 1 di p. 205 essi sono isomorfi come R_j-moduli. Poiché $R_k I = 0 = R_k I'$ per $k \neq j$, sono anche isomorfi come R-moduli. Se invece $j \neq j'$, allora $R_j I = I$ e $R_j I' = 0$, il che esclude un R-isomorfismo. □

Anche per le rappresentazioni irriducibili di un anello artiniano (a sinistra) qualsiasi si ottiene un risultato conclusivo.

Teorema 4.5. *Sia R artiniano (a sinistra), $N = \operatorname{rad} R$ e $\bar{R} = R/N = R_1 \oplus \cdots \oplus R_s$, dove gli R_i sono le componenti semplici. Per ciascun j, $1 \leq j \leq s$, sia I_j un ideale sinistro minimale di R_j. Allora I_j è un R-modulo irriducibile, $I_j \ncong I_{j'}$ come R-moduli se $j \neq j'$, e ogni R-modulo irriducibile è isomorfo a uno degli I_j.*

Dimostrazione. Ogni R-modulo irriducibile M è annullato da N, dunque si può considerare come un $\bar{R}$-modulo irriducibile. Viceversa, ogni $\bar{R}$-modulo irriducibile è un R-modulo irriducibile. È anche chiaro che due R-moduli irriducibili sono isomorfi se e soltanto se lo sono come $\bar{R}$-moduli. La tesi segue immediatamente dal teorema 4.4. □

Esercizi

1. Per un elemento nilpotente z di un anello, l'*indice di nilpotenza* è il minimo t tale che $z^t = 0$, $z^{t-1} \neq 0$. Una definizione analoga vale per gli ideali nilpotenti. Osservare che, se N è un ideale nilpotente, gli indici di nilpotenza degli elementi di N sono limitati. Usare questo fatto per costruire un ideale nil che non sia nilpotente.

2. Dimostrare che il centro di ogni anello semplice è un campo.

3. Mostrare che, se $R = R_1 \oplus \cdots \oplus R_s$ con gli R_i semplici, il centro C di R è $C = C_1 \oplus \cdots \oplus C_s$, dove $C_i = C \cap R_i$ è il centro di R_i. Quindi C è un anello commutativo semisemplice artiniano. Osservare che gli R_i sono determinati dalle componenti semplici C_i di C, poiché $R_i = C_i R$.

4. Sia R artiniano a sinistra, $N = \operatorname{rad} R$, e sia $N^t = 0$, $N^{t-1} \neq 0$. Mostrare che R/N e gli N^i/N^{i+1}, $1 \leq i \leq t-1$, sono R-moduli completamente riducibili di dimensione finita. Usare questo fatto per dimostrare che ${}_R R$ possiede una serie di composizione e che pertanto R è noetheriano a sinistra.

I quattro esercizi seguenti danno condizioni per l'anti-isomorfismo di anelli semplici artiniani e permettono di determinarne gli anti-isomorfismi e le involuzioni.

5. Sia V uno spazio vettoriale su un anello di divisione Δ dotato di un anti-automorfismo $j\colon \delta \mapsto \bar{\delta}$. Una *forma sesquilineare* su V (rispetto a j) è un'applicazione $f\colon V \times V \to \Delta$ tale che
$$\begin{aligned} f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y), \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2), \\ f(\delta x, y) = \delta f(x, y), &\qquad f(x, \delta y) = f(x, y)\bar{\delta} \end{aligned}$$
per $x, y \in V$, $\delta \in \Delta$. Si dica f *non degenere* se $f(z, y) = 0$ per ogni y implica $z = 0$ e $f(x, z) = 0$ per ogni x implica $z = 0$. Mostrare che, se V ha dimensione finita e f è non degenere, per ogni trasformazione Δ-lineare l di V esiste un *aggiunto* (sinistro) *rispetto a* f, ossia una trasformazione lineare l' tale che $f(lx, y) = f(x, l'y)$ per ogni x, y. Mostrare che $l \mapsto l'$ è un anti-isomorfismo e che è un'involuzione se f è hermitiana, ossia $f(y, x) = \overline{f(x, y)}$ per ogni x, y, oppure antihermitiana, ossia $f(y, x) = -\overline{f(x, y)}$.

6. Siano V, Δ come nell'esercizio 5; sia $V^* = \hom_\Delta(V, \Delta)$ lo spazio duale. È uno spazio vettoriale destro su Δ, quindi sinistro su Δ^{op}. Se l è una trasformazione Δ-lineare di V, sia l^* la sua trasposta in V^*. Mostrare che, in dimensione finita, $l \mapsto l^*$ è un anti-isomorfismo di $\operatorname{End}_\Delta V$ su $\operatorname{End}(V^*_\Delta)$. Dedurne che, dati due spazi vettoriali V_i di dimensione finita su anelli di divisione Δ_i, gli anelli $\operatorname{End}_{\Delta_1} V_1$ ed $\operatorname{End}_{\Delta_2} V_2$ sono anti-isomorfi se e soltanto se Δ_1 e Δ_2 sono anti-isomorfi e V_1 e V_2 hanno la stessa dimensione.

7. Sia V uno spazio vettoriale di dimensione finita su un anello di divisione Δ e supponiamo che $\operatorname{End}_\Delta V$ ammetta un anti-automorfismo J. Osservare che $J(l) \mapsto l^*$ è un isomorfismo di $\operatorname{End}_\Delta V$ su $\operatorname{End}_{\Delta^{\mathrm{op}}} V^*$, considerando V^* nel modo consueto come spazio sinistro su Δ^{op} ($\alpha x^* = x^* \alpha$). Esiste quindi un isomorfismo semilineare s da V su Δ a V^* su Δ^{op}, tale che $l^* = sJ(l)s^{-1}$ per $l \in \operatorname{End}_\Delta V$. Per $x, y \in V$ si ponga $f(x, y) = (sy)(x)$. Mostrare che f è una forma sesquilineare non degenere su V corrispondente all'anti-automorfismo σ che, visto come isomorfismo di Δ su Δ^{op}, è associato a s. Mostrare che J è l'applicazione che associa a un operatore il suo aggiunto rispetto a f.

8. (Continuazione dell'esercizio 7.) Mostrare che, se J è un'involuzione ($J^2 = 1$), allora o f è antihermitiana, oppure si può sostituire f con ρf, $0 \neq \rho \in \Delta$, in modo che ρf sia hermitiana e J sia l'applicazione di aggiunzione rispetto a ρf. (Traccia: per ogni $v \in V$ l'applicazione $x \mapsto \sigma^{-1}(f(v, x))$ è una forma lineare, quindi esiste $v' \in V$ tale che $f(v, x) = \overline{f(x, v')}$ per $x \in V$. Mostrare che per ogni $u \in V$ l'applicazione $l\colon x \mapsto f(x, u)v$ appartiene a $\operatorname{End}_\Delta V$ e che il suo aggiunto rispetto a f è $y \mapsto \sigma^{-1}(f(v, y))u = f(y, v')u$. Dedurre da $J^2(l) = l$ che esiste $0 \neq \delta \in \Delta$ tale che $f(x, y) = \delta \overline{f(y, x)}$ per ogni $x, y \in V$. Mostrare che $\bar{\delta} = \delta^{-1}$ e che, se $\delta \neq -1$, per $\rho = \delta + 1$ la forma ρf è hermitiana e J è l'applicazione di aggiunzione rispetto a ρf.)

9. Osservare che il teorema di Wedderburn–Artin per gli anelli semplici ha la seguente formulazione matriciale: ogni anello semplice artiniano è isomorfo a un anello di matrici $M_n(\Delta')$, dove Δ' è un anello di divisione ($\Delta' \cong \Delta^{\mathrm{op}}$ con la notazione dell'enunciato del teorema). Dal teorema di isomorfismo segue che, per anelli di divisione Δ'_1, Δ'_2, l'isomorfismo $M_{n_1}(\Delta'_1) \cong M_{n_2}(\Delta'_2)$ implica $n_1 = n_2$ e $\Delta'_1 \cong \Delta'_2$. Mostrare che dal teorema di isomorfismo segue anche che gli automorfismi di $M_n(\Delta')$ hanno la forma $A \mapsto S({}^{\sigma}A)S^{-1}$, dove $S \in M_n(\Delta')$ è invertibile, σ è un automorfismo dell'anello di divisione dei coefficienti e ${}^{\sigma}A = (\sigma(\alpha_{ij}))$ per $A = (\alpha_{ij})$.

10. Formulare in termini matriciali i risultati degli esercizi 6–8.

4.5 Teoria della struttura delle algebre

In questo paragrafo estenderemo alle algebre su anelli commutativi la teoria della struttura degli anelli sviluppata nei primi quattro paragrafi del capitolo. Ci specializzeremo poi al caso delle algebre di dimensione finita su un campo.

Ricordiamo che un'algebra A su un anello commutativo K è un K-modulo (sinistro) e un anello tali che il modulo A e l'anello A hanno lo stesso gruppo additivo $(A, +, 0)$ e l'azione di K e la moltiplicazione dell'anello sono legate dalle relazioni

$$k(ab) = (ka)b = a(kb) \tag{28}$$

per $a, b \in A$, $k \in K$ (p. 44). Abbiamo l'omomorfismo di anelli

$$\varepsilon\colon k \longmapsto k1 \tag{29}$$

da K in A (p. 138). La sua immagine $K1 = \{k1 \mid k \in K\}$ è contenuta nel centro di A, e ka, per $k \in K$, $a \in A$, coincide con $(k1)a = a(k1)$. Viceversa, dati un anello R e un sottoanello K del suo centro, R diventa una K-algebra se, per $k \in K$ e $a \in R$, si prende come ka il prodotto nell'anello. Si osservi inoltre che gli anelli sono $\mathbb{Z}$-algebre, dove na, per $n \in \mathbb{Z}$ e $a \in R$, è il multiplo di a secondo l'intero n. Pertanto la teoria degli anelli è un caso particolare di quella delle algebre.

Gli esempi fondamentali di K-algebre sono le algebre $\mathrm{End}_K M$, dove M è un modulo sull'anello commutativo K. Per $k \in K$, $f \in \mathrm{End}_K M$, il prodotto kf è definito da $(kf)(x) = kf(x) = f(kx)$, $x \in M$ (p. 139). Se A è una K-algebra arbitraria, definiamo una *rappresentazione* di A come un omomorfismo di K-algebre da A in un'algebra $\mathrm{End}_K M$. Se ρ è una rappresentazione di A nel K-modulo M, poniamo $ax = \rho(a)x$ per $a \in A$, $x \in M$, così che M diventa un A-modulo oltre che un K-modulo. Poiché $\rho(ka) = k\rho(a)$ e $\rho(a)$ è un K-endomorfismo, si ha

$$k(ax) = (ka)x = a(kx) \tag{30}$$

per $k \in K$, $a \in A$, $x \in M$. Diamo dunque la seguente definizione.

Definizione 4.3. *Se A è un'algebra sull'anello commutativo K, un modulo (sinistro) per l'algebra A è un gruppo abeliano, scritto additivamente, che è simultaneamente un K-modulo (sinistro) e un modulo (sinistro) sull'anello A, in modo che valga la (30) per ogni $k \in K$, $a \in A$, $x \in M$.*

Se M è un modulo per A, otteniamo una rappresentazione ρ_M di A definendo $\rho_M(a)$, per $a \in A$, come l'applicazione $x \mapsto ax$. Essa appartiene a $\mathrm{End}_K M$, e $a \mapsto \rho_M(a)$ è un omomorfismo di algebre. Dalla (30) segue che $kx = (k1)x$. Pertanto, se M e N sono moduli per l'algebra A, ogni omomorfismo f da M in N come moduli sull'anello A è anche un K-omomorfismo. È chiaro

inoltre che ogni A-sottomodulo è anche un K-sottomodulo e dà luogo a un modulo quoziente M/N per l'algebra A nel senso della definizione 4.3. Se M è un modulo sull'anello A, si ottiene su M una struttura di K-modulo ponendo $kx = (k1)x$; vale la (30) e dunque M è un modulo per l'algebra A. L'algebra A stessa è un A-modulo nel quale A agisce per moltiplicazione a sinistra e K agisce come nella definizione di A. I sottomoduli sono gli ideali sinistri, che coincidono con gli ideali sinistri di A come anello. Per $k \in K$ e $f \in \hom_A(M, N)$, con M, N moduli per A, definiamo kf mediante $(kf)(x) = kf(x)$, $x \in M$. Tale applicazione appartiene a $\hom_A(M, N)$ e questa azione di K dà a $\hom_A(M, N)$ una struttura di modulo. È immediato che $\operatorname{End}_A M$ è un'algebra su K.

Possiamo ora trasferire alle algebre le definizioni e i risultati sul radicale, sulla primitività e sulla semiprimitività. Un'algebra si dice *primitiva* se ha una rappresentazione irriducibile fedele, e *semiprimitiva* se le rappresentazioni irriducibili sono sufficienti a distinguerne gli elementi. Il radicale è l'intersezione dei nuclei delle rappresentazioni irriducibili dell'algebra. I risultati dimostrati per gli anelli si trasferiscono parola per parola alle algebre. Abbiamo osservato che per un'algebra A su K gli ideali sinistri di A come anello sono anche ideali sinistri di A come algebra, e naturalmente vale il viceversa. Poiché in entrambi i casi il radicale di A è l'intersezione degli ideali sinistri massimali, $\operatorname{rad} A$ è lo stesso insieme con le stesse operazioni di addizione e moltiplicazione, sia che si consideri A come anello o come algebra. Analogamente A è primitiva (semiprimitiva) come algebra se e soltanto se lo è come anello.

La teoria della struttura e delle rappresentazioni degli anelli artiniani si trasferisce alle algebre. In particolare si applica alle algebre di dimensione finita su un campo, poiché ogni loro ideale sinistro è un sottospazio e vale la condizione delle catene discendenti per i sottospazi. Per il resto del paragrafo, salvo in alcuni esercizi, considereremo questo caso classico: A sarà un'algebra di dimensione finita su un campo F. Allora $\operatorname{rad} A$ è un ideale nilpotente che contiene ogni ideale unilatero nil di A. Se $\operatorname{rad} A = 0$, allora $A = A_1 \oplus A_2 \oplus \cdots \oplus A_s$, dove gli A_i sono ideali che sono algebre semplici. Se A è semplice, è isomorfa all'algebra delle trasformazioni lineari di uno spazio vettoriale M di dimensione finita su un'algebra di divisione Δ. Qui M è un qualunque modulo irriducibile per A, e Δ è l'algebra di divisione $\operatorname{End}_A M$ del lemma di Schur. Ricordiamo inoltre che si può prendere $M = A/I$, dove I è un ideale sinistro massimale di A, e che Δ è anti-isomorfa a B/I, dove B è l'idealizzatore di I (proposizione 4.7, p. 203). Dunque Δ è un'algebra di divisione di dimensione finita su F. Poiché, per M di dimensione n su Δ, $\operatorname{End}_\Delta M$ è anti-isomorfa a $M_n(\Delta)$ e quest'ultima è anti-isomorfa a $M_n(\Delta^{\mathrm{op}})$, si vede che A è un'algebra semplice di dimensione finita su F se e soltanto se è isomorfa a un'algebra $M_n(\Delta')$, dove Δ' è un'algebra di divisione di dimensione finita su F. Questi risultati furono dimostrati da Wedderburn nel 1908.

In BAI, pp. 451–454, abbiamo determinato le algebre di divisione di dimensione finita sui campi algebricamente chiusi, reali chiusi e finiti. Abbiamo dimostrato che, se F è algebricamente chiuso, F è la sola algebra di divisione di dimensione finita su F. Se F è reale chiuso, vi sono tre possibilità: (1) F, (2) $F(\sqrt{-1})$, (3) l'algebra dei quaternioni su F con base $(1, i, j, k)$ tale che $i^2 = -1 = j^2$ e $ij = k = -ji$. Se F è finito, per il teorema di Wedderburn le algebre di divisione di dimensione finita su F sono campi. Ne esiste una per ogni dimensione finita e due della stessa dimensione finita sono isomorfe (BAI, pp. 287–290). Combinando questi risultati con i teoremi di struttura si determinano completamente le algebre semisemplici di dimensione finita sui campi algebricamente chiusi, reali chiusi o finiti.

Anche i risultati sulle rappresentazioni degli anelli artiniani si applicano alle algebre di dimensione finita sui campi. Se A è semisemplice su F, ogni sua rappresentazione è completamente riducibile e si ha una corrispondenza biunivoca fra le classi di isomorfismo dei moduli irriducibili e le componenti semplici dell'algebra.

Possiamo applicare la teoria delle algebre allo studio di insiemi arbitrari di trasformazioni lineari di uno spazio vettoriale V di dimensione finita su un campo F. Dato un tale insieme S, indichiamo con $\operatorname{Env} S$ la sottoalgebra di $\operatorname{End}_F V$ generata da S. La chiamiamo *algebra inviluppante* di S. Evidentemente $\operatorname{Env} S$ consiste delle combinazioni lineari di 1 e dei prodotti $s_1 s_2 \cdots s_r$, $s_i \in S$, e $\dim \operatorname{Env} S \leq n^2$ per $n = \dim V$. L'inclusione in $\operatorname{End}_F V$ è una rappresentazione di $\operatorname{Env} S$. Tramite questa rappresentazione si può applicare la teoria delle algebre allo studio di S. Usiamo ora questo metodo e il teorema di densità per ottenere un teorema classico della teoria delle rappresentazioni dei gruppi.

Teorema di Burnside. *Sia G un monoide di trasformazioni lineari di uno spazio vettoriale V di dimensione finita su un campo algebricamente chiuso F. Si supponga che G agisca irriducibilmente su V, ossia che i soli sottospazi stabili per G siano V e 0. Allora G contiene una base di* $\operatorname{End}_F V$ *su F.*

Dimostrazione. Per ipotesi G contiene 1 ed è chiuso rispetto alla moltiplicazione. Allora $\operatorname{Env} G = FG$, l'insieme delle combinazioni F-lineari degli elementi di G. Inoltre V è un modulo irriducibile per $A = \operatorname{Env} G$ e $A' = \operatorname{End}_A V$ è un'algebra di divisione per il lemma di Schur. Evidentemente A' è il centralizzante di A in $\operatorname{End}_F V$, dunque è un'algebra di dimensione finita su F. Poiché F è algebricamente chiuso, $A' = F1$. Per il teorema di densità, $\operatorname{End}_{A'} V = A$. Pertanto $A = FG = \operatorname{End}_F V$. Ne segue che G contiene una base di $\operatorname{End}_F V$. □

Se S è un insieme arbitrario di trasformazioni lineari di V su F che agisce irriducibilmente, il teorema di Burnside si può applicare al sottomonoide G generato da S. Si ottiene che esiste una base di $\operatorname{End}_F V$ i cui elementi sono scelti fra 1 e i prodotti di elementi di S.

Esercizi

In questi esercizi A è un'algebra su un campo F. Negli esercizi 1–5 è ammesso che A abbia dimensione infinita; negli esercizi successivi tutti gli spazi vettoriali hanno dimensione finita.

1. Sia $a \in A$ e siano $\alpha_1, \ldots, \alpha_m$ elementi di F tali che $a - \alpha_i 1$ sia invertibile in A. Mostrare che a è algebrico su F oppure gli elementi $(a - \alpha_i 1)^{-1}$, $1 \leq i \leq m$, sono linearmente indipendenti su F.[8]

2. Sia A un'algebra di divisione con una base numerabile su un campo algebricamente chiuso non numerabile F (per esempio $F = \mathbb{C}$). Mostrare che $A = F$.

3. Sia A finitamente generata su un campo algebricamente chiuso non numerabile F e sia M un A-modulo irriducibile. Mostrare che $\operatorname{End}_A M = F$.

4. Mostrare che gli elementi di $\operatorname{rad} A$ sono nilpotenti oppure trascendenti su F.

5. Sia A finitamente generata su un campo non numerabile F. Mostrare che $\operatorname{rad} A$ è un ideale nil.

6. Si supponga che F contenga n radici n-esime distinte dell'unità e sia ε una di esse primitiva. Siano s e t le trasformazioni lineari dello spazio vettoriale V/F con base $(x_1, x_2, \ldots, x_n)$ le cui matrici rispetto a tale base sono, rispettivamente,

$$\sigma = \begin{pmatrix} 1 & & & & 0 \\ & \varepsilon & & & \\ & & \varepsilon^2 & & \\ & & & \ddots & \\ 0 & & & & \varepsilon^{n-1} \end{pmatrix}, \qquad \tau = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 1 & & & & 0 \end{pmatrix}.$$

[8] Per l'indipendenza lineare si intendono gli α_i a due a due distinti. [N.d.T.]

Verificare che $s^n = 1 = t^n$, $st = \varepsilon ts$ e $\mathrm{Env}\{s,t\} = \mathrm{End}_F V$. Siano u, v trasformazioni lineari di uno spazio vettoriale W/F tali che $u^n = 1 = v^n$ e $uv = \varepsilon vu$. Applicare la teoria delle rappresentazioni delle algebre semplici per mostrare che $\dim W = r \dim V$ e che esiste una base di W su F rispetto alla quale le matrici di u e v sono, rispettivamente, $\mathrm{diag}(\sigma, \ldots, \sigma)$ e $\mathrm{diag}(\tau, \ldots, \tau)$.

7. Se a è una trasformazione lineare di uno spazio vettoriale V su F con base $(x_1, \ldots, x_n)$ e $ax_i = \sum_j \alpha_{ij} x_j$, la traccia di a, $\mathrm{tr}\, a = \sum_i \alpha_{ii}$, è indipendente dalla scelta della base (BAI, p. 196). Inoltre $\mathrm{tr}\, a$ è la somma delle radici caratteristiche di a. Si ponga $t(a,b) = \mathrm{tr}(ab)$. Mostrare che $t(a,b)$ è una forma bilineare simmetrica non degenere su $\mathrm{End}_F V$ (BAI, p. 346).

8. Siano G, V, F come nel teorema di Burnside e si supponga finito l'insieme $\mathrm{tr}\, G = \{\mathrm{tr}\, a \mid a \in G\}$. Mostrare che G è finito e $|G| \leq |\mathrm{tr}\, G|^{n^2}$, con $n = \dim V$. (*Suggerimento.* Per il teorema di Burnside, G contiene una base $(a_1, \ldots, a_{n^2})$ di $\mathrm{End}_F V$. Considerare l'applicazione $a \mapsto (t(a,a_1), \ldots, t(a,a_{n^2}))$, dove $t(a,b) = \mathrm{tr}(ab)$ come nell'esercizio 7.)

9. Una trasformazione lineare si dice *unipotente* se è della forma $1 + z$, con z nilpotente. Sia G un monoide di trasformazioni lineari unipotenti di uno spazio vettoriale V di dimensione finita su un campo algebricamente chiuso F. Dimostrare il teorema di Kolchin: V ammette una base rispetto alla quale la matrice di ogni $a \in G$ ha la forma

$$\begin{pmatrix} 1 & & & * \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}.$$

(*Suggerimento.* Si prenda una serie di composizione $V = V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_{r+1} = 0$ di V come $A = FG$-modulo e si applichi l'esercizio 7 alle trasformazioni indotte nei moduli irriducibili V_i/V_{i+1}.) Estendere il teorema a un campo base F arbitrario.

10. (Burnside.) Sia G un gruppo di trasformazioni lineari di uno spazio vettoriale V di dimensione finita su un campo algebricamente chiuso F. Si supponga che esista un intero m, non divisibile per la caratteristica di F, tale che $a^m = 1$ per ogni $a \in G$. Dimostrare che G è finito. (*Suggerimento.* Se G agisce irriducibilmente, il risultato segue dall'esercizio 8. Altrimenti esiste un sottospazio $U \neq 0, V$ stabile per G. Procedere per induzione sulla dimensione per concludere che i gruppi di trasformazioni indotti su U e V/U sono finiti. Siano K_1, K_2 i nuclei degli omomorfismi da G sui gruppi indotti su U e V/U. Allora K_1 e K_2, e quindi $K_1 \cap K_2$, hanno indice finito in G. Mostrare infine che $K_1 \cap K_2 = 1$.)

4.6 Algebre semplici centrali di dimensione finita

Un'algebra A su un campo F si dice *centrale* se il suo centro è $C = F1 = \{\alpha 1 \mid \alpha \in F\}$. Se A è un'algebra semplice di dimensione finita su F, si ha $A \simeq M_n(\Delta)$, dove Δ è un'algebra con divisione di dimensione finita su F. Il centro C di A è isomorfo al centro di Δ, ed è dunque un campo (cfr. l'esercizio 2, p. 209). Possiamo ora considerare A come algebra su C. In questo modo A diventa un'algebra semplice centrale di dimensione finita su C. Vedremo in questo paragrafo e nel successivo che la classe delle algebre semplici centrali di dimensione finita ha alcune proprietà notevoli. Per ricavarle ci converrà raccogliere anzitutto alcuni semplici risultati sui prodotti tensoriali di moduli e di algebre su campi, che ci occorreranno nella parte principale della trattazione.

Osserviamo anzitutto che ogni F-modulo (ossia spazio vettoriale su F), essendo libero, è proiettivo, e quindi piatto (p. 154). Se dunque $i\colon V' \to V$ è un'applicazione lineare iniettiva di F-moduli, $i \otimes 1$ e $1 \otimes i$ sono applicazioni iniettive rispettivamente di $V' \otimes U$ in $V \otimes U$ e di $U \otimes V'$ in $U \otimes V$, per ogni F-modulo U. Se $\{x_\alpha \mid \alpha \in I\}$ è una base di V su F, ogni elemento di $U \otimes V$ si scrive in uno e un solo modo come somma finita $\sum a_{\alpha_i} \otimes x_{\alpha_i}$, con $a_{\alpha_i} \in U$ e indici distinti. È chiaro che una tale scrittura esiste, poiché ogni elemento di $U \otimes V$ ha la forma $\sum a_j \otimes b_j$, con $a_j \in U$, $b_j \in V$. L'unicità segue dall'isomorfismo

$$U \otimes V = U \otimes \bigoplus_\alpha Fx_\alpha \simeq \bigoplus_\alpha (U \otimes Fx_\alpha)$$

(proposizione 3.3, p. 131), per il quale $\sum a_{\alpha_i} \otimes x_{\alpha_i} = 0$ implica $a_{\alpha_i} \otimes x_{\alpha_i} = 0$ per ogni i. Gli isomorfismi $U \otimes Fx_\alpha \simeq U \otimes F \simeq U$ mostrano poi che $a_\alpha \otimes x_\alpha = 0$ se e soltanto se $a_\alpha = 0$. Analogamente, se $\{y_\beta \mid \beta \in J\}$ è una base di U, ogni elemento di $U \otimes V$ si scrive in uno e un solo modo come $\sum y_{\beta_j} \otimes b_j$, con $b_j \in V$. È anche chiaro che, se $\{x_\alpha \mid \alpha \in I\}$ è una base di V e $\{y_\beta \mid \beta \in J\}$ una base di U, allora $\{y_\beta \otimes x_\alpha \mid \beta \in J,\ \alpha \in I\}$ è una base di $U \otimes V$. Dunque $[U \otimes V : F] = [U : F][V : F]$.

Se A e B sono algebre sul campo F, $A \otimes B$ contiene le sottoalgebre $1 \otimes B = \{1 \otimes b \mid b \in B\}$ e $A \otimes 1 = \{a \otimes 1 \mid a \in A\}$. Le applicazioni $b \mapsto 1 \otimes b$ e $a \mapsto a \otimes 1$ le identificano rispettivamente con B e con A. Possiamo così identificare B con la sottoalgebra $1 \otimes B$ e A con la sottoalgebra $A \otimes 1$ di $A \otimes B$. Scrivendo a per $a \otimes 1$ e b per $1 \otimes b$, abbiamo $ab = ba$ e $A \otimes B = AB = BA$. Dimostreremo ora il seguente risultato, che dà in sostanza caratterizzazioni interne dei prodotti tensoriali di algebre su un campo.

Proposizione 4.8. *Se A e B sono sottoalgebre di un'algebra D su un campo F, allora $D = A \otimes_F B$ se valgono le seguenti condizioni.*

(1) *$ab = ba$ per ogni $a \in A$, $b \in B$.*

(2) *Esiste una base (x_α) di A tale che ogni elemento di D si possa scrivere in uno e un solo modo come $\sum b_i x_{\alpha_i}$, con $b_i \in B$.*

Se D ha dimensione finita, si può sostituire la condizione (2) con

$$(2') \qquad D = AB, \qquad [D : F] = [A : F][B : F].$$

Dimostrazione. La prima condizione assicura l'esistenza di un omomorfismo di algebre di $A \otimes B$ in D tale che $a \otimes b \mapsto ab$, per $a \in A$, $b \in B$ (p. 144). La seconda condizione garantisce che esso è biiettivo, e dunque un isomorfismo. Se D ha dimensione finita, l'implicazione $(2') \Rightarrow (2)$ è immediata. □

Come prima applicazione di questo criterio dimostriamo la proposizione seguente.

Proposizione 4.9. *Se B è un'algebra su F, allora $M_n(B) \simeq M_n(F) \otimes_F B$.*

Dimostrazione. Si applichi il criterio alle sottoalgebre $M_n(F)$ e $B1 = \{b1 \mid b \in B\}$, dove

$$b1 = \begin{pmatrix} b & & & 0 \\ & b & & \\ & & \ddots & \\ 0 & & & b \end{pmatrix}.$$

Se $\{e_{ij} \mid 1 \le i, j \le n\}$ è l'usuale base di unità matriciali di $M_n(F)$, si ha $(b1)e_{ij} = e_{ij}(b1)$. Vale dunque la condizione (1). Inoltre $(b1)e_{ij}$ è la matrice che ha b nella posizione (i, j) e zeri altrove. Ne segue la condizione (2). □

Dimostriamo ora la proposizione seguente.

Proposizione 4.10. $M_m(F) \otimes M_n(F) \simeq M_{mn}(F)$.

Dimostrazione. Basta applicare il criterio alle sottoalgebre costituite, rispettivamente, dalle matrici

$$\begin{pmatrix} b & & 0 \\ & b & \\ & \ddots & \\ 0 & & b \end{pmatrix}, \qquad b \in M_m(F),$$

e dalle matrici

$$\begin{pmatrix} \alpha_{11}1_m & \cdots & \alpha_{1n}1_m \\ \vdots & & \vdots \\ \alpha_{n1}1_m & \cdots & \alpha_{nn}1_m \end{pmatrix}, \qquad \alpha_{ij} \in F.$$

Lasciamo i particolari al lettore. □

Se A è un'algebra qualsiasi, poniamo $A^e = A \otimes_F A^{\mathrm{op}}$ e chiamiamo questa l'*algebra inviluppante* di A. Se A è una sottoalgebra di un'altra algebra B, si ha su B un'azione naturale di A^e definita da

$$\Big(\sum a_i \otimes b_i\Big) y = \sum a_i y b_i, \tag{31}$$

dove $a_i \in A$, $b_i \in A^{\mathrm{op}}$, $y \in B$. Dalla proprietà universale del prodotto tensoriale risulta che, per y fissato, abbiamo un omomorfismo di A^e in B tale che $\sum a_i \otimes b_i \mapsto \sum a_i y b_i$. La (31) è dunque ben definita. Una verifica diretta mostra che essa definisce una struttura di modulo. In particolare abbiamo su A un'azione di A^e. I sottomoduli di A come A^e-modulo sono gli ideali di A. Dunque, se A è semplice, A è A^e-irriducibile. Ricordiamo che gli endomorfismi di A, considerata nel modo naturale come A-modulo sinistro (rispettivamente destro), sono le moltiplicazioni a destra $x \mapsto xa$ (rispettivamente a sinistra $x \mapsto ax$). Ne segue che $\mathrm{End}_{A^e} A$ è l'insieme delle applicazioni che sono al tempo stesso moltiplicazioni a sinistra e a destra, $x \mapsto cx = xd$. Ponendo $x = 1$ si ottiene $d = c$, sicché $\mathrm{End}_{A^e} A$ è l'insieme delle applicazioni $x \mapsto cx$ con c nel centro. Se A è centrale, si tratta delle applicazioni $x \mapsto (\alpha 1)x = \alpha x$, $\alpha \in F$. Applichiamo queste osservazioni per dimostrare il nostro primo teorema fondamentale sulle algebre semplici centrali di dimensione finita.

Teorema 4.6. *Se A è un'algebra semplice centrale di dimensione finita su un campo F, allora $A^e = A \otimes_F A^{\mathrm{op}} \simeq M_n(F)$, dove $n = \dim A$.*

Dimostrazione. Consideriamo A come A^e-modulo nel modo appena descritto. Allora A è irriducibile e $\mathrm{End}_{A^e} A = F$. Inoltre A ha dimensione finita su F. Per il teorema di densità, A^e si applica dunque su $\mathrm{End}_F A$. Poiché A^e ed $\mathrm{End}_F A$ hanno entrambe dimensione n^2, si ha un isomorfismo di A^e su $\mathrm{End}_F A$. La tesi segue da $\mathrm{End}_F A \simeq M_n(F)$. □

Vediamo ora come un'algebra semplice centrale A di dimensione finita sia situata in una qualsiasi algebra B (anche di dimensione infinita) che la contenga come sottoalgebra. Si ha il seguente risultato.

Teorema 4.7. *Sia A una sottoalgebra semplice centrale di dimensione finita di un'algebra B. Allora $B = A \otimes_F C$, dove C è il centralizzante di A in B. L'applicazione $I \mapsto AI$ è una biiezione dall'insieme degli ideali di C all'insieme degli ideali di B. Inoltre il centro di B coincide con il centro di C.*

Dimostrazione. Consideriamo B come A^e-modulo nel modo già descritto. Per il teorema precedente A^e è semplice. Dunque B è somma diretta di A^e-moduli irriducibili, tutti isomorfi ad A, poiché A è A^e-irriducibile e due A^e-moduli irriducibili qualsiasi sono isomorfi. Osserviamo

ora che il generatore 1 di A come A^e-modulo soddisfa $(a \otimes 1)1 = a1 = 1a = (1 \otimes a)1$, e che $(a \otimes 1)1 = 0$ implica $a = 0$. In ogni A^e-modulo irriducibile possiamo dunque scegliere un c tale che $(a \otimes 1)c = (1 \otimes a)c$ e che $(a \otimes 1)c = 0$ implichi $a = 0$. Applicando ciò a B come A^e-modulo, vediamo che possiamo scrivere $B = \bigoplus_\alpha Ac_\alpha$, dove $ac_\alpha = c_\alpha a$ per ogni $a \in A$ e $ac_\alpha = 0$ implica $a = 0$. Allora $c_\alpha \in C$ e ogni elemento di B si scrive in uno e un solo modo come somma finita $\sum a_\alpha c_\alpha$, con $a_\alpha \in A$. Se $c \in C$, abbiamo $c = \sum a_\alpha c_\alpha$ e $ac = ca$ implica $aa_\alpha = a_\alpha a$. Ne segue che ogni a_α appartiene a $F1$ e $c \in \sum Fc_\alpha$. Dunque $C = \sum Fc_\alpha$ e $\{c_\alpha\}$ è una base di C. Dalla proposizione 4.8 risulta ora che $A \otimes_F C = B$.

Sia ora I un ideale di C. Allora AI è un ideale di $B = AC$. Inoltre $AI \cap C = I$. Infatti, se $(x_1 = 1, x_2, \ldots, x_n)$ è una base di A, dall'isomorfismo canonico di $A \otimes_F C$ su B (p. 144) segue che ogni elemento di B si scrive in uno e un solo modo come $\sum c_i x_i$, con $c_i \in C$. Gli elementi di AI hanno la forma $\sum d_i x_i$, con $d_i \in I$; se un tale elemento appartiene a C, esso ha anche la forma $c_1 x_1$, con $c_1 \in C$. Ne segue che $C \cap AI$ è l'insieme degli elementi $d_1 x_1 = d_1 \in I$. Dunque $C \cap AI = I$, e l'applicazione $I \mapsto AI$ dagli ideali di C agli ideali di B è iniettiva. Per vederne la suriettività, sia I' un ideale qualsiasi di B. Allora I' è un sottomodulo di B come A^e-modulo. Dunque $I' = \sum Ad_\beta$, con $d_\beta \in I = I' \cap C$, e pertanto $I' = AI$. Così $I \mapsto AI$ è anche suriettiva.

Resta da provare che il centro di B è il centro di C. Il centro di B è contenuto in C, e perciò nel centro di C. D'altra parte, se c appartiene al centro di C, commuta con ogni elemento di $B = AC$ e appartiene quindi al centro di B. □

Dal teorema precedente segue che B è semplice se e soltanto se C è semplice, e che B è centrale se e soltanto se C è centrale. Il teorema si può applicare ai prodotti tensoriali nei quali uno dei fattori sia semplice centrale di dimensione finita. Sia dunque $B = A \otimes_F C$, con A semplice centrale di dimensione finita. Identifichiamo A e C con le corrispondenti sottoalgebre $A \otimes 1$ e $1 \otimes C$ di $A \otimes C$. Affermiamo che C è il centralizzante di A in B. Sia infatti $\{y_\beta\}$ una base di C su F. Ogni elemento di B si scrive in uno e un solo modo come $b = \sum a_\beta y_\beta$, con $a_\beta \in A$. Per $a \in A$ l'uguaglianza $ab = ba$ equivale ad $aa_\beta = a_\beta a$ per ogni a_β. Ne segue che b commuta con ogni $a \in A$ se e soltanto se $b = \sum \gamma_\beta y_\beta$, con $\gamma_\beta \in F$, ossia se e soltanto se $b \in C$. Il teorema 4.7 dà ora il seguente corollario.

Corollario 1. *Sia A un'algebra semplice centrale di dimensione finita su F e sia C un'algebra qualsiasi su F. Allora $I \mapsto A \otimes_F I$ è una biiezione dall'insieme degli ideali di C all'insieme degli ideali di $B = A \otimes_F C$. Inoltre il centro di B coincide con il centro di C, identificato con la corrispondente sottoalgebra di B.*

Un importante caso particolare è il seguente.

Corollario 2. *Sia A un'algebra semplice centrale di dimensione finita su F e sia C un'algebra qualsiasi su F. Allora $A \otimes_F C$ è semplice se C è semplice ed è centrale se C è centrale.*

Iterando il corollario 2 si ottiene la seguente conseguenza.

Corollario 3. *Il prodotto tensoriale $A_1 \otimes_F A_2 \otimes_F \cdots \otimes_F A_r$ di un numero finito di algebre semplici centrali di dimensione finita è semplice centrale di dimensione finita.*

Hanno particolare interesse i prodotti tensoriali in cui uno dei fattori è un campo di estensione E del campo base F. Se A è un'algebra qualsiasi su F, si può considerare $A \otimes_F E$ come algebra su E. Questa algebra su E si denota con A_E e si dice *ottenuta da A estendendo il campo base a E* (si veda l'esercizio 13, p. 148). Se (x_α) è una base di A su F, identificando A con $A \otimes 1$ in A_E possiamo dire che (x_α) è una base di A_E su E. La dimensione di A su F è dunque la stessa di A_E su E. Ne segue anche che, se K è un campo di estensione di E, allora $(A_E)_K = A_K$. Se B è una seconda algebra su F con base (y_β), l'algebra $A \otimes_F B$ ha per base su F la famiglia $(x_\alpha y_\beta) = (x_\alpha \otimes y_\beta)$, che è anche una base su E di $(A \otimes_F B)_E$ e di $A_E \otimes_E B_E$. Se ne deduce che $(A \otimes_F B)_E \simeq A_E \otimes_E B_E$. (Risultati più generali sono indicati nell'esercizio 13, p. 148.)

Se A è semplice centrale di dimensione finita su F, il corollario 2 al teorema 4.7 mostra che A_E è semplice centrale di dimensione finita su E. Ricordiamo inoltre che $M_n(F)$ è semplice centrale di dimensione finita su F. Queste algebre sono gli esempi più semplici di algebre semplici centrali. Diamo ora la definizione seguente.

Definizione 4.4. *L'algebra di matrici $M_n(F)$ si dice un'algebra semplice centrale* spezzata *su F. Se A è semplice centrale di dimensione finita su F, un campo di estensione E di F si dice un* campo di spezzamento *di A se A_E è spezzata su E, ossia se $A_E \simeq M_n(E)$ per qualche n.*

È evidente che ogni campo di estensione di F è un campo di spezzamento di $M_n(F)$ e che, se E è un campo di spezzamento di A e di B, è anche un campo di spezzamento dell'algebra semplice centrale $A \otimes_F B$. Infatti da $A_E \simeq M_n(E)$ e $B_E \simeq M_m(E)$ segue

$$(A \otimes_F B)_E \simeq A_E \otimes_E B_E \simeq M_n(E) \otimes_E M_m(E) \simeq M_{nm}(E).$$

Osserviamo inoltre che, se E è un campo di spezzamento di A, lo è anche di A^{op}. Infatti $(A^{\mathrm{op}})_E = (A_E)^{\mathrm{op}} \simeq M_n(E)^{\mathrm{op}}$, e poiché $M_n(E)$ ammette un antiautomorfismo, $M_n(E)^{\mathrm{op}} \simeq M_n(E)$. Se $A \simeq M_r(B)$, dove B è semplice centrale su F, E è un campo di spezzamento di A se e soltanto se lo è di B. Abbiamo $A_E \simeq M_r(B_E)$, poiché $M_r(B) \simeq M_r(F) \otimes_F B$ e

$$M_r(B)_E \simeq M_r(F)_E \otimes_E B_E \simeq M_r(B_E).$$

Ora $B_E \simeq M_s(\Delta)$, dove Δ è un'algebra con divisione centrale su E. Allora $A_E \simeq M_{rs}(\Delta)$. Se E spezza A (ossia è un campo di spezzamento di A), abbiamo $A_E \simeq M_n(E)$ e quindi $M_n(E) \simeq M_{rs}(\Delta)$, da cui $rs = n$ e $\Delta \simeq E$. Allora $B_E \simeq M_s(E)$ ed E spezza B. L'implicazione inversa è chiara per la proposizione 4.10. In particolare, se $A = M_r(\Delta)$ e Δ è un'algebra con divisione centrale su F, allora E spezza A se e soltanto se spezza Δ. Basta dunque considerare i campi di spezzamento delle algebre con divisione centrali. Osserviamo infine che ogni campo di estensione K di un campo di spezzamento è a sua volta un campo di spezzamento. Ciò è chiaro, poiché $(A_E)_K \simeq A_K$ e $M_n(E)_K \simeq M_n(K)$.

Se E è un campo di estensione algebricamente chiuso di F, le uniche algebre semplici di dimensione finita su E sono le algebre $M_n(E)$ (p. 213). Pertanto ogni campo di estensione algebricamente chiuso E di F è un campo di spezzamento di ogni algebra semplice centrale di dimensione finita su F. Vedremo più avanti che ogni campo si può immergere in un campo algebricamente chiuso (ğ 8.1). Una volta acquisito quel risultato, esso dimostra l'esistenza di campi di spezzamento per le algebre semplici centrali di dimensione finita.

Dimostreremo ora l'esistenza di campi di spezzamento di dimensione finita per ogni algebra semplice centrale A di dimensione finita. Scrivendo $A = M_n(\Delta)$, dove Δ è un'algebra con divisione centrale di dimensione finita, mostreremo che ogni sottocampo massimale di Δ è un campo di spezzamento. Ciò seguirà dal risultato che segue, che preciseremo nel teorema 4.12.

Teorema 4.8. *Sia Δ un'algebra con divisione centrale di dimensione finita su F. Un campo di estensione E di dimensione finita su F è un campo di spezzamento di Δ se e soltanto se E è un sottocampo di un'algebra $A = M_r(\Delta)$ tale che il centralizzante $C_A(E)$ coincida con E.*

Dimostrazione. Supponiamo soddisfatta la condizione enunciata, ossia che E sia un sottocampo di $A = M_r(\Delta)$ con $C_A(E) = E$. Possiamo identificare A con $\mathrm{End}_{\Delta'} V$, dove V è uno spazio vettoriale di dimensione r su $\Delta' = \Delta^{\mathrm{op}}$. Allora V è un $\Delta' \otimes_F E$-modulo tale che $(d \otimes e)x = dex = edx$ per $d \in \Delta'$, $e \in E \subseteq A$. Poiché $\Delta' \otimes_F E$ è semplice, la sua rappresentazione in V è fedele e possiamo identificare $\Delta' \otimes_F E$ con il corrispondente anello di endomorfismi di V. Poiché $\Delta' \otimes_F E$ è semplice di dimensione finita su F, V è completamente riducibile come $\Delta' \otimes_F E$-modulo, e possiamo applicare il teorema di densità. Ora $\mathrm{End}_{\Delta'} V = A$, sicché $\mathrm{End}_{\Delta' \otimes E} V$ è il centralizzante di E in A. Per ipotesi esso è E. Lo spazio V ha dimensione finita su F, poiché

ha dimensione finita su Δ' e Δ' ha dimensione finita su F. Dunque V ha dimensione finita su E. Per il teorema di densità, $\Delta' \otimes_F E$ è pertanto isomorfa all'intera algebra delle trasformazioni lineari di V su E. Se $[V : E] = n$, allora $\Delta' \otimes_F E \simeq M_n(E)$. Dunque E è un campo di spezzamento di Δ' su F, e quindi di Δ su F.

Viceversa, supponiamo che $\Delta \otimes_F E \simeq M_n(E)$. Allora anche $\Delta' \otimes_F E \simeq M_n(E)$. Sia V un modulo irriducibile su $\Delta' \otimes_F E$. Poiché $\Delta' \otimes_F E \simeq M_n(E)$, V è uno spazio vettoriale di dimensione n su E e possiamo identificare $\Delta' \otimes_F E$ con $\mathrm{End}_E V$. Inoltre V è uno spazio vettoriale su Δ'. Sia $[V : \Delta'] = r$. Poiché E centralizza Δ', abbiamo $E \subseteq \mathrm{End}_{\Delta'} V$. Il centralizzante di E in $\mathrm{End}_{\Delta'} V$ è contenuto nel centralizzante di $\Delta' \otimes E$ in $\mathrm{End}_E V$. Poiché $\Delta' \otimes E = \mathrm{End}_E V$, questo è E. Pertanto $C_{\mathrm{End}_{\Delta'} V}(E) = E$ e $C_{M_r(\Delta)}(E) = E$. □

Poiché $[\Delta : F] < \infty$, l'esistenza di un sottocampo massimale di Δ è chiara. Abbiamo ora il seguente corollario, che dimostra l'esistenza di campi di spezzamento di dimensione finita per ogni algebra semplice centrale di dimensione finita.

Corollario. *Sia A semplice centrale di dimensione finita su F e sia $A = M_r(\Delta)$, dove Δ è un'algebra con divisione. Allora ogni sottocampo massimale E di Δ è un campo di spezzamento di A.*

Dimostrazione. Basta mostrare che E è un campo di spezzamento di Δ. Poniamo $E' = C_\Delta(E)$. Allora $E' \supseteq E$ e, se $E' \neq E$, possiamo scegliere $c \in E' \setminus E$. L'algebra con divisione generata da E e da c è commutativa, ed è quindi un sottocampo di Δ che contiene propriamente E, contro la massimalità di E. Dunque $C_\Delta(E) = E$. Per il teorema 4.8, con $A = \Delta$, E è perciò un campo di spezzamento. □

Se E è un campo di spezzamento di A, sicché $A_E \simeq M_n(E)$, allora $[A : F] = [A_E : E] = [M_n(E) : E] = n^2$. Vediamo dunque che la dimensione di ogni algebra semplice centrale di dimensione finita è un quadrato. La radice quadrata n di questa dimensione si chiama *grado* di A.

Dimostreremo ora un importante teorema sul prolungamento degli omomorfismi.

Teorema 4.9. *Sia A una sottoalgebra semplice di un'algebra semplice centrale B di dimensione finita. Allora ogni omomorfismo di A in B si può prolungare a un automorfismo interno di B.*

Dimostrazione. Formiamo l'algebra $E = A \otimes_F B^{\mathrm{op}}$, che è semplice e di dimensione finita. Ogni E-modulo è completamente riducibile, e due E-moduli irriducibili qualsiasi sono isomorfi. Ne segue che due E-moduli aventi la stessa dimensione finita su F sono isomorfi. Diamo ora a B due strutture di E-modulo. Nella prima l'azione è $(\sum a_i \otimes b_i)x = \sum a_i x b_i$, nella seconda è $(\sum a_i \otimes b_i)x = \sum f(a_i) x b_i$, dove f è l'omomorfismo dato di A in B. È chiaro che entrambe le azioni definiscono strutture di modulo e che i due moduli sono isomorfi. Esiste pertanto una trasformazione F-lineare biiettiva l di B tale che

$$\sum a_i l(x) b_i = l\Big(\sum f(a_i) x b_i\Big) \tag{32}$$

per ogni $a_i \in A$, $x, b_i \in B$. In particolare, $l(x)b = l(xb)$ per ogni $x, b \in B$. Ne segue che l ha la forma $x \mapsto dx$, dove d è un elemento invertibile di B. Abbiamo anche $al(x) = l(f(a)x)$ per ogni $a \in A$, $x \in B$. Allora $adx = df(a)x$. Ponendo $x = 1$ otteniamo $f(a) = d^{-1}ad$. Si può dunque prolungare f all'automorfismo interno $b \mapsto d^{-1}bd$ di B. □

Prendendo $A = B$ nel teorema 4.9 si ottiene l'importante corollario seguente.[9]

Corollario (Skolem–Noether). *Ogni automorfismo di un'algebra semplice centrale di dimensione finita è interno.*

[9] L'originale reca $A = F1$. Per dedurre il corollario dal teorema 4.9 si prende $A = B$. [N.d.T.]

Dimostriamo ora un importante teorema del doppio centralizzante per le algebre semplici centrali.

Teorema 4.10. *Sia A una sottoalgebra semisemplice di un'algebra semplice centrale B di dimensione finita. Allora il doppio centralizzante soddisfa $C_B(C_B(A)) = A$.*

Dimostrazione. Consideriamo l'algebra $B \otimes B^{\mathrm{op}}$ e la sua sottoalgebra $A \otimes B^{\mathrm{op}}$. Identificando B con $B \otimes 1$, si vede facilmente, come nella dimostrazione del teorema 4.7, che $B \cap (A \otimes B^{\mathrm{op}}) = A$. Consideriamo ora B come $B \otimes B^{\mathrm{op}}$-modulo nel modo consueto. Per la dimostrazione del teorema 4.6, l'algebra $B \otimes B^{\mathrm{op}}$ è isomorfa all'algebra delle trasformazioni F-lineari di B della forma $x \mapsto \sum b_i x b_i'$, con $b_i, b_i' \in B$. L'uguaglianza $B \cap (A \otimes B^{\mathrm{op}}) = A$ implica dunque che, se una trasformazione lineare di B ha al tempo stesso la forma $x \mapsto \sum a_i x b_i$, con $a_i \in A$, $b_i \in B$, e la forma $x \mapsto bx$, $b \in B$, allora $b = a \in A$. Consideriamo ora l'algebra $A \otimes B^{\mathrm{op}}$. Affermiamo che è semisemplice. Scriviamo infatti $A = A_1 \oplus \cdots \oplus A_s$, dove gli A_i sono ideali semplici. Allora

$$A \otimes B^{\mathrm{op}} = (A_1 \otimes B^{\mathrm{op}}) \oplus \cdots \oplus (A_s \otimes B^{\mathrm{op}})$$

e ciascun $A_i \otimes B^{\mathrm{op}}$ è un ideale di $A \otimes B^{\mathrm{op}}$. Poiché A_i è semplice e B^{op} è semplice centrale di dimensione finita, $A_i \otimes B^{\mathrm{op}}$ è semplice per il corollario 2 di p. 219. Così $A \otimes B^{\mathrm{op}}$ è una somma diretta di ideali che sono algebre semplici, ed è quindi semisemplice. Consideriamo ora B come $A \otimes B^{\mathrm{op}}$-modulo restringendo l'azione di $B \otimes B^{\mathrm{op}}$ alla sottoalgebra $A \otimes B^{\mathrm{op}}$. Poiché $A \otimes B^{\mathrm{op}}$ è semisemplice, B è completamente riducibile come modulo su $E = A \otimes B^{\mathrm{op}}$. Consideriamo $E' = \mathrm{End}_E B$. Tenendo presente che gli endomorfismi di B come B-modulo destro sono le moltiplicazioni a sinistra, vediamo che E' è l'insieme delle applicazioni $x \mapsto cx$, con $c \in C_B(A)$. Poiché B ha dimensione finita su F ed è completamente riducibile come $A \otimes B^{\mathrm{op}}$-modulo, dal teorema di densità segue che $\mathrm{End}_{E'} B$ è l'insieme delle applicazioni $x \mapsto \sum a_i x b_i$, con $a_i \in A$, $b_i \in B$.

Sia ora $c' \in C_B(C_B(A))$. Allora $x \mapsto c'x$ commuta con $x \mapsto cx$ per $c \in C_B(A)$ e con $x \mapsto xb$ per $b \in B$. Ne segue che $x \mapsto c'x$ appartiene a $\mathrm{End}_{E'} B$. Pertanto $x \mapsto c'x$ ha anche la forma $x \mapsto \sum a_i x b_i$, con $a_i \in A$, $b_i \in B$. Abbiamo visto che questo implica $c' \in A$. Abbiamo così dimostrato $C_B(C_B(A)) \subseteq A$. Poiché l'inclusione $A \subseteq C_B(C_B(A))$ è evidente, si ha $C_B(C_B(A)) = A$. □

Il risultato precedente non ci dà informazioni sulla struttura delle varie algebre che intervengono nella dimostrazione, né sulle loro relazioni. Esamineremo ora la questione e, per semplicità, ci limiteremo al caso più interessante, quello in cui A è una sottoalgebra semplice dell'algebra semplice centrale B. L'estensione al caso di A semisemplice si ottiene agevolmente e sarà indicata negli esercizi.

Supponiamo A semplice. Allora $E = A \otimes B^{\mathrm{op}}$ è semplice, e quindi $E \simeq M_r(\Delta)$, dove Δ è un'algebra con divisione. Poniamo $d = [\Delta : F]$. Abbiamo

$$[E : F] = [A : F][B : F] = r^2 d. \tag{33}$$

Se $\{e_{ij} \mid 1 \leq i, j \leq r\}$ è l'usuale insieme di unità matriciali di $M_r(\Delta)$, è chiaro che $\Delta \simeq e_{11} M_r(\Delta) e_{11}$, che è precisamente l'insieme delle matrici aventi un elemento di Δ nella posizione $(1, 1)$ e zeri altrove. Inoltre $M_r(\Delta)$ è somma diretta degli r ideali sinistri minimali $M_r(\Delta)e_{ii}$, i quali sono moduli isomorfi sull'algebra $M_r(\Delta)$. Ciascuno di questi moduli irriducibili ha dimensione $r^2 d/r = rd$ su F. Consideriamo B come modulo su $E = A \otimes B^{\mathrm{op}}$. Poiché E è semplice, B, come E-modulo, è somma diretta di un certo numero s di sottomoduli irriducibili, tutti isomorfi a ideali sinistri minimali di E. Poiché $E \simeq M_r(\Delta)$, ogni E-modulo irriducibile ha dimensione rd su F. Abbiamo pertanto

$$[B : F] = srd. \tag{34}$$

Dalle (33) e (34) vediamo che $s \mid r$ e

$$[A : F] = r/s. \tag{35}$$

Consideriamo ora $C_B(A) \simeq E' = \mathrm{End}_E B$. Poiché B è somma diretta di s moduli irriducibili su E e questi sono isomorfi a ideali sinistri minimali Ee di E, con $e^2 = e$, possiamo determinare la struttura di $\mathrm{End}_E B$, e dunque di $C_B(A)$, mediante il lemma seguente.

Lemma. *Sia e un idempotente non nullo di un'algebra E. Sia $I = Ee$ e sia $I^{(s)}$ la somma diretta di s copie di I. Allora $\mathrm{End}_E I^{(s)}$ è isomorfa a $M_s((eEe)^{\mathrm{op}})$.*

Dimostrazione. Per il lemma 2 di p. 198, $\mathrm{End}_E I^{(s)}$ è costituita dalle applicazioni $(u_1, \ldots, u_s) \mapsto (v_1, \ldots, v_s)$ in cui $v_i = \sum_j a'_{ij} u_j$ e $a'_{ij} \in \mathrm{End}_E I$. Ne risulta un'applicazione $(a'_{ij}) \mapsto \eta((a'_{ij}))$ di $M_s(\mathrm{End}_E I)$ in $\mathrm{End}_E I^{(s)}$. Una verifica diretta mostra che è un isomorfismo. Consideriamo ora $\mathrm{End}_E I = \mathrm{End}_E Ee$. Come nella dimostrazione del lemma (1) di p. 180, $\mathrm{End}_E Ee$ è l'insieme delle applicazioni $ae \mapsto aebe$, $a, b \in E$. Si ottiene così un'applicazione di eEe in $\mathrm{End}_E Ee$ che associa a ebe l'applicazione $\eta(ebe)\colon ae \mapsto aebe$. Una verifica diretta mostra che si tratta di un anti-isomorfismo. Dunque $\mathrm{End}_E I \simeq (eEe)^{\mathrm{op}}$ ed $\mathrm{End}_E I^{(s)} \simeq M_s((eEe)^{\mathrm{op}})$. □

Applicando il lemma a B come E-modulo, vediamo che

$$\mathrm{End}_E B \simeq M_s((e_{11} M_r(\Delta) e_{11})^{\mathrm{op}}) \simeq M_s(\Delta^{\mathrm{op}}).$$

Dunque $C_B(A) \simeq M_s(\Delta^{\mathrm{op}})$ e

$$[C_B(A) : F] = s^2 d. \tag{36}$$

Allora

$$[A : F][C_B(A) : F] = (r/s)s^2 d = rsd = [B : F]. \tag{37}$$

Riassumiamo questi risultati nel teorema seguente.

Teorema 4.11. *Sia A una sottoalgebra semplice di un'algebra semplice centrale B di dimensione finita. Allora $[B : F] = [A : F][C_B(A) : F]$, e si ha $A \otimes B^{\mathrm{op}} \simeq M_r(\Delta)$, con Δ algebra con divisione, e $C_B(A) \simeq M_s(\Delta^{\mathrm{op}})$. Inoltre $s \mid r$, $[B : F] = rsd$, dove $d = [\Delta : F]$, e $[A : F] = r/s$.*

La relazione $[B : F] = [A : F][C_B(A) : F]$ mostra che, se A è un campo, $C_B(A) = A$ se e soltanto se $[B : F] = [A : F]^2$. Ne risulta la seguente caratterizzazione precisa dei campi di spezzamento di dimensione finita di un'algebra con divisione centrale.

Teorema 4.12. *Un campo di estensione E di dimensione finita su F è un campo di spezzamento di un'algebra con divisione centrale Δ se e soltanto se $[E : F] = nr$, dove n è il grado di Δ, ed E è isomorfo a un sottocampo di $M_r(\Delta)$.*

Esercizi

1. Sia Δ un'algebra con divisione centrale di dimensione finita su F e sia E un sottocampo massimale di Δ. Mostrare che $[\Delta : F] = [E : F]^2$.

2. (Dimostrazione del teorema di Wedderburn sugli anelli con divisione finiti.) Sia Δ un anello con divisione finito e sia F il suo centro, sicché Δ è un'algebra con divisione centrale su F. Mostrare che, se E_1 ed E_2 sono sottocampi massimali di Δ, essi sono coniugati, nel senso che esiste $s \in \Delta^\times$ tale che $E_2 = sE_1 s^{-1}$. Dedurne che il gruppo moltiplicativo Δ^* degli elementi non nulli di Δ è unione dei coniugati del sottogruppo E_1^*. Concludere che $\Delta = E_1 = F$ è commutativo (si veda l'esercizio 7, p. 77 di BAI).

3. (Dimostrazione del teorema di Frobenius sulle algebre con divisione reali.) Sia Δ un'algebra con divisione di dimensione finita su $\mathbb{R}$. Se Δ è commutativa, allora $\Delta = \mathbb{R}$ oppure $\Delta = \mathbb{C}$. Se Δ non è commutativa, il suo centro è $\mathbb{R}$ oppure $\mathbb{C}$. Il campo $\mathbb{C}$ è escluso, poiché è algebricamente chiuso e non ammette quindi algebre con divisione di dimensione finita su di esso diverse da sé stesso. Supponiamo ora che Δ sia centrale su $\mathbb{R}$ e che $\Delta \neq \mathbb{R}$. Allora Δ contiene un elemento i tale che $i^2 = -1$ e, poiché $\mathbb{C} = \mathbb{R}(i)$ ha un automorfismo che manda i in $-i$, esiste un j in Δ tale che $ji = -ij$. Mostrare che la sottoalgebra generata da i e j è l'algebra dei quaternioni di Hamilton $\mathbb{H}$. Usare l'esercizio 1 per provare che $[\Delta : \mathbb{R}] = 4$ e che $\Delta = \mathbb{H}$.

4. Sia E un'estensione ciclica di F, $[E : F] = n$, e sia $\mathrm{Gal}(E/F) = \langle s \rangle$ il gruppo di Galois di E/F. Sia (E, s, γ) la sottoalgebra di $M_n(E)$ generata da tutte le matrici diagonali

$$\bar{b} = \mathrm{diag}\{b, sb, \ldots, s^{n-1}b\}, \qquad b \in E, \tag{38}$$

e dalla matrice

$$z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \\ \gamma & 0 & \cdots & \cdots & 0 \end{pmatrix}, \tag{39}$$

dove γ è un elemento non nullo di F. Osservare che $b \mapsto \bar{b}$ è un monomorfismo e identificare b con $\bar{b}$. Valgono allora le relazioni

$$zb = s(b)z, \qquad z^n = \gamma, \tag{40}$$

e ogni elemento di (E, s, γ) si può scrivere in uno e un solo modo nella forma

$$b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}, \tag{41}$$

con $b_i \in E$. Dimostrare che (E, s, γ) è semplice centrale e che $[(E, s, \gamma) : F] = n^2$.

5. Siano E, F, G, s come nell'esercizio 4. Osservare che $s \in \mathrm{End}_F E$ e che per ogni $b \in E$ l'applicazione $x \mapsto bx$ appartiene a $\mathrm{End}_F E$. Identificandola con b, si ha $sb = s(b)s$. Mostrare che l'algebra L delle trasformazioni F-lineari di E generata dalle moltiplicazioni $b \in E$ e da s è isomorfa all'algebra $(E, s, 1)$ dell'esercizio 4. Concludere che $L = \mathrm{End}_F E$ e $(E, s, 1) \simeq M_n(F)$.

6. Dimostrare che $(E, s, \gamma) \simeq M_n(F)$ se e soltanto se γ è la norma di un elemento di E. (*Suggerimento.* Usare il teorema 4.9, p. 222.) Mostrarne come conseguenza che, se $n = p$ è primo e γ non è una norma da E, allora (E, s, γ) è un'algebra con divisione.

7. Sia $E = \mathbb{Q}(r)$, dove r è una radice di $x^3 + x^2 - 2x - 1$. Mostrare che $E/\mathbb{Q}$ è ciclica (si veda BAI, p. 236, esercizio 1). Mostrare che, se γ è un intero non divisibile per 8, γ non è la norma di alcun elemento di E.[10] Dedurre quindi dall'esercizio 6 che (E, s, γ) è un'algebra con divisione.

[10] Così l'originale. L'enunciato va ristretto, ad esempio, agli interi *pari* non divisibili per 8. Nella formulazione stampata $\gamma = 1$ è un controesempio, poiché $N_{E/\mathbb{Q}}(1) = 1$. [N.d.T.]

8. Sia A un'algebra su F con base $(u_1, \dots, u_n)$ e sia $\rho(a)$ la rappresentazione matriciale regolare determinata da questa base. Porre $N(a) = \det \rho(a)$ (si veda BAI, p. 403). Mostrare che A è un'algebra con divisione se e soltanto se $N(a) \neq 0$ per ogni $a \neq 0$ in A. Usare questo criterio per mostrare che, se t è un'indeterminata, A è un'algebra con divisione se e soltanto se lo è $A_{F(t)}$. Generalizzare mostrando che, se $t_1, \dots, t_r$ sono indeterminate, $A_{F(t_1,\dots,t_r)}$ è un'algebra con divisione se e soltanto se A è un'algebra con divisione.

9. Mostrare che, se Δ_1 e Δ_2 sono algebre con divisione di dimensione finita su F e Δ_1 è centrale, allora $\Delta_1 \otimes_F \Delta_2 \simeq M_r(E)$, dove E è un'algebra con divisione e $r \mid [\Delta_i : F]$ per $i = 1, 2$. Dedurne che $\Delta_1 \otimes \Delta_2$ è un'algebra con divisione se $([\Delta_1 : F], [\Delta_2 : F]) = 1$.

10. Se A è una sottoalgebra di un'algebra B, un'applicazione lineare D di A in B si dice *derivazione di A in B* se

$$D(a_1 a_2) = a_1 D(a_2) + D(a_1) a_2 \tag{42}$$

per $a_i \in A$. Formare $B^{(2)}$ e porre

$$a(x, y) = (ax + D(a)y, ay) \tag{43}$$

per $a \in A$, $(x, y) \in B^{(2)}$. Verificare che $B^{(2)}$ è un A-modulo con quest'azione. Mostrare che $B^{(2)}$ è un $A \otimes B^{\mathrm{op}}$-modulo in cui

$$(a \otimes b)(x, y) = (axb + D(a)yb, ayb).$$

11. Una derivazione di B in B si dice una *derivazione in B*. Se $d \in B$, l'applicazione $x \mapsto [d, x] = dx - xd$ è una derivazione in B, detta la *derivazione interna* determinata da d. Dimostrare che, se A è una sottoalgebra semisemplice di un'algebra semplice centrale B di dimensione finita, ogni derivazione di A in B si può prolungare a una derivazione interna di B.

12. Sia A una sottoalgebra semisemplice di un'algebra semplice centrale B di dimensione finita. Mostrare che $C_B(A)$ è semisemplice e studiare la relazione fra le strutture di A, $A \otimes B^{\mathrm{op}}$ e $C_B(A)$.

4.7 Il gruppo di Brauer

I risultati del paragrafo precedente sui prodotti tensoriali di algebre semplici centrali di dimensione finita portano a introdurre un gruppo importante, definito per la prima volta da R. Brauer nel 1929. I suoi elementi sono classi di similitudine di algebre semplici centrali di dimensione finita. Date due tali algebre A e B, si dice che A è *simile* a B ($A \sim B$) se esistono interi positivi m, n tali che $M_m(A) \simeq M_n(B)$, o equivalentemente $M_m(F) \otimes A \simeq M_n(F) \otimes B$. La relazione di similitudine è evidentemente riflessiva e simmetrica. È anche transitiva: se

$$M_m(F) \otimes A \simeq M_n(F) \otimes B, \qquad M_r(F) \otimes B \simeq M_s(F) \otimes C,$$

allora

$$\begin{aligned} M_{mr}(F) \otimes A &\simeq M_r(F) \otimes M_m(F) \otimes A \simeq M_r(F) \otimes M_n(F) \otimes B \\ &\simeq M_n(F) \otimes M_r(F) \otimes B \simeq M_n(F) \otimes M_s(F) \otimes C \simeq M_{ns}(F) \otimes C. \end{aligned}$$

Abbiamo usato l'associatività e la commutatività del prodotto tensoriale e la formula $M_n(F) \otimes M_m(F) \simeq M_{mn}(F)$, stabilita nella proposizione 4.10, p. 217. Quindi $\sim$ è una relazione di

equivalenza. Indichiamo con $[A]$ la classe di similitudine di A, ossia la classe di equivalenza delle algebre semplici centrali di dimensione finita simili ad A. Supponiamo $A \sim A'$ e $B \sim B'$. Esistono allora interi positivi m, m', n, n' tali che $A \otimes M_n(F) \simeq A' \otimes M_{n'}(F)$ e $B \otimes M_m(F) \simeq B' \otimes M_{m'}(F)$. Ne segue che $A \otimes B \otimes M_{nm}(F) \simeq A' \otimes B' \otimes M_{n'm'}(F)$, dunque $A \otimes B \sim A' \otimes B'$. Sulle classi di similitudine è quindi ben definita la legge di composizione binaria

$$[A][B] = [A \otimes B]. \tag{44}$$

È manifestamente associativa e commutativa. Inoltre le algebre di matrici $M_n(F)$ costituiscono, a meno di isomorfismo, una classe di similitudine 1, che funge da elemento neutro poiché $A \sim A \otimes M_n(F)$. Nel teorema 4.6, p. 218, abbiamo visto che $A \otimes A^{\mathrm{op}} \sim 1$. Pertanto $[A][A^{\mathrm{op}}] = 1 = [A^{\mathrm{op}}][A]$.

Se A è semplice centrale di dimensione finita su F, si può scrivere $A \simeq M_n(F) \otimes \Delta$, dove Δ è un'algebra di divisione centrale di dimensione finita. Viceversa, per una Δ di questo tipo, $M_n(F) \otimes \Delta$ è semplice centrale di dimensione finita su F. Ricordiamo che, per il teorema di isomorfismo degli anelli artiniani semplici (p. 206), se $M_n(\Delta) \simeq M_m(\Delta')$ con Δ, Δ' algebre di divisione, allora $m = n$ e $\Delta \simeq \Delta'$. Ne segue che nella formula $A \simeq M_n(F) \otimes \Delta$ l'algebra di divisione Δ è determinata da A a meno di isomorfismo. Dunque ogni classe di similitudine $[A]$ contiene un'unica classe di isomorfismo di algebre di divisione centrali di dimensione finita, e a classi di similitudine diverse corrispondono algebre di divisione non isomorfe. Ora, le sottoalgebre delle algebre di matrici $M_n(F)$, $n = 1, 2, 3, \ldots$, costituiscono un insieme, e ogni algebra di dimensione finita su F è isomorfa a un suo elemento. Le classi di isomorfismo di tali algebre formano quindi un insieme, del quale le classi di isomorfismo delle algebre di divisione centrali su F di dimensione finita costituiscono un sottoinsieme. Pertanto le classi di similitudine delle algebre semplici centrali di dimensione finita su F formano un insieme. I risultati ottenuti mostrano che esso è un gruppo rispetto alla legge (44). Lo indichiamo con $\mathrm{Br}(F)$ e lo chiamiamo *gruppo di Brauer* del campo F. Determinare $\mathrm{Br}(F)$ equivale dunque a classificare completamente le algebre di divisione centrali di dimensione finita su F.

Se F è algebricamente chiuso oppure finito, $\mathrm{Br}(F) = 1$. Se $F = \mathbb{R}$, il teorema di Frobenius dice che il gruppo di Brauer è ciclico di ordine due. Nel capitolo 9 (§ 9.14) determineremo $\mathrm{Br}(F)$ per F campo p-adico. Fra i risultati più importanti dell'algebra e della teoria dei numeri degli anni Trenta vi fu la determinazione di $\mathrm{Br}(\mathbb{Q})$ e, più in generale, di $\mathrm{Br}(F)$ per un campo di numeri F (ossia per un'estensione di grado finito di $\mathbb{Q}$). Vi intervengono alcuni profondi risultati aritmetici.

Sia E un'estensione di F. Se A è semplice centrale di dimensione finita su F, l'algebra A_E è semplice centrale di dimensione finita su E. Si ha $(A \otimes_F B)_E \simeq A_E \otimes_E B_E$ e $M_n(F)_E \simeq M_n(E)$. Abbiamo quindi un omomorfismo da $\mathrm{Br}(F)$ in $\mathrm{Br}(E)$ che manda $[A]$ in $[A_E]$. Il nucleo, che denoteremo con $\mathrm{Br}(E/F)$, è l'insieme delle classi $[A]$ tali che $A_E \sim 1$ (in questo contesto è consuetudine indicare il campo base con 1), ossia delle classi $[A]$ per le quali E è un campo di spezzamento di A. Nel capitolo 8 studieremo questo gruppo nel caso di un'estensione di Galois E/F di grado finito.

Esercizio

1. Usare il teorema 4.11 (p. 224) per mostrare che, se A è semplice centrale di dimensione finita su F ed E è un sottocampo di A contenente F, si ha $C_A(E) \sim A_E$ in $\mathrm{Br}(E)$.

4.8 Algebre di Clifford

Applicheremo alcuni dei risultati sulle algebre semplici centrali allo studio di certe algebre, le *algebre di Clifford*, definite mediante forme quadratiche. Esse svolgono un ruolo importante nello studio delle forme quadratiche e dei gruppi ortogonali. I risultati su questi argomenti di cui ci serviremo si trovano nel capitolo 6 di BAI.

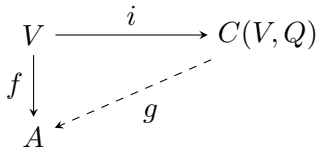
Sia V uno spazio vettoriale di dimensione finita su un campo F, munito di una forma quadratica Q. Ricordiamo la definizione: Q è un'applicazione da V nel campo base F tale che (1) $Q(\alpha x) = \alpha^2 Q(x)$ per $\alpha \in F$, $x \in V$; (2) $B(x,y) = Q(x+y) - Q(x) - Q(y)$ è bilineare. Evidentemente B è simmetrica, ossia $B(y,x) = B(x,y)$, e $B(x,x) = 2Q(x)$. Serviamoci di Q per definire un'algebra nel modo seguente.

Definizione 4.5. *Sia Q una forma quadratica su uno spazio vettoriale V sul campo F. Sia $T(V) = F \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$ l'algebra tensoriale di V (p. 140), e sia K_Q l'ideale di $T(V)$ generato dagli elementi*

$$x \otimes x - Q(x)1, \qquad x \in V. \tag{45}$$

L'algebra di Clifford della forma quadratica Q è l'algebra $C(V,Q) = T(V)/K_Q$.

Per $a \in T(V)$ scriviamo $\bar{a} = a + K_Q \in C(V,Q)$ e indichiamo con i l'applicazione $x \mapsto \bar{x}$ di V in $C(V,Q)$. Poiché V genera $T(V)$, $i(V)$ genera l'algebra di Clifford. Si ha $\bar{x}^2 = Q(x)\bar{1}$. L'applicazione i gode della seguente proprietà universale. Se f è un'applicazione lineare da V in un'algebra A tale che $f(x)^2 = Q(x)1$ per $x \in V$, allora esiste un unico omomorfismo di algebre $g\colon C(V,Q) \to A$ che rende commutativo il diagramma

(46)


Infatti, per la proprietà fondamentale dell'algebra tensoriale ogni applicazione lineare f da V in un'algebra A si estende in modo unico a un omomorfismo di algebre $f'\colon T(V) \to A$ (p. 140). Per la f assegnata, $\ker f'$ contiene ogni elemento $x \otimes x - Q(x)1$, poiché $f'(x \otimes x - Q(x)1) = f(x)^2 - Q(x)1 = 0$. Quindi $K_Q \subseteq \ker f'$ ed è indotto l'omomorfismo $g\colon a + K_Q \mapsto f'(a)$. In particolare $g(\bar{x}) = f'(x) = f(x)$, che esprime la commutatività della (46). Poiché gli $\bar{x}$ generano $C(V,Q)$, g è unico.

L'ideale K_Q che definisce $C(V,Q)$ contiene, per $x, y \in V$, ogni elemento

$$\begin{aligned}(x+y) \otimes (x+y) - Q(x+y)1 = x \otimes x + y \otimes x + x \otimes y + y \otimes y \\ - Q(x)1 - B(x,y)1 - Q(y)1.\end{aligned}$$

Poiché $x \otimes x - Q(x)1$ e $y \otimes y - Q(y)1$ appartengono a K_Q, otteniamo

$$x \otimes y + y \otimes x - B(x,y)1 \in K_Q, \qquad x, y \in V. \tag{47}$$

Equivalentemente, in $C(V,Q)$ valgono le relazioni

$$\bar{x}\bar{y} + \bar{y}\bar{x} = B(x,y)\bar{1} \tag{47'}$$

oltre a $\bar{x}^2 = Q(x)\bar{1}$. Ne deduciamo il seguente lemma.

Lemma 1. *Se $u_1, \ldots, u_n$ generano lo spazio vettoriale V su F, gli elementi*

$$1 = \bar{1}, \quad \bar{u}_{i_1}\bar{u}_{i_2}\cdots\bar{u}_{i_r}, \qquad i_1 < i_2 < \cdots < i_r, \quad 1 \le r \le n, \tag{48}$$

generano lo spazio vettoriale $C(V,Q)$ su F.

Dimostrazione. V genera $T(V)$ come algebra e gli u_i generano V come spazio vettoriale; quindi gli u_i generano $T(V)$ come algebra e ogni elemento di $T(V)$ è combinazione lineare di 1 e di monomi di grado positivo negli u_i. Chiamiamo *standard* 1 e i monomi $u_{i_1}\cdots u_{i_r}$ con $i_1 < \cdots < i_r$, $1 \le r \le n$, e sia S il loro insieme. Dimostriamo per induzione su i e sul grado di $u \in S$ che $u_i u$ è congruo modulo K_Q a una combinazione lineare di monomi standard di grado al più $\deg u + 1$. Ciò è evidente se $\deg u = 0$. Sia dunque $u = u_{i_1}\cdots u_{i_r}$ con $r \ge 1$. Per $i = 1$ la conclusione è immediata se $i_1 > 1$, mentre se $i_1 = 1$ si ha

$$u_1 u = u_1^2 u_{i_2}\cdots u_{i_r} \equiv Q(u_1) u_{i_2}\cdots u_{i_r} \pmod{K_Q}.$$

Sia ora $i > 1$. Se $i \le i_1$ si ragiona come per $i = 1$. Supponiamo quindi $i > i_1$. Per la (47),

$$u_i u_{i_1} u_{i_2}\cdots u_{i_r} \equiv -u_{i_1} u_i u_{i_2}\cdots u_{i_r} + B(u_i, u_{i_1}) u_{i_2}\cdots u_{i_r} \pmod{K_Q}.$$

Per induzione sul grado, $u_i u_{i_2}\cdots u_{i_r}$ è congruo a una combinazione lineare di monomi standard di grado al più r. Per induzione sull'indice, essendo $i_1 < i$, anche $u_{i_1} u_i u_{i_2}\cdots u_{i_r}$, e di conseguenza $u_i u_{i_1}\cdots u_{i_r}$, è congruo a una combinazione lineare di monomi standard di grado al più $r+1$. Se ora C è il sottospazio di $C(V,Q)$ generato dagli elementi della (48), quanto dimostrato dà $\bar{u}_i C \subseteq C$. Ne segue $CC \subseteq C$, sicché C è una sottoalgebra di $C(V,Q)$. Essa contiene $\bar{V} = \{\bar{x} \mid x \in V\}$ e $\bar{V}$ genera $C(V,Q)$. Perciò $C = C(V,Q)$. □

Il lemma implica in particolare che, se $\dim V = n$, allora $\dim C(V,Q) \le 2^n$, essendo 2^n il numero dei monomi standard negli u_i.

Per semplicità, nel resto del testo di questo paragrafo supporremo $\operatorname{char} F \ne 2$. L'estensione dei risultati al caso della caratteristica due sarà indicata negli esercizi. Supponiamo dapprima che B sia non degenere e trattiamo a parte le dimensioni minime $n = 1, 2$.

Caso $n = 1$. Si ha $\dim C(V,Q) \le 2$ e, se $V = Fu$, $\bar{u}^2 = Q(u)\bar{1}$ con $Q(u) \ne 0$ perché B è non degenere. Sia $A = F[t]/(t^2 - Q(u)1)$, con t indeterminata. Una base di A è $(1, \bar{t})$, dove $\bar{t} = t + (t^2 - Q(u)1)$. Da $\bar{t}^2 = Q(u)1$ segue che l'applicazione lineare $f\colon V \to A$ determinata da $f(u) = \bar{t}$ soddisfa $f(x)^2 = Q(x)1$. Abbiamo quindi un omomorfismo suriettivo da $C(V,Q)$ in A che manda $\bar{u}$ in $\bar{t}$. Essendo $\dim A = 2$ e $\dim C(V,Q) \le 2$, segue $\dim C(V,Q) = 2$ e l'omomorfismo è un isomorfismo. Se $Q(u)$ non è un quadrato in F, il polinomio $t^2 - Q(u)1$ è irriducibile in $F[t]$ e $C(V,Q)$ è un campo. Se $Q(u) = \beta^2$, con $\beta \in F$, l'elemento $e' = \bar{u} - \beta 1$ soddisfa

$$(e')^2 = \bar{u}^2 - 2\beta\bar{u} + \beta^2 1 = 2Q(u)1 - 2\beta\bar{u} = -2\beta e'.$$

Dunque $e = -(2\beta)^{-1} e'$ è un idempotente distinto da 0 e 1; si ha $C(V,Q) = Fe \oplus F(1-e)$, somma diretta di due copie di F. Abbiamo così il seguente lemma.

Lemma 2. *Se $B(x,y)$ è non degenere e $n = 1$, allora* $\dim C(V,Q) = 2$. *Se $V = Fu$, l'algebra $C(V,Q)$ è un campo oppure è la somma diretta di due copie di F secondo che $Q(u)$ non sia o sia un quadrato in F.*

Caso $n = 2$. Scegliamo una base ortogonale (u, v) di V. Allora $Q(u)Q(v) \ne 0$. Sia C' l'algebra di Clifford di Fu rispetto alla restrizione Q' di Q a Fu. Essa ha base $(1, \bar{u})$ con $\bar{u}^2 = Q(u)1$. Consideriamo in $M_2(C')$ le matrici

$$u' = \begin{pmatrix} \bar{u} & 0 \\ 0 & -\bar{u} \end{pmatrix}, \qquad v' = \begin{pmatrix} 0 & 1 \\ Q(v)1 & 0 \end{pmatrix}.$$

Si ha

$$u'v' = \begin{pmatrix} 0 & \bar{u} \\ -Q(v)\bar{u} & 0 \end{pmatrix}, \qquad v'u' = \begin{pmatrix} 0 & -\bar{u} \\ Q(v)\bar{u} & 0 \end{pmatrix},$$

sicché $u'v'+v'u' = 0$. Inoltre $(u')^2 = Q(u)1$, $(v')^2 = Q(v)1$. Dunque $A = F1+Fu'+Fv'+Fu'v'$ è una sottoalgebra di $M_2(C')$. Dalla forma delle matrici è chiaro che $1, u', v', u'v'$ sono linearmente indipendenti, e pertanto $\dim A = 4$. Le relazioni su u' e v' implicano che l'applicazione lineare $f\colon V \to A$ tale che $u \mapsto u'$, $v \mapsto v'$ soddisfa $f(x)^2 = Q(x)1$ per $x \in V$. Esiste dunque un omomorfismo $g\colon C(V,Q) \to A$ con $g(\bar{u}) = u'$, $g(\bar{v}) = v'$. Esso è suriettivo; da $\dim C(V,Q) \leq 4$ e $\dim A = 4$ deduciamo che g è un isomorfismo e che $\dim C(V,Q) = 4$.

Un'algebra A su un campo F di caratteristica diversa da due si chiama *algebra dei quaternioni (generalizzata)* se è generata da due elementi i, j tali che

$$i^2 = \alpha 1 \neq 0, \qquad j^2 = \beta 1 \neq 0, \qquad ij = -ji, \tag{49}$$

con $\alpha, \beta \in F$. Indichiamo quest'algebra con (α, β) o con $(\alpha, \beta)/F$ per specificare il campo base.

Lemma 3. *Ogni algebra dei quaternioni è semplice centrale di dimensione quattro su F.*

Dimostrazione. Dalle (49) segue che gli elementi $1, i, j, ij$ generano A come spazio vettoriale. Sia $\lambda 1 + \mu i + \nu j + \rho ij = 0$ con $\lambda, \mu, \nu, \rho \in F$. Moltiplicando a sinistra per i e a destra per $i^{-1} = \alpha^{-1} i$ si ha $\lambda 1 + \mu i - \nu j - \rho ij = 0$. Quindi $\lambda 1 + \mu i = 0$ e $\nu j + \rho ij = 0$. Moltiplicando queste relazioni a sinistra per j e a destra per $j^{-1} = \beta^{-1} j$, otteniamo $\lambda 1 - \mu i = 0$ e $\nu j - \rho ij = 0$. Ne segue $\lambda 1 = \mu i = \nu j = \rho ij = 0$ e infine $\lambda = \mu = \nu = \rho = 0$. Pertanto $1, i, j, ij$ sono linearmente indipendenti e formano una base di A, che ha dimensione quattro. Sia ora $I \neq A$ un ideale di A e scriviamo $\bar{1} = 1 + I$, $\bar{i} = i + I$, $\bar{j} = j + I$. Allora $\bar{i}^2 = \alpha\bar{1} \neq 0$, $\bar{j}^2 = \beta\bar{1} \neq 0$, $\bar{i}\bar{j} = -\bar{j}\bar{i}$. Anche A/I è dunque un'algebra dei quaternioni, perciò $\dim A/I = 4$. Si ha $I = 0$ ed A è semplice. Resta da mostrarne la centralità. Sia $c = \lambda 1 + \mu i + \nu j + \rho ij$ un elemento del centro. Da $ci = ic$ si ricava $\nu = \rho = 0$; dal fatto che $\lambda 1 + \mu i$ commuta con j segue $\mu = 0$. Dunque $c = \lambda 1$ e il centro è $F1$. □

Il risultato ottenuto in dimensione due si può ora enunciare così.

Lemma 4. *Se $B(x,y)$ è non degenere e $n = 2$, $C(V,Q)$ è un'algebra dei quaternioni.*

Dimostrazione. Abbiamo ottenuto un isomorfismo di $C(V,Q)$ con l'algebra A generata da u', v' con $(u')^2 = Q(u)1 \neq 0$, $(v')^2 = Q(v)1 \neq 0$ e $u'v' = -v'u'$. Dunque A, e con essa $C(V,Q)$, è un'algebra dei quaternioni. □

Ricordiamo che, data una forma bilineare simmetrica B su uno spazio vettoriale V con base $(u_1, \ldots, u_n)$, si chiama *un discriminante* di B lo scalare $\delta = \det(B(u_i, u_j))$. Un cambiamento di base sostituisce a δ lo scalare $\delta\beta^2$, dove $\beta \neq 0$ è il determinante della matrice del cambiamento di base. La forma B è non degenere se e soltanto se $\delta \neq 0$. Ricordiamo inoltre che, se la restrizione di B a un sottospazio U di V è non degenere, $V = U \oplus U^\perp$; se anche B è non degenere su V, la sua restrizione a $U^\perp$ è non degenere. Dimostriamo la seguente proprietà di fattorizzazione.

Lemma 5. *Siano B non degenere e $\dim V \geq 3$. Sia U un sottospazio bidimensionale sul quale B abbia restrizione non degenere. Scriviamo $V = U \oplus U^\perp$ e siano Q', Q'' le restrizioni di Q a U e a $U^\perp$. Allora*

$$C(V,Q) \simeq C(U,Q') \otimes C(U^\perp, -\delta' Q''), \tag{50}$$

dove δ' è un discriminante della restrizione di B a U.

Dimostrazione. Useremo due proprietà universali per costruire isomorfismi inversi tra i due membri della (50). Indichiamo con $i'\colon y \mapsto y'$ e $i''\colon z \mapsto z''$ le applicazioni canoniche di U in $C(U,Q')$ e di $U^\perp$ in $C(U^\perp, -\delta' Q'')$. Sia (u,v) una base ortogonale di U e poniamo $d = 2\bar{u}\bar{v}$ in $C(V,Q)$. Si ha $\bar{u}^2 = Q(u)1$, $\bar{v}^2 = Q(v)1$, $\bar{u}\bar{v} = -\bar{v}\bar{u}$. Dunque $d^2 = -4Q(u)Q(v)1 = -B(u,u)B(v,v)1 = -\delta' 1$, poiché $B(x,x) = 2Q(x)$ e δ' è il discriminante corrispondente alla base (u,v). Inoltre, per $y \in U$ e $z \in U^\perp$, si ha $\bar{y}d = -d\bar{y}$, $\bar{y}\bar{z} = -\bar{z}\bar{y}$ e $d\bar{z} = \bar{z}d$. Pertanto

$$\bar{y}(d\bar{z}) = (d\bar{z})\bar{y}, \qquad (d\bar{z})^2 = -\delta' Q(z)1. \tag{51}$$

Poiché $\bar{y}^2 = Q(y)1$ e $(d\bar{z})^2 = -\delta' Q(z)1$, per la proprietà universale delle algebre di Clifford esistono omomorfismi da $C(U, Q')$ e da $C(U^\perp, -\delta' Q'')$ in $C(V, Q)$ che mandano rispettivamente y' in $\bar{y}$ e z'' in $d\bar{z}$. Gli elementi $\bar{y}$ e $d\bar{z}$ generano le rispettive immagini e, per la (51), commutano fra loro. Pertanto le due immagini si centralizzano a vicenda. Dalla proprietà universale del prodotto tensoriale otteniamo un omomorfismo h da $C(U, Q') \otimes C(U^\perp, -\delta' Q'')$ in $C(V, Q)$ tale che

$$y' \longmapsto \bar{y}, \qquad z'' \longmapsto d\bar{z}, \qquad y \in U,\ z \in U^\perp. \tag{52}$$

Consideriamo ora $d' = 2u'v'$ in $C(U, Q')$. I calcoli precedenti danno $d'y' = -y'd'$ e $(d')^2 = -\delta' 1$, perciò d' è invertibile. Nel prodotto tensoriale consideriamo $y' + (d')^{-1} z''$. Si ha

$$\begin{aligned}(y' + (d')^{-1} z'')^2 &= (y')^2 + (y'(d')^{-1} + (d')^{-1} y') z'' + (d')^{-2} (z'')^2 \\ &= Q(y)1 + Q(z)1 = Q(y+z)1.\end{aligned}$$

Nell'ultimo termine dello sviluppo si è esplicitato il fattore $(d')^{-2}$, omesso nell'originale. Per la proprietà universale di $C(V, Q)$ esiste perciò un omomorfismo g da $C(V, Q)$ in $C(U, Q') \otimes C(U^\perp, -\delta' Q'')$ tale che

$$\bar{y} + \bar{z} \longmapsto y' + (d')^{-1} z''. \tag{53}$$

Verificando sui generatori mediante le (52) e (53), vediamo che $gh = 1$ sul prodotto tensoriale e $hg = 1$ su $C(V, Q)$. La (50) è dimostrata. □

Possiamo ora dimostrare il teorema principale sulla struttura delle algebre di Clifford.

Teorema 4.13. *Sia Q una forma quadratica su uno spazio vettoriale V di dimensione n su un campo F di caratteristica diversa da due. Allora:*

(1) $\dim C(V, Q) = 2^n$. *Se $(u_1, \dots, u_n)$ è una base di V, gli elementi*

$$1 = \bar{1}, \quad \bar{u}_{i_1} \bar{u}_{i_2} \cdots \bar{u}_{i_r}, \qquad i_1 < \cdots < i_r, \quad 1 \le r \le n, \tag{54}$$

costituiscono una base di $C(V, Q)$ su F.

(2) L'applicazione canonica $i\colon x \mapsto \bar{x}$ da V in $C(V, Q)$ è iniettiva.

(3) Se la forma bilineare B associata a Q è non degenere, allora $C(V, Q)$ è semplice centrale per n pari. Se $n = 2\nu + 1$, con $\nu \in \mathbb{Z}$, $C(V, Q)$ è semplice con centro un campo di dimensione due, oppure è somma diretta di due algebre semplici centrali isomorfe, secondo che $(-1)^\nu 2\delta$, per un discriminante δ di B, non sia o sia un quadrato in F.

Dimostrazione. Anzitutto, la seconda affermazione di (1) e l'affermazione (2) seguono dalla formula $\dim C(V, Q) = 2^n$. Per il lemma 1, infatti, gli elementi della (54) generano $C(V, Q)$. Sono al più 2^n; se la dimensione è 2^n devono quindi essere tutti distinti e formare una base. In particolare, gli $\bar{u}_i$, $1 \le i \le n$, sono linearmente indipendenti e l'applicazione lineare $i\colon x \mapsto \bar{x}$ è iniettiva.

Dimostriamo la formula della dimensione e la (3) nel caso non degenere. Per $n = 1$ basta il lemma 2, e per $n = 2$ bastano i lemmi 3 e 4. Sia ora $n > 2$. Possiamo scegliere un sottospazio bidimensionale U su cui B ha restrizione non degenere. Allora $V = U \oplus U^\perp$ e anche la restrizione di B a $U^\perp$ è non degenere. Per il lemma 5,

$$C(V, Q) \simeq C(U, Q') \otimes C(U^\perp, -\delta' Q''),$$

dove δ' è un discriminante della restrizione di B a U. Inoltre $C(U, Q')$ è un'algebra dei quaternioni, quindi è semplice centrale di dimensione quattro. Procedendo per induzione sulla dimensione possiamo supporre provato il risultato per la forma quadratica $-\delta' Q''$ su $U^\perp$. Si ha

allora $\dim C(U^\perp, -\delta' Q'') = 2^{n-2}$ e, se $n-2$ è pari, l'algebra è semplice centrale. Ne segue $\dim C(V,Q) = 2^2\, 2^{n-2} = 2^n$ e, per il corollario 2 al teorema 4.7 (p. 219), quest'algebra è semplice centrale se n è pari. Se $n = 2\nu+1$, allora $n-2 = 2(\nu-1)+1$. Per l'ipotesi induttiva, detto δ'' un discriminante della restrizione di B a $U^\perp$, l'algebra $C(U^\perp, -\delta' Q'')$ è semplice con centro di dimensione due, oppure è la somma diretta di due algebre semplici centrali isomorfe, secondo che $(-1)^{\nu-1} 2(-\delta')^{n-2}\delta''$ non sia o sia un quadrato in F. Lo stesso vale allora per $C(V,Q)$. Ora

$$(-1)^{\nu-1} 2(-\delta')^{n-2}\delta'' = (-1)^\nu (\delta')^{n-3} 2\delta'\delta'' = (-1)^\nu (\delta')^{n-3} 2\delta,$$

e, poiché $n-3$ è pari, tale elemento è un quadrato se e soltanto se è un quadrato $(-1)^\nu 2\delta$. Ciò dimostra (3).

Resta la formula della dimensione nel caso degenere. Immergeremo V in uno spazio W di dimensione finita con una forma quadratica che prolunga Q e la cui forma bilineare associata è non degenere. Scriviamo $V = V^\perp \oplus U$ scegliendo un complemento U del radicale $V^\perp$. La restrizione di B a U è non degenere. Poniamo $W = V^\perp \oplus U \oplus (V^\perp)^*$, dove $(V^\perp)^*$ è lo spazio delle forme lineari su $V^\perp$. Per $x = z + y + f$ con $z \in V^\perp$, $y \in U$, $f \in (V^\perp)^*$, definiamo

$$\widetilde{Q}(x) = Q(z) + Q(y) + f(z). \tag{55}$$

Si verifica facilmente che $\widetilde{Q}$ è una forma quadratica su W la cui forma bilineare simmetrica associata $\widetilde{B}$ è non degenere. Sia $x \mapsto \widetilde{x}$ l'applicazione canonica da W in $C(W, \widetilde{Q})$. Per la proprietà universale di $C(V,Q)$ esiste un omomorfismo da $C(V,Q)$ in $C(W,\widetilde{Q})$ con $\bar{x} \mapsto \widetilde{x}$ per $x \in V$. Sia $(u_1, \dots, u_n, u_{n+1}, \dots, u_q)$ una base di W che prolunga la base $(u_1, \dots, u_n)$ di V. Poiché $\widetilde{B}$ è non degenere, i monomi $\widetilde{u}_{j_1} \cdots \widetilde{u}_{j_s}$, $j_1 < \cdots < j_s$, $1 \le s \le q$, insieme con 1, sono distinti e linearmente indipendenti. Lo stesso vale quindi per quelli che usano i soli indici $1, \dots, n$. Poiché l'omomorfismo manda $\bar{u}_{i_1} \cdots \bar{u}_{i_r}$ in $\widetilde{u}_{i_1} \cdots \widetilde{u}_{i_r}$, ne segue l'indipendenza lineare dei monomi della (54), e quindi $\dim C(V,Q) = 2^n$. □

Essendo iniettiva l'applicazione $i\colon x \mapsto \bar{x}$, possiamo identificare V con il corrispondente sottospazio di $C(V,Q)$. D'ora in avanti supporremo quindi $V \subseteq C(V,Q)$. Se U è un sottospazio di V, la sottoalgebra di $C(V,Q)$ generata da U si identifica con $C(U,Q')$, dove Q' è la restrizione di Q a U. Ciò è chiaro dall'ultima parte della dimostrazione del teorema 4.13: se $(u_1, \dots, u_m)$ è una base di U su F, l'argomento mostra che 1 e gli $u_{i_1} \cdots u_{i_r}$ con $i_1 < \cdots < i_r$, $1 \le r \le m$, sono linearmente indipendenti; dunque l'omomorfismo canonico da $C(U,Q')$ in $C(V,Q)$ è un monomorfismo.

Dalle definizioni si vede subito che per $Q = 0$ si ottiene l'algebra esterna $E(V)$ (p. 141). Le parti (1) e (2) del teorema 4.13 danno un'altra dimostrazione delle proprietà di $E(V)$ stabilite in BAI, pp. 411–414. Osserviamo infine che la dimostrazione della parte (3) fornisce un risultato più forte dell'enunciato.

Corollario. *Sia Q una forma quadratica su uno spazio V di dimensione n sopra un campo F di caratteristica diversa da due, e sia non degenere la forma bilineare associata. Se n è pari, $C(V,Q)$ è un prodotto tensoriale di algebre dei quaternioni. Se n è dispari, è un prodotto tensoriale di algebre dei quaternioni e del proprio centro. In quest'ultimo caso il centro ha dimensione due ed è della forma $F[c]$, con $c^2 = (-1)^\nu 2^{-n}\delta 1$, dove $n = 2\nu+1$ e δ è un discriminante. Esso è un campo o una somma diretta di due copie di F secondo che $(-1)^\nu 2\delta$ non sia o sia un quadrato in F.*

Dimostrazione. La prima affermazione segue per induzione sulla dimensione, usando il lemma di fattorizzazione (lemma 5). Per determinare il centro in dimensione dispari scegliamo una base ortogonale $(u_1, u_2, \dots, u_n)$, con $n = 2\nu+1$. Allora $u_i u_j = -u_j u_i$ per $i \ne j$ e quindi $c = u_1 u_2 \cdots u_n$ commuta con ogni u_i. Dunque c appartiene al centro; poiché $c \notin F1$ e il centro

ha dimensione due, esso è $F[c]$. Si ha

$$\begin{aligned} c^2 &= u_1 \cdots u_n u_1 \cdots u_n = (-1)^{n(n-1)/2} u_1^2 \cdots u_n^2 \\ &= (-1)^\nu \prod_{i=1}^{n} Q(u_i)1 = (-1)^\nu 2^{-n}\delta 1, \end{aligned} \tag{56}$$

dove δ è il discriminante determinato dalla base $(u_1, \dots, u_n)$. Allora $F[c]$ è un campo o una somma diretta di due copie di F secondo che $(-1)^\nu 2^{-n}\delta$ non sia o sia un quadrato. Poiché $n = 2\nu + 1$, la stessa alternativa vale per $(-1)^\nu 2\delta$. □

Nel resto di questo paragrafo accenneremo ad alcune applicazioni delle algebre di Clifford allo studio dei gruppi ortogonali. Occorre introdurre l'*algebra di Clifford pari* (o *seconda*) $C^+(V, Q)$, la sottoalgebra di $C(V, Q)$ generata da tutti i prodotti uv con $u, v \in V$, cioè da V^2. Ricordiamo che un vettore u si dice *non isotropo* se $Q(u) \neq 0$. Se u_1 è non isotropo, si ha

$$(u_1 u)(u_1 v) = u_1(-u_1 u + B(u, u_1)1)v = -Q(u_1)uv + B(u, u_1)u_1 v.$$

Dunque

$$uv = Q(u_1)^{-1}\big(B(u, u_1)u_1 v - (u_1 u)(u_1 v)\big),$$

e $C^+ = C^+(V, Q)$ è generata dagli elementi $u_1 u$, $u \in V$. Si può scrivere $V = Fu_1 \oplus (Fu_1)^\perp$ e $u = \alpha u_1 + v$, con $\alpha \in F$ e $v \perp u_1$. Allora $u_1 u = \alpha Q(u_1)1 + u_1 v$, sicché C^+ è generata dal sottospazio $V_1 = u_1(Fu_1)^\perp$, di dimensione $n - 1$. Si ha

$$(u_1 v)^2 = -u_1^2 v^2 = -Q(u_1)Q(v)1. \tag{57}$$

La restrizione di $-Q(u_1)Q$ a $(Fu_1)^\perp$ è una forma quadratica Q_1 con forma bilineare non degenere B_1. Esiste pertanto un omomorfismo suriettivo da $C((Fu_1)^\perp, Q_1)$ su C^+. D'altra parte, data una base $(u_1, \dots, u_n)$ di V, gli elementi 1 e $u_{i_1} \cdots u_{i_r}$ con $i_1 < \cdots < i_r$ formano una base di $C(V, Q)$. Tra questi, 1 e i monomi di lunghezza pari appartengono a C^+ e sono in numero di 2^{n-1}. Quindi $\dim C^+ \geq 2^{n-1}$, mentre $\dim C((Fu_1)^\perp, Q_1) = 2^{n-1}$. Ne segue che $C^+ \simeq C((Fu_1)^\perp, Q_1)$, il che dimostra la prima parte del teorema seguente.

Teorema 4.14. *Siano B non degenere e* $\operatorname{char} F \neq 2$. *Si ha $C^+(V, Q) \simeq C((Fu_1)^\perp, Q_1)$, dove u_1 è un qualunque vettore non isotropo e Q_1 è la restrizione di $-Q(u_1)Q$ a $(Fu_1)^\perp$. Per $n = \dim V$ dispari l'algebra $C^+(V, Q)$ è semplice centrale; per $n = 2\nu$ è il prodotto tensoriale di un'algebra semplice centrale e di un'algebra bidimensionale D. Quest'ultima è un campo o una somma diretta di due copie di F secondo che $(-1)^\nu\delta$ non sia o sia un quadrato in F, dove δ è un discriminante di B.*

Dimostrazione. La seconda affermazione segue immediatamente dalla prima e dal teorema 4.13. Sia n pari e poniamo $c = u_1 \cdots u_n$, dove $(u_1, \dots, u_n)$ è una base ortogonale di V. Allora $c \in C^+$, $u_i c = -cu_i$ e $u_i u_j c = cu_i u_j$. Quindi c appartiene al centro di C^+ e $c \notin F1$. Il centro di C^+ è perciò $F[c]$. Come nella (56) si ha $c^2 = (-1)^\nu \beta^2 \delta 1$ con $\beta = 2^{-\nu}$, e $F[c]$ è un campo o una somma diretta di due copie di F secondo che $(-1)^\nu \beta^2 \delta$, o equivalentemente $(-1)^\nu \delta$, non sia o sia un quadrato. □

Tanto in dimensione pari quanto in dimensione dispari, il sottospazio Fc, con $c = u_1 \cdots u_n$ associato a una base ortogonale, è indipendente dalla scelta della base. Infatti $F[c]$ è il centro di $C(V, Q)$ o quello di $C^+(V, Q)$. Inoltre $c \notin F1$ e $c^2 \in F1$. È facile vedere che queste due condizioni caratterizzano, dentro $F[c]$, l'insieme degli elementi non nulli di Fc.

Sia ora f una trasformazione ortogonale di V. Si ha $f(x)^2 = Q(f(x))1 = Q(x)1$. Per la proprietà universale di $C(V, Q)$, f si estende in modo unico a un automorfismo g di $C(V, Q)$. Questo stabilizza $C^+(V, Q)$ e i centri di $C(V, Q)$ e di $C^+(V, Q)$. Uno di essi è $F[c]$, che g dunque

stabilizza. Dalla caratterizzazione degli elementi non nulli di Fc segue $g(c) = \alpha c$ con $0 \neq \alpha \in F$. Poiché $g(c)^2 = g(c^2)$, si ha $\alpha = \pm 1$ e dunque $g(c) = \pm c$. Scriviamo $g(u_i) = f(u_i) = \sum_j \alpha_{ij} u_j$, $\alpha_{ij} \in F$, dove (α_{ij}) è la matrice della trasformazione ortogonale. Allora

$$g(c) = f(u_1) \cdots f(u_n) = \sum_{j_1,\ldots,j_n} \alpha_{1j_1}\alpha_{2j_2} \cdots \alpha_{nj_n} u_{j_1} u_{j_2} \cdots u_{j_n}.$$

Poiché $u_i u_j = -u_j u_i$ per $i \neq j$ e $u_i^2 = Q(u_i)1$, dalla definizione del determinante si vede che la somma si scrive come $\det(\alpha_{ij}) u_1 \cdots u_n$ più una combinazione lineare di monomi $u_{i_1} \cdots u_{i_r}$ a indici crescenti con $r < n$ (cfr. BAI, p. 416). Questi elementi insieme con $u_1 \cdots u_n$ costituiscono una base e $g(c) = \pm c$; pertanto $g(c) = \det(\alpha_{ij}) c$. Dunque $g(c) = c$ se f è una rotazione e $g(c) = -c$ altrimenti.

Osserviamo ora che ogni automorfismo g di un'algebra semisemplice A di dimensione finita che fissi gli elementi del centro C è interno. Infatti, se $A = A_1 \oplus \cdots \oplus A_s$ è la decomposizione in componenti semplici, $1 = 1_1 + \cdots + 1_s$, dove 1_i è l'unità di A_i, e $A = A1_1 \oplus \cdots \oplus A1_s$, $C = C1_1 \oplus \cdots \oplus C1_s$. Dunque $g(1_i) = 1_i$, per cui g stabilizza ogni A_i e fissa gli elementi del suo centro $C1_i$. Per il teorema di Skolem–Noether esiste un elemento invertibile $u_i \in A_i$ tale che $g|_{A_i}$ sia l'automorfismo interno determinato da u_i. Allora g è l'automorfismo interno determinato da $u = \sum_i u_i$.

Applicando questo fatto alla situazione precedente, vediamo che, se la trasformazione ortogonale f è una rotazione, esiste un elemento invertibile $u \in C(V, Q)$ tale che

$$f(x) = uxu^{-1}, \qquad x \in V. \tag{58}$$

Queste considerazioni conducono ai gruppi seguenti.

Definizione 4.6. *Il gruppo di Clifford $\Gamma(V, Q)$ è il sottogruppo degli elementi invertibili $u \in C(V, Q)$ tali che $uxu^{-1} \in V$ per ogni $x \in V$. È evidentemente un sottogruppo del gruppo moltiplicativo degli invertibili di $C(V, Q)$. Il gruppo di Clifford pari è $\Gamma^+(V, Q) = \Gamma(V, Q) \cap C^+(V, Q)$.*

Per $x \in V$ e $u \in \Gamma = \Gamma(V, Q)$ si ha $uxu^{-1} \in V$ e $(uxu^{-1})^2 = ux^2u^{-1} = Q(x)1$. Quindi la trasformazione lineare $x \mapsto uxu^{-1}$ di V appartiene al gruppo ortogonale $O(V, Q)$. L'applicazione χ che associa a u tale trasformazione è un omomorfismo da $\Gamma(V, Q)$ in $O(V, Q)$, chiamato *rappresentazione vettoriale* del gruppo di Clifford.

Sia $v \in V$ non isotropo. Allora v è invertibile in $C(V, Q)$ e per $x \in V$ si ha

$$2vxv = v(vx + xv) + (xv + vx)v - v^2x - xv^2 = 2B(v, x)v - 2Q(v)x.$$

Poiché $vxv^{-1} = vxvv^{-2} = Q(v)^{-1}vxv$, ne risulta

$$vxv^{-1} = -x + Q(v)^{-1}B(v, x)v. \tag{59}$$

Dunque $v \in \Gamma$. Ricordiamo che l'applicazione

$$x \longmapsto x - Q(v)^{-1}B(v, x)v \tag{60}$$

è ortogonale e prende il nome di *simmetria* S_v associata al vettore non isotropo v (BAI, p. 363). Si ha evidentemente $S_{\alpha v} = S_v$ per $0 \neq \alpha \in F$. Ricordiamo anche che ogni trasformazione ortogonale è un prodotto di simmetrie e che ogni rotazione è un prodotto di un numero pari di simmetrie. La (59) si scrive ora

$$\chi(v) = -S_v. \tag{61}$$

Se i v_i sono non isotropi, è quindi chiaro che $v_1 \cdots v_r \in \Gamma(V,Q)$ e che l'elemento appartiene a $\Gamma^+(V,Q)$ per r pari. Inoltre $\Gamma^+(V,Q)$ contiene il gruppo F^* degli elementi non nulli di F. Possiamo ora provare il teorema seguente.

Teorema 4.15. *Il gruppo di Clifford pari Γ^+ coincide con l'insieme dei prodotti $v_1 \cdots v_{2r}$, con i v_i non isotropi in V. Si ha la successione esatta*

$$1 \longrightarrow F^* \longrightarrow \Gamma^+(V,Q) \xrightarrow{\chi} O^+(V,Q) \longrightarrow 1, \tag{62}$$

dove la seconda applicazione è l'inclusione di F^*.

Dimostrazione. Sia $u \in \Gamma^+$. L'automorfismo $a \mapsto uau^{-1}$ di $C(V,Q)$ fissa $c = u_1 \cdots u_n$ per ogni base ortogonale $(u_1, \ldots, u_n)$ di V. Come sopra se ne deduce $\chi(u) \in O^+(V,Q)$. Viceversa, per $f \in O^+(V,Q)$ scriviamo $f = S_{v_1} \cdots S_{v_{2r}}$ con $v_i \in V$ non isotropi. Allora $v_1 \cdots v_{2r} \in \Gamma^+$ e, per la (61), $\chi(v_1 \cdots v_{2r}) = S_{v_1} \cdots S_{v_{2r}}$. Dunque $\chi(\Gamma^+) \supseteq O^+$. Il nucleo della restrizione di χ a Γ^+ è l'intersezione di Γ^+ con il centro di $C(V,Q)$. Poiché una delle algebre $C(V,Q)$ e $C^+(V,Q)$ è semplice centrale, tale intersezione è F^*. Abbiamo così l'esattezza della (62). Inoltre, se $u \in \Gamma^+$, allora $\chi(u) \in O^+$, per cui esiste un prodotto $v_1 \cdots v_{2r}$ con $\chi(v_1 \cdots v_{2r}) = \chi(u)$. Segue che $u = \alpha v_1 \cdots v_{2r}$, con $\alpha \in F^*$, e dunque $u = (\alpha v_1)v_2 \cdots v_{2r}$. Ciò dimostra la prima affermazione del teorema. □ Sia C^{op} l'algebra opposta di $C = C(V,Q)$. Per $x \in V \subset C^{\mathrm{op}}$ si ha $x^2 = Q(x)1$. Esiste dunque un unico omomorfismo di C in C^{op} che manda x in x. Ciò significa che esiste un antiomomorfismo ι di C in C che manda x in x. Allora ι^2 è un omomorfismo che fissa ogni $x \in V$, e dunque $\iota^2 = 1$. Pertanto ι è un'involuzione di C, cioè un antiautomorfismo tale che $\iota^2 = 1$. La si può caratterizzare come *l'*involuzione di C che fissa tutti gli elementi di V. Chiamiamo ι l'*involuzione principale* di C. Evidentemente ι stabilizza C^+, sicché la restrizione $\iota|_{C^+}$ è un'involuzione di C^+.

Sia ora $u \in \Gamma^+$ e scriviamo $u = v_1 \cdots v_{2r}$. Allora

$$\begin{aligned} N(u) \equiv \iota(u)u &= v_{2r} \cdots v_1 v_1 \cdots v_{2r} \\ &= \prod_{i=1}^{2r} Q(v_i) \in F^*. \end{aligned} \tag{63}$$

Se $u' \in \Gamma^+$, abbiamo

$$\begin{aligned} N(uu') &= \iota(uu')uu' = \iota(u')\iota(u)uu' \\ &= N(u)\iota(u')u' = N(u)N(u'). \end{aligned} \tag{64}$$

Quindi $u \mapsto N(u)$ è un omomorfismo di Γ^+ in F^*. Dalla (63) si vede che $N(\Gamma^+)$ è l'insieme dei prodotti $\prod_{i=1}^{2r} Q(v_i)$ con i v_i non isotropi in V, e che esso contiene F^{*2}, l'insieme dei quadrati degli elementi di F^*. Se f è una rotazione qualsiasi, esiste un $u \in \Gamma^+$ tale che $\chi(u) = f$, e u è determinato a meno di un fattore in F^*. Pertanto la classe laterale $N(u)F^{*2}$ nel gruppo F^*/F^{*2} è determinata da f. Diamo ora la definizione seguente, che collega questi concetti.

Definizione 4.7. *Il nucleo dell'omomorfismo N di Γ^+ in F^* si chiama* gruppo spinoriale $\mathrm{Spin}(V,Q)$. *La sua immagine $O'(V,Q)$ mediante la rappresentazione vettoriale χ si chiama* gruppo ortogonale ridotto. *Se f è una rotazione qualsiasi e $\chi(u) = f$, si chiama* norma spinoriale *di f la classe $N(u)F^{*2}$.*

Anche l'applicazione norma spinoriale è un omomorfismo (di $O^+(V,Q)$ in F^*/F^{*2}). La norma spinoriale di una rotazione si può definire direttamente, senza ricorrere all'algebra di Clifford. Data una rotazione f, possiamo scrivere $f = S_{v_1} \cdots S_{v_{2r}}$ e definire semplicemente la norma spinoriale di f come la classe $(\prod_{i=1}^{2r} Q(v_i))F^{*2}$. Poiché $\chi(v_1 \cdots v_{2r}) = f$ e $N(v_1 \cdots v_{2r}) = \prod_{i=1}^{2r} Q(v_i)$, si tratta dello stesso elemento di F^*/F^{*2} che abbiamo chiamato norma spinoriale. La difficoltà

della definizione diretta è che non risulta evidente che la norma spinoriale sia ben definita, poiché una rotazione si può scrivere in molti modi come prodotto di simmetrie. La definizione mediante l'algebra di Clifford mostra che si ottiene lo stesso elemento di F^*/F^{*2} qualunque sia la fattorizzazione di f in prodotto di simmetrie.

Ora il gruppo ortogonale ridotto si può definire anche come nucleo dell'applicazione norma spinoriale. Infatti, se $f \in O' = O'(V,Q)$, esiste un $u \in \mathrm{Spin}(V,Q)$ tale che $\chi(u) = f$. Allora la norma spinoriale di f è $N(u)F^{*2} = F^{*2}$. Viceversa, se la norma spinoriale della rotazione f è F^{*2}, si ha $f = S_{v_1} \cdots S_{v_{2r}}$ e $\prod_{i=1}^{2r} Q(v_i) = \beta^2$, con $\beta \neq 0$. Sostituendo v_1 con $\beta^{-1}v_1$, possiamo supporre che $\prod_{i=1}^{2r} Q(v_i) = 1$. Allora $\chi(v_1 \cdots v_{2r}) = f$ e $N(v_1 \cdots v_{2r}) = 1$, sicché la norma spinoriale di f è F^{*2}.

Il gruppo ortogonale ridotto contiene il sottogruppo dei commutatori Ω di O, poiché ogni commutatore si può scrivere nella forma

$$\begin{aligned}(S_{v_1} \cdots S_{v_r})(S_{v_{r+1}} \cdots S_{v_s})(S_{v_1} \cdots S_{v_r})^{-1}(S_{v_{r+1}} \cdots S_{v_s})^{-1} \\ = S_{v_1} \cdots S_{v_r}\, S_{v_{r+1}} \cdots S_{v_s}\, S_{v_r} \cdots S_{v_1}\, S_{v_s} \cdots S_{v_{r+1}},\end{aligned}$$

da cui è chiaro che la norma spinoriale è F^{*2}. Fra i vari sottogruppi di $O = O(V,Q)$ che abbiamo definito valgono dunque le inclusioni

$$O \supset O^+ \supset O' \supset \Omega. \tag{65}$$

Inoltre $O' \triangleleft O^+$ e O^+/O' è isomorfo al sottogruppo di F^*/F^{*2} formato dalle classi βF^{*2} in cui β è della forma $\prod_{i=1}^{2r} Q(v_i)$, con i v_i non isotropi. Nel caso in cui Q abbia indice di Witt positivo (BAI, p. 369) possiamo dire molto di più.

Teorema 4.16. *Sia Q di indice di Witt positivo. Allora il gruppo ortogonale ridotto $O'(V,Q)$ coincide con il sottogruppo dei commutatori Ω di $O(V,Q)$ e $O^+(V,Q)/O'(V,Q) \cong F^*/F^{*2}$.*

Dimostrazione. Poiché Q ha indice di Witt positivo, esiste un sottospazio U di V che è un piano iperbolico. Si ha quindi $V = U \oplus U^\perp$ e U ha una base (u,v) tale che $Q(u) = 0 = Q(v)$ e $B(u,v) = 1$. Le trasformazioni ortogonali che stabilizzano U e agiscono come l'identità su $U^\perp$ formano un sottogruppo O_1 isomorfo al gruppo ortogonale di U. Il gruppo $O_1^+ = O_1 \cap O^+(V,Q)$ è l'insieme delle applicazioni lineari f_α definite da $u \mapsto \alpha u$, $v \mapsto \alpha^{-1}v$, $w \mapsto w$ per $w \in U^\perp$, con $\alpha \in F^*$ (BAI, pp. 365–366). Si ha $f_\alpha = S_{u-v}S_{u-\alpha v}$, sicché la norma spinoriale di f_α è $Q(u-v)Q(u-\alpha v) = (-1)(-\alpha) = \alpha$. Poiché α può essere un qualsiasi elemento di F^*, questo prova che $O^+(V,Q)/O'(V,Q) \cong F^*/F^{*2}$. Sia ora y un vettore non isotropo qualsiasi di V e sia $Q(y) = \alpha$. Si ha allora $Q(u+\alpha v) = \alpha = Q(y)$. Per il teorema di Witt esiste dunque una trasformazione ortogonale g tale che $g(u+\alpha v) = y$ (BAI, p. 351). Allora $S_y = gS_{u+\alpha v}g^{-1}$. Sia $f \in O'$ e scriviamo $f = S_{v_1} \cdots S_{v_{2r}}$ con $\alpha_i = Q(v_i)$, sicché $\prod_{i=1}^{2r} \alpha_i \in F^{*2}$. Esistono pertanto trasformazioni ortogonali g_i tali che $S_{v_i} = g_i S_{u+\alpha_i v} g_i^{-1}$, $1 \leq i \leq 2r$. Quindi

$$f = g_1 S_{u+\alpha_1 v} g_1^{-1} \cdots g_{2r} S_{u+\alpha_{2r} v} g_{2r}^{-1}.$$

Poiché $O(V,Q)/\Omega$ è abeliano,

$$f \equiv h = S_{u+\alpha_1 v} \cdots S_{u+\alpha_{2r} v} \pmod{\Omega},$$

e per dimostrare che $f \in \Omega$ basta perciò provare che $h \in \Omega$. Ora $f \in O'$ e, poiché $\Omega \subset O'$, anche $h \in O'$. Quindi $h \in O_1^+$, sicché $h = f_\alpha = S_{u-v}S_{u-\alpha v}$, come sopra, e $\alpha = \beta^2$. Allora $h = f_\alpha = S_{u-v} f_\beta^{-1} S_{u-v} f_\beta \in \Omega$. □

Il principale teorema di struttura sui gruppi ortogonali, che abbiamo ricavato in BAI, afferma che, se Q ha indice di Witt positivo e $n \geq 3$, il gruppo $\Omega/(\Omega \cap \{1,-1\})$ è semplice, salvo nei casi

$n = 4$ con indice di Witt 2, e $n = 3$ con $|F| = 3$. Una domanda interessante è quando si abbia $-1 \in \Omega$. Ciò può avvenire soltanto per n pari. In questo caso vale la proposizione seguente.

Proposizione 4.11. *Sia n pari e sia Q di indice di Witt positivo. Allora $-1 \in \Omega$ se e solo se il discriminante è un quadrato.*

Dimostrazione. Sia $(u_1, u_2, \dots, u_n)$ una base ortogonale. Il discriminante ottenuto da questa base è $2^{-n} \prod_{i=1}^{n} Q(u_i)$, ed è un quadrato se e solo se $\prod_{i=1}^{n} Q(u_i)$ è un quadrato. D'altra parte $-1 = S_{u_1} S_{u_2} \cdots S_{u_n}$, perciò la norma spinoriale di -1 è $\prod_{i=1}^{n} Q(u_i)$. Per il teorema 4.15, dunque, $-1 \in \Omega$ se e solo se $\prod_{i=1}^{n} Q(u_i)$ è un quadrato. □

Esercizi

1. Mostrare che ogni algebra semplice centrale di grado due (p. 222) su un campo F di caratteristica diversa da due è un'algebra di quaternioni nel senso della definizione di p. 232 e che ogni tale algebra è isomorfa a un'algebra di Clifford $C(V, Q)$ con $\dim V = 2$.

Negli esercizi 2–9, Q è una forma quadratica su uno spazio vettoriale V di dimensione n su un campo F di caratteristica diversa da due; la forma bilineare associata B è non degenere.

2. Sia n pari e sia $(u_1, \dots, u_n)$ una base ortogonale di V su F, con $Q(u_i) = \gamma_i \neq 0$. Ottenere una formula esplicita

   $$C(V, Q) \cong (\alpha_1, \beta_1) \otimes (\alpha_2, \beta_2) \otimes \cdots \otimes (\alpha_\nu, \beta_\nu), \qquad \nu = n/2, \tag{66}$$

   dove (α, β) indica l'algebra con base $(1, i, j, k)$ e relazioni $i^2 = \alpha 1$, $j^2 = \beta 1$, $ij = k = -ji$.

3. Usare l'esercizio 2 per mostrare che $C(V, Q) \sim 1$ se Q ha indice di Witt massimo (uguale a ν; si veda BAI, p. 370).

4. Sia n dispari e si mantengano per il resto le notazioni dell'esercizio 2. Ottenere per $C(V, Q)$ una formula come la (66) tensorizzata con il centro, e per $C^+(V, Q)$ una formula come la (66).

5. Applicare l'esercizio 4 per ottenere la struttura di $C(V, Q)$ e di $C^+(V, Q)$ quando n è dispari e Q ha indice di Witt massimo.

6. Siano $n = 4$ e $F = \mathbb{R}$. Determinare la struttura di $C(V, Q)$ nei casi seguenti. Si prende una base ortogonale (u_1, u_2, u_3, u_4) di V e la matrice diagonale con elementi $Q(u_1), Q(u_2), Q(u_3), Q(u_4)$ è, rispettivamente,

   I. $\operatorname{diag}(1, 1, 1, 1)$,
   II. $\operatorname{diag}(1, 1, 1, -1)$,
   III. $\operatorname{diag}(1, 1, -1, -1)$,
   IV. $\operatorname{diag}(1, -1, -1, -1)$,
   V. $\operatorname{diag}(-1, -1, -1, -1)$.

7. Si osservi che $a \mapsto a^{\mathsf{t}}$, la trasposizione, è un'involuzione di $M_n(F)$. Usare il teorema di Skolem–Noether per mostrare che ogni involuzione di $M_n(F)$ è della forma $J_s \colon a \mapsto s a^{\mathsf{t}} s^{-1}$ con $s^{\mathsf{t}} = \pm s$. Sia $\operatorname{Sym} J_s$ il sottospazio di $M_n(F)$ degli elementi J_s-simmetrici, ossia tali che $J_s(a) = a$. Mostrare che $\dim \operatorname{Sym} J_s = n(n+1)/2$ se $s^{\mathsf{t}} = s$, e che $\dim \operatorname{Sym} J_s = n(n-1)/2$ se $s^{\mathsf{t}} = -s$.

8. Siano A un'algebra semplice centrale di dimensione finita su F ed E un suo campo di spezzamento. Considerando A come sottoalgebra di $A_E \cong M_n(E)$, mostrare che ogni involuzione J di A si prolunga in un unico modo a un'involuzione E-lineare J_E di A_E. Allora $J_E = J_s$ per qualche $s \in M_n(E)$ con $s^{\mathsf{t}} = \pm s$. Si dice che J è di *tipo ortogonale* o di *tipo simplettico* secondo che s sia simmetrica o antisimmetrica. Mostrare che J è di tipo ortogonale (simplettico) se e soltanto se $\dim \operatorname{Sym} J = n(n+1)/2$ (rispettivamente $n(n-1)/2$).

9. Determinare il tipo dell'involuzione principale di $C(V,Q)$ per n pari e quello dell'involuzione indotta dall'involuzione principale su $C^+(V,Q)$ per n dispari.

Se J e K sono involuzioni rispettivamente di A e di B, scriveremo $(A,J) \cong (B,K)$ se esiste un isomorfismo η di A su B tale che $\eta J = K\eta$.

10. Dimostrare la seguente estensione del lemma 5. Sia U un sottospazio di V di dimensione 2ν su cui la restrizione di B è non degenere; siano Q' e Q'' le restrizioni a U e a $U^\perp$ e δ' un discriminante di $B|_U$. Allora

$$C(V,Q) \cong C(U,Q') \otimes C(U^\perp, (-1)^\nu \delta' Q'').$$

Se ν è pari, tale isomorfismo identifica ι con $\iota \otimes \iota$ (qui ι è l'involuzione principale).[11]

11. Siano c il coniugio $a \mapsto \bar{a}$ in $\mathbb{C}$ e s l'involuzione standard $a \mapsto \bar{a}$ in $\mathbb{H}$. Mostrare che

$$(\mathbb{C} \otimes \mathbb{H}, c \otimes s) \cong (M_2(\mathbb{C}), *), \qquad (\mathbb{H} \otimes \mathbb{H}, s \otimes s) \cong (M_4(\mathbb{R}), t),$$

dove $(a_{ij})^* = (\bar{a}_{ji})$.

I tre esercizi successivi riguardano isomorfismi per $(C(V,Q), \iota)$, dove V è uno spazio vettoriale reale di dimensione finita e Q una forma quadratica definita positiva su V.

12. Mostrare che

$$\begin{array}{lll} \text{(i)} & (C(V,Q),\iota) \cong (\mathbb{R}\oplus\mathbb{R}, 1_{\mathbb{R}\oplus\mathbb{R}}) & \dim V = 1, \\ \text{(ii)} & (C(V,Q),\iota) \cong (M_2(\mathbb{R}), t) & \dim V = 2, \\ \text{(iii)} & (C(V,Q),\iota) \cong (M_2(\mathbb{C}), *) & \dim V = 3, \\ \text{(iv)} & (C(V,Q),\iota) \cong (M_2(\mathbb{H}), *) & \dim V = 4, \end{array}$$

dove nei casi (iii) e (iv) si pone $a^* = \bar{a}^{\mathsf{t}}$.

13. Mostrare che, se $n = 2\nu$, con $*$ come nell'esercizio 12,

$$(C(V,Q),\iota) \cong \begin{cases} (M_{2^\nu}(\mathbb{R}), t), & \nu \equiv 0,1 \pmod 4, \\ (M_{2^{\nu-1}}(\mathbb{H}), *), & \nu \equiv 2,3 \pmod 4. \end{cases}$$

L'ordine delle matrici è determinato dalla dimensione 2^n dell'algebra.[12]

[11] L'originale stampa U anche nel secondo fattore e vi scrive $-\delta' Q''$. Con il discriminante non segnato definito nel testo, il quadrato del prodotto degli elementi di una base ortogonale di U ha classe $(-1)^\nu \delta'$ modulo quadrati. Per $\nu = 1$ si ritrova il lemma 5. [N.d.T.]

[12] Nella scansione compaiono gli ordini $2^{2\nu}$ e $2^{2\nu-1}$. Quelli riportati nel testo italiano soddisfano rispettivamente $(2^\nu)^2 = 2^{2\nu}$ e $4(2^{\nu-1})^2 = 2^{2\nu}$. [N.d.T.]

14. Mostrare che, se $n = 2\nu - 1$, si ha

$$(C(V,Q),\iota) \cong \begin{cases} (M_{2^{\nu-1}}(\mathbb{R}), t)^{\oplus 2}, & \nu \equiv 1 \pmod 4, \\ (M_{2^{\nu-2}}(\mathbb{H}), *)^{\oplus 2}, & \nu \equiv 3 \pmod 4, \\ (M_{2^{\nu-1}}(\mathbb{C}), *), & \nu \equiv 0, 2 \pmod 4. \end{cases}$$

Nota di traduzione. L'originale riunisce i casi $\nu \equiv 1, 3 \pmod 4$ in una somma di due algebre reali di matrici con ordini stampati $2^{\nu-1}$ e $2^{2\nu-1}$. I due addendi sono isomorfi: per $n \equiv 1 \pmod 8$ sono reali, per $n \equiv 5 \pmod 8$ quaternionici. Nei tre casi della formula la dimensione reale totale è $2^{2\nu-1}$.

Gli esercizi 15–18 tracciano una dimostrazione del teorema fondamentale di struttura delle algebre di Clifford su campi arbitrari, compresa la caratteristica due.

15. Definire un'algebra di quaternioni su un campo arbitrario F come un'algebra generata da due elementi i, j con le relazioni

(67) $$i^2 = i + \alpha 1, \qquad 4\alpha + 1 \neq 0, \qquad j^2 = \beta 1 \neq 0, \qquad ji = (1 - i)j.$$

Mostrare che ogni algebra di questo tipo è semplice centrale di dimensione quattro. Mostrare che, se $\operatorname{char} F \neq 2$, la definizione è equivalente a quella data nel testo.

Sia ora V uno spazio vettoriale di dimensione n, munito di una forma quadratica Q con forma bilineare associata non degenere. Si osservi che, se $\operatorname{char} F = 2$, B è alternante e quindi n è pari.

16. Mostrare che, se $n = 2$, $C(V,Q)$ è un'algebra di quaternioni.

17. Mostrare che il lemma 5 vale su un campo F arbitrario. (*Suggerimento.* Sia (u, v) una base qualunque di U e si ponga $\bar{d} = \bar{u}\bar{v} - \bar{v}\bar{u}$. Servirsi di questo $\bar{d}$ al posto di quello impiegato nel testo per estendere la dimostrazione al caso di un campo arbitrario.)

18. Dimostrare il teorema 4.13 per B non degenere su un campo F arbitrario. Si osservi che la dimostrazione di $\dim C(V,Q) = 2^n$ data nel testo mediante riduzione al caso non degenere si estende a ogni F.

Negli esercizi 19–21 si suppone $\operatorname{char} F = 2$.

19. Definire $C^+ = C^+(V,Q)$ come per $\operatorname{char} F \neq 2$: è la sottoalgebra generata da tutti i prodotti uv, $u, v \in V$. Mostrare che $\dim C^+ = 2^{n-1}$ e che, fissato un qualsiasi vettore non isotropo u_1, C^+ è generata dagli elementi $u_1 v$, $v \in V$. Mostrare che la sottoalgebra C' di C^+ generata dagli $u_1 v$ per $Q(u_1) \neq 0$ e $v \perp u_1$ è isomorfa a un'algebra di Clifford determinata da uno spazio di dimensione $n - 2$, e che quest'algebra è semplice centrale di dimensione 2^{n-2}. Sia $(u_1, v_1, \ldots, u_\nu, v_\nu)$ una base simplettica, ossia $B(u_i, v_j) = \delta_{ij}$ e $B(u_i, u_j) = 0 = B(v_i, v_j)$. Mostrare che $c = \sum_{i=1}^{\nu} u_i v_i$ appartiene al centro di C^+, che $c \notin F1$ e che

$$c^2 + c + \sum_{i=1}^{\nu} Q(u_i) Q(v_i) = 0.$$

Dedurre che $C^+ \cong F[c] \otimes C'$ e che $F[c]$ è il centro di C^+. Mostrare che $F[c]$ è un campo oppure la somma diretta di due copie di F, secondo che $\sum_{i=1}^{\nu} Q(u_i) Q(v_i)$ non sia, oppure sia, della forma $\beta^2 + \beta$, $\beta \in F$. Concludere che nel primo caso C^+ è semplice, nel secondo è somma diretta di due algebre semplici centrali isomorfe.

20. Sia $F^{[2]}$ l'insieme degli elementi della forma $\beta^2 + \beta$, con $\beta \in F$. Mostrare che $F^{[2]}$ è un sottogruppo del gruppo additivo di F e porre $G = F/F^{[2]}$. Per una base simplettica $(u_1, v_1, \ldots, u_\nu, v_\nu)$ di V, definire in G l'elemento

$$\operatorname{Arf} Q = \sum_{i=1}^{\nu} Q(u_i)Q(v_i) + F^{[2]}. \tag{68}$$

Mostrare che esso è indipendente dalla scelta della base simplettica. Si chiama $\operatorname{Arf} Q$ l'*invariante di Arf* di Q. Si osservi che l'ultimo risultato dell'esercizio 19 si può enunciare così: $C^+(V, Q)$ è semplice se e soltanto se $\operatorname{Arf} Q \neq 0$.[13]

21. Mostrare che esiste un'unica derivazione D di $C = C(V, Q)$ tale che $Dx = x$ per ogni $x \in V$. Mostrare che $C^+(V, Q)$ è la sottoalgebra delle D-costanti, cioè degli elementi a tali che $Da = 0$.

Nota storica

Le algebre di Clifford, definite per generatori e relazioni, furono introdotte da W. K. Clifford in un articolo apparso nel 1878 nel primo volume dell'*American Journal of Mathematics*. In quel lavoro Clifford diede una fattorizzazione tensoriale delle sue algebre in algebre di quaternioni e nel centro. La prima applicazione delle algebre di Clifford ai gruppi ortogonali fu data da R. Lipschitz nel 1884. Il fisico P. A. M. Dirac riscoprì le algebre di Clifford nel caso $n = 4$ e le impiegò nella sua teoria dello spin dell'elettrone. Di qui le espressioni «gruppo spinoriale» e «norma spinoriale». Nel caso reale i gruppi spinoriali sono gruppi di rivestimento semplicemente connessi dei gruppi ortogonali propri.[14] Come nella teoria delle funzioni di variabile complessa, rappresentazioni a più valori del gruppo ortogonale diventano a un sol valore per il gruppo spinoriale. Rappresentazioni di questo tipo comparivano nella teoria di Dirac. L'argomento fu ripreso con vari gradi di generalità da R. Brauer e H. Weyl (1935) e da E. Cartan (1938), e in piena generalità da C. Chevalley (1954).

Riferimenti bibliografici

N. Jacobson, *Structure of Rings*, American Mathematical Society Colloquium Publications, XXXVII, Providence, 1956; edizione riveduta, 1964.

I. Herstein, *Noncommutative Rings*, Carus Mathematical Monographs, n. 15, Mathematical Association of America, John Wiley, New York, 1968.

C. Faith, *Algebra II. Ring Theory*, Springer, New York, 1976.

Per le algebre di Clifford:

C. Chevalley, *The Algebraic Theory of Spinors*, Columbia University Press, New York, 1954.

[13] Il rinvio a «exercise 14» nell'originale si riferisce all'esercizio 19. [N.d.T.]

[14] Per il gruppo ortogonale speciale euclideo questa affermazione vale in dimensione almeno tre; in dimensione due il rivestimento spinoriale è un doppio rivestimento del cerchio. [N.d.T.]

5 Teoria classica delle rappresentazioni dei gruppi finiti

Fra gli strumenti più potenti per lo studio dei gruppi finiti vi sono la teoria delle rappresentazioni e, in particolare, la teoria dei caratteri. Estese ai gruppi localmente compatti, queste teorie costituiscono un importante ramo dell'analisi moderna, che generalizza l'analisi classica di Fourier. La teoria delle rappresentazioni dei gruppi finiti è quasi interamente opera di Frobenius. Notevoli perfezionamenti e semplificazioni sono dovuti a Schur. Negli ultimi cinquant'anni Brauer vi ha aggiunto risultati profondi. La teoria delle rappresentazioni ha avuto una parte importante nello straordinario sviluppo della teoria della struttura dei gruppi finiti iniziato quando Feit e Thompson dimostrarono una congettura centenaria di Burnside, secondo cui ogni gruppo finito di ordine dispari è risolubile.

In questo capitolo studieremo la teoria classica delle rappresentazioni dei gruppi finiti su spazi vettoriali di dimensione finita sul campo $\mathbb{C}$ dei numeri complessi o, più in generale, su campi di caratteristica che non divide l'ordine del gruppo. Questa condizione sulla caratteristica implica la completa riducibilità delle rappresentazioni o, equivalentemente, la semisemplicità delle algebre di gruppo. Ciò permette di applicare la teoria della struttura e delle rappresentazioni delle algebre semisemplici di dimensione finita alla teoria delle rappresentazioni dei gruppi finiti. Ma vi è ancora molto da dire, e precisamente sulla teoria dei caratteri, che si può sviluppare in gran parte senza ricorrere alla teoria delle algebre.

Ricaveremo i risultati classici di Frobenius, Schur e Burnside e quelli di Brauer sui caratteri indotti e sui campi di spezzamento. Fra i contributi più importanti di Brauer vi è la teoria modulare, che studia le rappresentazioni sui campi la cui caratteristica divide l'ordine del gruppo e i legami fra queste rappresentazioni e quelle su $\mathbb{C}$. Questa teoria esula dalla nostra esposizione. Daremo varie applicazioni della teoria dei caratteri a risultati sulla struttura dei gruppi finiti.

5.1 Rappresentazioni e rappresentazioni matriciali dei gruppi

Definizione 5.1. *Per rappresentazione ρ di un gruppo G intendiamo un omomorfismo di G nel gruppo* $\mathrm{GL}(V)$ *delle trasformazioni lineari biiettive di uno spazio vettoriale V di dimensione finita su un campo F.*

Diremo che ρ è una rappresentazione di G su F e che agisce su V/F. La dimensione di V si chiama *grado* della rappresentazione. Per definizione ρ è un'applicazione $G \to \mathrm{GL}(V)$ tale che

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2), \qquad g_i \in G. \tag{1}$$

Ne segue immediatamente che $\rho(1) = 1_V$, $\rho(g^{-1}) = \rho(g)^{-1}$ e, in generale, $\rho(g^m) = \rho(g)^m$ per $m \in \mathbb{Z}$. Osserviamo inoltre che le condizioni $\rho(g) \in \mathrm{GL}(V)$ e (1) si possono sostituire con le tre condizioni $\rho(g) \in \mathrm{End}_F V$, (1) e $\rho(1) = 1$. Esse implicano subito che $\rho(g) \in \mathrm{GL}(V)$, quindi ρ è una rappresentazione.

Sia $B = (u_1, u_2, \ldots, u_n)$ una base di V/F. Per $a \in \mathrm{End}_F V$ scriviamo

$$a u_i = \sum_{j=1}^{n} \alpha_{ji} u_j, \qquad 1 \le i \le n, \tag{2}$$

ottenendo la matrice (α) di elemento (j, i) uguale ad α_{ji}. L'applicazione $a \mapsto (\alpha)$ è un isomorfismo di $\mathrm{End}_F V$ su $M_n(F)$. Pertanto, se ρ è una rappresentazione di G su V, l'applicazione

$$g \longmapsto \rho_B(g), \tag{3}$$

dove $\rho_B(g)$ denota la matrice di $\rho(g)$ nella base B, è un omomorfismo da G nel gruppo $\mathrm{GL}_n(F)$ delle matrici invertibili $n \times n$ a elementi in F. Tale omomorfismo si chiama *rappresentazione*

matriciale di grado n di G. Se si passa dalla base B alla base $C = (v_1, \dots, v_n)$, con $v_i = \sum_j \beta_{ji} u_j$ e $(\beta) \in \mathrm{GL}_n(F)$, ρ_B viene sostituita da ρ_C, dove

$$\rho_C(g) = (\beta)^{-1} \rho_B(g)(\beta). \tag{4}$$

Questa rappresentazione matriciale si dice *simile* a ρ_B. È chiaro che ogni rappresentazione matriciale si ottiene da una rappresentazione nel modo appena descritto.

Un omomorfismo di G nel gruppo simmetrico S_n, o, equivalentemente, un'azione di G sull'insieme finito $\{1, 2, \dots, n\}$ (BAI, p. 71), dà luogo a una rappresentazione. Sia l'azione descritta da

$$gi = \pi(g)i, \tag{5}$$

dove $\pi : G \to S_n$ è l'omomorfismo dato. Sia V lo spazio vettoriale di base $(u_1, u_2, \dots, u_n)$ e sia $\rho(g)$ la trasformazione lineare di V tale che

$$\rho(g)u_i = u_{\pi(g)i}. \tag{6}$$

Allora $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ e $\rho(1) = 1$, sicché ρ è una rappresentazione di G. Le rappresentazioni così ottenute si chiamano *rappresentazioni di permutazione*. Le caratterizza la proprietà di stabilizzare una qualche base B di V/F. Particolarmente interessante è quella ottenuta dall'azione di G su sé stesso per traslazioni sinistre (BAI, p. 72). Essa si chiama *rappresentazione regolare* di G.

Esempi.

1. Sia G il gruppo ciclico generato da un elemento g di ordine n. Si ha un omomorfismo di G in S_n che manda g nel ciclo $(12 \cdots n)$. Quest'azione equivale all'azione di G su sé stesso per traslazioni sinistre. La rappresentazione di permutazione associata manda g nella trasformazione lineare $\rho(g)$ tale che

   $$\rho(g)u_i = u_{i+1} \quad (1 \le i < n), \qquad \rho(g)u_n = u_1. \tag{7}$$

   Nella corrispondente rappresentazione matriciale g è rappresentato dalla matrice

   $$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}. \tag{8}$$

   La si ottiene applicando la (2) al caso (6).

2. Sia $G = S_3$, di elementi $1, (12), (13), (23), (123), (132)$. L'applicazione identica è un isomorfismo di G su sé stesso. Ne risultano una rappresentazione di permutazione e la rappresentazione matriciale associata

$$1 \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (12) \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$(13) \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (23) \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$(123) \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad (132) \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Fissati un gruppo G e un campo F, consideriamo la classe $\Sigma(G,F)$ delle rappresentazioni di G su spazi vettoriali di campo base F. Su $\Sigma(G,F)$ si può definire una ricca struttura algebrica. Siano anzitutto ρ_1, ρ_2 rappresentazioni di G rispettivamente su $V_1/F, V_2/F$. Formiamo lo spazio $V_1 \otimes_F V_2$ e definiamo $\rho_1 \otimes \rho_2$ ponendo

$$(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g), \tag{9}$$

dove, come di consueto, per trasformazioni lineari a_i di V_i, $a_1 \otimes a_2$ è la trasformazione lineare di $V_1 \otimes V_2$ tale che

$$(a_1 \otimes a_2)(x_1 \otimes x_2) = a_1 x_1 \otimes a_2 x_2. \tag{10}$$

Se b_i, $i = 1, 2$, è una seconda trasformazione lineare di V_i, si ha $(a_1 \otimes a_2)(b_1 \otimes b_2) = a_1 b_1 \otimes a_2 b_2$. Quindi per $g_1, g_2 \in G$

$$\begin{aligned}(\rho_1 \otimes \rho_2)(g_1 g_2) &= \rho_1(g_1 g_2) \otimes \rho_2(g_1 g_2) \\ &= \rho_1(g_1)\rho_1(g_2) \otimes \rho_2(g_1)\rho_2(g_2) \\ &= (\rho_1(g_1) \otimes \rho_2(g_1))(\rho_1(g_2) \otimes \rho_2(g_2)) \\ &= ((\rho_1 \otimes \rho_2)(g_1))((\rho_1 \otimes \rho_2)(g_2)).\end{aligned}$$

Dunque $\rho_1 \otimes \rho_2$ è una rappresentazione, detta *prodotto tensoriale* delle rappresentazioni ρ_1, ρ_2.

Se $(u_1, \ldots, u_n)$ è una base di V_1/F e $(v_1, \ldots, v_m)$ una base di V_2/F, gli mn vettori $u_i \otimes v_j$ formano una base di $(V_1 \otimes V_2)/F$. Li ordiniamo lessicograficamente:

$$(u_1 \otimes v_1, \ldots, u_1 \otimes v_m, u_2 \otimes v_1, \ldots, u_2 \otimes v_m, \ldots, u_n \otimes v_m). \tag{11}$$

Se $a_1 \in \mathrm{End}_F V_1$ ha matrice $(\alpha^{(1)})$ nella base $(u_1, \ldots, u_n)$ e $a_2 \in \mathrm{End}_F V_2$ ha matrice $(\alpha^{(2)})$ in $(v_1, \ldots, v_m)$, si ha

$$a_1 u_i = \sum_j \alpha^{(1)}_{ji} u_j, \quad a_2 v_k = \sum_l \alpha^{(2)}_{lk} v_l, \quad (a_1 \otimes a_2)(u_i \otimes v_k) = \sum_{j,l} \alpha^{(1)}_{ji} \alpha^{(2)}_{lk} (u_j \otimes v_l).$$

La matrice di $a_1 \otimes a_2$ nella base (11) è quindi

$$\begin{pmatrix} \alpha^{(1)}_{11}(\alpha^{(2)}) & \alpha^{(1)}_{12}(\alpha^{(2)}) & \cdots & \alpha^{(1)}_{1n}(\alpha^{(2)}) \\ \alpha^{(1)}_{21}(\alpha^{(2)}) & \alpha^{(1)}_{22}(\alpha^{(2)}) & \cdots & \alpha^{(1)}_{2n}(\alpha^{(2)}) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(1)}_{n1}(\alpha^{(2)}) & \alpha^{(1)}_{n2}(\alpha^{(2)}) & \cdots & \alpha^{(1)}_{nn}(\alpha^{(2)}) \end{pmatrix}. \tag{12}$$

Indichiamo questa matrice con $(\alpha^{(1)}) \otimes (\alpha^{(2)})$. In particolare, se $\rho_{1B_1}(g)$ è la matrice di $\rho_1(g)$ nella base $B_1 = (u_1, \ldots, u_n)$ e $\rho_{2B_2}(g)$ quella di $\rho_2(g)$ nella base $B_2 = (v_1, \ldots, v_m)$, la matrice di $(\rho_1 \otimes \rho_2)(g)$ nella base (11) è $\rho_{1B_1}(g) \otimes \rho_{2B_2}(g)$.

Indichiamo come di consueto con V^* lo spazio duale dei funzionali lineari su V/F. Alla base $(u_1, \ldots, u_n)$ di V/F corrisponde la base duale (o complementare) $(u_1^*, \ldots, u_n^*)$ di V^*/F, dove $u_i^*(u_j) = \delta_{ij}$, $1 \le j \le n$. Se a è una trasformazione lineare di V/F, la *trasposta* a^* in V^* è tale che

$$(a^* x^*)(y) = x^*(ay), \qquad y \in V,\ x^* \in V^*. \tag{13}$$

Se $a u_i = \sum_j \alpha_{ji} u_j$ e $a^* u_k^* = \sum_l \beta_{lk} u_l^*$, allora $(a^* u_k^*)(u_i) = \sum_l \beta_{lk} u_l^*(u_i) = \beta_{ik}$ e $u_k^*(a u_i) = u_k^*(\sum_j \alpha_{ji} u_j) = \alpha_{ki}$. Pertanto $\beta_{ik} = \alpha_{ki}$ e la matrice di a^* nella base duale è la trasposta della

matrice di a nella base $(u_1, \dots, u_n)$. L'applicazione $a \mapsto a^*$ è un anti-isomorfismo di $\mathrm{End}_F V$ su $\mathrm{End}_F V^*$. Ne segue che $a \mapsto (a^*)^{-1}$ è un isomorfismo dal gruppo $\mathrm{GL}(V)$ delle trasformazioni lineari biiettive di V su $\mathrm{GL}(V^*)$.

Componiamo una rappresentazione ρ di G su V con questo isomorfismo. Otteniamo una rappresentazione $g \mapsto (\rho(g)^*)^{-1}$ di G su V^*, detta *rappresentazione contragrediente* di ρ e indicata con ρ^*. Evidentemente ha lo stesso grado di ρ. Se $B = (u_1, \dots, u_n)$ e B^* è la base duale di V^*, le rappresentazioni matriciali corrispondenti sono legate da $\rho^*_{B^*}(g) = ({}^t\rho_B(g))^{-1}$.

L'applicazione $\rho \mapsto \rho^*$ si può considerare come un'operazione unaria in $\Sigma(G, F)$. Vi è anche un'importante operazione nullaria, la *rappresentazione unità* 1 o 1_G, per la quale V ha dimensione uno e $1(g) = 1_V$ per ogni g. La corrispondente rappresentazione matriciale, rispetto a una base qualsiasi, è $g \mapsto (1)$, dove (1) è la matrice 1×1 di elemento 1.

Siano ρ_i, $i = 1, 2$, rappresentazioni di G su V_i/F. Diciamo che ρ_1, ρ_2 sono *equivalenti* se esiste un'applicazione lineare biiettiva $\eta : V_1 \to V_2$ tale che

$$\rho_2(g) = \eta \rho_1(g) \eta^{-1}, \qquad g \in G. \tag{14}$$

Esercizi.

1. Sia ρ la rappresentazione del gruppo ciclico $\langle g \rangle$ dell'esempio 1 e sia $\mathbb{C}$ il campo base. Mostrare che ρ è equivalente alla rappresentazione ρ' tale che $\rho'(g)u_i = \zeta^i u_i$, dove $\zeta = e^{2\pi i/n}$.

2. Siano ρ_i, $i = 1, 2$, rappresentazioni di G su V_i/F e sia $V = \hom_F(V_1, V_2)$. Per $l \in V$, porre $\rho(g)l = \rho_2(g) l \rho_1(g)^{-1}$. Verificare che ρ è una rappresentazione e mostrare che è equivalente a $\rho_1^* \otimes \rho_2$.

3. Sia ι l'applicazione identica di $\mathrm{GL}(V)$, che è una rappresentazione di $\mathrm{GL}(V)$ su V. Considerare la rappresentazione $\iota^* \otimes \iota$ su $V^* \otimes V$. Mostrare che i vettori $c \in V^* \otimes V$ tali che $(\iota^* \otimes \iota)(a)c = c$ per ogni $a \in \mathrm{GL}(V)$ formano un sottospazio di dimensione uno di $V^* \otimes V$. Trovarvi un vettore non nullo.

4. Mostrare che, se ρ_i è una rappresentazione su V_i, $i = 1, 2$, allora $\rho_1 \otimes \rho_2$ e $\rho_2 \otimes \rho_1$ sono equivalenti.

5.2 Completa riducibilità

Lo studio delle rappresentazioni di un gruppo G si può ricondurre a quello delle rappresentazioni della sua algebra di gruppo. Dati un gruppo G e un campo F, l'algebra di gruppo $F[G]$ è l'algebra su F di base G e con moltiplicazione

$$\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) = \sum_{g,h} \alpha_g \beta_h gh, \qquad \alpha_g, \beta_h \in F. \tag{15}$$

Se ρ rappresenta G sullo spazio vettoriale V/F, l'omomorfismo di gruppi ρ si estende in modo unico all'omomorfismo di algebre da $F[G]$ in $\mathrm{End}_F V$ dato da

$$\sum \alpha_g g \longmapsto \sum \alpha_g \rho(g). \tag{16}$$

Viceversa, se $\rho : F[G] \to \mathrm{End}_F V$ è un omomorfismo e V/F ha dimensione finita, la restrizione di ρ a G è una rappresentazione, poiché $\rho(1) = 1$ implica $\rho(g) \in \mathrm{GL}(V)$ per ogni g. Ricordiamo

che, data una rappresentazione di $F[G]$, ossia un omomorfismo $F[G] \to \mathrm{End}_F V$, si può fare di V un $F[G]$-modulo. Basta definire l'azione di $F[G]$ su V ponendo

$$\Big(\sum \alpha_g g\Big)\, x = \sum \alpha_g \rho(g) x, \qquad x \in V. \tag{17}$$

Viceversa, un $F[G]$-modulo V è un F-modulo, dunque uno spazio vettoriale su F. Se V/F ha dimensione finita si ottiene una rappresentazione ρ di G prendendo per $\rho(g)$ l'applicazione $x \mapsto gx$, trasformazione lineare di V/F. Le rappresentazioni di G su spazi vettoriali di dimensione finita su F equivalgono dunque agli $F[G]$-moduli di dimensione finita come F-moduli.

Attraverso l'algebra di gruppo i concetti usuali della teoria dei moduli si trasferiscono alle rappresentazioni dei gruppi. Se ρ rappresenta G su V, un sottomodulo U dell'$F[G]$-modulo V è precisamente un sottospazio $\rho(G)$-*invariante*, cioè stabile per ogni $\rho(g)$, $g \in G$. Si ottiene una rappresentazione $\rho|U$ di G su U, dove $(\rho|U)(g)$ è la restrizione di $\rho(g)$ a U. La chiamiamo una *sottorappresentazione* di ρ. Si ha anche il modulo V/U, cui corrisponde la rappresentazione $\rho|V/U$ di G, dove $(\rho|V/U)(g)$ è la trasformazione lineare $x + U \mapsto \rho(g)x + U$. La chiamiamo *rappresentazione quoziente* di ρ.

Sia $B = (u_1, \dots, u_n)$ una base di V tale che $(u_1, \dots, u_r)$ sia base del sottospazio $\rho(G)$-invariante U. Consideriamo la corrispondente rappresentazione matriciale ρ_B. Poiché ogni $\rho(g)$ stabilizza U, per $1 \le i \le r$ il vettore $\rho(g)u_i$ è combinazione lineare di $u_1, \dots, u_r$. Quindi ogni $\rho_B(g)$, $g \in G$, ha la forma «ridotta»

$$\left(\begin{array}{ccc|ccc} \rho_{11} & \cdots & \rho_{1r} & \rho_{1,r+1} & \cdots & \rho_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \rho_{r1} & \cdots & \rho_{rr} & \rho_{r,r+1} & \cdots & \rho_{rn} \\ \hline & & & \rho_{r+1,r+1} & \cdots & \rho_{r+1,n} \\ & 0 & & \vdots & & \vdots \\ & & & \rho_{n,r+1} & \cdots & \rho_{nn} \end{array}\right). \tag{18}$$

I blocchi in alto a sinistra sono le matrici della rappresentazione di G su U nella base $(u_1, \dots, u_r)$, e quelli in basso a destra sono le matrici della rappresentazione di G su V/U nella base $(u_{r+1} + U, \dots, u_n + U)$. Viceversa, se esiste una base $(u_1, \dots, u_n)$ nella quale tutte le matrici delle $\rho(g)$ hanno la forma (18), $U = \sum_{j=1}^{r} F u_j$ è un sottospazio $\rho(G)$-invariante e dunque un $F[G]$-sottomodulo di V.

Se $V = U \oplus U'$ con U, U' sottomoduli, possiamo scegliere una base $B = (u_1, \dots, u_n)$ in cui $(u_1, \dots, u_r)$ sia base di U e $(u_{r+1}, \dots, u_n)$ base di U'. Le matrici $\rho_B(g)$ hanno allora forma (18) e i blocchi $r \times (n - r)$ in alto a destra sono tutti nulli. Posto $\rho_1 = \rho|U$, $\rho_2 = \rho|U'$, diciamo che ρ è *somma diretta* delle sottorappresentazioni ρ_1, ρ_2 e scriviamo $\rho = \rho_1 \oplus \rho_2$. Sia p la proiezione su U determinata dalla decomposizione $V = U \oplus U'$. Scrivendo $x \in V$ come $x = y + y'$, $y \in U$, $y' \in U'$, si ha $\rho(g)x = \rho(g)y + \rho(g)y'$, con $\rho(g)y \in U$, $\rho(g)y' \in U'$ per ogni $g \in G$. Poiché p è l'applicazione $x \mapsto y$, si ha $p\rho(g)x = \rho(g)y = \rho(g)px$. Dunque p commuta con ogni $\rho(g)$. Viceversa, se U è un sottospazio $\rho(G)$-invariante e vi è una proiezione p di V su U che commuta con ogni $\rho(g)$, possiamo scrivere $V = pV \oplus (1 - p)V$, con $pV = U$. Inoltre $\rho(g)(1 - p)V = (1 - p)\rho(g)V = (1 - p)V$. Dunque $U' = (1 - p)V$ è $\rho(G)$-invariante e si ha $V = U \oplus U'$.

Una rappresentazione ρ di G si dice *irriducibile* (*completamente riducibile*) se tale è l'$F[G]$-modulo corrispondente. Ricordiamo che un modulo V è completamente riducibile se e solo se soddisfa una qualunque delle condizioni seguenti: (1) $V = \sum_i V_i$, con V_i sottomoduli irriducibili; (2) $V \neq 0$ e per ogni sottomodulo U esiste un sottomodulo U' tale che $V = U \oplus U'$ (teorema 3.10). Useremo queste condizioni per provare due teoremi che danno condizioni sufficienti per

la completa riducibilità. Il primo è fondamentale per la teoria delle rappresentazioni dei gruppi finiti.

Teorema di Maschke. *Ogni rappresentazione ρ di un gruppo finito G su uno spazio vettoriale V/F è completamente riducibile se la caratteristica di F non divide $|G|$.*

Dimostrazione. Sia U un sottospazio $\rho(G)$-invariante di V. Scriviamo $V = U \oplus U_0$, con U_0 sottospazio, anche non invariante, e sia p_0 la corrispondente proiezione su U. Mediante una media costruiremo una proiezione su U che commuti con ogni $\rho(g)$, $g \in G$. Poniamo

$$p = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} p_0 \rho(g). \tag{19}$$

Poiché $\operatorname{char} F \nmid |G|$, esiste $|G|^{-1}$ in F e p è ben definito. Per $g' \in G$,

$$\begin{aligned} \rho(g')^{-1} p \rho(g') &= \frac{1}{|G|} \sum_{g \in G} \rho(g')^{-1} \rho(g)^{-1} p_0 \rho(g) \rho(g') \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(gg')^{-1} p_0 \rho(gg') \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} p_0 \rho(g) = p. \end{aligned}$$

Pertanto $\rho(g')p = p\rho(g')$ per ogni g'. Evidentemente $p \in \operatorname{End}_F V$. Se $y \in U$, allora $p_0 y = y$ e, poiché $\rho(g)y \in U$, $p_0 \rho(g) y = \rho(g) y$. Dunque $\rho(g)^{-1} p_0 \rho(g) y = y$, e

$$py = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} p_0 \rho(g) y = \frac{1}{|G|} |G| y = y. \tag{20}$$

Per $x \in V$ si ha $p_0 x \in U$ e $\rho(g)^{-1} p_0 \rho(g) x \in U$, dunque $px \in U$. Le due condizioni $py = y$ per $y \in U$ e $px \in U$ per $x \in V$ implicano che p è una proiezione su U. Allora $V = U \oplus U'$, dove $U' = (1-p)V$ è $\rho(G)$-invariante perché p commuta con ogni $\rho(g)$. □

La formulazione in termini di rappresentazioni matriciali è immediata dalla discussione precedente. H. Maschke dimostrò il risultato in forma matriciale per $F = \mathbb{C}$. L. E. Dickson osservò per primo che vale per ogni F tale che $\operatorname{char} F \nmid |G|$.

Se ρ è una rappresentazione completamente riducibile di G su V, l'$F[G]$-modulo V si decompone come

$$V = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_2^{(m_2)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)},$$

dove i $V_i^{(k)}$ sono irriducibili e $V_i^{(k)} \cong V_i^{(l)}$ per ogni k, l, mentre $V_i^{(k)} \ncong V_j^{(l)}$ se $i \neq j$. Per il teorema 3.12, i sottomoduli $W_i = \sum_k V_i^{(k)}$ sono le componenti omogenee di V. Se ρ_i è una qualsiasi rappresentazione irriducibile di G equivalente alla sottorappresentazione determinata dai $V_i^{(k)}$, scriviamo

$$\rho \sim m_1 \rho_1 \oplus m_2 \rho_2 \oplus \cdots \oplus m_r \rho_r. \tag{21}$$

Chiamiamo ρ_i un *costituente irriducibile* di ρ e m_i la sua *molteplicità*. Per il teorema 3.14 le classi di equivalenza dei costituenti irriducibili e le loro molteplicità sono determinate univocamente. Si osservi anche che $m_i = q_i/n_i$, dove $q_i = \dim W_i$, $n_i = \dim V_i^{(k)}$. Anche da ciò risulta che m_i è indipendente dalla particolare decomposizione di V in somma diretta di sottomoduli irriducibili.

Se H è un sottogruppo di G e ρ rappresenta G su V, la restrizione di ρ a H è una rappresentazione di H che indicheremo con ρ_H. Mostreremo che se $H \trianglelefteq G$ e ρ è completamente

riducibile, anche ρ_H lo è. Basta provarlo per ρ irriducibile, e in tal caso si possono precisare le relazioni fra i costituenti irriducibili e le loro molteplicità. Dobbiamo prima definire il coniugio di rappresentazioni di un sottogruppo normale.

Sia $H \trianglelefteq G$ e sia σ una rappresentazione di H su U. Per ogni $g \in G$ l'applicazione

$$h \longmapsto \sigma(ghg^{-1}) \tag{22}$$

è la composizione dell'automorfismo $h \mapsto ghg^{-1}$ di H con l'omomorfismo σ. La (22) è dunque una rappresentazione di H su U, che indicheremo con ${}^g\sigma$. Una rappresentazione equivalente a ${}^g\sigma$ si dirà una *coniugata* di σ, o più precisamente una sua *g-coniugata*. Ogni sottospazio $\sigma(H)$-invariante è evidentemente ${}^g\sigma(H)$-invariante e, poiché $\sigma = {}^{g^{-1}}({}^g\sigma)$, le due rappresentazioni hanno lo stesso reticolo di $F[H]$-sottomoduli. In particolare, se σ è irriducibile, ogni sua coniugata è irriducibile. Siano ora σ_1, σ_2 rappresentazioni equivalenti di H su U_1, U_2. Esiste un'applicazione lineare biiettiva $\eta : U_1 \to U_2$ tale che $\sigma_2(h) = \eta\sigma_1(h)\eta^{-1}$ per $h \in H$. Vale dunque anche $\sigma_2(ghg^{-1}) = \eta\sigma_1(ghg^{-1})\eta^{-1}$, cosicché ${}^g\sigma_1$ e ${}^g\sigma_2$ sono equivalenti. Possiamo ora dimostrare il seguente risultato.

Teorema di (A. H.) Clifford. *Sia $H \trianglelefteq G$ e sia ρ una rappresentazione irriducibile di G. Allora ρ_H è completamente riducibile e tutti i suoi costituenti irriducibili sono coniugati e hanno la stessa molteplicità.*

Dimostrazione. Sia V lo spazio su cui agisce ρ e sia U un $F[H]$-sottomodulo irriducibile di V. Evidentemente $\sum_{g\in G} \rho(g)U$ è un sottospazio $\rho(G)$-invariante di V contenente U, dunque $V = \sum \rho(g)U$. Per $h \in H$, $y \in U$, si ha

$$\rho(h)\rho(g)y = \rho(hg)y = \rho(gg^{-1}hg)y = \rho(g)\rho(g^{-1}hg)y \in \rho(g)U. \tag{23}$$

Pertanto $\rho(g)U$ è $\rho(H)$-invariante. Sia σ la rappresentazione di H su U e sia σ' quella su $\rho(g)U$. Per la (23), $\sigma'(h)\rho(g)y = \rho(g)\,{}^{g^{-1}}\sigma(h)y$. Poiché $y \mapsto \rho(g)y$ manda biiettivamente e linearmente U su $\rho(g)U$, si vede che σ' è una coniugata di σ. Dunque $\rho(g)U$ è un $F[H]$-modulo irriducibile e $V = \sum \rho(g)U$ esprime V come somma di $F[H]$-moduli irriducibili le cui rappresentazioni sono coniugate. Allora V è somma diretta di alcuni dei $\rho(g)U$, quindi ρ_H è completamente riducibile e i suoi costituenti irriducibili sono coniugati. Se U_1, U_2 sono $F[H]$-sottomoduli irriducibili isomorfi, anche $\rho(g)U_1, \rho(g)U_2$ sono $F[H]$-sottomoduli isomorfi. Di conseguenza ogni $\rho(g)$ permuta le componenti omogenee dell'$F[H]$-modulo V. Otteniamo così un'azione di G, attraverso $\rho(G)$, sull'insieme S di queste componenti. L'azione è transitiva, poiché, dato un qualunque $F[H]$-sottomodulo irriducibile U, ogni altro sottomodulo irriducibile è isomorfo a $\rho(g)U$ per qualche $g \in G$. Ne segue che tutti i costituenti irriducibili hanno la stessa molteplicità. □

Esercizi.

1. Provare la seguente estensione del teorema di Maschke. Sia ρ una rappresentazione di un gruppo G anche infinito. Supporre che G contenga un sottogruppo normale H di indice finito $[G : H]$ non divisibile per $\operatorname{char} F$. Mostrare che, se $\rho|H$ è completamente riducibile, anche ρ lo è.

2. Sia $F = \mathbb{C}$ e sia $H(x, y)$ una forma hermitiana definita positiva su $V/\mathbb{C}$, cioè tale che $H(x, x) > 0$ per ogni $x \neq 0$ (BAI, pp. 381–384). Sia ρ una rappresentazione di un gruppo G su V per la quale ogni $\rho(g)$ è unitario rispetto a H, ossia $H(\rho(g)x, \rho(g)y) = H(x, y)$ per $x, y \in V$. Una tale rappresentazione si dice *unitaria*. Mostrare che, se U è $\rho(G)$-invariante, anche $U^\perp$ lo è. Dedurne che ρ è completamente riducibile.

3. Con le notazioni dell'esercizio 2, siano G finito, ρ una rappresentazione di G su V e $H_0(x, y)$ una qualsiasi forma hermitiana definita positiva su $V/\mathbb{C}$. Porre

$H(x,y) = \sum_{g\in G} H_0(\rho(g)x, \rho(g)y)$. Mostrare che H è hermitiana definita positiva e che ogni $\rho(g)$ è unitario rispetto a H. Servirsi di questo fatto e dell'esercizio 2 per dimostrare il teorema di Maschke nel caso $F = \mathbb{C}$.

4. Il gruppo lineare proiettivo di uno spazio vettoriale V/F di dimensione finita è $\mathrm{PGL}(V) = \mathrm{GL}(V)/F^*1$, dove F^* è il gruppo moltiplicativo degli elementi non nulli di F. Un omomorfismo da G in $\mathrm{PGL}(V)$ si chiama *rappresentazione proiettiva* di G. Per ogni $g \in G$ si scelga un rappresentante $\rho(g) \in \mathrm{GL}(V)$ della classe corrispondente a g. Si ha allora $\rho(g_1g_2) = \gamma_{g_1,g_2}\rho(g_1)\rho(g_2)$ con $\gamma_{g_1,g_2} \in F^*$. Definire i sottospazi $\rho(G)$-invarianti e la completa riducibilità come per le rappresentazioni ordinarie. Dimostrare l'analogo del teorema di Maschke per le rappresentazioni proiettive.

5. Mostrare che ρ è irriducibile (completamente riducibile) se e solo se ρ^* è irriducibile (completamente riducibile).

6. Siano ψ una rappresentazione di G su W e V un sottospazio $\psi(G)$-invariante. Posto $\rho = \psi|V$, mostrare che $\rho^* \otimes \psi$ ha una sottorappresentazione equivalente alla rappresentazione unità.

7. Siano ψ, ρ rappresentazioni di G rispettivamente su W, V. Se ρ è irriducibile e $\rho^* \otimes \psi$ ha una sottorappresentazione equivalente alla rappresentazione unità, mostrare che ψ ha una sottorappresentazione equivalente a ρ.

8. Mostrare che i seguenti gruppi di trasformazioni lineari di uno spazio V/F di dimensione finita sono irriducibili: (1) $\mathrm{GL}(V)$; (2) $\mathrm{O}(V,Q)$, gruppo delle trasformazioni ortogonali rispetto a una forma quadratica non degenere Q; (3) $\mathrm{O}^+(V,Q)$, sottogruppo delle rotazioni di $\mathrm{O}(V,Q)$. (Si veda il capitolo 6 di BAI.)

5.3 Applicazione della teoria delle rappresentazioni delle algebre

Vi sono due metodi principali per sviluppare la teoria delle rappresentazioni dei gruppi finiti: la teoria della struttura e delle rappresentazioni delle algebre di dimensione finita, applicata alle algebre di gruppo, e la teoria dei caratteri. Molti risultati si possono ottenere con entrambi i metodi e la scelta è spesso una questione di gusto. In questo paragrafo introduciamo il primo metodo, mentre la teoria dei caratteri comparirà nel ğ 5. Ci occuperemo principalmente di rappresentazioni di gruppi finiti su campi la cui caratteristica non divide l'ordine del gruppo. I primi due teoremi, tuttavia, non richiedono queste restrizioni.

Cominciamo col definire alcune algebre di trasformazioni lineari associate a una rappresentazione ρ di un gruppo G che agisce su uno spazio vettoriale V/F. Abbiamo anzitutto l'*algebra inviluppante* $\mathrm{Env}\,\rho(G)$, costituita dalle trasformazioni lineari della forma $\sum_{g\in G} \alpha_g\rho(g)$, $\alpha_g \in F$. Se estendiamo ρ a un omomorfismo ρ di $A = F[G]$ come nella (16), allora $\mathrm{Env}\,\rho(G) = \rho(A)$. Abbiamo poi l'algebra $A' = \mathrm{End}_A V$. Essa è evidentemente l'insieme delle trasformazioni lineari di V che commutano con ogni $a \in \rho(A)$, dunque $\mathrm{End}_A V$ è il centralizzante di $\rho(A)$ in $\mathrm{End}_F V$. Se ρ è irriducibile, per il lemma di Schur A' è un'algebra con divisione. Consideriamo quindi $A'' = \mathrm{End}_{A'} V$, l'algebra delle trasformazioni lineari che commutano con ogni $a' \in A'$. Evidentemente $A'' \supseteq \mathrm{Env}\,\rho(G) = \rho(A)$. Osserviamo che, se poniamo $A''' = \mathrm{End}_{A''} V$, si vede subito che $A''' = A'$. Pertanto il procedimento di formazione di algebre mediante il passaggio all'algebra degli endomorfismi si arresta ad A''. Chiamiamo quest'ultima il *doppio centralizzante* di $\rho(A)$ e diciamo che ρ ha la *proprietà del doppio centralizzante* se $A'' = \rho(A)$. Per le rappresentazioni completamente riducibili vale il seguente risultato generale.

Teorema 5.1. *Ogni rappresentazione completamente riducibile ρ di un gruppo G ha la proprietà del doppio centralizzante.*

Dimostrazione. Si vede facilmente che questo è un caso particolare del teorema 4.10 (p. 222). È però un po' più semplice fondare la dimostrazione direttamente sul teorema di densità. Sia $(u_1, u_2, \dots, u_n)$ una base di V/F e sia l un elemento del doppio centralizzante di $\rho(A)$. Per il teorema di densità esiste $a \in \rho(A)$ tale che $au_i = lu_i$, $1 \leq i \leq n$. Quindi $l = a \in \rho(A)$ e $A'' = \rho(A)$. □

Enunciamo ora il seguente teorema.

Teorema 5.2. *Un gruppo finito ha soltanto un numero finito di rappresentazioni irriducibili a due a due inequivalenti.*

Ciò segue applicando il teorema 4.5 (p. 208) all'anello artiniano $A = F[G]$. Omettiamo i dettagli, poiché questo risultato non avrà alcun ruolo nel seguito. Dimostriamo ora il

Teorema 5.3. *L'algebra di gruppo $A = F[G]$ di un gruppo finito G su un campo F è semisemplice se e solo se* $\operatorname{char} F \nmid |G|$.

Dimostrazione. Supponiamo dapprima che $\operatorname{char} F \nmid |G|$. Allora ogni rappresentazione di G è completamente riducibile. Quindi A, considerata come A-modulo (sinistro), è completamente riducibile. Ne segue che A è semisemplice per il teorema di struttura degli anelli artiniani semiprimitivi (p. 203). Supponiamo ora che $\operatorname{char} F \mid |G|$. Consideriamo l'elemento di A

$$z = \sum_{g \in G} g. \tag{24}$$

È diverso da zero e si ha evidentemente

$$g'z = z = zg' \tag{25}$$

per ogni $g' \in G$. Dunque Fz è un ideale di A. Dalla (25) otteniamo $z^2 = \sum_{g' \in G} g'z = |G|z = 0$, poiché $\operatorname{char} F \mid |G|$. Quindi Fz è un ideale nilpotente non nullo di A, e A non è semisemplice. □

Per il resto del paragrafo supporremo che G sia finito e che $\operatorname{char} F \nmid |G|$. Si ha

$$A = F[G] = A_1 \oplus A_2 \oplus \cdots \oplus A_s, \tag{26}$$

dove le A_i sono le componenti semplici. Per la forma matriciale del teorema di Wedderburn,

$$A_i \simeq M_{n_i}(\Delta_i), \tag{27}$$

dove Δ_i è un'algebra con divisione su F. Se I_i è un ideale sinistro minimale di A_i, esso è un ideale sinistro minimale di A e fornisce perciò una rappresentazione irriducibile di G. Inoltre $I_i \not\simeq I_j$ se $i \neq j$, e ogni rappresentazione irriducibile di G è equivalente a una ottenuta da uno degli I_i (teorema 4.4, p. 208). Vi sono dunque s classi di equivalenza di rappresentazioni irriducibili di G.

Determiniamo ora il grado della rappresentazione irriducibile fornita da I_i. Sia $\{e_{ij} \mid 1 \leq i, j \leq n\}$ il consueto sistema di unità matriciali in $M_n(\Delta)$, dove Δ è un'algebra con divisione. Allora

$$M_n(\Delta) = M_n(\Delta)e_{11} \oplus \cdots \oplus M_n(\Delta)e_{nn}, \tag{28}$$

e $M_n(\Delta)e_{ii}$ è un ideale sinistro minimale, mentre ogni ideale sinistro minimale di $M_n(\Delta)$ è isomorfo, come $M_n(\Delta)$-modulo sinistro, a $M_n(\Delta)e_{ii}$. Abbiamo la sottoalgebra $\Delta 1$ delle matrici

$d1 = \operatorname{diag}\{d, d, \dots, d\}$ e possiamo considerare $M_n(\Delta)$ come spazio vettoriale (sinistro) su Δ, definendo $d(a)$, per la matrice (a), come $(d1)(a)$. Allora $\{e_{ij}\}$ è una base di $M_n(\Delta)$ su Δ, sicché la dimensione su Δ è n^2. Analogamente $M_n(\Delta)e_{ii} = \Delta e_{1i} \oplus \cdots \oplus \Delta e_{ni}$, dunque la dimensione di $M_n(\Delta)e_{ii}$ su Δ è n. La dimensione di $M_n(\Delta)e_{ii}$ su F è allora

$$[M_n(\Delta)e_{ii} : \Delta]\,[\Delta : F] = nd, \tag{29}$$

dove $d = [\Delta : F]$. Ne segue che $[I_i : F] = n_i d_i$, dove $d_i = [\Delta_i : F]$, e questo è il grado della rappresentazione irriducibile fornita da I_i. Possiamo raccogliere tali risultati nel seguente teorema.

Teorema 5.4. *Sia $A = F[G]$ l'algebra di gruppo di un gruppo finito G su un campo F tale che* $\operatorname{char} F \nmid |G|$. *Sia $A = A_1 \oplus \cdots \oplus A_s$, dove le A_i sono le componenti semplici dell'algebra semisemplice A. Supponiamo $A_i \simeq M_{n_i}(\Delta_i)$, con Δ_i algebra con divisione, e poniamo $[\Delta_i : F] = d_i$. Se I_i è un ideale sinistro minimale di A_i, esso fornisce una rappresentazione irriducibile di G, e le rappresentazioni irriducibili ottenute dagli I_i, $1 \le i \le s$, costituiscono un sistema di rappresentanti delle classi di equivalenza di rappresentazioni irriducibili di G. Inoltre la rappresentazione irriducibile fornita da I_i ha grado $n_i d_i$.*

Sia $\{\rho_i \mid 1 \le i \le s\}$ un sistema di rappresentanti delle classi di equivalenza di rappresentazioni irriducibili di G. Come sopra, possiamo prendere per ρ_i la rappresentazione irriducibile fornita da un ideale sinistro minimale I_i di A_i. Possiamo comunque supporre che ρ_i sia equivalente alla rappresentazione irriducibile determinata da I_i. Se ρ è una rappresentazione qualsiasi di G che agisce su V, allora $V = V_1 \oplus \cdots \oplus V_r$, dove i V_j sono $\rho(G)$-invarianti e $\rho|V_j$ è irriducibile. Si ha allora $\rho|V_j \sim \rho_i$ per qualche i e, fissato i, il numero m_i degli indici j tali che $\rho|V_j \sim \rho_i$ è indipendente dalla decomposizione $V = V_1 \oplus \cdots \oplus V_r$. Come a p. 254, possiamo scrivere $\rho \sim m_1\rho_1 \oplus m_2\rho_2 \oplus \cdots \oplus m_s\rho_s$ e chiamare m_i la *molteplicità* di ρ_i nella rappresentazione ρ.

Consideriamo ora A come A-modulo (sinistro). Indichiamo con ρ la rappresentazione di G determinata da questo modulo. Ogni $\rho(g)\colon x \mapsto gx$ manda la base G di A in sé. È chiaro che ρ è la rappresentazione regolare di G (p. 248). Le decomposizioni (26) e (28) mostrano che la molteplicità, nella rappresentazione regolare, della rappresentazione irriducibile ρ_i determinata da I_i è n_i. Abbiamo dunque il seguente risultato sulla rappresentazione regolare di G.

Teorema 5.5. *Con le notazioni del teorema 5.4, la molteplicità di ρ_i nella rappresentazione regolare è n_i.*

Il numero delle classi di equivalenza di rappresentazioni irriducibili di G è il numero s di componenti semplici A_i di $A = F[G]$. Indichiamo con $\operatorname{cent} A$ il centro di A. Allora

$$\operatorname{cent} A = \operatorname{cent} A_1 \oplus \cdots \oplus \operatorname{cent} A_s, \tag{30}$$

dove il centro $\operatorname{cent} A_i$ è isomorfo al centro di $M_{n_i}(\Delta_i)$ e quindi al centro di Δ_i. Pertanto $\operatorname{cent} A_i$ è un campo ed è una componente semplice dell'algebra commutativa semisemplice $\operatorname{cent} A$. Dunque s è il numero delle componenti semplici di $\operatorname{cent} A$. Determiniamo ora una base di quest'algebra.

Proposizione 5.1. *Sia $G = C_1 \cup C_2 \cup \cdots \cup C_r$, con $C_1 = \{1\}$, la decomposizione di G in classi di coniugio (*BA I*, p. 74). Poniamo*

$$c_i = \sum_{g_i \in C_i} g_i. \tag{31}$$

Allora $(c_1, c_2, \dots, c_r)$ è una base di $\operatorname{cent} F[G]$.

Dimostrazione. Se $g \in G$, si ha $g^{-1}c_i g = \sum_{g_i \in C_i} g^{-1}g_i g = \sum g_i = c_i$, poiché l'applicazione $x \mapsto g^{-1}xg$ permuta gli elementi della classe di coniugio C_i. Quindi c_i commuta con ogni $g \in G$

e con ogni $\sum \alpha_g g \in F[G]$. Pertanto $c_i \in \operatorname{cent} F[G]$. Sia ora $c = \sum \gamma_g g \in \operatorname{cent} F[G]$. Se $h \in G$,

$$h^{-1}ch = \sum_g \gamma_g h^{-1}gh = \sum_g \gamma_{hgh^{-1}} g,$$

sicché la condizione $h^{-1}ch = c$ dà $\gamma_{hgh^{-1}} = \gamma_g$, $h \in G$. Due elementi g e g' della stessa classe di coniugio hanno dunque lo stesso coefficiente nell'espressione $c = \sum \gamma_g g$, e c è una combinazione lineare dei c_i. I c_i sono evidentemente linearmente indipendenti e perciò $(c_1, c_2, \ldots, c_r)$ è una base di $\operatorname{cent} F[G]$. □

Il risultato precedente, insieme al fatto che il numero s di classi di equivalenza di rappresentazioni irriducibili di G è il numero delle componenti semplici, mostra che $s \leq r$, dove r è il numero delle classi di coniugio. Più precisamente, $r = \sum_i [\operatorname{cent} A_i : F]$. Ciò mostra che $s = r$ se e solo se $\operatorname{cent} A_i = F$ per ogni i, ossia se le A_i sono semplici centrali. Poiché $\operatorname{cent} A_i$ è un'estensione di grado finito di F, se F è algebricamente chiuso si ha $\operatorname{cent} A_i = F$ per ogni i. In questo caso importante il numero delle classi di equivalenza di rappresentazioni irriducibili è dunque il numero delle classi di coniugio. Nel caso algebricamente chiuso si ha il seguente importante risultato.

Teorema 5.6. *Siano G un gruppo finito e F un campo algebricamente chiuso tale che* $\operatorname{char} F \nmid |G|$. *Sia s il numero delle classi di coniugio di G. Il numero delle classi di equivalenza di rappresentazioni irriducibili su F (che agiscono su spazi vettoriali V/F) è s e, se $\rho_1, \ldots, \rho_s$ sono rappresentanti di queste classi e n_i è il grado di ρ_i, allora*

$$|G| = \sum_{i=1}^{s} n_i^2. \tag{32}$$

Dimostrazione. La prima affermazione è già stata dimostrata. Per la seconda, usiamo le (26) e (27) e il fatto che, essendo F algebricamente chiuso, l'unica algebra con divisione di dimensione finita su F è F stesso. Allora $A = F[G] = A_1 \oplus \cdots \oplus A_s$ e $A_i \simeq M_{n_i}(F)$. Sicché $[A : F] = |G| = \sum_{i=1}^{s} n_i^2$, e il teorema 5.4 mostra che n_i è il grado della rappresentazione irriducibile ρ_i associata ad A_i. □

Esempi.

1. Sia $G = \langle z \rangle$ il gruppo ciclico di ordine n generato da z, e sia $F = \mathbb{C}$. Allora $A = \mathbb{C}[G]$ è somma diretta di n copie di $\mathbb{C}$. Vi sono pertanto n rappresentazioni irriducibili inequivalenti, tutte di grado 1. È chiaro che nelle rappresentazioni matriciali corrispondenti si ha $z \mapsto (e^{2\pi i r/n})$, dove le parentesi indicano una matrice 1×1 e $r = 1, 2, \ldots, n$.

2. Sia $G = D_n$ il gruppo diedrale di ordine $2n$ generato da due elementi r, s tali che $r^n = 1$, $s^2 = 1$, $srs^{-1} = r^{-1}$ (*BA I*, pp. 34, 70). Gli elementi di D_n sono r^k, $r^k s$, $0 \leq k \leq n-1$, e vale la relazione $sr^k = r^{-k}s$. Quindi $(r^k s)^2 = 1$, e gli n elementi $r^k s$ hanno periodo due. Dalla tavola di moltiplicazione

$$\begin{aligned} r^k r^l &= r^{k+l}, & r^k (r^l s) &= r^{k+l} s, \\ (r^l s) r^k &= r^{l-k} s, & (r^k s)(r^l s) &= r^{k-l} \end{aligned}$$

si vede facilmente che, se $n = 2\nu + 1$ è dispari, con $\nu \geq 1$, vi sono $\nu + 2$ classi di coniugio con rappresentanti 1, r^k $(1 \leq k \leq \nu)$, s. Se $n = 2\nu$, con $\nu \geq 1$, vi sono $\nu + 3$ classi di coniugio con rappresentanti 1, r^k $(1 \leq k \leq \nu)$, s, rs.

D'altra parte possiamo elencare, nei due casi, altrettante rappresentazioni matriciali irriducibili inequivalenti su $\mathbb{C}$.

Caso $n = 2\nu + 1$, $\nu \geq 1$. Abbiamo ρ_1, la rappresentazione unità; ρ_2, la rappresentazione matriciale di grado 1 in cui $r \mapsto (1)$ e $s \mapsto (-1)$; e, per $1 \leq l \leq \nu$, le rappresentazioni matriciali σ_l di grado 2 date da

$$r \longmapsto \begin{pmatrix} \omega^l & 0 \\ 0 & \omega^{-l} \end{pmatrix}, \qquad s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \omega = e^{2\pi i/n}.$$

Caso $n = 2\nu$, $\nu \geq 1$. Abbiamo ρ_1, la rappresentazione unità; ρ_2, la rappresentazione matriciale di grado 1 in cui $r \mapsto (1)$, $s \mapsto (-1)$; ρ_3, la rappresentazione matriciale di grado 1 in cui $r \mapsto (-1)$, $s \mapsto (1)$; ρ_4, la rappresentazione matriciale di grado 1 in cui $r \mapsto (-1)$, $s \mapsto (-1)$; e le rappresentazioni σ_l di cui sopra, per $1 \leq l \leq \nu - 1$.

È facile verificare che le rappresentazioni elencate sono irriducibili e inequivalenti. Esse costituiscono pertanto un sistema di rappresentanti delle classi di equivalenza di rappresentazioni irriducibili di D_n. Come controllo, possiamo verificare la relazione (32) fra i gradi nei due casi:

$$\begin{aligned} n = 2\nu + 1, &\qquad 1 + 1 + 4\nu = 2(2\nu + 1) = 2n, \\ n = 2\nu, &\qquad 4 \cdot 1 + 4(\nu - 1) = 4\nu = 2n. \end{aligned}$$

Consideriamo ora un procedimento di estensione del campo base di una rappresentazione. Occorre richiamare alcuni semplici fatti sull'estensione del campo base di uno spazio vettoriale. Per i nostri scopi basta limitarsi a spazi vettoriali di dimensione finita. Sia dunque V/F uno spazio vettoriale di dimensione n sul campo F e sia K un'estensione di F. Possiamo formare il prodotto tensoriale $V_K = K \otimes_F V$, che si può considerare come spazio vettoriale su K. L'applicazione iniettiva $v \mapsto 1 \otimes v$ permette di identificare V con un F-sottospazio di V_K tale che $KV = V_K$. Inoltre elementi di V indipendenti su F sono indipendenti su K, e ogni base di V/F è una base di V_K/K (si veda p. 220). Una trasformazione lineare l di V/F ha un'unica estensione a una trasformazione lineare di V_K/K. Indichiamo anche l'estensione con l. Queste estensioni generano $\operatorname{End}_K V_K$ come spazio vettoriale su K, ossia $\operatorname{End}_K V_K = K \operatorname{End}_F V$. Inoltre $\operatorname{End}_K V_K \simeq K \otimes_F \operatorname{End}_F V$.

Supponiamo ora che ρ sia una rappresentazione di G che agisce su V/F. Le relazioni di definizione $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$, $\rho(1) = 1_V$, danno le relazioni $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$, $\rho(1) = 1_{V_K}$, per le estensioni. Dunque $\rho_K \colon g \mapsto \rho(g)$ (in V_K) è una rappresentazione di G che agisce su V_K. La chiamiamo la rappresentazione ottenuta da ρ per *estensione del campo base* a K. È chiaro che, posto $A = F[G]$, si ha $K[G] \simeq A_K$ e $\rho_K(K[G]) = K\rho(A) \simeq \rho(A)_K$. Vale inoltre il seguente utile risultato.

Proposizione 5.2.

$$\operatorname{End}_{K[G]} V_K = K \operatorname{End}_{F[G]} V \simeq (\operatorname{End}_{F[G]} V)_K.$$

Dimostrazione. Gli elementi di $\operatorname{End}_{F[G]} V$ (rispettivamente di $\operatorname{End}_{K[G]} V_K$) sono le trasformazioni lineari di V (rispettivamente di V_K) che commutano con ogni $\rho(g)$, $g \in G$. È dunque chiaro che $K \operatorname{End}_{F[G]} V \subseteq \operatorname{End}_{K[G]} V_K$. Per dimostrare l'inclusione opposta, scegliamo una base (λ_i) di K/F. Ogni elemento di $\operatorname{End}_K V_K$ si può scrivere in uno e un solo modo nella forma $\sum_i \lambda_i l_i$, con $l_i \in \operatorname{End}_F V$. Le condizioni che esprimono che questa somma commuta con ogni $\rho(g)$ implicano che gli l_i commutano con ogni $\rho(g)$ e quindi che $l_i \in \operatorname{End}_{F[G]} V$. Abbiamo dunque l'uguaglianza $\operatorname{End}_{K[G]} V_K = K \operatorname{End}_{F[G]} V$. Abbiamo osservato che $\operatorname{End}_K V_K \simeq K \otimes_F \operatorname{End}_F V$.

Ciò implica che, per ogni sottospazio E di $\operatorname{End}_F V$ su F, si ha $KE \simeq K \otimes_F E$. In particolare $K \operatorname{End}_{F[G]} V \simeq K \otimes_F \operatorname{End}_{F[G]} V = (\operatorname{End}_{F[G]} V)_K$. □

È chiaro che, se U è un sottospazio $\rho(G)$-invariante di V, allora $KU = U_K$ è un sottospazio $\rho(G)$-invariante di V_K. Perciò, se ρ_K è irriducibile, anche ρ è irriducibile. Il viceversa può non valere, come mostrano i seguenti esempi.

Esempi.

1. Sia $G = \langle g \rangle$ il gruppo ciclico di ordine 4 e sia $F = \mathbb{R}$. Consideriamo la rappresentazione di grado due su $\mathbb{R}$ in cui $\rho(g)$ è la trasformazione lineare di matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

rispetto alla base (u, v) di $V/\mathbb{R}$. Poiché il polinomio caratteristico di questa matrice è $\lambda^2 + 1$, $\rho(g)$ agisce irriducibilmente su V. Consideriamo ora $\rho_{\mathbb{C}}$. Abbiamo la base $(z = u + iv, w = u - iv)$ di $V_{\mathbb{C}}/\mathbb{C}$ e

$$\rho(g)_{\mathbb{C}} z = \rho(g)u + i\rho(g)v = -v + iu = iz,$$
$$\rho(g)_{\mathbb{C}} w = \rho(g)u - i\rho(g)v = -v - iu = -iw.$$

Dunque $\mathbb{C}z$ e $\mathbb{C}w$ sono sottospazi $\rho_{\mathbb{C}}(G)$-invarianti. Le rappresentazioni irriducibili $\rho_{\mathbb{C}}|_{\mathbb{C}z}$ e $\rho_{\mathbb{C}}|_{\mathbb{C}w}$ sono inequivalenti.

2. Sia G il gruppo dei quaternioni $\{\pm 1, \pm i, \pm j, \pm k\}$, sottogruppo del gruppo moltiplicativo dell'algebra H dei quaternioni di Hamilton su $\mathbb{R}$. Sia ρ la rappresentazione di G per la quale $\rho(g)$ è la moltiplicazione a sinistra $x \mapsto gx$, $x \in H$, $g \in G$. La rappresentazione ρ è irriducibile poiché H è un'algebra con divisione. D'altra parte $H_{\mathbb{C}} \simeq M_2(\mathbb{C})$, poiché $\mathbb{C}$ è un campo di spezzamento per H (p. 228). Poiché $M_2(\mathbb{C})$ è somma diretta di due ideali sinistri minimali, ne segue che $H_{\mathbb{C}}$ è somma diretta di due sottospazi $\rho_{\mathbb{C}}(G)$-invarianti I_1 e I_2. Le rappresentazioni $\rho_{\mathbb{C}}|_{I_1}$ e $\rho_{\mathbb{C}}|_{I_2}$ sono irriducibili ed equivalenti.

Una rappresentazione ρ si dice *assolutamente irriducibile* se ρ_K è irriducibile per ogni estensione K del campo base F. Per l'irriducibilità e l'irriducibilità assoluta vale il seguente criterio.

Teorema 5.7. *Siano G un gruppo finito e ρ una rappresentazione di G che agisce su V/F, con $\operatorname{char} F \nmid |G|$, e sia $A = F[G]$. Allora ρ è irriducibile se e solo se $A' = \operatorname{End}_A V$ è un'algebra con divisione, e ρ è assolutamente irriducibile se e solo se $A' = F1$.*

Dimostrazione. Se ρ è irriducibile, A' è un'algebra con divisione per il lemma di Schur; se ρ è assolutamente irriducibile, $A'_K = \operatorname{End}_{K[G]} V_K$ è un'algebra con divisione per ogni estensione K di F. Ciò implica $A' = F1$. Supponiamo infatti $A' \neq F1$ e sia $c \in A'$, $c \notin F1$. Il polinomio minimo $f(\lambda)$ di c su F ha allora grado maggiore di 1 ed è irriducibile, poiché A' è un'algebra con divisione. Poniamo $K = F[\lambda]/(f(\lambda))$ e consideriamo A'_K. Il polinomio minimo di $c \in A'_K$ è $f(\lambda)$, che è riducibile in $K[\lambda]$. Pertanto A'_K non è un'algebra con divisione, contrariamente a quanto abbiamo dimostrato. Dunque $A' = F1$.

Supponiamo ora che ρ sia riducibile, sicché esiste un sottospazio $\rho(G)$-invariante $U \neq V, 0$. Per il teorema di Maschke esiste una proiezione p su U che commuta con ogni $\rho(g)$. Allora p è un idempotente di A' diverso da 0 e da 1, e A' non è un'algebra con divisione. Quindi, se A' è un'algebra con divisione, ρ è irriducibile. Poiché $A' = F1$ implica $A'_K = K1$, ne segue che, se $A' = F1$, ρ è assolutamente irriducibile. □

Un campo F si dice *campo di spezzamento* per il gruppo G se ogni rappresentazione irriducibile di G su F è assolutamente irriducibile. Vale il seguente teorema.

Teorema 5.8. *Siano G un gruppo finito e F un campo tale che* $\operatorname{char} F \nmid |G|$. *Allora F è un campo di spezzamento per G se e solo se $F[G]$ è somma diretta di algebre di matrici $M_n(F)$.*

Dimostrazione. Sia $A = F[G] = A_1 \oplus \cdots \oplus A_s$, dove le A_i sono le componenti semplici di A, e sia I_i un ideale sinistro minimale di A_i. La rappresentazione ρ_i di G che agisce su I_i è irriducibile e ogni rappresentazione irriducibile di G su F è equivalente a una delle ρ_i. Dunque F è un campo di spezzamento per G se e solo se ogni ρ_i è assolutamente irriducibile. Per il teorema 5.7 ciò accade se e solo se $\operatorname{End}_A I_i = F1$ per $1 \leq i \leq s$. Ora $\operatorname{End}_A I_i = \Delta_i'$ è un'algebra con divisione e, per il teorema 5.1, $\rho_i(A) = \operatorname{End}_{\Delta_i'} I_i \simeq M_{n_i}(\Delta_i)$, dove $\Delta_i = (\Delta_i')^{\mathrm{op}}$ e n_i è la dimensione di I_i come spazio vettoriale su Δ_i'. D'altra parte, poiché le A_j, $j \neq i$, annullano I_i e A_i è semplice, si ha $\rho_i(A) \simeq A_i$. Dunque $A_i \simeq M_{n_i}(\Delta_i)$. Supponiamo ora che F sia un campo di spezzamento. Allora $\Delta_i' = F$ e $A_i \simeq M_{n_i}(F)$. Viceversa, supponiamo $A_i \simeq M_{n_i'}(F)$ per qualche n_i'. Allora $M_{n_i'}(F) \simeq M_{n_i}(\Delta_i)$. Per il teorema di isomorfismo delle algebre artiniane semplici, ciò implica $n_i' = n_i$ e $\Delta_i = F$. Quindi $\Delta_i' = F1$, $\operatorname{End}_A I_i = \Delta_i' = F1$, e F è un campo di spezzamento. □

Esercizi.

1. Sia G finito e sia ρ una rappresentazione irriducibile di G su F, con $\operatorname{char} F \nmid |G|$. Mostrare che $\sum_{g \in G} \rho(g) = |G|1$ se ρ è la rappresentazione unità e che $\sum_{g \in G} \rho(g) = 0$ negli altri casi.

2. Sia G un gruppo finito e sia $F = \mathbb{Q}$ oppure $\mathbb{Z}/(p)$, dove $p \nmid |G|$. Mostrare che esiste un'estensione di grado finito di F che è un campo di spezzamento per G.

3. Siano ρ_1 e ρ_2 rappresentazioni di G su un campo infinito F e sia K un'estensione di F. Mostrare che, se ρ_{1K} e ρ_{2K} sono equivalenti, allora ρ_1 e ρ_2 sono equivalenti. Vale lo stesso se F è finito?

5.4 Rappresentazioni irriducibili di S_n

In generale è difficile determinare la struttura dell'algebra di gruppo $F[G]$ di un dato gruppo finito G. Come abbiamo visto nel paragrafo precedente, se $\operatorname{char} F \nmid |G|$, ciò equivale a determinare un sistema di rappresentanti delle classi di equivalenza di rappresentazioni irriducibili di G su F o, come diremo d'ora innanzi per brevità, a determinare le rappresentazioni irriducibili di G su F. In questo paragrafo trattiamo un esempio importante in cui ciò è possibile, quello di $G = S_n$. Determineremo un insieme di idempotenti che generano ideali sinistri minimali di $F[S_n]$ ($\operatorname{char} F \nmid n!$) e forniscono le rappresentazioni irriducibili di S_n su F. Questi risultati sono dovuti a Frobenius e ad A. Young. La nostra esposizione segue quella di J. von Neumann, nella forma presentata da van der Waerden in *Algebra*, vol. 2, p. 246.

Ricordiamo che il numero delle classi di coniugio di S_n è $p(n)$, il numero delle partizioni (non ordinate) di n (BAI, p. 75). Se $\{r_1, r_2, \ldots, r_h\}$ è una tale partizione (ossia $r_i \geq 1$ e $\sum_{i=1}^h r_i = n$), le permutazioni che sono prodotti di cicli disgiunti di lunghezze $r_1, r_2, \ldots, r_h$ formano una classe di coniugio, e ogni classe di coniugio si ottiene in questo modo. Per la partizione $\alpha = \{r_1, r_2, \ldots, r_h\}$ supponiamo $r_1 \geq r_2 \geq \cdots \geq r_h$ e ci serviamo di quest'ordine per ordinare lessicograficamente l'insieme delle partizioni. Così, se $\beta = \{s_1, s_2, \ldots, s_k\}$, con $s_1 \geq s_2 \geq \cdots \geq s_k$, si ha $\alpha > \beta$ se $r_i > s_i$ nel primo posto in cui $r_i \neq s_i$. Ogni partizione

$\alpha = \{r_1, r_2, \ldots, r_h\}$ definisce una *tavola (di Young)*

$$
\begin{array}{llllllll}
\square & \square & \cdot & \cdot & \cdot & \cdot & \square & r_1 \text{ caselle} \\
\square & \square & \cdot & \cdot & \cdot & \square & & r_2 \text{ caselle} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\
\square & \square & \cdot & \cdot & \square & & & r_h \text{ caselle}
\end{array}
\tag{33}
$$

e ogni tavola definisce un insieme di *diagrammi* $D_\alpha, E_\alpha, \ldots$, ottenuti distribuendo i numeri $1, 2, \ldots, n$ nelle caselle in modo che due numeri non figurino mai nella stessa casella. Per esempio, se $\alpha = \{3, 2, 2\}$, uno dei D è

$$
\begin{array}{lll}
\boxed{1} & \boxed{3} & \boxed{7} \\
\boxed{2} & \boxed{6} & \\
\boxed{4} & \boxed{5} &
\end{array}
\quad .
\tag{34}
$$

Se D $(= D_\alpha)$ è un diagramma, definiamo il *gruppo* $R(D)$ *delle permutazioni di riga* di D come il sottogruppo di S_n formato dalle permutazioni che stabilizzano i sottoinsiemi disposti nelle righe di D. Per il D della (34), dunque, $R(D)$ è l'insieme dei prodotti di cicli i cui numeri, per ciascun ciclo, compaiono tutti in una delle righe $\{1, 3, 7\}$, $\{2, 6\}$ o $\{4, 5\}$ (così $R(D)$ contiene $1, (13), (17), (37), (137), (173), (26), (45), (13)(26)$, ecc.). Analogamente definiamo il sottogruppo $C(D)$ delle *permutazioni di colonna* di D come il sottogruppo di S_n formato dalle permutazioni che stabilizzano le colonne di D.

Se D_α è un diagramma e $\sigma \in S_n$, allora σD_α è il diagramma che si ottiene da D_α applicando σ ai suoi elementi. Evidentemente si tratta di un E_α, e ogni E_α è un σD_α per qualche $\sigma \in S_n$. È chiaro che $R(\sigma D_\alpha) = \sigma R(D_\alpha)\sigma^{-1}$ e $C(\sigma D_\alpha) = \sigma C(D_\alpha)\sigma^{-1}$.

A ogni diagramma D $(= D_\alpha)$ assoceremo nel modo seguente alcuni elementi dell'algebra di gruppo $F[S_n]$. Poniamo

$$
\begin{gathered}
S_D = \sum_{\sigma \in R(D)} \sigma, \qquad A_D = \sum_{\tau \in C(D)} (\operatorname{sg}\tau)\tau, \\
F_D = A_D S_D = \sum_{\substack{\sigma \in R(D) \\ \tau \in C(D)}} (\operatorname{sg}\tau)\tau\sigma,
\end{gathered}
\tag{35}
$$

dove $\operatorname{sg}\tau$ denota il segno della permutazione τ. Evidentemente $S_D \neq 0$ e $A_D \neq 0$ in $F[S_n]$. Ma anche $F_D \neq 0$. Infatti $R(D) \cap C(D) = 1$, poiché un elemento comune ai due sottogruppi stabilizza ogni riga e ogni colonna, e fissa quindi ciascun elemento di $\{1, 2, \ldots, n\}$. Ne segue che, se $\sigma_1, \sigma_2 \in R(D)$ e $\tau_1, \tau_2 \in C(D)$, da $\tau_1\sigma_1 = \tau_2\sigma_2$ si ricava $\sigma_2\sigma_1^{-1} = \tau_2^{-1}\tau_1$ e quindi $\sigma_1 = \sigma_2$ e $\tau_1 = \tau_2$. I prodotti $\tau\sigma$ che figurano in F_D sono dunque distinti, perciò $F_D \neq 0$.

Poiché per $\rho \in S_n$ si ha $R(\rho D) = \rho R(D)\rho^{-1}$ e $C(\rho D) = \rho C(D)\rho^{-1}$, e poiché $\operatorname{sg}(\rho\tau\rho^{-1}) = \operatorname{sg}\tau$, segue che $S_{\rho D} = \rho S_D \rho^{-1}$, $A_{\rho D} = \rho A_D \rho^{-1}$ e $F_{\rho D} = \rho F_D \rho^{-1}$. Inoltre, se $\sigma \in R(D)$ e $\tau \in C(D)$, dalla definizione (35) si ottiene

$$
\sigma S_D = S_D = S_D \sigma, \qquad \tau A_D = (\operatorname{sg}\tau) A_D = A_D \tau.
\tag{36}
$$

Dedurremo le principali proprietà degli elementi S_D, A_D, F_D dal seguente risultato combinatorio.

Lemma 1. *Siano α, β partizioni tali che $\alpha \geq \beta$, e siano D_α, E_β diagrammi associati. Supponiamo che due numeri che compaiono in una stessa riga di D_α non appartengano mai alla stessa colonna di E_β. Allora $\alpha = \beta$ ed $E_\alpha = \sigma\tau D_\alpha$ per qualche $\sigma \in R(D_\alpha)$ e qualche $\tau \in C(D_\alpha)$.*

Dimostrazione. Il numero di elementi nella prima riga di D_α è maggiore o uguale a quello degli elementi nella prima riga di E_β. Se fosse maggiore, poiché il numero delle colonne di E_β è il

numero degli elementi della sua prima riga, due elementi della prima riga di D_α comparirebbero nella stessa colonna di E_β, contro l'ipotesi. I due diagrammi hanno dunque lo stesso numero di elementi nella prima riga. Esiste inoltre una permutazione di colonna τ_1' di E_β tale che la prima riga di $\tau_1' E_\beta$ contenga gli stessi elementi della prima riga di D_α. Osserviamo ora che gli elementi della seconda riga di D_α compaiono in colonne distinte di $\tau_1' E_\beta$ e in righe successive alla prima. Ne segue che D_α e $\tau_1' E_\beta$, e quindi D_α ed E_β, hanno lo stesso numero di elementi nella seconda riga, e una permutazione di colonna τ_2' di $\tau_1' E_\beta$ (e di E_β) porta questi elementi nella seconda riga. Procedendo così, vediamo che $\beta = \alpha$ e che esiste $\tau' \in C(E_\alpha)$ tale che ogni riga di $\tau' E_\alpha$ contenga gli stessi elementi della corrispondente riga di D_α. Esiste quindi $\sigma \in R(D_\alpha)$ tale che $\sigma D_\alpha = \tau' E_\alpha$. Ora

$$\tau' \in C(E_\alpha) = C(\tau' E_\alpha) = C(\sigma D_\alpha) = \sigma C(D_\alpha)\sigma^{-1}.$$

Pertanto $\tau' = \sigma\tau^{-1}\sigma^{-1}$, con $\tau^{-1} \in C(D_\alpha)$, e $\sigma\tau^{-1}\sigma^{-1}E_\alpha = \sigma D_\alpha$. Si ha dunque $E_\alpha = \sigma\tau D_\alpha$. □

Supponiamo ora $\alpha > \beta$. Il lemma 1 implica che esistono i, j, con $i \neq j$, in una riga di D_α e in una colonna di E_β. Se $\pi = (ij)$, allora $\pi \in R(D_\alpha)$. Per la (36), $\pi S_{D_\alpha} = S_{D_\alpha} = S_{D_\alpha}\pi$ e $\pi A_{E_\beta} = -A_{E_\beta}$. Quindi

$$S_{D_\alpha} A_{E_\beta} = (S_{D_\alpha}\pi)A_{E_\beta} = S_{D_\alpha}(\pi A_{E_\beta}) = -S_{D_\alpha} A_{E_\beta},$$
$$A_{E_\beta} S_{D_\alpha} = A_{E_\beta}(\pi S_{D_\alpha}) = (A_{E_\beta}\pi)S_{D_\alpha} = -A_{E_\beta} S_{D_\alpha}.$$

Ne segue $S_{D_\alpha} A_{E_\beta} = 0 = A_{E_\beta} S_{D_\alpha}$. Se ρ è un elemento qualsiasi di S_n, si ha $S_{\rho D_\alpha} = \rho S_{D_\alpha}\rho^{-1}$ e, poiché $S_{\rho D_\alpha} A_{E_\beta} = 0 = A_{E_\beta} S_{\rho D_\alpha}$, otteniamo $S_{D_\alpha}\rho^{-1} A_{E_\beta} = 0$ e $A_{E_\beta}\rho S_{D_\alpha} = 0$. Dunque

$$S_{D_\alpha} F[S_n] A_{E_\beta} = 0 = A_{E_\beta} F[S_n] S_{D_\alpha} \qquad \text{se } \alpha > \beta. \tag{37}$$

Lemma 2. *Un elemento $a \in F[S_n]$ soddisfa le equazioni $\tau a \sigma = (\operatorname{sg}\tau)a$ per ogni $\sigma \in R(D)$ e ogni $\tau \in C(D)$ se e soltanto se $a = \gamma F_D$, con $\gamma \in F$ e $F_D = A_D S_D$.*

Dimostrazione. Si ha $F_D\sigma = A_D S_D \sigma = A_D S_D = F_D$ e $\tau F_D = \tau A_D S_D = (\operatorname{sg}\tau) A_D S_D = (\operatorname{sg}\tau) F_D$. Quindi ogni γF_D, $\gamma \in F$, soddisfa le condizioni. Supponiamo ora che $a = \sum_{\rho \in S_n} \gamma_\rho \rho$ soddisfi le condizioni date. Allora

$$\gamma_\rho = (\operatorname{sg}\tau)\gamma_{\tau\rho\sigma} \tag{38}$$

per $\sigma \in R(D)$ e $\tau \in C(D)$. In particolare, $\gamma_{\tau\sigma} = \gamma_1 \operatorname{sg}\tau$. Per la (35), basterà quindi mostrare che $\gamma_\rho = 0$ se ρ non ha la forma $\tau\sigma$, con $\tau \in C(D)$ e $\sigma \in R(D)$, per ottenere $a = \gamma_1 F_D$. Supponiamo dunque $\rho \neq \tau\sigma$ per ogni $\tau \in C(D)$ e $\sigma \in R(D)$. Allora $\rho^{-1} \neq \sigma\tau$ per $\sigma \in R(D)$ e $\tau \in C(D)$. Quindi $\rho^{-1} D \neq \sigma\tau D$, e il lemma 1 implica che esiste una trasposizione $\pi \in R(D)$ tale che $\pi \in C(\rho^{-1}D) = \rho^{-1}C(D)\rho$. Si ha pertanto $\pi = \rho^{-1}\pi'\rho$, dove π' è una trasposizione appartenente a $C(D)$. Allora $\rho = \pi'\rho\pi$ e, per la (38), $\gamma_{\pi'\rho\pi} = \gamma_\rho = -\gamma_{\pi'\rho\pi}$. Dunque $\gamma_\rho = 0$ e la dimostrazione è completa. □

Sia ora $x \in F[S_n]$ e consideriamo l'elemento $F_D x F_D = A_D S_D x A_D S_D$. Per la (36) si ha $\tau F_D x F_D \sigma = (\operatorname{sg}\tau) F_D x F_D$ per $\sigma \in R(D)$ e $\tau \in C(D)$. Per il lemma 2 si ha quindi $F_D x F_D = \gamma F_D$ con $\gamma \in F$. In particolare $F_D^2 = \gamma F_D$. Mostriamo che $\gamma \neq 0$. A questo scopo consideriamo l'applicazione $x \mapsto F_D x$ di $F[S_n]$ in sé. Se $\gamma = 0$, allora $F_D^2 = 0$ e l'applicazione $x \mapsto F_D x$ è nilpotente, quindi ha traccia zero. D'altra parte, per $\rho \in S_n$, esaminando la matrice di $x \mapsto \rho x$ rispetto alla base costituita dalle permutazioni, vediamo che la traccia di questa applicazione è 0 se $\rho \neq 1$, ed è $n!$ se $\rho = 1$. Poiché la formula (35) mostra che il coefficiente di 1 nell'espressione di F_D è 1, la traccia di $x \mapsto F_D x$ è $n! \neq 0$ (dato che $\operatorname{char} F \nmid n!$).

Poniamo ora $e_D = \gamma^{-1} F_D$. Si ha $e_D^2 = e_D \neq 0$ ed $e_D F[S_n] e_D = F e_D$. Inoltre, se α e β sono partizioni distinte, dalla (37) segue $e_{D_\alpha} F[S_n] e_{E_\beta} = 0$ se D_α è un diagramma associato ad α ed E_β un diagramma associato a β.

Ricordiamo che, se e ed f sono idempotenti di un anello A, i gruppi additivi $\hom_A(Ae, Af)$ ed eAf sono isomorfi, mentre gli anelli $\mathrm{End}_A\, Ae$ ed eAe sono anti-isomorfi (p. 180). Applicando questo fatto e il teorema 5.7 alla rappresentazione del gruppo che agisce su $F[S_n]e_{D_\alpha}$, vediamo che tale rappresentazione è assolutamente irriducibile e che, se $\alpha \neq \beta$, le rappresentazioni fornite da $F[S_n]e_{D_\alpha}$ e $F[S_n]e_{E_\beta}$ non sono equivalenti. Poiché il numero delle classi di coniugio di S_n è $p(n)$, otteniamo in tal modo un sistema completo di rappresentanti delle classi di equivalenza di rappresentazioni irriducibili. In termini dell'algebra di gruppo $F[S_n]$, il risultato che abbiamo dimostrato è il seguente.

Teorema 5.9. *Se F è un campo di caratteristica zero o di caratteristica prima maggiore di n, allora*

$$F[S_n] \cong M_{n_1}(F) \oplus M_{n_2}(F) \oplus \cdots \oplus M_{n_{p(n)}}(F).$$

Il metodo di dimostrazione è costruttivo e si può in linea di principio adoperare per eseguire la decomposizione di $F[S_n]$ in componenti semplici. Gli n_i, che sono i gradi delle rappresentazioni irriducibili, si possono determinare calcolando i caratteri di S_n, che nel prossimo paragrafo definiremo per un gruppo arbitrario. Sui caratteri di S_n esiste una vasta letteratura, di cui qui non ci occuperemo. Il teorema 5.9 ha evidentemente la conseguenza seguente.

Corollario. *Il campo $\mathbb{Q}$ e ogni campo $\mathbb{Z}/(p)$ con $p > n$ sono campi di spezzamento per S_n.*

5.5 Caratteri. Relazioni di ortogonalità

Definizione 5.2. *Sia ρ una rappresentazione di un gruppo G che agisce su uno spazio vettoriale V/F. La funzione su G a valori in F definita da*

$$\chi_\rho \colon g \longmapsto \mathrm{tr}\, \rho(g),$$

dove $\mathrm{tr}\, \rho(g)$ è la traccia della trasformazione lineare $\rho(g)$, si chiama carattere *di G associato a ρ. Se ρ è irriducibile, χ_ρ si dice* irriducibile. *Se $F = \mathbb{C}$, χ_ρ si dice un* carattere complesso. *Il grado di ρ si chiama* grado *di χ_ρ.*

Come vedremo fra poco, due rappresentazioni di G su $\mathbb{C}$ sono equivalenti se e soltanto se hanno lo stesso carattere. Una lunga esperienza ha inoltre mostrato che i caratteri racchiudono precisamente quelle informazioni sulle rappresentazioni che si prestano all'uso nelle applicazioni. È dunque giusto dire che il problema centrale della teoria delle rappresentazioni è quello di determinare i caratteri complessi irriducibili di un gruppo dato, o, più precisamente, di elaborare metodi per determinarli.

Cominciamo elencando alcuni semplici fatti sui caratteri.

1. Rappresentazioni equivalenti hanno lo stesso carattere. Se ρ_1 su V_1 è equivalente a ρ_2 su V_2, esiste un'applicazione lineare biiettiva η di V_1 su V_2 tale che $\rho_2(g) = \eta\rho_1(g)\eta^{-1}$. Ne segue $\mathrm{tr}\, \rho_2(g) = \mathrm{tr}\, \rho_1(g)$ e quindi $\chi_{\rho_2} = \chi_{\rho_1}$.

2. Ogni carattere è una *funzione di classe*, ossia è costante su ogni classe di coniugio e definisce pertanto un'applicazione dall'insieme delle classi di coniugio nel campo base. Siano $g, h \in G$. Allora

$$\mathrm{tr}\, \rho(hgh^{-1}) = \mathrm{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{tr}\, \rho(g).$$

   Dunque $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$.

3. Se $\mathrm{char}\, F = 0$, il grado di ρ è $\chi_\rho(1)$. Infatti $\rho(1) = 1_V$, sicché $\chi_\rho(1) = \mathrm{tr}\, \rho(1) = \dim V$.

4. Sia U un sottospazio $\rho(G)$-invariante dello spazio V su cui agisce ρ, e siano $\rho|U$ e $\rho|V/U$ le corrispondenti sottorappresentazione e rappresentazione quoziente. Si ha

$$\chi_\rho(g) = \chi_{\rho|U}(g) + \chi_{\rho|V/U}(g).$$

Per vederlo, scegliamo una base $(u_1, \dots, u_n)$ di V tale che $(u_1, \dots, u_r)$ sia una base di U, e quindi $(u_{r+1} + U, \dots, u_n + U)$ sia una base di V/U. Le matrici delle $\rho(g)$ hanno allora tutte la forma ridotta (18), da cui segue il risultato.

5. Se ρ_1 e ρ_2 sono rappresentazioni di G, allora

$$\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \chi_{\rho_2},$$

ossia, per ogni $g \in G$, $\chi_{\rho_1 \otimes \rho_2}(g) = \chi_{\rho_1}(g)\chi_{\rho_2}(g)$. Consideriamo infatti la matrice (12) della trasformazione lineare $a_1 \otimes a_2$ di $V_1 \otimes V_2$, dove a_i è una trasformazione lineare di V_i. Da essa risulta che $\operatorname{tr}(a_1 \otimes a_2) = (\operatorname{tr} a_1)(\operatorname{tr} a_2)$, e dunque $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1}\chi_{\rho_2}$.

Per le applicazioni ci interessano soprattutto i caratteri complessi. Ne osserviamo ora alcune proprietà.

6. Se G è finito, ogni valore di un carattere complesso di G è una somma di radici m-esime dell'unità, dove m è l'*esponente* di G, definito come il minimo comune multiplo degli ordini degli elementi di G. Se $g \in G$, si ha $g^m = 1$ e quindi $\rho(g)^m = 1$. Il polinomio minimo di $\rho(g)$ è pertanto un divisore di $x^m - 1$ e ha radici distinte, tutte radici m-esime dell'unità. Ne segue che $\rho(g)$ ammette una matrice della forma

$$\operatorname{diag}\{\omega_1, \omega_2, \dots, \omega_n\}, \tag{39}$$

dove le ω_i sono radici m-esime dell'unità. Allora $\chi_\rho(g) = \sum_i \omega_i$.

Questo risultato ha parecchie conseguenze utili. Cominciamo con la seguente.

Proposizione 5.3. *Sia ρ una rappresentazione complessa di grado n di un gruppo finito G. Per ogni $g \in G$ si ha*

$$|\chi_\rho(g)| \le n = \deg \chi_\rho, \tag{40}$$

e si ha

$$|\chi_\rho(g)| = n \tag{41}$$

se e soltanto se $\rho(g) = \omega 1$, dove ω è una radice m-esima dell'unità ed m è l'esponente di G. In particolare, se

$$\chi_\rho(g) = n, \tag{42}$$

allora $\rho(g) = 1$.

Dimostrazione. Abbiamo $\chi_\rho(g) = \sum_i \omega_i$, dove ogni ω_i è una radice m-esima dell'unità. Quindi

$$|\chi_\rho(g)| = \Big| \sum_i \omega_i \Big| \le \sum_i |\omega_i| = n.$$

Inoltre vale l'uguaglianza se e soltanto se tutte le ω_i appartengono alla stessa semiretta uscente dall'origine. Poiché si trovano sulla circonferenza unitaria, ciò accade se e soltanto se sono uguali.

Dunque $|\chi_\rho(g)| = n$ se e soltanto se $\rho(g) = \omega 1$. L'ultima affermazione ne è una conseguenza immediata. □

Il fatto che $\chi_\rho(g) = n$ implichi $\rho(g) = 1$, insieme con l'ovvia implicazione inversa, ci induce a definire il *nucleo* del carattere χ_ρ come l'insieme degli elementi g tali che $\chi_\rho(g) = n$, dove n è il grado di ρ. Allora $\ker \chi_\rho = \ker \rho$ è un sottogruppo normale di G. Definiamo anche

$$Z(\chi_\rho) = \{g \in G \mid |\chi_\rho(g)| = n\}.$$

Abbiamo dimostrato che $Z(\chi_\rho)$ è l'insieme degli elementi g tali che $\rho(g) = \omega 1$. È chiaro che essi formano un sottogruppo normale di G contenente $\ker \chi_\rho$ e che $Z(\chi_\rho)/\ker \rho$ è isomorfo a un sottogruppo del gruppo moltiplicativo delle radici m-esime dell'unità. Quindi $Z(\chi_\rho)/\ker \rho$ è ciclico.

Un'altra conseguenza importante della dimostrazione della proprietà 6 è la seguente.

7. Siano ρ una rappresentazione complessa di un gruppo finito G e ρ^* la rappresentazione contragrediente. Allora

   $$\chi_{\rho^*} = \overline{\chi_\rho}, \tag{43}$$

   ossia $\chi_{\rho^*}(g) = \overline{\chi_\rho(g)}$ per $g \in G$. Sia infatti $g \in G$ e scegliamo una base B di V rispetto alla quale la matrice di $\rho(g)$ sia la (39). La matrice di $\rho^*(g)$ rispetto alla base duale B^* (p. 250) è allora

   $$\big(\mathrm{diag}\{\omega_1, \dots, \omega_n\}^{-1}\big)^{\mathtt{t}} = \mathrm{diag}\{\omega_1^{-1}, \dots, \omega_n^{-1}\} = \mathrm{diag}\{\bar\omega_1, \dots, \bar\omega_n\}.$$

   Dunque $\chi_{\rho^*}(g) = \sum_i \bar\omega_i = \overline{\chi_\rho(g)}$.

Esempi

1. Sia 1 la rappresentazione unità, in cui V ha dimensione uno e $1(g) = 1_V$ per $g \in G$. Il carattere a essa associato è il *carattere unità* $\chi_1 \colon g \mapsto 1 \in F$.

2. Sia G finito e sia ρ la rappresentazione regolare di G. Per determinare χ_ρ usiamo la base $G = \{g_1 = 1, g_2, \dots, g_n\}$ di $F[G]$. Abbiamo $\chi_\rho(1) = n$. D'altra parte, se $i > 1$, tutti gli elementi diagonali della matrice di $\rho(g_i)$ rispetto alla base G sono nulli, poiché $g_i g_j \neq g_j$. Dunque $\chi_\rho(g_i) = 0$. Il carattere della rappresentazione regolare è quindi dato da

   $$\chi_\rho(1) = |G|1, \qquad \chi_\rho(g) = 0 \quad \text{se } g \neq 1. \tag{44}$$

3. Sia $G = D_n$ il gruppo diedrale di ordine $2n$ generato da r, s con $r^n = 1$, $s^2 = 1$, $srs^{-1} = r^{-1}$. Dai risultati dell'esempio 2 di p. 261 otteniamo le seguenti tavole dei caratteri.

$n = 2\nu + 1, \quad \nu \geq 1$

	1	s	r^k
χ_1	1	1	1
χ_{ρ_2}	1	-1	1
χ_{σ_l}	2	0	$2\cos(2kl\pi/n)$

$n = 2\nu, \quad \nu \geq 2$

	1	s	rs	r^k
χ_1	1	1	1	1
χ_{ρ_2}	1	-1	-1	1
χ_{ρ_3}	1	1	-1	$(-1)^k$
χ_{ρ_4}	1	-1	1	$(-1)^k$
χ_{σ_l}	2	0	0	$2\cos(2kl\pi/n)$

In queste tavole la prima riga elenca i rappresentanti delle classi di coniugio e le righe successive corrispondono alle rappresentazioni irriducibili date in precedenza. In entrambi i casi $1 \leq k \leq \nu$. Si ha $1 \leq l \leq \nu$ per $n = 2\nu + 1$ e $1 \leq l \leq \nu - 1$ per $n = 2\nu$.

Ricaveremo ora alcune fondamentali *relazioni di ortogonalità* fra i caratteri complessi irriducibili di un gruppo finito. Consideriamo dapprima un risultato più generale. Siano G un gruppo finito e F un campo di spezzamento di G con $\operatorname{char} F \nmid |G|$. Sia $\{\rho_1, \ldots, \rho_s\}$ un insieme di rappresentanti delle rappresentazioni (assolutamente) irriducibili di G su F e supponiamo che ρ_i agisca su V_i, $1 \leq i \leq s$. Supponiamo anche che ρ_1 sia la rappresentazione unità. Siano $1 \leq i, j \leq s$ e consideriamo $\hom_F(V_i, V_j)$. Su questo spazio agisce una rappresentazione ρ_{ij} di G definita ponendo

$$\rho_{ij}(g)f = \rho_j(g) f \rho_i(g)^{-1} \tag{45}$$

per $f \in \hom_F(V_i, V_j)$. È chiaro che si ottiene una rappresentazione di G (esercizio 2, p. 251). Sia ora l un elemento qualsiasi di $\hom_F(V_i, V_j)$ e formiamo l'elemento

$$\eta(l) = \sum_g \rho_{ij}(g) l = \sum_g \rho_j(g) l \rho_i(g)^{-1}. \tag{46}$$

Si ha

$$\begin{aligned} \rho_j(h)\eta(l) &= \sum_g \rho_j(hg) l \rho_i(g)^{-1} = \sum_g \rho_j(g) l \rho_i(h^{-1}g)^{-1} \\ &= \sum_g \rho_j(g) l \rho_i(g^{-1}h) = \eta(l)\rho_i(h). \end{aligned}$$

Ciò implica che $\eta(l)$ è un omomorfismo di V_i, considerato come $F[G]$-modulo, in V_j, anch'esso considerato come $F[G]$-modulo. In altri termini, $\eta(l) \in \hom_{F[G]}(V_i, V_j)$. Ora, se $i \neq j$, V_i e V_j sono $F[G]$-moduli irriducibili non isomorfi. Per il lemma di Schur si ha dunque

$$\sum_g \rho_j(g) l \rho_i(g)^{-1} = 0 \tag{47}$$

se $i \neq j$ e l è un elemento qualsiasi di $\hom_F(V_i, V_j)$. Supponiamo ora $i = j$. Allora $\eta(l) \in \operatorname{End}_{F[G]} V_i = F1$, perciò

$$\sum_g \rho_i(g) l \rho_i(g)^{-1} \in F1 \tag{48}$$

per ogni $l \in \operatorname{End}_F V_i$. Dalle (47) e (48) si può ricavare il seguente risultato, dovuto a Schur.

Teorema 5.10. *Sia G un gruppo finito e sia F un campo di spezzamento di G con* $\operatorname{char} F \nmid |G|$. *Sia $\{\rho_1, \ldots, \rho_s\}$ un insieme di rappresentanti delle classi di equivalenza delle rappresentazioni irriducibili di G su F. Per ogni i sia $\rho^{(i)}$ una rappresentazione matriciale data da ρ_i. Allora* $\operatorname{char} F \nmid \deg \rho_i$ *e valgono le relazioni*

$$\begin{aligned} &\sum_g \rho^{(j)}_{kl}(g)\rho^{(i)}_{rt}(g^{-1}) = 0 && \text{se } i \neq j, \\ &\sum_g \rho^{(i)}_{kl}(g)\rho^{(i)}_{rt}(g^{-1}) = \delta_{kt}\delta_{lr}|G|/\deg \rho_i, \end{aligned} \tag{49}$$

dove $\rho^{(i)}(g) = (\rho^{(i)}_{rt}(g))$.

Queste relazioni si chiamano *relazioni di Schur*.

Dimostrazione. Sia $(u_1^{(i)}, \dots, u_{n_i}^{(i)})$ una base dello spazio V_i su cui agisce ρ_i tale che $\rho_i(g)u_t^{(i)} = \sum_r \rho_{rt}^{(i)}(g)u_r^{(i)}$, e sia f_{lr} l'elemento di $\hom_F(V_i, V_j)$ tale che $f_{lr}u_t^{(i)} = \delta_{rt}u_l^{(j)}$. Si ha allora

$$\rho_j(g)f_{lr}\rho_i(g^{-1})u_t^{(i)} = \sum_k \rho_{rt}^{(i)}(g^{-1})\rho_{kl}^{(j)}(g)u_k^{(j)}.$$

Dalla (47) segue il primo gruppo di relazioni (49). Inoltre, per $j = i$, dalle relazioni precedenti e dalla (48) si ha

$$\sum_g \sum_k \rho_{rt}^{(i)}(g^{-1})\rho_{kl}^{(i)}(g)u_k^{(i)} = \lambda_{lr}u_t^{(i)}, \qquad \lambda_{lr} \in F.$$

Dunque

$$\sum_g \rho_{rt}^{(i)}(g^{-1})\rho_{kl}^{(i)}(g) = \delta_{kt}\lambda_{lr}. \tag{50}$$

Poniamo $t = k$ in queste equazioni e sommiamo rispetto a k. Otteniamo

$$(\deg \rho_i)\lambda_{lr} = \delta_{rl}|G|,$$

da cui $\operatorname{char} F \nmid \deg \rho_i$ e $\lambda_{lr} = \delta_{rl}|G|/\deg \rho_i$. Sostituendo nella (50) si ottiene il secondo gruppo di relazioni di Schur. □

Abbiamo $\chi_{\rho_i}(g) = \sum_k \rho_{kk}^{(i)}(g)$. Ponendo dunque $l = k$ e $t = r$ nelle (49) e sommando rispetto a k e a r, otteniamo

$$\begin{aligned} &\sum_g \chi_{\rho_j}(g)\chi_{\rho_i}(g^{-1}) = 0 \qquad \text{se } i \neq j, \\ &\sum_g \chi_{\rho_i}(g)\chi_{\rho_i}(g^{-1}) = |G|. \end{aligned} \tag{51}$$

Supponiamo ora $F = \mathbb{C}$. Dal fatto che $\rho_i(g)$ ammette una matrice della forma $\operatorname{diag}\{\omega_1, \dots, \omega_{n_i}\}$, con le ω radici dell'unità (si veda la proprietà 6), segue che $\chi_{\rho_i}(g^{-1}) = \overline{\chi_{\rho_i}(g)}$. Dalle (51) otteniamo pertanto le fondamentali *relazioni di ortogonalità* per i caratteri complessi irriducibili,

$$\begin{aligned} &\sum_g \overline{\chi_{\rho_i}(g)}\chi_{\rho_j}(g) = 0 \qquad \text{se } i \neq j, \\ &\sum_g |\chi_{\rho_i}(g)|^2 = |G|. \end{aligned} \tag{52}$$

Consideriamo ora lo spazio vettoriale complesso $\mathbb{C}^G$ delle funzioni su G a valori complessi. L'addizione e la moltiplicazione per numeri complessi hanno le definizioni consuete. Se $\varphi, \psi \in \mathbb{C}^G$, allora $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$ e $(\alpha\varphi)(g) = \alpha\varphi(g)$ per $\alpha \in \mathbb{C}$. Definiamo su $\mathbb{C}^G$ una forma hermitiana ponendo

$$(\varphi \mid \psi) = \frac{1}{|G|}\sum_g \overline{\varphi(g)}\psi(g). \tag{53}$$

Si ha

$$(\varphi \mid \varphi) = \frac{1}{|G|}\sum_g |\varphi(g)|^2 \geq 0,$$

e vale l'uguaglianza se e soltanto se $\varphi = 0$. La forma $(\varphi \mid \psi)$ è quindi definita positiva. Scriveremo d'ora in poi χ_i per χ_{ρ_i}. Le relazioni (52) equivalgono allora a

$$(\chi_i \mid \chi_j) = \delta_{ij}. \tag{54}$$

Esse esprimono il fatto che $\{\chi_1, \ldots, \chi_s\}$ è un insieme ortonormale di vettori di $\mathbb{C}^G$, ossia che essi sono a due a due ortogonali e tutti di norma uno. Ne risulta che i caratteri complessi irriducibili sono linearmente indipendenti su $\mathbb{C}$. Abbiamo osservato che i caratteri sono funzioni di classe. L'insieme delle funzioni di classe forma un sottospazio $\mathrm{cf}(G)$ di $\mathbb{C}^G$ la cui dimensione è il numero delle classi di coniugio. Abbiamo visto che questo numero è uguale al numero s delle rappresentazioni irriducibili su $\mathbb{C}$. È chiaro, quindi, che i caratteri irriducibili costituiscono una base di $\mathrm{cf}(G)$.

Sia ora ρ una rappresentazione complessa qualsiasi di G e sia χ il suo carattere. A p. 255 abbiamo definito la molteplicità m_i di ρ_i in ρ. Dalla definizione e dal fatto che le rappresentazioni sono completamente riducibili risulta che due rappresentazioni sono equivalenti se e soltanto se, per ogni $i = 1, 2, \ldots, s$, la molteplicità di ρ_i nelle due rappresentazioni è la stessa. È pure chiaro che si ha la formula

$$\chi = m_1\chi_1 + m_2\chi_2 + \cdots + m_s\chi_s, \tag{55}$$

dove m_i è la molteplicità di ρ_i in ρ. Per la (54),

$$m_i = (\chi_i \mid \chi). \tag{56}$$

Le m_i sono dunque determinate da χ, e di conseguenza due rappresentazioni complesse sono equivalenti se e soltanto se hanno lo stesso carattere. Per la (55) abbiamo inoltre

$$(\chi \mid \chi) = \sum_i m_i^2, \tag{57}$$

e questa quantità vale 1 se e soltanto se una delle m_i è 1 e le altre sono nulle. Ciò mostra che un carattere è irriducibile se e soltanto se ha norma 1 nella metrica hermitiana di $\mathbb{C}^G$.

Siano $C_1 = \{1\}, C_2, \ldots, C_s$ le classi di coniugio di G e sia $h_k = |C_k|$. Scriviamo ora χ_{ik} per $\chi_i(g)$, $g \in C_k$. Le relazioni di ortogonalità danno

$$\begin{aligned} |G|\delta_{ij} &= \sum_g \overline{\chi_i(g)}\chi_j(g) = \sum_{k=1}^{s} \sum_{g \in C_k} \overline{\chi_i(g)}\chi_j(g) \\ &= \sum_{k=1}^{s} \bar{\chi}_{ik} h_k \chi_{jk}. \end{aligned}$$

Abbiamo dunque

$$\sum_{k=1}^{s} \bar{\chi}_{ik} h_k \chi_{jk} = |G|\delta_{ij}. \tag{58}$$

Siano $X = (\chi_{ij}) \in M_s(\mathbb{C})$ e $H = \mathrm{diag}\{h_1, \ldots, h_s\}$. Le relazioni precedenti si esprimono con l'equazione matriciale

$$\bar{X} H X^{\mathsf{t}} = |G|1. \tag{59}$$

Ne segue $X^{\mathsf{t}}\bar{X} = |G|H^{-1}$, che equivale a

$$\sum_{i=1}^{s} \chi_{ij}\bar{\chi}_{ik} = \frac{|G|}{h_k}\delta_{jk}. \tag{60}$$

Chiameremo le (58) e (60), rispettivamente, *relazioni di ortogonalità per righe* e *per colonne* dei caratteri. Osserviamo che, ponendo $j = k = 1$ nella (60), si ottiene $\sum_i n_i^2 = |G|$, dove

$n_i = \chi_i(1) = \deg \chi_i$. Questa è la relazione (32), che avevamo ottenuto in una situazione più generale mediante la teoria delle algebre.

Se ρ è una rappresentazione di un gruppo G che agisce su V/F, essa si prolunga in modo unico a un omomorfismo di $F[G]$ in $\mathrm{End}_F V$. Questo manda l'elemento $\sum_g \gamma_g g$ dell'algebra del gruppo in $\sum_g \gamma_g \rho(g)$. Indicheremo anche questo prolungamento con ρ. Analogamente, il carattere χ_ρ definito su G si prolunga in modo unico a un'applicazione lineare χ_ρ di $F[G]$ in F ponendo

$$\chi_\rho\Big(\sum_g \gamma_g g\Big) = \operatorname{tr} \rho\Big(\sum_g \gamma_g g\Big) = \sum_g \gamma_g \operatorname{tr} \rho(g) = \sum_g \gamma_g \chi_\rho(g).$$

Se $c \in \operatorname{cent} F[G]$, il centro dell'algebra del gruppo, $\rho(c)$ appartiene al centralizzante di ρ. Se dunque ρ è assolutamente irriducibile, $\rho(c) = \omega(c)1$, con $\omega(c) \in F$. Se il grado di ρ è n, si ha $\chi_\rho(c) = n\omega(c)$, e quindi

$$\rho(c) = \frac{1}{n}\chi_\rho(c)1. \tag{61}$$

Poiché $c \mapsto \rho(c)$ è un omomorfismo di algebre da $\operatorname{cent} F[G]$ in $F1$, è chiaro che $c \mapsto (1/n)\chi_\rho(c)$ è un omomorfismo di algebre.

Abbiamo visto che, posto $c_j = \sum_{g \in C_j} g$, la famiglia $(c_1, \dots, c_s)$ è una base di $\operatorname{cent} F[G]$. Evidentemente $c_j c_k = \sum_g n_{jkg} g$, con $n_{jkg} \in \mathbb{N}$, l'insieme degli interi non negativi. Poiché $c_j c_k \in \operatorname{cent} F[G]$, si ha $h^{-1} c_j c_k h = c_j c_k$ per $h \in G$. Ne segue $n_{jkg} = n_{jk,hgh^{-1}}$ per $g, h \in G$. Abbiamo dunque per la base $(c_1, \dots, c_s)$ di $\operatorname{cent} F[G]$ su F una tavola di moltiplicazione della forma

$$c_j c_k = \sum_{l=1}^{s} m_{jkl} c_l, \qquad 1 \le j, k \le s, \tag{62}$$

con $m_{jkl} \in \mathbb{N}$. Si vede subito che m_{jkl} è il numero di coppie (x, y), con $x \in C_j$, $y \in C_k$, tali che xy sia uguale a un elemento z fissato in C_l.

Supponiamo ora $F = \mathbb{C}$ e conserviamo le notazioni precedenti. Applicando la rappresentazione ρ_i alla (62) otteniamo $\rho_i(c_j)\rho_i(c_k) = \sum_l m_{jkl} \rho_i(c_l)$. Se $n_i = \deg \rho_i = \chi_i(1)$, si ha $\rho_i(c_j) = (\chi_i(c_j)/n_i)1$. Vale dunque la relazione fra caratteri

$$(\chi_i(c_j)/n_i)(\chi_i(c_k)/n_i) = \sum_l m_{jkl} \chi_i(c_l)/n_i. \tag{63}$$

Usando la definizione $c_j = \sum_{g \in C_j} g$ e il fatto che i caratteri sono funzioni di classe, otteniamo $\chi_i(c_j) = h_j \chi_i(g_j)$ per ogni $g_j \in C_j$, ossia $\chi_i(c_j) = h_j \chi_{ij}$. Vale dunque la relazione

$$(h_j \chi_{ij}/n_i)(h_k \chi_{ik}/n_i) = \sum_{l=1}^{s} m_{jkl} (h_l \chi_{il}/n_i), \tag{64}$$

ossia

$$(h_j \chi_{ij})(h_k \chi_{ik}) = \sum_{l=1}^{s} m_{jkl} h_l n_i \chi_{il}. \tag{64'}$$

Per *tavola dei caratteri* di un gruppo G intendiamo una tavola che riporta i valori χ_{ij} dei caratteri complessi irriducibili. Un problema fondamentale nello studio di un gruppo G dato è il calcolo della sua tavola dei caratteri. A titolo di illustrazione consideriamo l'esempio seguente.

Esempio. Vogliamo determinare una tavola dei caratteri di S_4. Un elenco di rappresentanti delle classi di coniugio è $1, (12), (123), (1234), (12)(34)$. Indichiamo le classi corrispondenti con C_1, C_2, C_3, C_4, C_5. Le loro cardinalità sono, nell'ordine, $(h_1, h_2, h_3, h_4, h_5) = (1, 6, 8, 6, 3)$. Il gruppo alterno A_4 è un sottogruppo normale di indice 2 in S_4, e $V = \{1, (12)(34), (13)(24), (14)(23)\}$ è un sottogruppo normale di indice 6 in S_4 (BAI, p. 261, esercizio 4). Se S_3 denota il sottogruppo di S_4 che fissa 4, allora S_4 è prodotto semidiretto di V e S_3. Ogni elemento di S_4 si scrive in uno e un solo modo come prodotto sv, con $s \in S_3$, $v \in V$. Se $s_i \in S_3$ e $v_i \in V$, allora

$$(s_1 v_1)(s_2 v_2) = (s_1 s_2)(s_2^{-1} v_1 s_2 v_2), \qquad s_2^{-1} v_1 s_2 \in V.$$

Dunque $sv \mapsto s$ è un omomorfismo η di S_4 su S_3 di nucleo V. Se ρ è una rappresentazione di S_3, $\rho\eta$ è una rappresentazione di S_4 di carattere $\chi_\rho \eta$.

Ora $S_3 \simeq D_3$ mediante un'applicazione tale che $(12) \mapsto s$, $(123) \mapsto r$. Dalla tavola dei caratteri di D_3 ricaviamo pertanto la seguente tavola dei caratteri di S_3,

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

Indichiamo ancora con χ_1, χ_2, χ_3 i caratteri che si ottengono componendo questi con η. Poiché $(12)(13)(24) = (1324)$, la parte della tavola dei caratteri data da questi tre caratteri è

	1	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	−1	1	−1	1
χ_3	2	0	−1	0	2

Se n_i è il grado di χ_i, $1 \le i \le 5$, da $\sum_i n_i^2 = 24$ segue $n_4^2 + n_5^2 = 18$. Dunque $n_4 = n_5 = 3$ e i due caratteri irriducibili mancanti hanno grado tre. Le ultime due righe della tavola dei caratteri hanno quindi la forma $(3, \alpha, \beta, \gamma, \delta)$ e $(3, \alpha', \beta', \gamma', \delta')$. Dalla relazione (60), con $j = 1$ e $k = 2, 3, 4, 5$, ricaviamo

$$\alpha + \alpha' = 0, \quad \beta + \beta' = 0, \quad \gamma + \gamma' = 0, \quad \delta + \delta' = -2.$$

L'ultima riga è dunque $(3, -\alpha, -\beta, -\gamma, -2 - \delta)$. Usando la (58) con $i = 4$ e $j = 1, 2, 3$ otteniamo le relazioni

$$\begin{aligned} 3 + 6\alpha + 8\beta + 6\gamma + 3\delta &= 0, \\ 3 - 6\alpha + 8\beta - 6\gamma + 3\delta &= 0, \\ 6 - 8\beta + 6\delta &= 0. \end{aligned}$$

Queste equazioni danno $\beta = 0$, $\delta = -1$, $\gamma = -\alpha$. La relazione di ortogonalità (60) per $j = 2$, $k = 4$ dà $\alpha\bar{\gamma} = -1$. D'altra parte $\alpha = \chi_4((12))$ è una somma di radici quadrate di 1, quindi è reale. Pertanto $\alpha\bar{\gamma} = \alpha(-\alpha) = -\alpha^2 = -1$ e $\alpha^2 = 1$, sicché $\alpha = \pm 1$ e $\gamma = \mp 1$. Le ultime due righe sono dunque $(3, 1, 0, -1, -1)$ e $(3, -1, 0, 1, -1)$, oppure $(3, -1, 0, 1, -1)$ e $(3, 1, 0, -1, -1)$. Le due determinazioni danno la stessa tavola, a meno dell'ordine delle ultime due righe.

L'esempio precedente illustra come si possano usare le relazioni di ortogonalità, insieme con le altre informazioni di cui si riesca a disporre, per calcolare una tavola dei caratteri. Altri risultati che ricaveremo fra breve forniranno ulteriori elementi utili per questi calcoli. Va anche ricordato che esiste una vasta letteratura sui caratteri di S_n, a partire da un lavoro classico pubblicato

da Frobenius nel 1900, che dà formule per i caratteri di un qualsiasi S_n. Si veda ad esempio *Classical Groups* di Weyl, p. 213.

Esercizi

1. Determinare una tavola dei caratteri di A_4.

2. Determinare una tavola dei caratteri del gruppo dei quaternioni.

3. Sia G un sottogruppo di S_n, sia ρ la corrispondente rappresentazione di permutazione di G su $\mathbb{C}$ e sia χ il suo carattere. Mostrare che $\sum_{g\in G}\chi(g) = r|G|$, dove r è la molteplicità della rappresentazione unità ρ_1 in ρ. Mostrare che $\sum_{g\in G}\chi(g)$ è anche il numero totale dei punti fissi in $\{1, 2, \ldots, n\}$, sommato su tutti i $g \in G$.

4. Con le notazioni dell'esercizio 3, mostrare che il numero delle orbite di G in $\{1, 2, \ldots, n\}$ è la molteplicità r di ρ_1 in ρ.

5. Un gruppo di permutazioni G si dice k *volte transitivo*, per $k = 1, 2, \ldots$, se, date due k-uple qualsiasi $(i_1, i_2, \ldots, i_k)$ e $(j_1, j_2, \ldots, j_k)$ con gli i distinti fra loro e i j distinti fra loro, esiste un $g \in G$ tale che $gi_l = j_l$, $1 \le l \le k$. Sia G doppiamente (ossia due volte) transitivo e sia ρ la rappresentazione di permutazione corrispondente. Mostrare che $\rho \sim \rho_1 \oplus \rho_i$, dove ρ_i è una rappresentazione irriducibile non equivalente a ρ_1.

6. Siano $\chi_1, \ldots, \chi_s$ i caratteri complessi irriducibili di G, siano $C_1 = \{1\}, C_2, \ldots, C_s$ le classi di coniugio di G e sia $h_i = |C_i|$. Porre $c_i = \sum_{g\in C_i} g$ ed $e_i = \sum_j (\chi_i(1)/|G|)\bar{\chi}_{ij}c_j$, dove $\chi_{ij} = \chi_i(g)$ per un $g \in C_j$. Mostrare che gli e_i sono idempotenti ortogonali nel centro di $\mathbb{C}[G]$ e che $\sum_i e_i = 1$.

7. Mostrare che un elemento g di un gruppo finito G è coniugato al suo inverso g^{-1} se e soltanto se $\chi(g) \in \mathbb{R}$ per ogni carattere complesso irriducibile χ.

5.6 Prodotti diretti di gruppi. Caratteri dei gruppi abeliani

È facile vedere che, se G_1 e G_2 sono gruppi finiti, $F[G_1 \times G_2] \cong F[G_1] \otimes_F F[G_2]$. Se la caratteristica di F non divide gli ordini dei due gruppi e F è un campo di spezzamento per entrambi, questo fatto permette di ricondurre lo studio delle rappresentazioni di $G_1 \times G_2$ su F a quello delle rappresentazioni dei fattori. Nel caso più importante, quello di $F = \mathbb{C}$, si può giungere agli stessi risultati per mezzo dei caratteri. Seguiremo questa via.

Siano ρ_i, $i = 1, 2$, rappresentazioni di G_i agenti su V_i su un campo arbitrario F. Componendo la proiezione $(g_1, g_2) \mapsto g_1$ con ρ_1, otteniamo una rappresentazione ρ_1' di $G_1 \times G_2$. Evidentemente $G_2 \subseteq \ker \rho_1'$. Analogamente otteniamo una rappresentazione ρ_2' di $G_1 \times G_2$ componendo la proiezione $(g_1, g_2) \mapsto g_2$ con ρ_2. Formiamo il prodotto tensoriale $\rho_1' \otimes \rho_2'$, che indicheremo con $\rho_1 \# \rho_2$. Allora

$$(\rho_1 \# \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2), \tag{65}$$

e pertanto

$$\chi_{\rho_1\#\rho_2}(g_1, g_2) = \chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2). \tag{66}$$

Consideriamo le immersioni canoniche $g_1 \mapsto (g_1, 1_2)$ e $g_2 \mapsto (1_1, g_2)$ dei due gruppi in $G_1 \times G_2$. Si ha

$$\chi_{\rho_1\#\rho_2}(g_1, 1_2) = \chi_{\rho_1}(g_1)\chi_{\rho_2}(1_2) = (\deg \rho_2)\chi_{\rho_1}(g_1), \tag{67}$$

e analogamente

$$\chi_{\rho_1\#\rho_2}(1_1, g_2) = (\deg \rho_1)\chi_{\rho_2}(g_2). \tag{68}$$

Tutto ciò si estende immediatamente ai prodotti diretti con più di due fattori.

Supponiamo ora che i G_i siano finiti, $F = \mathbb{C}$ e ρ_i sia una rappresentazione irriducibile di G_i. Per $\chi = \chi_{\rho_1\#\rho_2}$ si ha

$$\begin{aligned}(\chi \mid \chi) &= \frac{1}{|G_1 \times G_2|} \sum_{(g_1,g_2)} |\chi(g_1, g_2)|^2 \\ &= \frac{1}{|G_1|\,|G_2|} \sum_{(g_1,g_2)} |\chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2)|^2 \\ &= \frac{1}{|G_1|\,|G_2|} \sum_{(g_1,g_2)} |\chi_{\rho_1}(g_1)|^2 |\chi_{\rho_2}(g_2)|^2 \\ &= \left(\frac{1}{|G_1|} \sum_{g_1} |\chi_{\rho_1}(g_1)|^2\right) \left(\frac{1}{|G_2|} \sum_{g_2} |\chi_{\rho_2}(g_2)|^2\right) = 1.\end{aligned}$$

Dunque $\rho_1 \# \rho_2$ è irriducibile. Siano ora $\chi_1^{(i)}, \ldots, \chi_{s_i}^{(i)}$ i caratteri irriducibili di G_i, e sia $\rho_k^{(i)}$ una rappresentazione di carattere $\chi_k^{(i)}$. Le rappresentazioni $\rho_k^{(1)} \# \rho_l^{(2)}$ di $G_1 \times G_2$ sono irriducibili, e dalle (67) e (68) segue che a coppie (k, l) e (k', l') distinte corrispondono rappresentazioni con caratteri distinti e quindi inequivalenti. Otteniamo così $s_1 s_2$ rappresentazioni irriducibili inequivalenti. Poiché il grado di ciascun prodotto è il prodotto dei gradi dei fattori, la somma dei quadrati dei gradi di queste rappresentazioni è il prodotto delle somme dei quadrati dei gradi delle rappresentazioni irriducibili di G_1 e di G_2. Si ottiene dunque $|G_1|\,|G_2| = |G_1 \times G_2|$. Ne segue che le rappresentazioni così costruite costituiscono un sistema di rappresentanti delle classi di equivalenza delle rappresentazioni irriducibili del prodotto. Abbiamo dimostrato il seguente teorema.

Teorema 5.11. *Siano G_1, G_2 gruppi finiti e sia $\{\rho_1^{(i)}, \ldots, \rho_{s_i}^{(i)}\}$ un sistema di rappresentanti delle classi di equivalenza delle rappresentazioni irriducibili di G_i su $\mathbb{C}$. Ogni $\rho_k^{(1)} \# \rho_l^{(2)}$ è una rappresentazione irriducibile di $G_1 \times G_2$, e l'insieme di tali prodotti costituisce un sistema di rappresentanti delle classi di equivalenza delle rappresentazioni irriducibili di $G_1 \times G_2$.*

Un carattere χ di grado uno è detto *lineare*. Evidentemente è irriducibile e si può identificare con la rappresentazione di cui è il carattere. È quindi un omomorfismo dal gruppo assegnato nel gruppo moltiplicativo di un campo. Viceversa ogni omomorfismo di un gruppo G nel gruppo moltiplicativo F^* di un campo F è un carattere lineare di G. Ricordiamo l'importante ruolo di questi caratteri nella teoria di Galois dei campi (BAI, p. 291). Se χ, χ' sono caratteri lineari di G, anche $\chi\chi'$, definito da $(\chi\chi')(g) = \chi(g)\chi'(g)$, è lineare. I caratteri lineari formano così un gruppo in cui il carattere unità $g \mapsto 1$ è l'elemento neutro e l'inverso di χ è $g \mapsto \chi(g)^{-1}$.

Per G abeliano ogni carattere complesso irriducibile è lineare. Infatti, se ρ è una rappresentazione irriducibile di G su uno spazio vettoriale complesso V, allora $\mathrm{End}_{\mathbb{C}[G]} V = \mathbb{C}1$ e, poiché G è abeliano, $\mathrm{Env}\,\rho \subseteq \mathrm{End}_{\mathbb{C}[G]} V$, dunque $\mathrm{Env}\,\rho = \mathbb{C}1$. Ogni sottospazio è allora $\rho(G)$-invariante. Per l'irriducibilità di ρ, V ha dimensione uno, dunque χ_ρ è lineare. Le classi di coniugio di G sono costituite da un solo elemento, sicché sono in numero di $|G|$. Pertanto G possiede $|G|$ caratteri complessi irriducibili.

Si può vedere quest'ultimo risultato anche senza la teoria delle rappresentazioni. Anzi, per ogni gruppo abeliano finito possiamo determinare facilmente la struttura del gruppo dei caratteri complessi irriducibili (ossia lineari). Per un gruppo abeliano G tale gruppo prende il nome di

gruppo dei caratteri di G. Sia ora G abeliano finito. Allora G è un prodotto diretto di gruppi ciclici (BAI, p. 195): $G = G_1 \times \cdots \times G_r$, dove $G_i = \langle g_i \rangle$ e g_i ha ordine e_i. Possiamo considerare i G_i come sottogruppi; ogni elemento di G si scrive in modo unico $g = g_1^{k_1} \cdots g_r^{k_r}$, con $0 \le k_i < e_i$. Sia $\chi \in \widehat{G}$, il gruppo dei caratteri. Poiché $\chi(g_i)^{e_i} = \chi(g_i^{e_i}) = \chi(1) = 1$, $\chi(g_i)$ è una radice e_i-esima dell'unità. Queste radici formano un sottogruppo ciclico Z_{e_i} di $\mathbb{C}^*$. Definiamo l'applicazione da $\widehat{G}$ a $Z_{e_1} \times \cdots \times Z_{e_r}$

$$\chi \longmapsto (\chi(g_1), \ldots, \chi(g_r)). \tag{69}$$

È chiaramente un omomorfismo. Il nucleo è l'insieme dei χ per i quali $\chi(g_i) = 1$ per ogni i. Allora $\chi(g_1^{k_1} \cdots g_r^{k_r}) = \chi(g_1)^{k_1} \cdots \chi(g_r)^{k_r} = 1$ e $\chi = 1$. La (69) è pertanto un monomorfismo. È inoltre suriettiva: dato $(u_1, \ldots, u_r) \in Z_{e_1} \times \cdots \times Z_{e_r}$, si ha $u_i^{e_i} = 1$, per cui esiste un omomorfismo di G_i in Z_{e_i} che manda g_i in u_i. Si ha quindi un omomorfismo χ da $G = G_1 \times \cdots \times G_r$ in $\mathbb{C}^*$ tale che $\chi(g_i) = u_i$ per $1 \le i \le r$. È un carattere con immagine $(u_1, \ldots, u_r)$ mediante la (69). Otteniamo così un isomorfismo di G con il suo gruppo dei caratteri $\widehat{G}$.

Esercizi

1. Mostrare che il numero dei caratteri complessi lineari di un gruppo finito G è l'indice $[G : G']$, dove G' è il sottogruppo dei commutatori.

2. Sia ρ la rappresentazione regolare del gruppo finito G sul campo F. Si formi il campo $F(x_{g_1}, \ldots, x_{g_m})$ in $m = |G|$ indeterminate, con $g \mapsto x_g$ biunivoca. Il determinante

   $$\det\left(\sum_{g \in G} x_g \rho(g)\right) \tag{70}$$

   si chiama *determinante di gruppo* di G su F. (Lo studio di questi determinanti fu uno dei motivi principali che condussero Frobenius a introdurre la teoria dei caratteri.) Mostrare che, se $F = \mathbb{C}$ e G è abeliano, allora

   $$\det\left(\sum_{g \in G} x_g \rho(g)\right) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} x_g \chi(g)\right). \tag{71}$$

   Il risultato è dovuto a R. Dedekind.

3. Sia **Fab** la categoria dei gruppi abeliani finiti con gli omomorfismi come morfismi. Si ha un funtore controvariante D da **Fab** in sé, dato da $A \mapsto \widehat{A}$ e, per $f\colon A \to B$, da $\widehat{f}\colon \widehat{B} \to \widehat{A}$, $\psi \mapsto \chi$, dove $\chi(x) = \psi(f(x))$ per $x \in A$. Mostrare che D^2, dato da $A \mapsto \widehat{\widehat{A}}$ e $f \mapsto \widehat{\widehat{f}}$, è naturalmente equivalente al funtore identico (cfr. p. 22).

4. Mostrare che, se H è un sottogruppo del gruppo abeliano finito G, il sottogruppo di $\widehat{G}$ dei caratteri χ tali che $\chi|_H = 1$ si identifica con $\widehat{G/H}$ e quindi ha ordine $|G/H|$. Usare questo fatto per mostrare che la restrizione $\chi \mapsto \chi|_H$ da $\widehat{G}$ in $\widehat{H}$ è suriettiva. Ne segue che ogni carattere lineare di H si prolunga a un carattere lineare di G.

5.7 Alcune considerazioni aritmetiche

In questo paragrafo G sarà finito e tutte le rappresentazioni e i caratteri saranno complessi. Applicheremo alcuni risultati elementari sugli interi algebrici complessi, esposti in BAI, pp. 279–281, per ottenere risultati importanti sui gradi delle rappresentazioni irriducibili e sui caratteri di S_n.

Ricordiamo che $a \in \mathbb{C}$ si dice *algebrico* se è algebrico sul sottocampo $\mathbb{Q}$, cioè se è radice di un polinomio non nullo a coefficienti razionali. Il numero complesso a è detto *intero algebrico* se è radice di un polinomio monico a coefficienti interi. Un criterio utile è il seguente: a è intero algebrico se e soltanto se esiste un $\mathbb{Z}$-sottomodulo finitamente generato M di $\mathbb{C}$ tale che $1 \in M$ e $aM \subseteq M$. Il sottoinsieme A di $\mathbb{C}$ costituito dai numeri algebrici è un sottocampo e il sottoinsieme I degli interi algebrici è un sottoanello. Inoltre, se $a \in \mathbb{C}$ è radice di un polinomio monico in $A[X]$ (rispettivamente in $I[X]$), allora $a \in A$ (rispettivamente $a \in I$). Abbiamo anche dimostrato che a è un intero algebrico se e soltanto se è algebrico e il suo polinomio minimo su $\mathbb{Q}$ ha coefficienti interi, e che i soli razionali interi algebrici sono gli elementi di $\mathbb{Z}$.

Abbiamo visto che i valori dei caratteri di G sono somme di radici dell'unità (proprietà 6, p. 270). Poiché queste ultime sono interi algebrici, $\chi(g)$ è un intero algebrico per ogni carattere χ e ogni $g \in G$. Richiamiamo le notazioni del § 5.5.

1. $\chi_1, \dots, \chi_s$ sono i caratteri irriducibili; χ_1 è il carattere unità, ossia il carattere della rappresentazione unità ρ_1.
2. $C_1 = \{1\}, C_2, \dots, C_s$ sono le classi di coniugio.
3. $\chi_{ij} = \chi_i(g_j)$, dove $g_j \in C_j$.
4. $n_i = \chi_{i1}$ è il grado della rappresentazione ρ_i con $\chi_{\rho_i} = \chi_i$.
5. $h_j = |C_j|$.

Ricordiamo anche le relazioni fra caratteri di p. 276:

$$(h_j\chi_{ij}/n_i)(h_k\chi_{ik}/n_i) = \sum_{l=1}^{s} m_{jkl}(h_l\chi_{il}/n_i), \qquad m_{jkl} \in \mathbb{N}. \tag{64}$$

Ne dedurremo la seguente proposizione.

Proposizione 5.4. *I numeri complessi $h_j\chi_{ij}/n_i$ sono interi algebrici.*

Dimostrazione. Fissiamo i e poniamo $u_k = h_k\chi_{ik}/n_i$ per $1 \le k \le s$, $u_0 = 1$. Sia $M = \sum_{j=0}^{s} \mathbb{Z}u_j$. Per la (64), $u_kM \subseteq M$. Il criterio appena ricordato mostra che u_k è intero algebrico. □

Possiamo ora dimostrare il seguente teorema.

Teorema 5.12. *Ogni n_i divide $|G|$.*

Dimostrazione. Usando la (58) per $i = j$ si ottiene $|G|/n_i = \sum_k \overline{\chi_{ik}}\,(h_k\chi_{ik}/n_i)$. Poiché $\overline{\chi_{ik}}$ e $h_k\chi_{ik}/n_i$ sono interi algebrici, lo è anche $|G|/n_i$. Essendo razionale, esso appartiene a $\mathbb{Z}$. Pertanto $n_i \mid |G|$. □

Il risultato precedente è dovuto a Frobenius. Sappiamo inoltre che, se G è abeliano, ogni n_i è uguale a uno. Entrambi i risultati sono casi particolari del seguente teorema di Schur.

Teorema 5.13. *Se Z è il centro di G, allora $n_i \mid [G : Z]$.*

Dimostrazione (Tate). Sia m un intero positivo e sia $G_m = G \times \cdots \times G$ con m fattori. Sia ρ_i una rappresentazione irriducibile di G su $\mathbb{C}$ di carattere χ_i, e sia V lo spazio vettoriale su cui agisce. La rappresentazione ρ di G_m su $V_m = V \otimes \cdots \otimes V$, con m fattori, è data da $\rho(g_1, \dots, g_m) = \rho_i(g_1) \otimes \cdots \otimes \rho_i(g_m)$ (si veda il § 5.6). Applicando ripetutamente il teorema 5.11 si vede che ρ è irriducibile. Per $c \in Z$ l'irriducibilità di ρ_i implica $\rho_i(c) = \gamma_i(c)1_V$, con $\gamma_i(c) \in \mathbb{C}$. Evidentemente γ_i è un omomorfismo da Z in $\mathbb{C}^*$. Per definizione di ρ si ha

$$\rho(1, \dots, 1, c, 1, \dots, 1) = \gamma_i(c)1_{V_m},$$

e pertanto, per $c_j \in Z$,

$$\rho(c_1, \ldots, c_m) = \gamma_i(c_1) \cdots \gamma_i(c_m) 1_{V_m} = \gamma_i(c_1 \cdots c_m) 1_{V_m}.$$

Il sottoinsieme D degli elementi $(c_1, \ldots, c_m)$ di G_m tali che $c_j \in Z$ e $\prod_{j=1}^m c_j = 1$ è dunque contenuto nel nucleo di ρ. Evidentemente D è normale in G_m e ρ induce una rappresentazione irriducibile $\bar{\rho}$ di G_m/D. Applicando il teorema 5.12 a $\bar{\rho}$ si ottiene $n_i^m \mid |G_m/D| = |G|^m/|Z|^{m-1}$. Ciò implica che $(|G|/(n_i|Z|))^m \in |Z|^{-1}\mathbb{Z}$, per ogni m. Poniamo $u = |G|/(n_i|Z|)$. Questa relazione mostra che il $\mathbb{Z}$-sottomodulo $M = \sum_{k=0}^{\infty} \mathbb{Z}u^k$ di $\mathbb{Q}$ è contenuto in $|Z|^{-1}\mathbb{Z}$. Poiché $\mathbb{Z}$ è noetheriano, lo è anche $|Z|^{-1}\mathbb{Z}$, e quindi lo è M. In particolare M è finitamente generato come $\mathbb{Z}$-modulo. Poiché $1 \in M$ e $uM \subseteq M$, il razionale u è un intero. Dunque $n_i|Z|$ divide $|G|$, ossia $n_i \mid [G : Z]$, come richiesto. □

Se F è un sottocampo di $\mathbb{C}$, $I \cap F$ è un sottoanello di F, detto *anello degli interi algebrici di* F. Lo studio dell'aritmetica di tali anelli costituisce la teoria algebrica dei numeri. Daremo un'introduzione a questa teoria nel capitolo 10. Supponiamo ora che F sia un campo di spezzamento per il gruppo finito G. Allora $F[G] \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_s}(F)$, dove s è il numero delle classi di coniugio di G (si veda p. 280). Vi sono s rappresentazioni irriducibili inequivalenti ρ_i su F che restano irriducibili estendendo F a $\mathbb{C}$. Quindi $\{\rho_{1\mathbb{C}}, \ldots, \rho_{s\mathbb{C}}\}$ è un sistema di rappresentanti delle classi delle rappresentazioni complesse irriducibili. Se ρ_i agisce su V_i/F, per calcolare $\chi_{\rho_i}(g)$, $g \in G$, scegliamo una base di V_i su F e prendiamo la traccia della matrice di $\rho_i(g)$ rispetto a tale base. Il passaggio a $\mathbb{C}$ lascia immutato il calcolo, per cui $\chi_{\rho_{i\mathbb{C}}}(g) = \chi_{\rho_i}(g)$. I caratteri complessi irriducibili assumono quindi valori in F. Sappiamo inoltre che tali valori appartengono a I. Poiché ogni carattere è una combinazione a coefficienti interi di caratteri irriducibili, si ha il teorema seguente.

Teorema 5.14. *Sia F un sottocampo di $\mathbb{C}$ che sia un campo di spezzamento per il gruppo finito G. I valori di ogni carattere complesso di G sono interi algebrici di F.*

Nel § 5.4 abbiamo mostrato che $\mathbb{Q}$ è un campo di spezzamento per S_n. Si ha quindi il seguente corollario.

Corollario. *I caratteri complessi di S_n assumono valori in $\mathbb{Z}$.*

5.8 Il teorema di Burnside sui gruppi di ordine $p^a q^b$

Una delle prime applicazioni della teoria dei caratteri fu la dimostrazione del seguente bel teorema di Burnside.

Teorema 5.15. *Se p e q sono primi, ogni gruppo di ordine $p^a q^b$ è risolubile.*

In tempi assai recenti John Thompson è riuscito a dimostrare questo teorema senza ricorrere alla teoria delle rappresentazioni. La sua dimostrazione è tuttavia notevolmente più complicata di quella originaria con i caratteri. Quest'ultima, che daremo qui, rimane un buon esempio di come la teoria delle rappresentazioni consenta di ottenere risultati sulla struttura dei gruppi finiti.

Dimostriamo dapprima il seguente lemma.

Lemma. *Sia χ un carattere complesso irriducibile di un gruppo finito G e sia ρ una rappresentazione di carattere χ. Se C è una classe di coniugio di G tale che $(|C|, \chi(1)) = 1$, per ogni $g \in C$ si ha $\chi(g) = 0$ oppure $\rho(g) \in \mathbb{C}1$.*

Dimostrazione. Poiché $(|C|, \chi(1)) = 1$, esistono interi l, m tali che $l|C| + m\chi(1) = 1$. Quindi

$$\frac{\chi(g)}{\chi(1)} = l\,|C|\,\frac{\chi(g)}{\chi(1)} + m\chi(g). \tag{72}$$

Ora $\chi(g)$ è un intero algebrico e, per la proposizione 5.4 (p. 283), anche $|C|\chi(g)/\chi(1) = |C|\chi(g)/n$, con $n = \deg\rho = \chi(1)$, è un intero algebrico. Pertanto $\chi(g)/n$ è intero algebrico. Ricordiamo inoltre che $|\chi(g)| \leq n$: lo si è dimostrato mostrando che $\chi(g)$ è la somma di n radici dell'unità (p. 270). Si ha quindi $\chi(g) = \omega_1 + \cdots + \omega_n$, con $\omega_i \in W$, dove W è un campo ciclotomico di radici complesse dell'unità (BAI, p. 252). Siano $H = \mathrm{Gal}(W/\mathbb{Q})$ e $s \in H$. Allora s manda radici dell'unità in radici dell'unità, sicché $s(\chi(g))$ è somma di n radici dell'unità. Pertanto $|s(\chi(g))| \leq n$ e $|s(\chi(g))/\chi(1)| \leq 1$. Poiché $a = \chi(g)/\chi(1)$ è un intero algebrico, lo è pure $s(a) = s(\chi(g))/\chi(1)$, con $|s(a)| \leq 1$. La norma $N_{W/\mathbb{Q}}(a) = \prod_{s\in H} s(a)$ soddisfa allora $|N_{W/\mathbb{Q}}(a)| \leq 1$. Essendo un intero algebrico e un numero razionale, è un intero razionale. O la norma è zero, nel qual caso $a = 0$ e $\chi(g) = 0$, oppure ha modulo uno. In quest'ultimo caso $|a| = 1$, $|\chi(g)| = n$ e per la proposizione 5.3 si ha $\rho(g) = \omega 1$, con ω radice dell'unità. □

Ricordiamo che i soli gruppi semplici abeliani sono i gruppi ciclici di ordine primo. Poiché questa classe di gruppi semplici è piuttosto elementare, di solito la si esclude dallo studio dei gruppi semplici. Seguiremo tale convenzione nel prossimo teorema.

Teorema 5.16. *Sia G un gruppo semplice finito non abeliano. Nessuna classe di coniugio di G ha cardinalità della forma p^a con p primo e $a > 0$.*

Dimostrazione. Supponiamo che C sia una classe di coniugio di G con $|C| = p^a$, p primo e $a > 0$. Siano $\rho_1, \ldots, \rho_s$ le rappresentazioni irriducibili di G e $\chi_1, \ldots, \chi_s$ i caratteri corrispondenti. Supponiamo che ρ_1 sia la rappresentazione unità, cosicché $\chi_1(g) = 1$ per ogni g. Sia $n_i = \chi_i(1)$ il grado di ρ_i. Se $p \nmid n_i$, per ogni $g \in C$ il lemma precedente dà $\chi_i(g) = 0$ oppure $\rho_i(g) \in \mathbb{C}1$. Gli elementi g di G per i quali $\rho_i(g) \in \mathbb{C}1$ formano un sottogruppo normale G_i. Se dunque $\chi_i(g) \neq 0$ per qualche $g \in C$, si ha $G_i \neq 1$, quindi $G_i = G$ per la semplicità di G. D'altra parte, se $i > 1$, poiché G è semplice e ρ_i non è la rappresentazione unità, si ha $G \cong \rho_i(G)$. È quindi impossibile che $\rho_i(G)$ sia abeliano, come accadrebbe se $G_i = G$. Dunque, se $p \nmid n_i$ e $i > 1$, allora $\chi_i(g) = 0$ per ogni $g \in C$. Usiamo ora la relazione di ortogonalità (60), che per $g \in C$ dà

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(1)} = \sum_{i=1}^{s} n_i\chi_i(g) = 0. \tag{73}$$

Poiché $n_1 = 1$ e $\chi_1(g) = 1$, almeno uno degli n_i con $i > 1$ è divisibile per p. Siano $n_2, \ldots, n_t$ tutti gli n_i, $i > 1$, divisibili per p. La (73) dà

$$\sum_{j=2}^{t} n_j\chi_j(g) = -1.$$

Poiché gli n_j sono divisibili per p e i $\chi_j(g)$ sono interi algebrici, ne seguirebbe che $1/p$ è un intero algebrico, mentre gli unici razionali interi algebrici sono gli elementi di $\mathbb{Z}$. □

Dimostrazione del teorema 5.15. Sia $|G| = p^a q^b$, con p, q primi. Sia P un p-sottogruppo di Sylow di G, scegliendo p divisore dell'ordine di G nel caso non banale. Poiché l'ordine di P è una potenza di un primo, il suo centro Z è diverso da 1. Sia $1 \neq z \in Z$. Il centralizzante $C(z)$ di z contiene P, quindi $[G : C(z)]$ è una potenza di q. Questo indice è la cardinalità della classe di coniugio contenente z (BAI, p. 75). Se $[G : C(z)] > 1$, G non può essere semplice non abeliano, per il teorema 5.16. Se invece $[G : C(z)] = 1$, z appartiene al centro di G; dunque il centro è non banale e neppure in questo caso G è semplice non abeliano. È chiaro allora che, salvo il caso di un gruppo ciclico di ordine primo (e quello banale), G contiene un sottogruppo normale $H \neq 1, G$. Per induzione su $|G|$ concludiamo che H e G/H sono risolubili. Allora G è risolubile (BAI, p. 247). □

5.9 Moduli indotti

Siano G un gruppo, H un sottogruppo di indice finito in G e σ una rappresentazione di H che agisce sullo spazio vettoriale U/F. Un importante procedimento, introdotto da Frobenius, permette di «estendere» σ a una rappresentazione σ^G di G. Ricordiamo che G agisce sull'insieme G/H delle classi laterali sinistre di H in G. Se $G/H = \{H_1 = H, H_2, \dots, H_r\}$ e $g \in G$, allora $gH_i = H_{\pi(g)i}$, dove $\pi(g)$ è una permutazione di $\{1, \dots, r\}$. L'applicazione $\pi\colon g \mapsto \pi(g)$ è un omomorfismo di G nel gruppo simmetrico S_r (*BA I*, p. 72). Poniamo $U^G = U^{(r)}$, la somma diretta di r copie di U. Sia $\{s_1, s_2, \dots, s_r\}$ un sistema di rappresentanti delle classi laterali sinistre di H, con $H_i = s_iH$, $1 \le i \le r$. D'ora in avanti chiameremo un tale insieme un *trasversale (sinistro)* di G rispetto ad H. Se $g \in G$, si ha

$$gs_i = s_{\pi(g)i}\mu_i(g), \tag{74}$$

dove $\mu_i(g) \in H$. Possiamo definire un'azione di G su $U^G = U^{(r)}$ ponendo

$$\begin{aligned} g(u_1, \dots, u_r) = \big(&\sigma(\mu_{\pi(g)^{-1}1}(g))u_{\pi(g)^{-1}1}, \dots, \\ &\sigma(\mu_{\pi(g)^{-1}r}(g))u_{\pi(g)^{-1}r}\big), \end{aligned} \tag{75}$$

dove gli u_j appartengono a U. Dal fatto che π è un omomorfismo e che H agisce su U si può verificare che la (75) definisce effettivamente un'azione di G su U^G. Poiché questa azione consiste di trasformazioni lineari in uno spazio vettoriale di dimensione finita, otteniamo una rappresentazione σ^G di G che agisce su U^G. Si può anche verificare che una diversa scelta del trasversale di G rispetto ad H definisce una rappresentazione equivalente. Tutto ciò risulterà evidente, senza calcoli, da una diversa definizione, di natura concettuale, di σ^G, che ora daremo.

Siano $B = F[H]$ l'algebra di gruppo di H e $A = F[G]$ l'algebra di gruppo di G. Assegnare una rappresentazione σ di H equivale ad assegnare un B-modulo U di dimensione finita come spazio vettoriale su F. Ora B è una sottoalgebra di A, e quindi A è un B-B-bimodulo in cui le azioni di B su A sono le moltiplicazioni a sinistra e a destra per elementi di B. Possiamo formare $A \otimes_B U$, che è un A-modulo sinistro in cui, per $a_1, a_2 \in A$ e $u \in U$, vale

$$a_1(a_2 \otimes u) = a_1a_2 \otimes u. \tag{76}$$

Mostreremo ora che $[A \otimes_B U : F] < \infty$, sicché l'$A$-modulo $A \otimes_B U$, con $A = F[G]$, definisce una rappresentazione di G. Vedremo inoltre che tale rappresentazione è equivalente a σ^G quale è stata definita sopra.

Come prima, sia $\{s_1, s_2, \dots, s_r\}$ un trasversale di G rispetto ad H. Ogni elemento di G si può scrivere in uno e un solo modo nella forma s_ih, $h \in H$. Poiché gli elementi di G formano una base di A, ne segue che A, considerata come B-modulo destro, è libera con base $(s_1, \dots, s_r)$. Ne segue che ogni elemento di $A \otimes_B U$ può essere scritto in uno e un solo modo nella forma

$$s_1 \otimes u_1 + s_2 \otimes u_2 + \cdots + s_r \otimes u_r, \tag{77}$$

con $u_i \in U$. Pertanto, se $(u^{(1)}, \dots, u^{(n)})$ è una base di U/F, allora

$$\big(s_1 \otimes u^{(1)}, \dots, s_1 \otimes u^{(n)}; \dots; s_r \otimes u^{(1)}, \dots, s_r \otimes u^{(n)}\big) \tag{78}$$

è una base di $A \otimes_B U$, e dunque $[A \otimes_B U : F] = rn < \infty$. Così il modulo $A \otimes_B U$ definisce una rappresentazione di G.

Sia ora $g \in G$. Per le (76) e (74) si ha

$$
\begin{aligned}
g\Big(\sum s_i \otimes u_i\Big) &= \sum g s_i \otimes u_i \\
&= \sum s_{\pi(g)i}\mu_i(g) \otimes u_i \\
&= \sum s_{\pi(g)i} \otimes \mu_i(g)u_i \\
&= \sum s_i \otimes \mu_{\pi(g)^{-1}i}(g)u_{\pi(g)^{-1}i} \\
&= \sum s_i \otimes \sigma(\mu_{\pi(g)^{-1}i}(g))u_{\pi(g)^{-1}i}.
\end{aligned} \tag{79}
$$

Il confronto con la (75) mostra che l'applicazione $\eta\colon (u_1, \dots, u_r) \mapsto \sum_{i=1}^r s_i \otimes u_i$ è un'equivalenza fra la rappresentazione indotta di G, secondo la prima definizione, e la rappresentazione di G fornita da $A \otimes_B U$.

Il modulo U^G (o $A \otimes_B U$) si chiama *G-modulo indotto* da U, e la rappresentazione associata σ^G si chiama *rappresentazione indotta* di G. Come abbiamo visto, se $(u^{(1)}, \dots, u^{(n)})$ è una base di U/F, la (78) è una base del modulo indotto. Supponiamo ora che

$$hu^{(i)} = \sum_j \alpha_{ji}(h)u^{(j)} \tag{80}$$

per $h \in H$, cosicché $h \mapsto \alpha(h) = (\alpha_{ij}(h))$ è una rappresentazione matriciale di H determinata da σ e

$$\chi_\sigma(h) = \sum_i \alpha_{ii}(h) \tag{81}$$

è il carattere di σ. Per la (79), si ottiene la matrice di $\sigma^G(g)$ rispetto alla base (78) applicando la permutazione $\pi(g)$ alle r righe di blocchi $n \times n$ della matrice

$$\operatorname{diag}\{\alpha(\mu_1(g)), \dots, \alpha(\mu_r(g))\}. \tag{82}$$

Alla traccia contribuiscono soltanto i blocchi diagonali non nulli della matrice così ottenuta. Un tale blocco si trova nell'i-esima riga di blocchi se e solo se $\pi(g)i = i$, condizione equivalente a $gs_iH = s_iH$ e a $s_i^{-1}gs_i \in H$. Ne segue che il carattere è

$$\chi_{\sigma^G}(g) = \sum{}' \chi_\sigma(s_i^{-1}gs_i), \tag{83}$$

dove la somma $\sum'$ è estesa agli i tali che $s_i^{-1}gs_i \in H$. Si può dare a questa espressione una forma migliore estendendo la funzione χ_σ da H in F a una funzione $\dot\chi_\sigma$ su G, definita ponendo $\dot\chi_\sigma(g) = 0$ se $g \in G - H$. Si ottiene così la formula

$$\chi_{\sigma^G}(g) = \sum_{i=1}^r \dot\chi_\sigma(s_i^{-1}gs_i). \tag{84}$$

Quando G è un gruppo finito, si può scrivere questa formula in un'altra forma osservando che $\dot\chi_\sigma(h^{-1}gh) = \dot\chi_\sigma(g)$ per $h \in H$. Ciò è chiaro se $g \in H$, poiché χ_σ è una funzione di classe; se $g \notin H$, allora $h^{-1}gh \notin H$ e $\dot\chi_\sigma(h^{-1}gh) = 0 = \dot\chi_\sigma(g)$. Dunque

$$\dot\chi_\sigma(s_i^{-1}gs_i) = \frac{1}{|H|}\sum_{h\in H} \dot\chi_\sigma((s_ih)^{-1}gs_ih).$$

La (84) dà allora la formula

$$\chi_{\sigma^G}(g) = \frac{1}{|H|}\sum_{a\in G} \dot\chi_\sigma(a^{-1}ga). \tag{85}$$

Esempi.

1. Sia G il gruppo diedrale D_n di ordine $2n$, generato da r, s tali che $r^n = 1$, $s^2 = 1$, $srs^{-1} = r^{-1}$. Sia $H = \langle r \rangle$ e sia σ una rappresentazione di grado 1 di H tale che $r \mapsto \omega 1$, dove $\omega^n = 1$. Come rappresentanti delle classi laterali di H possiamo prendere $s_1 = 1$, $s_2 = s$. Allora $\pi(r) = 1$, $\pi(s) = (12)$, e

$$\begin{aligned} rs_1 &= s_1 r, \quad rs_2 = s_2 r^{-1}, \\ ss_1 &= s_2 1, \quad ss_2 = s_1 1. \end{aligned}$$

   Ne segue che una rappresentazione matriciale determinata da σ^G è data da

$$r \longmapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

   (cfr. p. 262).

2. Sia G come nell'esempio 1, ma sia ora $H = \langle s \rangle$. Sia σ la rappresentazione di grado 1 tale che $s \mapsto -1$. Si ha $G = H \cup rH \cup \cdots \cup r^{n-1}H$, cosicché possiamo scegliere come sistema di rappresentanti delle classi laterali l'insieme $\{s_i\}$, con $s_i = r^{i-1}$, $1 \le i \le n$. Abbiamo

$$\begin{aligned} &rs_i = s_{i+1} \quad (1 \le i \le n-1), \quad rs_n = s_1, \\ &ss_1 = s_1 s, \qquad\qquad\qquad\qquad ss_i = s_{n+2-i} s \quad (i > 1). \end{aligned}$$

   Ne segue che σ^G determina una rappresentazione matriciale data da

$$r \longmapsto \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix},$$

$$s \longmapsto \begin{pmatrix} -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 \end{pmatrix}.$$

3. Un caso particolare interessante di induzione si ottiene partendo dalla rappresentazione unità $1 = 1_H$ del sottogruppo H, che agisce su uno spazio unidimensionale $U_1 = Fu$. Sia $\{s_1, \ldots, s_r\}$ un trasversale di G rispetto ad H e supponiamo $gs_i = s_{\pi(g)i}\mu_i(g)$, con $\mu_i(g) \in H$. L'insieme degli elementi $s_i \otimes u$, $1 \le i \le r$, è una base di U_1^G e, per definizione della rappresentazione indotta, l'azione di g su U_1^G è data da $g(s_i \otimes u) = s_{\pi(g)i} \otimes u$. D'altra parte abbiamo l'azione di G sull'insieme G/H delle classi laterali sinistre $\{s_i H \mid 1 \le i \le r\}$, data da $g(s_i H) = s_{\pi(g)i} H$. È dunque chiaro che 1^G è la rappresentazione di permutazione ottenuta dall'azione di G su G/H.

   Possiamo determinare il carattere χ_{1^G} della rappresentazione 1^G. Dalla formula $g(s_i \otimes u) = s_{\pi(g)i} \otimes u$ risulta che la traccia della matrice di $1^G(g)$ rispetto alla base $(s_1 \otimes u, \ldots, s_r \otimes u)$ è il numero dei punti fissi di $\pi(g)$. Si tratta del numero delle classi laterali aH tali che $g(aH) = aH$. Abbiamo dunque la formula

$$\chi_{1^G}(g) = |\{aH \mid gaH = aH\}|. \tag{86}$$

Osserviamo inoltre che la condizione $gaH = aH$ equivale a ${}^{a^{-1}}g = a^{-1}ga \in H$.

Ricordiamo che l'azione di G su G/H è transitiva e che ogni azione transitiva di G su un insieme finito $N = \{1, 2, \ldots, n\}$ è equivalente all'azione di G su un insieme di classi laterali sinistre rispetto a un sottogruppo H di indice n in G (*BA I*, p. 75). Infatti, se G agisce transitivamente su N, possiamo prendere come H lo stabilizzatore di un elemento qualsiasi di N. È dunque chiaro che lo studio delle rappresentazioni indotte della forma 1_H^G, dove 1_H è la rappresentazione unità di un sottogruppo H di indice finito in G, equivale sostanzialmente allo studio delle azioni transitive di G sugli insiemi finiti.

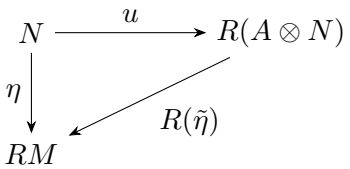
Daremo ora due utili caratterizzazioni dei moduli indotti nel caso generale in cui H è un sottogruppo di indice finito in G e U è un modulo per H. Siano $A = F[G]$, $B = F[H]$ e $\{s_1, \ldots, s_r\}$ un trasversale di G rispetto ad H. Consideriamo il modulo indotto U^G di G. Si ha $U^G = A \otimes_B U = \bigoplus_i (s_i \otimes U)$ e $[s_i \otimes U : F] = [U : F] = n$. Quindi l'applicazione $x \mapsto s_i \otimes x$ da U in $s_i \otimes U$ è un isomorfismo lineare. Poiché possiamo prendere uno degli s_i uguale a 1, vediamo che l'applicazione $x \mapsto 1 \otimes x$ è un isomorfismo lineare di U sul sottospazio $1 \otimes U = \{1 \otimes x \mid x \in U\}$ di U^G. Se $b \in B$, allora $b(1 \otimes x) = b \otimes x = 1b \otimes x = 1 \otimes bx$. Dunque $x \mapsto 1 \otimes x$ è un B-isomorfismo di U su $1 \otimes U$, che è un B-sottomodulo di U^G. Identifichiamo ora U con la sua immagine $1 \otimes U$ e consideriamo quindi U come B-sottomodulo di U^G. È anche chiaro che $U^G = s_1U \oplus \cdots \oplus s_rU$, somma diretta dei sottospazi s_iU. Le proprietà osservate danno un'utile caratterizzazione interna di U^G, che enunciamo nella seguente proposizione.

Proposizione 5.5. *Sia V un A-modulo. Allora V è isomorfo a U^G per un certo B-modulo U se e solo se V contiene U (a rigore, un B-sottomodulo isomorfo a U) in modo tale che $V = s_1U \oplus \cdots \oplus s_rU$ per un qualche trasversale $\{s_1, \ldots, s_r\}$ di G rispetto ad H.*

Dimostrazione. Abbiamo mostrato che U^G possiede le proprietà enunciate per il B-sottomodulo U ($= 1 \otimes U$) e per ogni trasversale di G rispetto ad H. Viceversa, sia V un A-modulo dotato delle proprietà enunciate. Allora $V = AU$. Poiché $s_i \in G$, s_i è invertibile in A, e dunque l'applicazione $x \mapsto s_i x$ è una biiezione. Ne segue che $[s_iU : F] = [U : F]$ e, poiché $V = s_1U \oplus \cdots \oplus s_rU$, si ha $[V : F] = [G : H][U : F]$. Abbiamo l'applicazione $(a, x) \mapsto ax$ da $A \times U$ in V, che è F-bilineare. Poiché $(ab)x = a(bx)$ per $b \in B$, ne segue che si ha un'applicazione F-lineare η da $A \otimes_B U$ in V tale che $\eta(a \otimes x) = ax$. Evidentemente η è un A-omomorfismo. Poiché $V = AU$, η è suriettivo e, poiché $[V : F] = [A \otimes_B U : F] < \infty$, η è iniettivo. Quindi V e U^G sono A-moduli isomorfi. □

La seconda caratterizzazione di U^G che daremo è di natura categoriale e si applica a un qualsiasi anello A e a un suo sottoanello B. Consideriamo le categorie di moduli A-**mod** e B-**mod**. Se M è un A-modulo, possiamo considerare M come B-modulo. Evidentemente gli omomorfismi di A-moduli sono omomorfismi di B-moduli. In tal modo otteniamo un funtore R dalla categoria A-**mod** alla categoria B-**mod**, che manda un A-modulo M in M considerato come B-modulo e gli A-omomorfismi nelle stesse applicazioni considerate come B-omomorfismi. Chiamiamo R il *funtore di restrizione degli scalari* da A-**mod** a B-**mod**. Sia ora N un B-modulo assegnato. Possiamo formare $A \otimes_B N$ e considerarlo come A-modulo nel modo consueto. Abbiamo un B-omomorfismo u da N in $A \otimes_B N$ che manda $y \in N$ in $1 \otimes y$. Affermiamo che la coppia $(A \otimes N, u)$ costituisce un universale da N al funtore R (p. 42). Ciò significa che, se M è un A-modulo (sinistro) e η è un B-omomorfismo da N in $RM = M$, esiste un unico omomorfismo di A-moduli $\tilde{\eta}$ da $A \otimes_B N$ in M che rende commutativo il diagramma

(87)



Per vederlo, consideriamo l'applicazione $(a, y) \mapsto a(\eta y)$ dall'insieme prodotto $A \times N$ in M. Evidentemente essa è additiva in a e in y, e se $b \in B$ allora $(ab)(\eta y) = a(b(\eta y)) = a(\eta(by))$. Dunque $(a, y) \mapsto a(\eta y)$ definisce un prodotto bilanciato da $A \times N$ in M (p. 126). Abbiamo quindi un omomorfismo di gruppi $\tilde{\eta}$ da $A \otimes N$ in M tale che $\tilde{\eta}(a \otimes y) = a(\eta y)$. È chiaro che $\tilde{\eta}$ è un omomorfismo di A-moduli e, se $y \in N$, si ha $R(\tilde{\eta})(uy) = R(\tilde{\eta})(1 \otimes y) = 1(\eta y) = \eta y$. Il diagramma (87) è dunque commutativo. Sia ora η' un qualsiasi A-omomorfismo da $A \otimes_B N$ in M tale che $\eta y = \eta' uy = \eta'(1 \otimes y)$. Allora $\eta'(a \otimes y) = \eta'(a(1 \otimes y)) = a\eta'(1 \otimes y) = a(\eta y)$. Quindi $\eta' = \tilde{\eta}$, e $\tilde{\eta}$ è unico.

Il fatto che, per ogni B-modulo N, $(A \otimes_B N, u)$ sia un universale da N al funtore R implica che esiste un funtore da B-**mod** ad A-**mod** che manda ciascun B-modulo N nell'A-modulo $A \otimes_B N$ e ogni omomorfismo η di B-moduli in $1 \otimes \eta$, che è un omomorfismo di A-moduli. Questo funtore è un aggiunto sinistro del funtore R (p. 49).

Ciò si applica in particolare ad $A = F[G]$ e $B = F[H]$, dove H è un sottogruppo di indice finito in G. In questo caso, dato un B-modulo U tale che $[U : F] < \infty$, otteniamo l'oggetto universale $U^G = A \otimes_B U$, che è di dimensione finita su F e fornisce quindi una rappresentazione di G.

Esercizio.

1. Siano G un gruppo finito, H un sottogruppo e σ la rappresentazione regolare di H. Mostrare che σ^G è la rappresentazione regolare di G.

5.10 Proprietà dell'induzione. Teorema di reciprocità di Frobenius

Ricaveremo ora le proprietà fondamentali delle rappresentazioni indotte. Dimostriamo anzitutto il seguente teorema.

Teorema 5.17. *Siano K un sottogruppo di indice finito in G, H un sottogruppo di indice finito in K, σ una rappresentazione di H su U, ρ una rappresentazione di G su V, e ρ_H la restrizione di ρ ad H. Allora*

1. *H ha indice finito in G e σ^G e $(\sigma^K)^G$ sono equivalenti.*
2. *Se W è un sottospazio di U invariante per $\sigma(H)$, allora W^G è un sottospazio di U^G invariante per $\sigma^G(G)$. Inoltre, se $U = W_1 \oplus W_2$ con i W_i invarianti per σ, allora $U^G = W_1^G \oplus W_2^G$.*
3. *$\sigma^G \otimes \rho$ e $(\sigma \otimes \rho_H)^G$ sono equivalenti.*

Dimostrazione. (1) Scriviamo $A = F[G]$, $B = F[H]$, $C = F[K]$. È chiaro che H ha indice finito in G (infatti $[G : H] = [G : K][K : H]$). Ora σ^K agisce su $C \otimes_B U$, $(\sigma^K)^G$ agisce su $A \otimes_C (C \otimes_B U)$ e σ^G agisce su $A \otimes_B U$. Gli A-moduli $A \otimes_C (C \otimes_B U)$ e $(A \otimes_C C) \otimes_B U$ sono isomorfi (proposizione 3.7, p. 135), e $A \otimes_C C$ e A sono isomorfi come A-moduli sinistri (proposizione 3.2, p. 130). Dunque $A \otimes_C (C \otimes_B U)$ e $A \otimes_B U$ sono isomorfi come A-moduli, il che significa che $(\sigma^K)^G$ e σ^G sono equivalenti.

(2) Se W è un sottospazio di U invariante per $\sigma(H)$, esso è un B-sottomodulo di U. Poiché A è libero come modulo destro su B, possiamo identificare $W^G = A \otimes_B W$ con la sua immagine in $U^G = A \otimes_B U$. Allora $(\sigma|_W)^G$ è una sottorappresentazione di σ^G. La seconda asserzione segue nello stesso modo.

(3) I due A-moduli da considerare sono $(A \otimes_B U) \otimes_F V$ e $A \otimes_B (U \otimes_F V)$. Nel primo caso $g \in G$ agisce secondo la regola $g((a \otimes_B x) \otimes_F y) = (ga \otimes_B x) \otimes_F gy$, nel secondo secondo la regola $g(a \otimes_B (x \otimes_F y)) = ga \otimes_B (x \otimes_F y)$. Perciò la corrispondenza $(a \otimes_B x) \otimes_F y \mapsto a \otimes_B (x \otimes_F y)$ fra i due spazi su F non fornisce un A-isomorfismo. Definiremo un A-isomorfismo di $A \otimes_B (U \otimes_F V)$ su $(A \otimes_B U) \otimes_F V$ tale che $1 \otimes_B (x \otimes_F y) \mapsto (1 \otimes_B x) \otimes_F y$ e quindi $g \otimes_B (x \otimes_F y) \mapsto (g \otimes_B x) \otimes_F gy$. Fissato $g \in G$, consideriamo l'applicazione $(x, y) \mapsto (g \otimes_B x) \otimes_F gy$ di $U \times V$ in $(A \otimes_B U) \otimes_F V$. Essendo F-bilineare, essa dà un F-omomorfismo τ_g di $U \otimes_F V$ in $(A \otimes_B U) \otimes_F V$ tale che $x \otimes_F y \mapsto (g \otimes_B x) \otimes_F gy$. Poiché G è una base di A/F, per ogni $a = \sum_g \alpha_g g$, con $\alpha_g \in F$, possiamo definire un F-omomorfismo fra gli stessi spazi ponendo $\tau_a = \sum_g \alpha_g \tau_g$. Allora $\tau_a(x \otimes_F y) = \sum_g \alpha_g (g \otimes_B x) \otimes_F gy$. Abbiamo così un'applicazione F-bilineare di $A \times (U \otimes_F V)$ in $(A \otimes_B U) \otimes_F V$. Inoltre, per $h \in H$,

$$\begin{aligned}\tau_{gh}(x \otimes_F y) - \tau_g(hx \otimes_F hy) &= (gh \otimes_B x) \otimes_F ghy - (g \otimes_B hx) \otimes_F ghy \\ &= (g \otimes_B hx) \otimes_F ghy - (g \otimes_B hx) \otimes_F ghy = 0.\end{aligned}$$

Otteniamo dunque un prodotto bilanciato di A, come B-modulo destro, e $U \otimes_F V$, come B-modulo sinistro. Ne segue un omomorfismo di $A \otimes_B (U \otimes_F V)$ in $(A \otimes_B U) \otimes_F V$ che manda $g \otimes_B (x \otimes_F y)$ in $(g \otimes_B x) \otimes_F gy$. È un F-omomorfismo e, se $g' \in G$, si ha

$$\begin{aligned}g'(g \otimes_B (x \otimes_F y)) &= g'g \otimes_B (x \otimes_F y), \\ (g'g \otimes_B x) \otimes_F g'gy &= g'((g \otimes_B x) \otimes_F gy).\end{aligned}$$

Quindi l'applicazione è un A-omomorfismo. Essa è manifestamente suriettiva e i due moduli hanno la stessa dimensione su F. Si tratta dunque di un isomorfismo. □

Per il prossimo risultato sulla rappresentazione contragrediente e sull'induzione ci serviremo di un'involuzione nell'algebra del gruppo (*BAI*, p. 112). Osserviamo anzitutto che, se $g, h \in G$, allora $(gh)^{-1} = h^{-1}g^{-1}$ e $(g^{-1})^{-1} = g$. Se $a \mapsto \bar{a}$ è la trasformazione lineare di $A = F[G]$ in sé tale che $\bar{g} = g^{-1}$, allora $\overline{ab} = \bar{b}\bar{a}$ e $\bar{\bar{a}} = a$. Dunque $a \mapsto \bar{a}$ è un'involuzione in A. La chiameremo *involuzione principale* di A e la indicheremo con j. Se H è un sottogruppo di G, l'involuzione principale di $B = F[H]$ è la restrizione a B di quella di A. Sia ora H di indice finito e sia $\{s_1, \ldots, s_r\}$ un sistema di rappresentanti. Ogni elemento di A si scrive in uno e un solo modo nella forma $a = \sum_i s_i b_i$, con $b_i \in B$. Per $c = \sum_i s_i c_i$, con $c_i \in B$, poniamo

$$(a \mid c) = \sum_i \bar{b}_i c_i \in B. \tag{88}$$

Si ottiene così l'applicazione $(a, c) \mapsto (a \mid c)$ di $A \times A$ in B. Elenchiamone le proprietà principali.

(i) $(a \mid c)$ è indipendente dalla scelta dei rappresentanti s_i. Ogni altra scelta è infatti della forma $s_i h_i$, con $h_i \in H$. Essa sostituisce b_i con $h_i^{-1} b_i$ e c_i con $h_i^{-1} c_i$. Ora $\overline{h_i^{-1} b_i}(h_i^{-1} c_i) = \bar{b}_i h_i h_i^{-1} c_i = \bar{b}_i c_i$, sicché la (88) resta invariata.

(ii) $(a \mid c)$ è F-bilineare. È evidente.

(iii) Per $b \in B$ si ha

$$(ab \mid c) = \bar{b}(a \mid c), \qquad (a \mid cb) = (a \mid c)b.$$

Ciò è immediato dalla definizione.

(iv) Per $e \in A$ si ha $(ea \mid c) = (a \mid \bar{e}c)$. Basta dimostrarlo per $e = g \in G$. Allora $gs_i = s_{\pi(g)i} p_i(g)$, dove $\pi(g) \in S_r$ e $p_i(g) \in H$. Si ha $ga = g(\sum_i s_i b_i) = \sum_i s_{\pi(g)i} p_i(g) b_i$ e

$g^{-1}s_{\pi(g)i} = s_i p_i(g)^{-1}$, onde $g^{-1}c = \sum_i s_i p_i(g)^{-1} c_{\pi(g)i}$. Dunque

$$(ga \mid c) = \sum_i \bar{b}_i p_i(g)^{-1} c_{\pi(g)i},$$
$$(a \mid g^{-1}c) = \sum_i \bar{b}_i p_i(g)^{-1} c_{\pi(g)i}.$$

Si ha dunque $(ga \mid c) = (a \mid g^{-1}c)$ per ogni $g \in G$.

(v) $(s_i \mid s_j) = \delta_{ij}1$. È immediato dalla definizione.

Mostriamo ora che l'induzione e il passaggio alla contragrediente commutano, come afferma il teorema seguente.

Teorema 5.18. *Se H è un sottogruppo di indice finito e σ è una rappresentazione di H, allora $(\sigma^G)^*$ e $(\sigma^*)^G$ sono equivalenti.*

Dimostrazione. Sia U lo spazio vettoriale su cui agisce σ e sia U^* lo spazio duale delle forme lineari su U. Per $x \in U$, $y^* \in U^*$, scriviamo $\langle y^* \mid x\rangle = y^*(x)$. Allora $\langle y^* \mid x\rangle$ è F-bilineare. Lo spazio U^* è un B-modulo sinistro definito dalla rappresentazione contragrediente σ^* di H. Possiamo farne un B-modulo destro ponendo $y^*b = \bar{b}y^*$, $b \in B$. Poiché $\langle hy^* \mid x\rangle = \langle y^* \mid h^{-1}x\rangle$ per $h \in H$, per definizione di σ^*, abbiamo $\langle y^*h \mid x\rangle = \langle y^* \mid hx\rangle$, e quindi

$$\langle y^*b \mid x\rangle = \langle y^* \mid bx\rangle \tag{89}$$

per $x \in U$, $y^* \in U^*$, $b \in B$. Introduciamo ora l'espressione

$$\langle y^*(a \mid c) \mid x\rangle \in F. \tag{90}$$

Essa è definita per $x \in U$, $a, c \in A$, $y^* \in U^*$, ed è F-bilineare in c, x per a, y^* fissati. Inoltre, per $b \in B$, la proprietà (iii) dà

$$\langle y^*(a \mid cb) \mid x\rangle = \langle y^*(a \mid c)b \mid x\rangle = \langle y^*(a \mid c) \mid bx\rangle.$$

Per la definizione del prodotto tensoriale, esiste quindi un'applicazione F-lineare di $A \otimes_B U$ in F che manda $c \otimes x$ in $\langle y^*(a \mid c) \mid x\rangle$. Abbiamo così un elemento φ_{a,y^*} del duale $(A \otimes_B U)^*$ tale che

$$\varphi_{a,y^*}(c \otimes x) = \langle y^*(a \mid c) \mid x\rangle. \tag{91}$$

L'applicazione $(a, y^*) \mapsto \varphi_{a,y^*}$ è F-bilineare e, poiché

$$\langle y^*(ab \mid c) \mid x\rangle = \langle y^*\bar{b}(a \mid c) \mid x\rangle = \langle (by^*)(a \mid c) \mid x\rangle,$$

vale $\varphi_{ab,y^*} = \varphi_{a,by^*}$. Esiste dunque un'applicazione lineare η di $A \otimes_B U^*$ in $(A \otimes_B U)^*$ che manda $a \otimes y^*$ in φ_{a,y^*}. Per $g \in G$ si ha

$$\begin{aligned}(g\varphi_{a,y^*})(c \otimes x) &= \varphi_{a,y^*}(g^{-1}(c \otimes x)) = \varphi_{a,y^*}(g^{-1}c \otimes x)\\ &= \langle y^*(a \mid g^{-1}c) \mid x\rangle.\end{aligned}$$

D'altra parte, $\varphi_{ga,y^*}(c \otimes x) = \langle y^*(ga \mid c) \mid x\rangle$. Per (iv) si ha quindi $(g\varphi_{a,y^*})(c \otimes x) = \varphi_{ga,y^*}(c \otimes x)$, il che implica che η è un A-omomorfismo. Per concludere mostreremo che η è iniettiva. Poiché $A \otimes_B U^*$ e $(A \otimes_B U)^*$ hanno la stessa dimensione finita su F, ne seguirà che η è un isomorfismo. Supponiamo $\eta(\sum_j a_j \otimes y_j^*) = 0$. Possiamo scrivere $\sum_j a_j \otimes y_j^* = \sum_i s_i \otimes z_i^*$. La condizione

$\eta(\sum_i s_i \otimes z_i^*) = 0$ implica che $\sum_i \langle z_i^*(s_i \mid c) \mid x\rangle = 0$ per ogni $c \in A$, $x \in U$, e quindi $\sum_i z_i^*(s_i \mid c) = 0$ per ogni c. Ponendo $c = s_j$ e servendoci di (v), otteniamo $z_j^* = 0$ e quindi $\sum_i s_i \otimes z_i^* = 0$. La dimostrazione è conclusa. □

Ci proponiamo ora di ricavare un importante teorema di reciprocità dovuto a Frobenius. Nella sua forma originaria esso afferma che, se ρ è una rappresentazione complessa irriducibile di un gruppo finito e σ è una rappresentazione complessa irriducibile di un sottogruppo H, la molteplicità di ρ in σ^G è uguale alla molteplicità di σ nella rappresentazione ρ_H di H. Come vedremo, basta un semplice calcolo con i caratteri per dimostrarlo. Daremo dapprima una dimostrazione concettuale di un'estensione del teorema di Frobenius. Essa si baserà sull'importante nozione di numero di intrecciamento di due rappresentazioni e sulla proposizione seguente.

Proposizione 5.6. *Se H è un sottogruppo di indice finito in G, U è un modulo su $B = F[H]$ e V è un modulo su $A = F[G]$, allora* $\hom_A(U^G, V)$ *e* $\hom_B(U, V_H)$ *sono isomorfi come spazi vettoriali su F.*

Dimostrazione. Questo risultato si può dedurre da un teorema generale sui funtori aggiunti, applicato al funtore di restrizione da $F[G]$-mod a $F[H]$-mod e al suo aggiunto sinistro. Ne daremo tuttavia una dimostrazione indipendente. Come prima, sia u l'applicazione di U in U^G definita da $x \mapsto 1 \otimes x$. Essa è un B-omomorfismo. Perciò, se $\zeta \in \hom_A(U^G, V)$, allora $\zeta u \in \hom_B(U, V_H)$. L'applicazione $\zeta \mapsto \zeta u$ è un'applicazione F-lineare di $\hom_A(U^G, V)$ in $\hom_B(U, V_H)$. Il risultato dimostrato con il diagramma (87) afferma che $\zeta \mapsto \zeta u$ è suriettiva. Essa è anche iniettiva. Infatti, se $\zeta u = 0$, allora $\zeta(1 \otimes x) = 0$ per ogni $x \in U$. Poiché ζ è un A-omomorfismo, $\zeta(a \otimes x) = \zeta(a(1 \otimes x)) = a\zeta(1 \otimes x) = 0$ per ogni $a \in A$, $x \in U$. Ne segue $\zeta = 0$. Dunque $\zeta \mapsto \zeta u$ è un isomorfismo fra gli spazi vettoriali su F dell'enunciato. □

Se ρ e τ sono rappresentazioni di G che agiscono rispettivamente su V e W, la dimensione

$$[\hom_A(V, W) : F]$$

si chiama *numero di intrecciamento* $i(\rho, \tau)$ di ρ e τ (o di V e W come $F[G]$-moduli). Se $V = V_1 \oplus \cdots \oplus V_m$, dove i V_i sono sottospazi invarianti per $\rho(G)$, scriviamo $\rho = \rho_1 \oplus \cdots \oplus \rho_m$ con $\rho_i = \rho|_{V_i}$. Analogamente, sia $\tau = \tau_1 \oplus \cdots \oplus \tau_l$, con $\tau_j = \tau|_{W_j}$ e W_j invariante per τ. Abbiamo la decomposizione di spazi vettoriali

$$\hom_A(V, W) = \bigoplus_{i,j} \hom_A(V_i, W_j). \tag{92}$$

Ne segue che

$$i(\rho, \tau) = \sum_{i,j} i(\rho_i, \tau_j). \tag{93}$$

Se ρ, τ sono completamente riducibili e le ρ_i, τ_j sono irriducibili, la formula riconduce il calcolo di $i(\rho, \tau)$ a quello dei numeri $i(\rho_i, \tau_j)$ per rappresentazioni irriducibili. Se ρ e τ sono irriducibili e inequivalenti, il lemma di Schur dà $i(\rho, \tau) = 0$. È chiaro inoltre che $i(\rho, \tau)$ resta invariato sostituendo a ρ o a τ una rappresentazione equivalente. Perciò, se ρ e τ sono equivalenti, $i(\rho, \tau) = i(\rho, \rho) = [\mathrm{End}_A(V, V) : F]$. Se ρ, τ sono irriducibili e F è algebricamente chiuso, si ha dunque

$$i(\rho, \tau) = \begin{cases} 0 & \text{se } \rho \text{ e } \tau \text{ sono inequivalenti,} \\ 1 & \text{se } \rho \text{ e } \tau \text{ sono equivalenti.} \end{cases} \tag{94}$$

Una conseguenza immediata di (93) e (94) è la seguente.

Proposizione 5.7. *Se F è algebricamente chiuso, ρ è irriducibile e τ è completamente riducibile, allora $i(\rho,\tau) = i(\tau,\rho)$ è la molteplicità di ρ in τ (ossia il numero delle componenti irriducibili di τ isomorfe a ρ).*

Possiamo ora dimostrare il fondamentale

Teorema di reciprocità di Frobenius. *Sia F un campo algebricamente chiuso. Siano ρ una rappresentazione irriducibile di G su F e σ una rappresentazione irriducibile di un sottogruppo H di indice finito in G. Supponiamo che σ^G e ρ_H siano completamente riducibili. Allora la molteplicità di ρ in σ^G è uguale alla molteplicità di σ in ρ_H.*

Dimostrazione. Per la proposizione 5.6, $i(\sigma^G,\rho) = i(\sigma,\rho_H)$. Per la proposizione 5.7, $i(\sigma^G,\rho)$ è la molteplicità di ρ in σ^G e $i(\sigma,\rho_H)$ è la molteplicità di σ in ρ_H. Queste molteplicità, dunque, coincidono. □

Il teorema di reciprocità di Frobenius si enuncia di solito per gruppi finiti e campi algebricamente chiusi di caratteristica che non divide l'ordine del gruppo. In questo caso le ipotesi che H sia di indice finito e che σ^G, ρ_H siano completamente riducibili sono automaticamente soddisfatte. Questo risultato e alcuni altri, fra quelli ottenuti per le rappresentazioni indotte dei gruppi finiti, si possono dimostrare mediante calcoli con i caratteri. Per illustrare il metodo dimostriamo così il teorema di reciprocità di Frobenius quando G è finito e $F = \mathbb{C}$. Conserviamo le notazioni precedenti e indichiamo con $\chi_\rho, \chi_\sigma, \ldots$ i caratteri di $\rho, \sigma, \ldots$. Ricordiamo che, se ρ è irriducibile e τ è arbitraria, $(\chi_\rho \mid \chi_\tau) = (\chi_\tau \mid \chi_\rho)$ è la molteplicità di ρ in τ. Il teorema equivale a

$$(\chi_{\sigma^G} \mid \chi_\rho)_G = (\chi_\sigma \mid \chi_{\rho_H})_H. \tag{95}$$

Dalla formula (85) per χ_{σ^G} otteniamo

$$\begin{aligned}(\chi_{\sigma^G} \mid \chi_\rho)_G &= \sum_{a,g\in G} \frac{1}{|G|}\frac{1}{|H|}\overline{\dot\chi_\sigma(a^{-1}ga)}\,\chi_\rho(g)\\ &= \sum_{a,g\in G} \frac{1}{|G|}\frac{1}{|H|}\overline{\dot\chi_\sigma(g)}\,\chi_\rho(aga^{-1})\\ &= \sum_{\substack{a\in G\\ h\in H}} \frac{1}{|G|}\frac{1}{|H|}\overline{\chi_\sigma(h)}\,\chi_\rho(aha^{-1}).\end{aligned}$$

D'altra parte,

$$\begin{aligned}(\chi_\sigma \mid \chi_{\rho_H})_H &= \sum_{h\in H} \frac{1}{|H|}\overline{\chi_\sigma(h)}\,\chi_\rho(h)\\ &= \sum_{\substack{h\in H\\ a\in G}} \frac{1}{|G|}\frac{1}{|H|}\overline{\chi_\sigma(h)}\,\chi_\rho(aha^{-1}),\end{aligned}$$

poiché χ_ρ è una funzione di classe su G. Il confronto fra le due formule dà la (95).

Esercizi.

1. Costruire la tavola dei caratteri di $G = A_5$. *Traccia.* In G vi sono cinque classi di coniugio, con rappresentanti $1, (12)(34), (123), (12345), (13524) = (12345)^2$, di cardinalità rispettivamente $1, 15, 20, 12, 12$. Sia χ_1 il carattere della rappresentazione identica di grado

uno e sia ν la rappresentazione per permutazioni ottenuta dall'azione naturale di G su $\{1,2,3,4,5\}$. Si ha la tavola

	1	$(12)(34)$	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_ν	5	1	2	0	0

Dal calcolo di $(\chi_\nu \mid \chi_\nu)$ e di $(\chi_\nu \mid \chi_1)$ segue $\chi_\nu = \chi_1 + \chi_2$, dove χ_2 è irriducibile. La tavola precedente determina allora χ_2. Per ottenere i tre caratteri irriducibili mancanti, consideriamo i caratteri indotti da caratteri lineari (di grado uno) del sottogruppo

$$\begin{aligned} H = \{&1, u = (12345), u^2 = (13524), u^3 = (14253),\\ &u^4 = (54321), (13)(54), (24)(15), (35)(21),\\ &(14)(23), (25)(34)\}. \end{aligned}$$

Poiché $\langle u \rangle$ ha indice due in H, su H abbiamo i caratteri lineari λ_1, λ_2, dove $\lambda_1 \equiv 1$, $\lambda_2(u^k) = 1$ e $\lambda_2(v) = -1$ se $v \notin \langle u \rangle$. L'insieme

$$\begin{aligned} C = \{&1, w = (13245), w^2 = (12534), w^3 = (14352),\\ &w^4 = (15423), (12)(34)\} \end{aligned}$$

è un sistema di rappresentanti di G rispetto ad H. Servendocene possiamo calcolare λ_1^G e λ_2^G, ottenendo

	1	$(12)(34)$	(123)	(12345)	(13524)
λ_1^G	6	2	0	1	1
λ_2^G	6	-2	0	1	1

Dai prodotti $(\lambda_i^G \mid \lambda_i^G)$, $i = 1, 2$, e $(\lambda_1^G \mid \chi_1)$ otteniamo $\lambda_1^G = \chi_1 + \chi_3$, dove χ_3 è irriducibile. Abbiamo inoltre $(\lambda_2^G \mid \chi_1) = (\lambda_2^G \mid \chi_2) = (\lambda_2^G \mid \lambda_1^G) = 0$, il che implica $\lambda_2^G = \chi_4 + \chi_5$, dove χ_4, χ_5 sono irriducibili. I valori di $\chi_i(1)$ per $1 \leq i \leq 3$ e la relazione $\sum_{i=1}^5 \chi_i(1)^2 = 60$ danno $\chi_4(1) = 3 = \chi_5(1)$. Otteniamo così la tavola

	1	$(12)(34)$	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	a	b	c	d
χ_5	3	a'	b'	c'	d'

Poiché $(54321) = (12345)^{-1}$ è coniugato a (12345), χ_4 e χ_5 sono reali (esercizio 7, p. 279). Da $\chi_4 + \chi_5 = \lambda_2^G$ otteniamo $a + a' = -2$, $b + b' = 0$, $c + c' = 1 = d + d'$. Usando $(\chi_4 \mid \chi_i) = \delta_{i4}$ per $i = 1, 2, 3, 4$, otteniamo un sistema di equazioni in a, b, c, d le cui soluzioni sono $a = -1$, $b = 0$, $c = (1 \pm \sqrt{5})/2$, $d = 1 - c$. Entrambe le scelte permettono di completare la tavola.

2. Dimostrare i teoremi 5.17 e 5.18 per le rappresentazioni complesse di gruppi finiti mediante calcoli con i caratteri.

3. Sia B un sottoanello di un anello A, e sia M un B-modulo (sinistro). Allora $\hom_B(A, M)$ diventa un A-modulo sinistro ponendo $(af)x = f(xa)$ per $f \in \hom_B(A, M)$, $a, x \in A$ (proposizione 3.4, p. 134). Esso si chiama *modulo coindotto* (o *prodotto*) di A determinato da M. Osservare che l'applicazione $v\colon f \mapsto f(1)$ di $\hom_B(A, M)$ in M è un B-omomorfismo. Mostrare che la coppia $(\hom_B(A, M), v)$ costituisce un universale dal funtore R di restrizione degli scalari a M (p. 137).

4. Siano G un gruppo, H un sottogruppo di indice finito, $A = F[G]$, $B = F[H]$, e sia U il B-modulo determinato da una rappresentazione σ di H. Allora $\hom_B(A, U)$ ha dimensione finita su F e definisce la *rappresentazione coindotta* ${}^G\sigma$ di G. Mostrare che ${}^G(\sigma^*)$ è equivalente a $(\sigma^G)^*$. (Ciò mostra che nella teoria delle rappresentazioni di dimensione finita i moduli coindotti sono superflui.)

5. Sia G finito e sia F un campo algebricamente chiuso la cui caratteristica non divide $|G|$. Sia ρ la rappresentazione per permutazioni di G determinata dall'azione di G su G/H, dove H è un sottogruppo. Servirsi della reciprocità di Frobenius per mostrare che lo spazio $\operatorname{Inv}\rho = \{x \mid gx = x,\ g \in G\}$ ha dimensione uno.

6. (*Complemento al teorema di Clifford.*) Sia ρ una rappresentazione irriducibile di G su V/F e sia $H \lhd G$. Sia W una componente omogenea di V come $F[H]$-modulo (si ricordi che, per il teorema di Clifford, ρ_H è completamente riducibile). Sia T il sottogruppo di G che stabilizza W. Mostrare che (i) $H \subseteq T \subseteq G$ e $[G : T] = m$, dove m è il numero delle componenti omogenee di V come $F[H]$-modulo, e (ii) se ψ è la rappresentazione di T su W, allora $\rho = \psi^G$ e ψ è irriducibile.

7. (*Mackey.*) Sia H un sottogruppo di indice finito in G e sia U un $F[H]$-modulo. Sia V l'insieme delle applicazioni $f\colon G \to U$ tali che $f(hg) = hf(g)$. Munire V dell'usuale struttura di spazio vettoriale e dell'azione di G definita da $(gf)(x) = f(xg)$, con $f \in V$, $g, x \in G$. Mostrare che V diventa un $F[G]$-modulo isomorfo a U^G.

5.11 Ulteriori risultati sui moduli indotti

Uno dei problemi principali che considereremo in questo paragrafo consiste nel trovare criteri applicabili per stabilire se una rappresentazione indotta (o un carattere indotto) sia irriducibile. A questo fine dovremo studiare il problema seguente. Supponiamo che H e K siano sottogruppi di un gruppo G, che H abbia indice finito in G e che σ sia una rappresentazione di H sullo spazio vettoriale U/F. Che cosa si può dire della struttura di ${\sigma^G}_K = (\sigma^G)_K$, restrizione a K della rappresentazione indotta σ^G di G? Se V è un $F[G]$-modulo, denotiamo con V_K lo stesso V considerato come $F[K]$-modulo. Ci interessa dunque la struttura di ${U^G}_K = (U^G)_K$. Identifichiamo U con l'$F[H]$-sottomodulo $1 \otimes U$ di U^G. Se $g \in G$, l'azione del sottogruppo ${}^gH = \{ghg^{-1} \mid h \in H\}$ stabilizza gU, poiché per $x \in U$ si ha $(ghg^{-1})gx = ghx \in gU$. Abbiamo così i sottomoduli $(gU)_{{}^gH}$ e $(gU)_{K \cap {}^gH}$, rispettivamente di $(U^G)_{{}^gH}$ e di $(U^G)_{K \cap {}^gH}$. Osserviamo che, siccome ${}^gH$ ha indice finito in G, anche $K \cap {}^gH$ ha indice finito in K. Possiamo dunque formare l'$F[K]$-modulo indotto $\left((gU)_{K \cap {}^gH}\right)^K$. Otterremo una decomposizione di $(U^G)_K$ in sottomoduli di questa forma. Per descriverla occorrono alcune semplici osservazioni sulle classi laterali doppie.

Ricordiamo che G è unione disgiunta delle classi laterali doppie KgH (BAI, p. 53). Inoltre KgH è unione di classi laterali sinistre kgH, $k \in K$, e, poiché H ha indice finito in G, sono in numero finito le classi laterali sinistre di H contenute in KgH. Osserviamo ora che, per $k_1, k_2 \in K$, si ha $k_1gH = k_2gH$ se e solo se $k_1(K \cap {}^gH) = k_2(K \cap {}^gH)$. Infatti $k_1gH = k_2gH$ se e solo se $k_2g = k_1gh$ con $h \in H$, e ciò accade se e solo se $k_1^{-1}k_2 = ghg^{-1}$ con $h \in H$. Quest'ultima condizione equivale a $k_1(K \cap {}^gH) = k_2(K \cap {}^gH)$. Ne segue che $\{k_i\}$ è un sistema di rappresentanti di K rispetto a $K \cap {}^gH$ se e solo se $\{k_ig\}$ è un sistema di rappresentanti delle classi laterali sinistre di H contenute in KgH.

Possiamo servirci di questo risultato per dimostrare il seguente importante teorema.

Teorema di decomposizione di Mackey. *Siano H un sottogruppo di indice finito in G, K un sottogruppo qualsiasi di G e U un $F[H]$-modulo. Identifichiamo U con l'$F[H]$-sottomodulo*

$1 \otimes U$ *di* U^G *e indichiamo con* Δ *l'insieme delle classi laterali doppie* $D = KgH$*. Allora*

$$(U^G)_K = \bigoplus_{D \in \Delta} DU,$$

dove $DU = \sum_{g \in D} gU$ *è un* $F[K]$*-sottomodulo di* $(U^G)_K$ *e* $DU \cong \big((gU)_{K \cap {}^gH}\big)^K$ *per ogni* $g \in D$*.*

Dimostrazione. Sia $\{s_1, \ldots, s_r\}$ un sistema di rappresentanti di G rispetto a H. Allora $U^G = s_1U \oplus \cdots \oplus s_rU$ (proposizione 5.5, p. 290). Se $g \in G$, abbiamo $D = KgH = s_{i_1}H \cup \cdots \cup s_{i_k}H$ con gli s_{i_j} distinti. Allora $DU = KgHU = s_{i_1}U \oplus \cdots \oplus s_{i_k}U$. Segue che $(U^G)_K = \bigoplus_{D \in \Delta} DU$. Ora $DU = KgU$ è un $F[K]$-sottomodulo di $(U^G)_K$ e contiene gU, che è un $F[K \cap {}^gH]$-sottomodulo. Abbiamo visto che, se $\{k_i \mid 1 \leq i \leq q\}$ è un sistema di rappresentanti di K rispetto a $K \cap {}^gH$, allora $\{k_ig\}$ rappresenta le classi laterali sinistre di H contenute in $D = KgH$. Possiamo dunque supporre che $\{k_ig\} = \{s_{i_1}, \ldots, s_{i_k}\}$, sicché $q = k$ e

$$DU = k_1gU \oplus \cdots \oplus k_qgU.$$

Per la proposizione 5.5, ne segue che DU, come $F[K]$-modulo, è isomorfo a $\big((gU)_{{}^gH \cap K}\big)^K$. □

Ricaveremo ora un teorema sulla struttura del prodotto tensoriale di due rappresentazioni indotte.

Teorema 5.19 (Mackey). *Per* $i = 1, 2$ *siano* H_i *un sottogruppo di indice finito in* G *e* σ_i *una rappresentazione di* H_i *su* U_i/F*. Sia* R *un sistema di rappresentanti delle classi laterali doppie* H_1gH_2*. Poniamo* $H^{(1,g)} = H_1 \cap {}^gH_2$*. Si ha allora l'isomorfismo di* $F[G]$*-moduli*

$$U_1^G \otimes U_2^G \cong \bigoplus_{g \in R} \big((U_1)_{H^{(1,g)}} \otimes (gU_2)_{H^{(1,g)}}\big)^G.$$

Dimostrazione. Per il teorema 5.17.3, $\sigma_1^G \otimes \sigma_2^G$ è equivalente a $\big(\sigma_1 \otimes (\sigma_2^G)_{H_1}\big)^G$ e, per la decomposizione di Mackey, $(U_2^G)_{H_1}$ è somma diretta di $F[H_1]$-sottomoduli isomorfi ai moduli $\big((gU_2)_{H^{(1,g)}}\big)^{H_1}$, $g \in R$. Pertanto $U_1^G \otimes U_2^G$ è $F[G]$-isomorfo a

$$\bigoplus_{g \in R} \big(U_1 \otimes \big((gU_2)_{H^{(1,g)}}\big)^{H_1}\big)^G.$$

Per il teorema 5.17.3,

$$U_1 \otimes \big((gU_2)_{H^{(1,g)}}\big)^{H_1} \cong \big((U_1)_{H^{(1,g)}} \otimes (gU_2)_{H^{(1,g)}}\big)^{H_1}.$$

Quindi, per la transitività dell'induzione (teorema 5.17.1),

$$\big(U_1 \otimes \big((gU_2)_{H^{(1,g)}}\big)^{H_1}\big)^G \cong \big((U_1)_{H^{(1,g)}} \otimes (gU_2)_{H^{(1,g)}}\big)^G.$$

Sostituendo nella formula per $U_1^G \otimes U_2^G$, si ottiene il teorema. □

Il risultato precedente permette di ottenere un criterio di irriducibilità per un modulo indotto. Occorrono anche alcuni risultati generali sui moduli, in parte già indicati negli esercizi (p. 251). Osserviamo anzitutto che, se V_i, $i = 1, 2$, è uno spazio vettoriale di dimensione finita su un campo F, esiste un isomorfismo canonico fra $V_1^* \otimes_F V_2$, dove V_1^* è lo spazio duale dei funzionali lineari su V_1, e $\hom_F(V_1, V_2)$. Esso manda $u^* \otimes v$, con $u^* \in V_1^*$, $v \in V_2$, nell'applicazione lineare $[u^*, v]$ tale che $[u^*, v](x) = u^*(x)v$ per $x \in V_1$ (p. 165). Per vedere che si ha un tale isomorfismo, osserviamo che la corrispondenza per u^* e v è bilineare. Esiste quindi un'applicazione lineare η di $V_1^* \otimes_F V_2$ in $\hom_F(V_1, V_2)$ tale che $\eta(u^* \otimes v) = [u^*, v]$. Si vede subito che η è suriettiva e,

poiché i due spazi $V_1^* \otimes_F V_2$ e $\hom_F(V_1, V_2)$ hanno la stessa dimensione $[V_1 : F][V_2 : F]$, ne segue che η è un isomorfismo lineare.

Supponiamo ora che ρ_i, $i = 1, 2$, sia una rappresentazione di un gruppo G su V_i/F. Come a p. 272, si ottiene una rappresentazione ρ di G su $\hom_F(V_1, V_2)$ ponendo $\rho(g)l = \rho_2(g)l\rho_1(g)^{-1}$ per $g \in G$, $l \in \hom_F(V_1, V_2)$. L'isomorfismo η fra $V_1^* \otimes_F V_2$ e $\hom_F(V_1, V_2)$ è un'equivalenza delle rappresentazioni $\rho_1^* \otimes \rho_2$ e ρ. Infatti siano $u^* \in V_1^*$, $v \in V_2$. Allora $\eta(\rho_1^*(g)u^* \otimes \rho_2(g)v)$ è l'applicazione

$$\begin{aligned} x &\longmapsto (\rho_1^*(g)u^*)(x)\rho_2(g)v \\ &= u^*(\rho_1(g)^{-1}x)\rho_2(g)v \\ &= \rho_2(g)(u^*(\rho_1(g)^{-1}x)v) \\ &= \rho_2(g)\eta(u^* \otimes v)\rho_1(g)^{-1}x. \end{aligned}$$

Dunque $\eta(\rho_1^*(g)u^* \otimes \rho_2(g)v) = \rho(g)\eta(u^* \otimes v)$, il che implica che η è un $F[G]$-isomorfismo di $V_1^* \otimes V_2$ su $\hom_F(V_1, V_2)$.

Consideriamo ora lo spazio vettoriale $\hom_{F[G]}(V_1, V_2)$. Esso è evidentemente un sottospazio di $\hom_F(V_1, V_2)$ e lo possiamo identificare con l'insieme degli $l \in \hom_F(V_1, V_2)$ tali che $\rho(g)l = l$ per $g \in G$. Infatti questa condizione equivale a $\rho_2(g)l\rho_1(g)^{-1} = l$, ossia a $\rho_2(g)l = l\rho_1(g)$, che è la condizione perché $l \in \hom_{F[G]}(V_1, V_2)$. In generale, se ρ è una rappresentazione di G su V, si denota con $\operatorname{Inv}\rho$ l'insieme degli $x \in V$ tali che $\rho(g)x = x$ per ogni $g \in G$. È evidentemente un sottospazio. È pure chiaro che $x \neq 0$ appartiene a $\operatorname{Inv}\rho$ se e solo se Fx è un sottospazio unidimensionale $\rho(G)$-invariante e la restrizione di ρ a Fx è la rappresentazione unità. Pertanto, se ρ è completamente riducibile, $[\operatorname{Inv}\rho : F]$ è la molteplicità della rappresentazione unità in ρ.

Se ρ_1 e ρ_2 sono rappresentazioni completamente riducibili, le diremo *disgiunte* quando non hanno costituenti irriducibili in comune, cioè quando non esiste alcuna rappresentazione irriducibile isomorfa a una sottorappresentazione sia di ρ_1 sia di ρ_2.

Dalle definizioni e dall'$F[G]$-isomorfismo fra $V_1^* \otimes_F V_2$ e $\hom_F(V_1, V_2)$ seguono facilmente i risultati seguenti.

Proposizione 5.8. *(i) Sia ρ_i, $i = 1, 2$, una rappresentazione di un gruppo G su V_i/F. Allora il numero di intreccio $i(\rho_1, \rho_2)$ è $[\operatorname{Inv}(\rho_1^* \otimes \rho_2) : F]$. Inoltre, se $\rho_1^* \otimes \rho_2$ è completamente riducibile, $i(\rho_1, \rho_2)$ è la molteplicità della rappresentazione unità in $\rho_1^* \otimes \rho_2$. (ii) Se ρ_1, ρ_2 e $\rho_1^* \otimes \rho_2$ sono completamente riducibili, ρ_1 e ρ_2 sono disgiunte se e solo se la rappresentazione unità non è una componente di $\rho_1^* \otimes \rho_2$. (iii) Sia F algebricamente chiuso e sia ρ una rappresentazione completamente riducibile di G su V/F, tale che anche $\rho^* \otimes \rho$ sia completamente riducibile. Allora ρ è irriducibile se e solo se la rappresentazione unità ha molteplicità uno in $\rho^* \otimes \rho$.*

Dimostrazione. (i) Per definizione, $i(\rho_1, \rho_2) = [\hom_{F[G]}(V_1, V_2) : F]$. Abbiamo anche visto che $\hom_{F[G]}(V_1, V_2) = \operatorname{Inv}\rho$, dove ρ è la rappresentazione di G su $\hom_F(V_1, V_2)$ tale che $\rho(g)l = \rho_2(g)l\rho_1(g)^{-1}$. Poiché ρ è equivalente a $\rho_1^* \otimes \rho_2$, si ha $[\operatorname{Inv}\rho : F] = [\operatorname{Inv}(\rho_1^* \otimes \rho_2) : F]$. Pertanto

$$i(\rho_1, \rho_2) = [\hom_{F[G]}(V_1, V_2) : F] = [\operatorname{Inv}\rho : F] = [\operatorname{Inv}(\rho_1^* \otimes \rho_2) : F].$$

Ciò dimostra la prima affermazione di (i). La seconda segue immediatamente dalla prima e dal fatto che, per ρ completamente riducibile, $[\operatorname{Inv}\rho : F]$ è la molteplicità della rappresentazione unità in ρ. (ii) Se ρ_1 e ρ_2 sono completamente riducibili, dalla (94) e dal lemma di Schur segue che esse sono disgiunte se e solo se $i(\rho_1, \rho_2) = 0$. Per (i) ciò vale se e solo se $\operatorname{Inv}(\rho_1^* \otimes \rho_2) = 0$. Se $\rho_1^* \otimes \rho_2$ è completamente riducibile, questo accade se e solo se la rappresentazione unità non è una sua componente. (iii) Per le (94) e (95), se F è algebricamente chiuso e ρ è completamente riducibile, ρ è irriducibile se e solo se $i(\rho, \rho) = 1$. Per (i), ciò equivale a $[\operatorname{Inv}(\rho^* \otimes \rho) : F] = 1$. Se $\rho^* \otimes \rho$ è completamente riducibile, questa condizione vale se e solo se la rappresentazione unità vi ha molteplicità uno. □

Le scomode ipotesi di completa riducibilità della proposizione si possono eliminare se G è finito e $\operatorname{char} F \nmid |G|$. In tal caso abbiamo il seguente criterio di irriducibilità per rappresentazioni indotte.

Teorema 5.20. *Siano G un gruppo finito, H un suo sottogruppo, F un campo algebricamente chiuso di caratteristica che non divide $|G|$ e σ una rappresentazione di H su U/F. Allora σ^G è irriducibile se e solo se (1) σ è irriducibile e (2) per ogni $g \notin H$ le rappresentazioni di $H \cap {}^gH$ su U e su gU sono disgiunte.*

Dimostrazione. Evidentemente (1) è una condizione necessaria perché σ^G sia irriducibile. Supponiamo ora σ irriducibile. Per la proposizione 5.8(iii), σ^G è irriducibile se e solo se la rappresentazione unità ha molteplicità 1 in $(\sigma^G)^* \otimes \sigma^G$. Poiché $(\sigma^G)^*$ e $(\sigma^*)^G$ sono equivalenti (teorema 5.18, p. 294), possiamo sostituire la prima con la seconda. Per il teorema 5.19,

$$(U^*)^G \otimes U^G \cong \bigoplus_g \big((U^*)_{H\cap {}^gH} \otimes (gU)_{H\cap {}^gH}\big)^G,$$

dove g percorre un sistema di rappresentanti dell'insieme Δ delle classi laterali doppie HgH. Ora $(U^*)_{H\cap {}^gH}$ e $(U_{H\cap {}^gH})^*$ indicano la stessa cosa, cioè U^* come modulo per $F[H \cap {}^gH]$ determinato dall'azione contragrediente. Dobbiamo dunque considerare in ciascun $\big((U_{H\cap {}^gH})^* \otimes (gU)_{H\cap {}^gH}\big)^G$ la molteplicità del modulo banale (che dà la rappresentazione unità). Osserviamo che, per un qualsiasi sottogruppo K di G e una rappresentazione τ di K su V/F, la molteplicità della rappresentazione unità τ_1 di K in τ è uguale a quella della rappresentazione unità ρ_1 di G in τ^G. Data la completa riducibilità, basta mostrare che, se τ è irriducibile, ρ_1 ha molteplicità 0 in τ^G salvo che per $\tau = \tau_1$, nel qual caso la molteplicità è 1. Ciò segue immediatamente dalla reciprocità di Frobenius. Applichiamo ora questa osservazione a $K = H \cap {}^gH$, $g \in G$, e a $V = (U_{H\cap {}^gH})^* \otimes (gU)_{H\cap {}^gH}$. Se $g \in H$, questi diventano H e $U^* \otimes U$. Poiché σ è irriducibile, la molteplicità della rappresentazione unità in $\sigma^* \otimes \sigma$ è 1. La componente $(U^* \otimes U)^G$ contribuisce dunque con molteplicità 1 alla rappresentazione unità di G su $(U^*)^G \otimes U^G$. Pertanto σ^G è irriducibile se e solo se la molteplicità della rappresentazione unità di $H \cap {}^gH$ su $(U_{H\cap {}^gH})^* \otimes (gU)_{H\cap {}^gH}$ è 0 per ogni $g \notin H$. Per la proposizione 5.8 ciò avviene se e solo se le rappresentazioni di $H \cap {}^gH$ su U e su gU sono disgiunte per ogni $g \notin H$. La dimostrazione è completa. □

Un interessante caso particolare del teorema 5.20 si ottiene prendendo per σ una rappresentazione di grado 1 di H. La rappresentazione σ^G si dice allora *monomiale*. Dalla forma matriciale di una rappresentazione indotta data a p. 288 risulta che una rappresentazione monomiale ammette una rappresentazione matriciale in cui tutte le matrici hanno un solo elemento non nullo in ogni riga e in ogni colonna.[15] Il teorema 5.20 si riduce al seguente criterio di irriducibilità per le rappresentazioni monomiali.

Corollario 1 (K. Shoda). *Sia ρ una rappresentazione monomiale di un gruppo finito G, indotta da una rappresentazione σ di grado uno di un sottogruppo H di G. Si supponga che il campo base sia algebricamente chiuso e di caratteristica che non divide $|G|$. Allora ρ è irriducibile se e solo se, per ogni $g \in G - H$, esiste un $h \in H \cap {}^gH$ tale che $\sigma(h) \neq \sigma(g^{-1}hg)$.*[16]

Un altro caso particolare interessante del teorema 5.20 è quello in cui $H \lhd G$. Allora ${}^gH = H$ per ogni $g \in G$ e la rappresentazione di H su gU è la rappresentazione coniugata ${}^g\sigma$ (p. 255). Dal criterio di irriducibilità del teorema 5.20 si ottiene evidentemente il risultato seguente.

Corollario 2. *Siano G, H, F, σ come nel teorema 5.20 e si supponga $H \lhd G$. Allora σ^G è irriducibile se e solo se σ è irriducibile e, per ogni $g \in G - H$, le rappresentazioni ${}^g\sigma$ e σ non sono equivalenti.*

[15] L'originale aggiunge che la posizione è la stessa per tutte le matrici. In generale essa dipende dalla permutazione delle classi laterali indotta dall'elemento del gruppo.

[16] Nella stampa si legge $\sigma(ghg^{-1})$. Poiché $h \in H \cap gHg^{-1}$, l'elemento cui si applica σ è $g^{-1}hg \in H$.

Ne ricaveremo ora un'importante estensione. Sia ancora $H \triangleleft G$ e sia σ una rappresentazione irriducibile di H su U/F. Poniamo

$$T(\sigma) = \{g \in G \mid {}^g\sigma \text{ è equivalente a } \sigma\}.$$

Allora $T(\sigma)$ è un sottogruppo di G contenente H, detto *gruppo d'inerzia* di σ. Si ha il risultato seguente.

Corollario 3. *Valgano le ipotesi del teorema 5.20, con $H \triangleleft G$. Sia ψ una rappresentazione irriducibile del gruppo d'inerzia $T(\sigma)$ tale che ψ_H abbia σ come componente irriducibile. Allora ψ^G è irriducibile.*

Dimostrazione. Sia V l'$F[T]$-modulo su cui agisce ψ. Per il teorema di Clifford applicato a $T = T(\sigma)$ e a $H \triangleleft T$, σ è l'unica componente irriducibile di ψ_H. Consideriamo ora V^G, che possiamo supporre contenga V come sottomodulo, e consideriamo il sottospazio gV di V^G come modulo per $F[T \cap {}^gT]$. Poiché $H \triangleleft G$, abbiamo $H \subset T \cap {}^gT$ e gV è somma di $F[H]$-sottomoduli irriducibili isomorfi a gU. La rappresentazione di H su gU è ${}^g\sigma$ e, per $g \notin T$, essa non è equivalente a σ. Segue che le rappresentazioni di H su V e su gV sono disgiunte. Altrettanto vale dunque per le rappresentazioni di $T \cap {}^gT$ su V e su gV. Per il teorema 5.20, ψ^G è allora irriducibile. □

Una conseguenza del corollario 3 che ci sarà utile nel seguito è la seguente.

Corollario 4. *Siano G un gruppo finito, $H \triangleleft G$ e ρ una rappresentazione irriducibile di G su un campo algebricamente chiuso F di caratteristica che non divide $|G|$. Siano σ una componente irriducibile di ρ_H e T il gruppo d'inerzia di σ. Allora $\rho = \psi^G$ per una rappresentazione irriducibile ψ di T.*

Dimostrazione. Poiché σ è una componente irriducibile di ρ_H, esiste una componente irriducibile ψ di ρ_T tale che σ sia una componente irriducibile di ψ_H. Allora ψ^G è irriducibile per il corollario 3. Poiché ψ è una componente irriducibile di ρ_T, per la reciprocità di Frobenius ρ è una componente irriducibile di ψ^G. Quindi $\rho = \psi^G$. □

L'importanza di questo risultato sta nel fatto che, se $T \neq G$, esso dà una formula per ρ come rappresentazione indotta da un sottogruppo proprio. Ciò permette di stabilire proprietà delle rappresentazioni irriducibili di G ragionando per induzione su $|G|$.

5.12 Il teorema di Brauer sui caratteri indotti

Per il resto di questo capitolo G sarà finito e il campo base F sarà un sottocampo di $\mathbb{C}$, di solito $\mathbb{C}$ stesso. In questo paragrafo dimostreremo un teorema fondamentale di Brauer sui caratteri indotti. Per enunciarlo occorre la definizione seguente.

Definizione 5.3. *Un gruppo G si dice p-elementare se $G = Z \times P$, dove Z è ciclico di ordine primo con p e P è un p-gruppo (cioè un gruppo di ordine p^n). Il gruppo G si dice elementare se è p-elementare per qualche primo p.*

Con questa definizione possiamo enunciare il teorema.

Teorema di Brauer sui caratteri indotti. *Ogni carattere complesso di un gruppo G è una combinazione lineare a coefficienti interi di caratteri indotti da caratteri lineari di sottogruppi elementari di G.*

La dimostrazione che daremo è dovuta a D. Goldschmidt e M. Isaacs. La prima dimostrazione di Brauer era piuttosto complicata. Una dimostrazione considerevolmente più semplice fu data indipendentemente da Brauer e Tate e da K. Asano. Tanto queste dimostrazioni quanto quella di Goldschmidt e Isaacs prendono le mosse dalle seguenti semplici osservazioni.

Sia $\mathrm{ch}(G)$ l'insieme delle combinazioni $\mathbb{Z}$-lineari dei caratteri complessi irriducibili $\chi_1, \ldots, \chi_s$ del gruppo G, dove χ_1 è il carattere unità. Gli elementi di $\mathrm{ch}(G)$ si chiamano *caratteri generalizzati*. Ogni carattere complesso è un carattere generalizzato e, poiché $\chi_i\chi_j$ è il carattere del prodotto tensoriale delle rappresentazioni irriducibili di caratteri χ_i e χ_j, si ha $\chi_i\chi_j \in \mathrm{ch}(G)$. Ne segue che $\mathrm{ch}(G)$ è un anello, più precisamente un sottoanello dell'anello $\mathbb{C}^G$ delle funzioni a valori complessi su G, con le consuete operazioni di addizione e moltiplicazione definite punto per punto. Il carattere χ_1 è l'unità di $\mathrm{ch}(G)$. Se H è un sottogruppo di G e ψ è una funzione di classe su H, definiamo la *funzione di classe indotta* ψ^G su G mediante

$$\psi^G(g) = \frac{1}{|H|}\sum_{a\in G} \dot{\psi}(a^{-1}ga), \tag{96}$$

dove $\dot{\psi}(h) = \psi(h)$ per $h \in H$ e $\dot{\psi}(g) = 0$ per $g \in G - H$. Questa è una funzione di classe su G e abbiamo visto nella (85) che, se ψ è il carattere di una rappresentazione σ di H, allora ψ^G è il carattere di σ^G. Se χ è il carattere di una rappresentazione ρ di G, si ha

$$\psi^G\chi = (\psi\chi_H)^G, \tag{97}$$

dove χ_H è la restrizione di χ a H, poiché $\sigma^G \otimes \rho \cong (\sigma \otimes \rho_H)^G$ (teorema 5.17.3, p. 292). Inoltre, dalla transitività dell'induzione delle rappresentazioni segue la formula di transitività

$$(\psi^K)^G = \psi^G \tag{98}$$

se K è un sottogruppo di G contenente H.

Sia ora $\mathcal{F}$ una famiglia qualsiasi di sottogruppi di G e sia $\mathrm{ch}_{\mathcal{F}}(G)$ l'insieme delle combinazioni $\mathbb{Z}$-lineari di caratteri della forma ψ^G, dove ψ è un carattere complesso di un sottogruppo $H \in \mathcal{F}$. Dalla (97) risulta che $\mathrm{ch}_{\mathcal{F}}(G)$ è un ideale di $\mathrm{ch}(G)$. Pertanto $\mathrm{ch}_{\mathcal{F}}(G) = \mathrm{ch}(G)$ se e solo se $\chi_1 \in \mathrm{ch}_{\mathcal{F}}(G)$.

La dimostrazione del teorema di Brauer data da Goldschmidt e Isaacs procede in due tappe. Nella prima si dimostra che $\chi_1 \in \mathrm{ch}_{\mathcal{F}}(G)$ per una famiglia di sottogruppi, i cosiddetti sottogruppi quasi-elementari, più ampia della famiglia dei sottogruppi elementari. Nella seconda si dimostra il teorema di Brauer per i sottogruppi quasi-elementari. Per questa seconda parte dimostreremo dapprima un'estensione, dovuta a Brauer, di un teorema di H. Blichfeldt secondo il quale ogni rappresentazione irriducibile di un gruppo quasi-elementare è monomiale. Ce ne serviremo poi per dimostrare il teorema di Brauer per i gruppi quasi-elementari.

Per un primo p, un gruppo G si dice *p-quasi-elementare* se contiene un sottogruppo ciclico normale Z tale che $p \nmid |Z|$ e G/Z sia un p-gruppo. Evidentemente, se G è p-elementare, è p-quasi-elementare. Un gruppo G si dice *quasi-elementare* se è p-quasi-elementare per qualche primo p.

Sia G p-quasi-elementare, con Z sottogruppo ciclico normale tale che $p \nmid |Z|$ e G/Z sia un p-gruppo. Ogni sottogruppo H di G è p-quasi-elementare. Infatti $H \cap Z$ è ciclico di ordine primo con p e $H/(H \cap Z) \cong HZ/Z$, un sottogruppo di G/Z. Quindi $H/(H \cap Z)$ è un p-gruppo. L'argomento mostra che, se $p \nmid |H|$, allora $|H/(H \cap Z)| = 1$ e pertanto $H \subset Z$. Ne segue che il sottogruppo Z specificato nella definizione di gruppo p-quasi-elementare è unico e, quindi, è un sottogruppo caratteristico di G (p. 109). Si può dare un'utile definizione alternativa: $G = AP$, dove A è ciclico e normale in G e P è un p-gruppo. Infatti, se così è, scriviamo $A = Z \times W$ con $p \nmid |Z|$ e $|W| = p^k$. Allora Z e W sono unici, dunque caratteristici in A e quindi normali in G. Evidentemente $G/Z \cong WP$, che è un p-gruppo. Viceversa, supponiamo che G sia p-quasi-elementare e che Z sia il sottogruppo della definizione. Sia P un p-sottogruppo di Sylow di G. Allora $P \cap Z = 1$ e $PZ = ZP$ è un sottogruppo tale che $|PZ| = |G|$. Dunque $G = ZP$, con

Z ciclico e normale in G e P un p-gruppo. Si vede subito che un gruppo p-quasi-elementare G è elementare se e solo se Z è contenuto nel centro e se e solo se un p-sottogruppo di Sylow è normale. Ne segue che ogni sottogruppo di un gruppo p-elementare è p-elementare.

La prima parte della dimostrazione del teorema di Brauer si basa sul seguente lemma.

Lemma 1 (B. Banaschewski). *Sia S un insieme finito non vuoto e sia R un sottoanello, non necessariamente unitario, di $\mathbb{Z}^S$ (un anello senza unità è detto* rng *in BAI, p. 155). Allora o R contiene 1_S (ed è quindi un sottoanello unitario), oppure esistono un $x \in S$ e un primo p tali che $f(x)$ è divisibile per p per ogni $f \in R$.*

Dimostrazione. Per $x \in S$ sia $I_x = \{f(x) \mid f \in R\}$. Questo è un sottogruppo del gruppo additivo di $\mathbb{Z}$. Dunque o $I_x = \mathbb{Z}$, oppure esiste un primo p tale che $p \mid f(x)$ per ogni $f \in R$. Se ciò accade per qualche x, abbiamo la seconda alternativa. Supponiamo ora che $I_x = \mathbb{Z}$ per ogni $x \in S$. Allora per ogni x possiamo scegliere $f_x \in R$ tale che $f_x(x) = 1$ e quindi $(f_x - 1_S)(x) = 0$. Ne segue che $\prod_{x \in S}(f_x - 1_S) = 0$. Sviluppando il prodotto si ottiene un'espressione per 1_S come polinomio nelle f_x a coefficienti interi. Dunque $1_S \in R$. □

Ci occorrerà anche il lemma seguente.

Lemma 2. *Per ogni $g \in G$ e ogni primo p esiste un sottogruppo p-quasi-elementare H di G tale che $\chi_{\sigma_1^G}(g)$ non è divisibile per p, dove σ_1 è la rappresentazione unità di H.*

Dimostrazione. Possiamo scrivere $\langle g \rangle = Z \times W$, con $p \nmid |Z|$ e $|W| = p^k$. Sia N il normalizzante di Z in G e sia $\bar{H}$ un p-sottogruppo di Sylow di $\bar{N} = N/Z$ contenente il p-gruppo $\langle g \rangle / Z$ (BAI, p. 81). Allora $\bar{H} = H/Z$, dove H è un sottogruppo di N che contiene $\langle g \rangle$. Poiché $Z \triangleleft H$, $p \nmid |Z|$ e $|H/Z|$ è una potenza di p, il gruppo H è p-quasi-elementare. Vogliamo mostrare che $\chi_{\sigma_1^G}(g)$ non è divisibile per p. Per la (86) ciò equivale a mostrare che il numero delle classi laterali aH tali che $g(aH) = aH$ non è divisibile per p. Se aH soddisfa questa condizione, si ha $a^{-1}ga \in H$ e quindi $a^{-1}Za \subset H$. Poiché H è p-quasi-elementare, Z è l'unico sottogruppo di H di ordine $|Z|$. Pertanto $a^{-1}Za = Z$ e $a \in N$. Dobbiamo dunque contare le classi laterali aH di H in N per cui $g(aH) = aH$. Consideriamo ora l'azione di $\langle g \rangle$ su N/H. Poiché $Z \triangleleft N$ e $Z \subset H$, si ha $z(aH) = aH$ per $z \in Z$ e $a \in N$. Dunque Z è contenuto nel nucleo dell'azione di $\langle g \rangle$ su N/H. Abbiamo pertanto l'azione di $\langle g \rangle / Z$ su N/H data da $(gZ)(aH) = gaH$. Poiché $|\langle g \rangle / Z| = p^k$, ogni orbita dell'azione di $\langle g \rangle / Z$, e quindi di $\langle g \rangle$, su N/H ha per cardinalità una potenza di p (BAI, p. 76). Ne segue che il numero delle classi laterali aH non fissate da g è divisibile per p. Pertanto il numero di quelle fisse soddisfa $\chi_{\sigma_1^G}(g) \equiv [N : H] \pmod{p}$. Siccome H contiene un p-sottogruppo di Sylow di N, l'indice $[N : H]$ non è divisibile per p. Nemmeno $\chi_{\sigma_1^G}(g)$ è quindi divisibile per p. □

Possiamo ora completare la prima parte della dimostrazione del teorema di Brauer dimostrando il teorema seguente.

Teorema 5.21. *Ogni carattere complesso di G è una combinazione lineare a coefficienti interi di caratteri indotti da sottogruppi quasi-elementari.*

Dimostrazione. Con le notazioni introdotte, se $\mathcal{Q}$ indica la famiglia dei sottogruppi quasi-elementari di G, questo significa che $\mathrm{ch}_{\mathcal{Q}}(G) = \mathrm{ch}(G)$. Poiché $\mathrm{ch}_{\mathcal{Q}}(G)$ è un ideale di $\mathrm{ch}(G)$, basta mostrare che $\chi_1 \in \mathrm{ch}_{\mathcal{Q}}(G)$. Sia R il sottoanello, inteso senza obbligo di unità, di $\mathrm{ch}_{\mathcal{Q}}(G)$ generato dai caratteri indotti σ_1^G dei caratteri unità σ_1 dei sottogruppi quasi-elementari di G. È chiaro che $\sigma_1^G \in \mathbb{Z}^G$, quindi $R \subset \mathbb{Z}^G$. Per il lemma di Banaschewski, se $\chi_1 \notin \mathrm{ch}_{\mathcal{Q}}(G)$, allora $\chi_1 \notin R$, e pertanto per qualche $g \in G$ esiste un primo p tale che $\chi(g) \equiv 0 \pmod{p}$ per ogni $\chi \in R$. Questo contraddice il lemma 2, che per ogni $g \in G$ e ogni primo p fornisce un $\chi \in R$ tale che $\chi(g)$ non è divisibile per p. Dunque $\mathrm{ch}_{\mathcal{Q}}(G) = \mathrm{ch}(G)$. □

Dimostriamo ora che ogni rappresentazione complessa irriducibile di un gruppo p-quasi-

elementare è monomiale e ha grado una potenza di p. In termini di caratteri il risultato si esprime nella forma seguente.

Teorema 5.22 (Blichfeldt–Brauer). *Sia χ un carattere irriducibile di un gruppo p-quasi-elementare G. Allora (1) il grado $\chi(1)$ è una potenza di p e (2) $\chi = \lambda^G$ per un carattere lineare λ di un sottogruppo di G.*

Dimostrazione. Si ha $G = ZP$, dove $Z \triangleleft G$, Z è ciclico con $p \nmid |Z|$ e P è un p-gruppo. Sia ρ una rappresentazione di G di carattere χ.

(1) Siano σ una componente irriducibile di ρ_Z e T il gruppo d'inerzia di σ. Allora $Z \triangleleft T$ e l'indice di T in G è una potenza di p. Per il corollario 4 al teorema 5.20, $\rho = \psi^G$ per una rappresentazione irriducibile ψ di T. Se $T \neq G$, il risultato segue dunque per induzione su $|G|$. Possiamo quindi supporre $T = G$. Poiché Z è abeliano, σ ha grado 1, e, poiché $Z \triangleleft G = T$ e ρ è irriducibile, dal teorema di Clifford segue che ogni $a \in Z$ agisce come uno scalare sullo spazio V su cui agisce ρ. Ciò implica evidentemente che ρ_P è irriducibile. Poiché P è un p-gruppo, il grado di ρ, che divide $|P|$, è una potenza di p.

(2) Sia $\chi(1) = p^n$ il grado. Procediamo per induzione su n. Per $n = 0$ il risultato è chiaro, poiché in tal caso χ è lineare. Supponiamo dunque $n > 0$. Se λ è un carattere lineare di G, allora $\chi\lambda$ è un carattere di grado $(\chi\lambda)(1) = \chi(1)$. Quindi o $\chi = \chi\lambda$, oppure χ non è una componente di $\chi\lambda$. La condizione $\chi = \chi\lambda$ equivale a $(\chi \mid \chi\lambda) = 1$ e, poiché

$$(\chi \mid \chi\lambda) = \frac{1}{|G|} \sum_g \overline{\chi(g)}\chi(g)\lambda(g) = (\chi\bar{\chi} \mid \lambda),$$

equivale anche a $(\chi\bar{\chi} \mid \lambda) = 1$. Ora $\chi\bar{\chi}$ è il carattere di $\rho \otimes \rho^*$ e $(\chi\bar{\chi} \mid \lambda) = 1$ equivale al fatto che λ abbia molteplicità 1 in $\chi\bar{\chi}$. Sia Λ l'insieme dei caratteri lineari λ di G tali che $\chi\lambda = \chi$. È chiaro che Λ è un gruppo rispetto alla moltiplicazione. Si ha

$$\chi\bar{\chi} = \sum_{\lambda \in \Lambda} \lambda + \sum \chi', \tag{99}$$

dove i χ' sono caratteri non lineari. Poiché $\chi(1)$ e i $\chi'(1)$ sono divisibili per p, mentre $\lambda(1) = 1$, dalla (99) segue che $|\Lambda| \equiv 0 \pmod{p}$. Esiste dunque un $\lambda_1 \in \Lambda$ tale che $\lambda_1 \neq \chi_1$ (il carattere unità) e $\lambda_1^p = \chi_1$. Poiché λ_1 è lineare, è un omomorfismo di G nel gruppo moltiplicativo dei numeri complessi e, poiché $\lambda_1^p = \chi_1$ e $\lambda_1 \neq \chi_1$, la sua immagine è il gruppo delle radici p-esime dell'unità. Dunque, posto $K = \ker \lambda_1$, si ha $K \triangleleft G$ e $[G : K] = p$. Per la (99),

$$\chi_K\bar{\chi}_K = \sum_{\lambda \in \Lambda} \lambda_K + \sum \chi'_K, \tag{100}$$

e $(\lambda_1)_K = (\chi_1)_K$. Ciò mostra che la molteplicità della rappresentazione unità in $\rho_K \otimes \rho_K^*$ è almeno due. Se $(\ \mid\ )_K$ denota il prodotto scalare su K, abbiamo quindi $(\chi_K\bar{\chi}_K \mid (\chi_1)_K)_K \geq 2$. Allora $(\chi_K \mid \chi_K)_K \geq 2$, il che implica che ρ_K è riducibile. Sia σ una componente irriducibile di ρ_K e sia ψ il carattere di σ. Poiché $\chi(1)$ e $\psi(1)$ sono potenze di p e $\psi(1) < \chi(1)$, si ha $\chi(1) \geq p\psi(1)$. Essendo σ una componente irriducibile di ρ_K, per la reciprocità di Frobenius ρ è una componente irriducibile di σ^G. Da $\psi^G(1) = p\psi(1)$ e $\chi(1) \geq p\psi(1)$ segue che $\chi = \psi^G$. Il risultato segue ora per induzione. □

Passiamo ora dai gruppi quasi-elementari ai gruppi elementari. Come prima, sia $G = ZP$, dove Z è un sottogruppo ciclico normale di G di ordine primo con p e P è un p-gruppo. Siano $W = C_Z(P) = Z \cap C_G(P)$, $H = WP$. Allora H è un sottogruppo p-elementare di G e P è un suo p-sottogruppo di Sylow normale. Ci occorre il seguente lemma.

Lemma. *Sia λ un carattere lineare di G tale che $H \subset \ker \lambda$. Allora $\lambda = \chi_1$, il carattere unità di G.*

Dimostrazione. Basta mostrare che $Z \subset \ker\lambda$. Sia $K = Z \cap \ker\lambda$. Siano $b \in Z$, $d \in P$. Allora $\lambda(b^{-1}dbd^{-1}) = 1$, poiché λ è un omomorfismo. Quindi $d(bK)d^{-1} = bK$, e ogni classe laterale bK di K in Z è stabilizzata dai coniugi mediante gli elementi di P. Abbiamo così un'azione di P per coniugio sulla classe laterale bK. Poiché $|P|$ è una potenza di p e $|bK| = |K|$ è primo con p, questa azione ha un punto fisso. Dunque $bK \cap C_Z(P) \neq \varnothing$, il che implica $\lambda(b) = 1$. Poiché b era arbitrario in Z, si ha $Z \subset \ker\lambda$. □

Possiamo ora dimostrare il risultato seguente.

Teorema 5.23. *Ogni carattere irriducibile di un gruppo quasi-elementare è una combinazione lineare a coefficienti interi di caratteri indotti da caratteri lineari di sottogruppi elementari.*

Dimostrazione. Sia χ un carattere complesso irriducibile di un gruppo p-quasi-elementare G. Se $\chi(1) > 1$, il risultato segue dal teorema 5.22 per induzione su $|G|$. Supponiamo dunque $\chi(1) = 1$, cioè χ lineare. Sia H il sottogruppo p-elementare WP definito sopra e sia $\eta = \chi_H$. Per il teorema di reciprocità di Frobenius la molteplicità di χ in η^G è 1. Sia ora χ' una componente lineare di η^G. Ancora per la reciprocità di Frobenius, η è un costituente di χ'_H. Dunque $\chi'_H = \eta = \chi_H$. Allora $\chi'' = \chi'\chi^{-1}$ è un carattere lineare su G tale che $H \subset \ker\chi''$. Per il lemma, χ'' è il carattere unità su G. Quindi $\chi' = \chi$. Si ha pertanto $\eta^G = \chi + \theta$, dove θ è somma di caratteri di grado maggiore di 1. Poiché per induzione su $|G|$ si sa che θ è una combinazione lineare a coefficienti interi di caratteri indotti da caratteri lineari di sottogruppi elementari, e poiché η è lineare sul sottogruppo elementare H, il risultato cercato segue per $\chi = \eta^G - \theta$. □

Evidentemente il teorema di Brauer è una conseguenza immediata dei teoremi 5.22 e 5.23 e della transitività dell'induzione.

Ne ricaveremo ora una conseguenza importante, una caratterizzazione dei caratteri generalizzati fra le funzioni di classe. Sia $\mathrm{cf}(G)$ l'insieme delle funzioni di classe complesse su G. Evidentemente $\mathrm{cf}(G)$ è un sottoanello di $\mathbb{C}^G$ che contiene $\mathrm{ch}(G)$. Sappiamo inoltre che $\mathrm{cf}(G)$ è lo spazio vettoriale complesso generato dai caratteri irriducibili $\chi_1, \ldots, \chi_s$, e mediante la (96) abbiamo definito ψ^G per una funzione di classe su un sottogruppo H. Poiché le applicazioni $\chi \mapsto \chi_H$ e $\psi \mapsto \psi^G$ sono lineari, è chiaro che la formula (97), $\psi^G\chi = (\psi\chi_H)^G$, vale anche per le funzioni di classe. Possiamo servircene per stabilire il risultato seguente.

Caratterizzazione di Brauer dei caratteri generalizzati. *Una funzione di classe φ su G è un carattere generalizzato se e solo se φ_H è un carattere generalizzato per ogni sottogruppo elementare H di G.*

Dimostrazione. Sia $\mathrm{ch}(G)'$ l'insieme delle funzioni di classe φ su G che soddisfano la condizione enunciata. È chiaro che $\mathrm{ch}(G)'$ è un sottoanello di $\mathrm{cf}(G)$ contenente $\mathrm{ch}(G)$. Sia ora ψ un carattere su un sottogruppo elementare H di G e sia $\chi \in \mathrm{ch}(G)'$. Allora $\chi_H \in \mathrm{ch}(H)$, sicché $\psi\chi_H \in \mathrm{ch}(H)$ e $(\psi\chi_H)^G \in \mathrm{ch}(G)$. Quindi $\psi^G\chi = (\psi\chi_H)^G \in \mathrm{ch}(G)$. Poiché ogni elemento di $\mathrm{ch}(G)$ è una combinazione lineare a coefficienti interi di caratteri della forma ψ^G, dove ψ è un carattere su un sottogruppo elementare, ciò implica che $\mathrm{ch}(G)$ è un ideale di $\mathrm{ch}(G)'$. Siccome $\chi_1 \in \mathrm{ch}(G)$, abbiamo $\mathrm{ch}(G)' = \mathrm{ch}(G)$, che equivale all'enunciato del criterio. □

Osserviamo che la caratterizzazione di Brauer fornisce anche una caratterizzazione dei caratteri irriducibili, poiché un $\chi \in \mathrm{ch}(G)$ è un carattere irriducibile se e solo se $(\chi \mid \chi) = 1$ e $\chi(1) > 0$. Infatti $\chi \in \mathrm{ch}(G)$ se e solo se $\chi = \sum_i n_i\chi_i$, $n_i \in \mathbb{Z}$, e $(\chi \mid \chi) = \sum_i n_i^2 = 1$ implica che tutti gli n_i sono nulli tranne uno, che vale ± 1. La condizione $\chi(1) > 0$ dà allora $\chi = \chi_j$ per qualche j.

Esercizi

1. Un gruppo G si dice un *M-gruppo* se ogni sua rappresentazione complessa irriducibile è monomiale. Si osservi che il teorema 5.22.2 afferma che ogni gruppo quasi-elementare è un M-gruppo. Dimostrare che il prodotto diretto di M-gruppi è un M-gruppo. Dimostrare che ogni gruppo nilpotente è un M-gruppo (si veda BAI, pp. 250–251, esercizi 4–11).

2. (Taketa.) Dimostrare che ogni M-gruppo è risolubile. (Traccia della dimostrazione. Se il risultato è falso, esiste un controesempio minimale, cioè un M-gruppo non risolubile G di ordine minimo. Poiché ogni immagine omomorfa di un M-gruppo è un M-gruppo, se $A \triangleleft G$ e $A \neq G$, allora G/A è risolubile. Siano A e B sottogruppi normali minimali di G. Se $A \neq B$, si ha $A \cap B = 1$ e G è isomorfo a un sottogruppo di $G/A \times G/B$, perciò è risolubile per la minimalità di G. Quindi $A = B$ ed esiste un unico sottogruppo normale minimale A di G. Esistono rappresentazioni irriducibili ρ di G tali che $\ker \rho \not\supset A$. Sia ρ una di grado minimo e sia $\rho = \sigma^G$, dove σ è una rappresentazione di grado 1 di un sottogruppo H. Si ponga $\rho' = \sigma_1^G$, dove σ_1 è la rappresentazione unità di H. Dimostrare che $\ker \rho'$ è un sottogruppo normale abeliano di G diverso da 1. Allora G è risolubile, contro l'ipotesi.)

Gli esercizi seguenti delineano una dimostrazione di un importante teorema sui caratteri indotti dovuto ad Artin.

Teorema 5.24. *Sia χ un carattere complesso di G a valori razionali (cioè $\chi(g) \in \mathbb{Q}$ per ogni $g \in G$). Allora*

$$\chi = \sum_Z \frac{a_Z}{[N(Z) : Z]} (\chi_{1Z})^G, \tag{101}$$

dove χ_1 è il carattere unità, gli a_Z appartengono a $\mathbb{Z}$ e la somma è estesa ai sottogruppi ciclici Z di G.

3. Sia χ un carattere a valori razionali su G e siano $g, h \in G$ tali che $\langle g \rangle = \langle h \rangle$. Dimostrare che $\chi(g) = \chi(h)$. (Suggerimento. Se $|\langle g \rangle| = m$, allora $h = g^k$ con $(k, m) = 1$. Sia $\Lambda^{(m)}$ il campo ciclotomico delle radici m-esime dell'unità su $\mathbb{Q}$, sicché $\Lambda^{(m)} = \mathbb{Q}(\varepsilon)$, dove ε è una radice primitiva m-esima dell'unità. Dimostrare che esiste un automorfismo σ di $\Lambda^{(m)}/\mathbb{Q}$ tale che $\sigma\varepsilon = \varepsilon^k$ e che, se $g \mapsto \operatorname{diag}\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\}$, con $\varepsilon_i \in \Lambda^{(m)}$, è una rappresentazione matriciale, allora $h = g^k \mapsto \operatorname{diag}\{\sigma\varepsilon_1, \sigma\varepsilon_2, \ldots, \sigma\varepsilon_n\}$. Concludere che $\chi(g) = \chi(h)$.)

4. Sia χ come nell'esercizio 3. Si definisca in G una relazione di equivalenza $\equiv$ ponendo $g \equiv h$ se $\langle g \rangle$ e $\langle h \rangle$ sono coniugati in G (cioè $\langle g \rangle = a\langle h \rangle a^{-1}$ per qualche $a \in G$). Siano $D_1, D_2, \ldots, D_t$ le distinte classi di equivalenza determinate da $\equiv$. Si osservi che esse sono unioni di classi di coniugio e si può supporre $D_1 = \{1\}$. Sia $g_i \in D_i$, sia $|\langle g_i \rangle| = n_i$ e sia $N(\langle g_i \rangle)$ il normalizzante di $\langle g_i \rangle$. Dimostrare che

   $$|D_i| = [G : N(\langle g_i \rangle)]\varphi(n_i), \tag{102}$$

   dove φ è la funzione φ di Eulero. Sia Φ_i la funzione caratteristica di D_i, cioè $\Phi_i(g) = 1$ se $g \in D_i$ e $\Phi_i(g) = 0$ altrimenti. Dimostrare per induzione su n_i che

   $$|N(\langle g_i \rangle)|\Phi_i = \sum_j a_j n_j (\chi_{1\langle g_j \rangle})^G, \tag{103}$$

   con $a_j \in \mathbb{Z}$, dove $a_j = 0$ a meno che $\langle g_j \rangle$ sia coniugato a un sottogruppo di $\langle g_i \rangle$.

5. Osservare che χ è una combinazione lineare a coefficienti interi delle funzioni Φ_i. Servirsi di questo fatto e della (103) per dimostrare il teorema di Artin.

5.13 Il teorema di Brauer sui campi di spezzamento

In questo paragrafo dimostreremo che, se m è l'esponente di un gruppo finito G, ossia il minimo comune multiplo degli ordini dei suoi elementi, allora il campo ciclotomico $\Lambda^{(m)}$ delle radici m-esime dell'unità su $\mathbb{Q}$ è un campo di spezzamento per G. Maschke congetturò questo risultato intorno al 1900. Solo nel 1945 Brauer ne diede una dimostrazione in piena generalità, basata sulla sua teoria delle rappresentazioni modulari. In seguito Brauer scoprì il suo teorema sui caratteri indotti e osservò che il teorema sul campo di spezzamento ne è una facile conseguenza. È questa la via che seguiremo.

Ricordiamo che una rappresentazione ρ di G su V/F si dice assolutamente irriducibile se la rappresentazione estesa ρ_K è irriducibile per ogni campo K/F (p. 263). Il campo F è un campo di spezzamento per G se ogni rappresentazione irriducibile di G su F è assolutamente irriducibile. Abbiamo dimostrato (teorema 5.8, p. 264) che F è un campo di spezzamento per G se e soltanto se $F[G]$ è somma diretta di algebre di matrici $M_n(F)$.

Supponiamo ora che F sia un sottocampo di $\mathbb{C}$. Possiamo allora dare una definizione alternativa, più intuitiva, di campo di spezzamento. Infatti, come mostreremo, F è un campo di spezzamento per G se e soltanto se per ogni rappresentazione ρ su uno spazio vettoriale $V/\mathbb{C}$ esiste una base di V tale che le matrici della corrispondente rappresentazione matriciale abbiano tutti gli elementi in F. Per la completa riducibilità delle rappresentazioni, questa condizione vale se e soltanto se vale per le rappresentazioni irriducibili. È chiaro inoltre che la condizione si può formulare interamente in termini di matrici: ogni rappresentazione matriciale complessa è simile a una rappresentazione matriciale su F. Supponiamo ora che F sia un campo di spezzamento. Allora

$$F[G] = M_{n_1}(F) \oplus \cdots \oplus M_{n_s}(F),$$
$$\mathbb{C}[G] = F[G]_{\mathbb{C}} = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_s}(\mathbb{C}).$$

Se I_j è un ideale sinistro minimale di $M_{n_j}(F)$, esso è un modulo irriducibile per $F[G]$ e $\{I_j \mid 1 \leq j \leq s\}$ è un sistema di rappresentanti dei $F[G]$-moduli irriducibili. Il grado della rappresentazione fornita da I_j è n_j, e $|G| = \sum_j n_j^2$. Ora $I_{j\mathbb{C}}$ è un ideale sinistro contenuto nella componente semplice $M_{n_j}(\mathbb{C})$. Poiché $[I_{j\mathbb{C}} : \mathbb{C}] = n_j$, esso è un ideale sinistro minimale di $M_{n_j}(\mathbb{C})$, e quindi gli $I_{j\mathbb{C}}$, $1 \leq j \leq s$, costituiscono un sistema di rappresentanti dei moduli irriducibili per $\mathbb{C}[G]$. Poiché ogni base di I_j/F è una base di $I_{j\mathbb{C}}/\mathbb{C}$, è chiaro che le rappresentazioni matriciali complesse irriducibili sono simili a rappresentazioni matriciali su F. Viceversa, supponiamo che questa condizione valga per un campo F. Allora ogni rappresentazione complessa irriducibile ha la forma $\sigma_{\mathbb{C}}$, dove σ è una rappresentazione di G su F. Sia $\rho_1, \ldots, \rho_s$ un sistema di rappresentanti delle rappresentazioni irriducibili complesse di G, sia n_j il grado di ρ_j e scegliamo una rappresentazione σ_j di G su F tale che $\sigma_{j\mathbb{C}} = \rho_j$. Allora le σ_j sono irriducibili e a due a due non equivalenti. Dalla relazione $|G| = \sum_j n_j^2$ segue che $F[G] = M_{n_1}(F) \oplus \cdots \oplus M_{n_s}(F)$ (si veda p. 259). Dunque F è un campo di spezzamento per G.

Siano χ e χ' i caratteri di rappresentazioni irriducibili non equivalenti ρ e ρ' di G su F. Se $F[G] = M_{m_1}(\Delta_1) \oplus \cdots \oplus M_{m_r}(\Delta_r)$, dove le Δ_i sono algebre di divisione, possiamo supporre che ρ agisca su un ideale sinistro minimale $I \subset M_{m_1}(\Delta_1)$ e che ρ' agisca su un ideale sinistro minimale I' di $M_{m_2}(\Delta_2)$. Passando a $\mathbb{C}[G] = F[G]_{\mathbb{C}}$, le algebre $M_{m_1}(\Delta_1)_{\mathbb{C}}$ e $M_{m_2}(\Delta_2)_{\mathbb{C}}$ si decompongono in somme dirette di componenti semplici di $\mathbb{C}[G]$, e questi ideali di $\mathbb{C}[G]$ non hanno componenti semplici in comune. Ne segue che, se $\chi_1, \chi_2, \ldots, \chi_s$ sono i caratteri complessi irriducibili, si ha $\chi = \sum_i m_i \chi_i$ e $\chi' = \sum_i m'_i \chi_i$, dove gli m_i e gli m'_i sono interi non negativi e per ogni i si ha $m_i = 0$ oppure $m'_i = 0$. Dunque $(\chi \mid \chi) = \sum_i m_i^2 > 0$ e $(\chi \mid \chi') = 0$. Inoltre χ è un carattere complesso irriducibile se e soltanto se $(\chi \mid \chi) = 1$, nel qual caso la rappresentazione complessa irriducibile di carattere χ è l'estensione $\rho_{\mathbb{C}}$. È anche chiaro che F è un campo di spezzamento per G se e soltanto se per ogni carattere complesso irriducibile χ_i esiste una rappresentazione ρ_i

di G su F tale che $\chi_{\rho_i} = \chi_i$.

Possiamo ora dimostrare il seguente teorema.

Teorema 5.25. *Se m è l'esponente di G, il campo ciclotomico $\Lambda^{(m)}/\mathbb{Q}$ delle radici m-esime dell'unità è un campo di spezzamento per G.*

Dimostrazione. Sia χ un carattere complesso irriducibile di G. Per il teorema di Brauer sui caratteri indotti, χ è una combinazione lineare a coefficienti interi di caratteri della forma λ^G, dove λ è un carattere lineare di un sottogruppo H di G. Ora λ è un omomorfismo di H nel gruppo moltiplicativo $\mathbb{C}^*$ dei numeri complessi e, se $h \in H$, si ha $h^m = 1$, quindi $\lambda(h)^m = 1$. Pertanto $\lambda(h) \in \Lambda^{(m)}$. Dalla definizione di rappresentazione indotta è chiaro che la rappresentazione di carattere λ^G può essere espressa mediante matrici con elementi in $\Lambda^{(m)}$. Dunque λ^G è il carattere di una rappresentazione di G su $\Lambda^{(m)}$. Ne segue che $\chi = \sum_{j=1}^{r} k_j\varphi_j$, dove $k_j \in \mathbb{Z}$ e $\varphi_1, \ldots, \varphi_r$ sono i caratteri delle rappresentazioni irriducibili a due a due non equivalenti di G su $\Lambda^{(m)}$. Allora $1 = (\chi \mid \chi) = \sum_j k_j^2(\varphi_j \mid \varphi_j)$ e, poiché ogni $(\varphi_j \mid \varphi_j)$ è un intero positivo, tutti i k_j tranne uno sono nulli e l'unico non nullo è 1. Dunque χ è il carattere di una rappresentazione irriducibile di G su $\Lambda^{(m)}$. Ciò implica che $\Lambda^{(m)}$ è un campo di spezzamento. □

5.14 L'indice di Schur

In questo paragrafo studieremo le relazioni fra le rappresentazioni irriducibili di un gruppo finito G su $\mathbb{C}$ e quelle su un sottocampo F di $\mathbb{C}$. Usiamo le notazioni del paragrafo precedente:

$$\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_s}(\mathbb{C}),$$
$$F[G] = M_{m_1}(\Delta_1) \oplus \cdots \oplus M_{m_r}(\Delta_r),$$

dove le Δ_i sono algebre di divisione. Scriviamo inoltre $A_i = M_{m_i}(\Delta_i)$.

Sia χ un carattere complesso irriducibile di G e sia ρ una rappresentazione di G su $\mathbb{C}$ avente carattere χ. Possiamo supporre che ρ sia la restrizione della rappresentazione regolare di G a un ideale sinistro minimale V di una delle componenti semplici $M_{n_j}(\mathbb{C})$. Allora V è contenuto in uno e uno solo degli $A_{i\mathbb{C}}$. Se $V \subset A_{i\mathbb{C}}$, allora $A_iV \neq 0$, ma $A_{i'}V = 0$ per ogni $i' \neq i$. Questa proprietà è indipendente dalla scelta della rappresentazione ρ di carattere χ. Diremo che A_i è la componente semplice di $F[G]$ *corrispondente a* χ. A χ possiamo associare anche un sottocampo di $\mathbb{C}/F$, precisamente il sottocampo generato su F dai numeri complessi $\chi(g)$, $g \in G$. Lo denotiamo con $F(\chi)$. Vale la seguente proposizione.

Proposizione 5.9. *Sia χ un carattere complesso irriducibile del gruppo finito G, sia F un sottocampo di $\mathbb{C}$ e sia $A = A_i$ la componente semplice di $F[G]$ corrispondente a χ. Allora $F(\chi)$ è isomorfo su F al centro di A.*

Dimostrazione. Come abbiamo indicato, possiamo prendere come rappresentazione ρ di carattere χ la restrizione della rappresentazione regolare a un ideale sinistro minimale $V \subset A_{\mathbb{C}}$. Possiamo considerare ρ come una rappresentazione di $\mathbb{C}[G]$ e identificare $F[G]$ con una F-sottoalgebra di $\mathbb{C}[G]$. Poiché ρ è irriducibile, dal lemma di Schur segue $\rho(\operatorname{cent}\mathbb{C}[G]) = \mathbb{C}1$. Ricordiamo che i centri di $F[G]$ e di $\mathbb{C}[G]$ sono generati come spazi vettoriali dagli elementi $\sum_{g\in C_i} g$, dove $C_1, \ldots, C_s$ sono le classi di coniugio di G. Se $g \in C_i$, allora $\sum_{a\in G} aga^{-1}$ è un multiplo non nullo di $\sum_{g\in C_i} g$. I centri sono quindi generati dagli elementi $c_g = \sum_{a\in G} aga^{-1}$. Si ha $\rho(c_g) = \gamma 1$, con $\gamma \in \mathbb{C}$, e quindi $\operatorname{tr}\rho(c_g) = n\gamma$, dove $n = \chi(1)$ è il grado di ρ. D'altra parte, $\operatorname{tr}\rho(c_g) = \sum_{a\in G} \operatorname{tr}\rho(aga^{-1}) = |G|\chi(g)$. Pertanto

$$\rho(c_g) = \frac{|G|}{n}\chi(g)1. \tag{104}$$

Restringiamo ora a $F[G]$ l'omomorfismo di $\mathbb{C}$-algebre ρ definito su $\mathbb{C}[G]$. Otteniamo così un omomorfismo di F-algebre definito su $F[G]$, che manda $\operatorname{cent} F[G]$ sull'insieme delle combinazioni

F-lineari degli elementi $\chi(g)1$. Poiché ρ manda in zero ogni componente semplice $A_i \neq A$, otteniamo un omomorfismo di cent A su $F(\chi)1$. Essendo cent A un campo, abbiamo un isomorfismo di cent A su $F(\chi)$. □

Diremo ora che un carattere complesso χ di G è *realizzabile sul sottocampo* F di $\mathbb{C}$ se χ è il carattere di una rappresentazione σ di G su F. Poiché il carattere determina la rappresentazione a meno di equivalenza, è chiaro che χ è realizzabile su F se e soltanto se ogni rappresentazione ρ di carattere χ è equivalente a $\sigma_{\mathbb{C}}$ per una tale σ. Inoltre, come abbiamo già osservato, ciò avviene se e soltanto se esiste una base dello spazio V su cui agisce ρ tale che tutti gli elementi delle matrici delle $\rho(g)$, $g \in G$, appartengano a F. Evidentemente, se χ è realizzabile su F, allora F contiene tutti i $\chi(g)$, $g \in G$.

Mostreremo ora che, se χ è un carattere complesso irriducibile di G e F è un sottocampo di $\mathbb{C}$ contenente tutti i $\chi(g)$, allora esiste un intero positivo d tale che il carattere $d\chi$ (della somma diretta di d copie della rappresentazione ρ di carattere χ) è realizzabile su F. Il minimo di tali d si chiama *indice di Schur di* χ *su* F. Il teorema seguente dimostra l'esistenza dell'indice di Schur e dà una descrizione strutturale di questo intero.

Teorema 5.26. *Sia χ un carattere complesso irriducibile di G, sia F un sottocampo di $\mathbb{C}$ contenente tutti i $\chi(g)$, $g \in G$, e sia $A = M_m(\Delta)$, dove Δ è un'algebra di divisione, la componente semplice di $F[G]$ corrispondente a χ. Allora $[\Delta : F] = d^2$ e il carattere $d\chi$ è realizzabile su F. Inoltre, se d' è un qualsiasi intero positivo tale che $d'\chi$ sia realizzabile su F, allora $d \mid d'$, e quindi d è l'indice di Schur di χ su F.*

Dimostrazione. Poiché $F = F(\chi)$, per la proposizione 5.9 l'algebra A è centrale semplice. Quindi Δ è centrale, $[\Delta : F] = d^2$ (p. 222) e $[A : F] = m^2d^2$. Due ideali sinistri minimali qualsiasi di A sono isomorfi come A-moduli e pertanto come spazi vettoriali su F. Inoltre $A = I_1 \oplus \cdots \oplus I_m$, dove ciascun I_j, $1 \leq j \leq m$, è un ideale sinistro minimale. Per un tale ideale I si ha quindi $[I : F] = md^2$ e $[I_{\mathbb{C}} : \mathbb{C}] = md^2$. Poiché A è centrale semplice, $A_{\mathbb{C}}$ è semplice ed è dunque una delle componenti semplici di $\mathbb{C}[G]$. Poiché $[A_{\mathbb{C}} : \mathbb{C}] = m^2d^2$, si ha $A_{\mathbb{C}} = M_{md}(\mathbb{C})$, e il calcolo fatto per F mostra che, se V è un ideale sinistro minimale di $A_{\mathbb{C}}$, allora $[V : \mathbb{C}] = md$. Abbiamo visto che come rappresentazione ρ di carattere χ si può prendere la restrizione della rappresentazione regolare a un ideale sinistro minimale contenuto in $A_{\mathbb{C}}$. Possiamo prendere come tale ideale V. Ora $I_{\mathbb{C}}$ è un ideale sinistro di $A_{\mathbb{C}}$ e $[I_{\mathbb{C}} : \mathbb{C}] = md^2$, mentre $[V : \mathbb{C}] = md$. Dunque $I_{\mathbb{C}}$ è somma diretta di d ideali sinistri isomorfi a V. Ciò implica che la somma diretta di d rappresentazioni complesse irriducibili equivalenti a ρ è equivalente a $\tau_{\mathbb{C}}$, dove τ è la rappresentazione di G su I/F. Pertanto $d\chi$ è realizzabile su F. Supponiamo ora che d' sia un intero positivo tale che $d'\chi$ sia realizzabile su F. Il $\mathbb{C}[G]$-modulo $V^{(d')}$, somma diretta di d' copie di V, è allora isomorfo a un modulo $I'_{\mathbb{C}}$, dove I' è un modulo per $F[G]$. Ora $V^{(d')}$ è annullato da ogni componente semplice di $F[G]$ diversa da A, perciò anche I' è annullato da ogni componente semplice di $F[G]$ diversa da A. Ne segue che $I' \cong I^{(h)}$, dove I è un ideale sinistro minimale di A. Allora

$$V^{(d')} \cong I'_{\mathbb{C}} \cong (I_{\mathbb{C}})^{(h)} \cong \left(V^{(d)}\right)^{(h)} \cong V^{(dh)}.$$

Pertanto $d' = dh$. Ciò implica evidentemente che d è l'indice di Schur. □

Il risultato precedente mostra che l'indice di Schur di χ è 1 se e soltanto se $\Delta = F$ e $A = M_m(F)$. Quindi χ è realizzabile su $F = F(\chi)$ se e soltanto se $A = M_m(F)$.

Sia ora E un sottocampo di $\mathbb{C}$ contenente $F = F(\chi)$ e consideriamo $E[G]$. Poiché la componente semplice A di $F[G]$ corrispondente a χ è centrale semplice, A_E è una componente semplice di $E[G]$. È evidente che questa è la componente semplice di $E[G]$ corrispondente a χ. Dunque χ è realizzabile su E se e soltanto se $A_E \cong M_n(E)$, ossia se E è un campo di spezzamento su F per A (p. 220). Ciò avviene se e soltanto se E è un campo di spezzamento per l'algebra di divisione Δ tale che $A = M_m(\Delta)$. Il criterio fondamentale a questo riguardo è stato dato nel teorema 4.7

(p. 218). Secondo tale risultato, un'estensione di campi E/F di dimensione finita è un campo di spezzamento per un'algebra di divisione centrale Δ/F di dimensione finita se e soltanto se E è isomorfo a una sottoalgebra E' di un'algebra di matrici $M_r(\Delta)$ tale che il centralizzante di E' in $M_r(\Delta)$ sia E' stesso. In tal caso $[E : F] = rd$, dove $[\Delta : F] = d^2$. Questo risultato e il teorema 5.26 danno il seguente teorema.

Teorema 5.27. *Con le notazioni del teorema 5.26, sia E un'estensione di dimensione finita di F contenuta in $\mathbb{C}$. Allora χ è realizzabile su E se e soltanto se E è isomorfo a una sottoalgebra E' dell'algebra di matrici $M_r(\Delta)$ tale che $C_{M_r(\Delta)}(E') = E'$. Inoltre, in tal caso $[E : F] = rd$, dove d è l'indice di Schur di χ su F.*

5.15 Gruppi di Frobenius

Concluderemo il capitolo applicando la teoria dei caratteri alla dimostrazione di un importante teorema di Frobenius sui gruppi finiti. Il teorema si può interpretare in due modi, anzitutto come teorema sui gruppi transitivi di permutazioni e poi come teorema sui gruppi astratti. Come vedremo, esso è inoltre connesso allo studio degli automorfismi senza punti fissi dei gruppi finiti. Considereremo infine un gruppo di Frobenius i cui caratteri conducono a una variante di una dimostrazione classica della legge di reciprocità quadratica della teoria dei numeri.

Sia dapprima G un gruppo di permutazioni dell'insieme $N = \{1, 2, \ldots, n\}$, $n > 1$, con le seguenti proprietà:

1. G è transitivo.
2. Per ogni i, lo stabilizzatore $\operatorname{Stab} i = \{g \in G \mid gi = i\}$ è diverso da 1.
3. Nessun elemento di G, eccettuato 1, fissa più di un elemento di $\{1, \ldots, n\}$.

Poniamo $H_i = \operatorname{Stab} i$. Allora la condizione (3) equivale a $H_i \cap H_j = 1$ per $i \neq j$. Due qualunque dei sottogruppi H_i, H_j sono coniugati: $H_j = {}^gH_i = gH_ig^{-1}$. Esiste infatti un $g \in G$ tale che $gi = j$, e quindi $\operatorname{Stab} j = \operatorname{Stab}(gi) = g(\operatorname{Stab} i)g^{-1}$. È anche chiaro che, se $g \notin H_i$, allora $gi = j \neq i$ e ${}^gH_i = H_j \neq H_i$. Osserviamo inoltre che $H_i \neq G$, giacché $n \geq 2$.

Introduciamo la seguente definizione.

Definizione 5.4. Un gruppo finito G si dice *gruppo di Frobenius* se contiene un sottogruppo H tale che (i) $1 \neq H \neq G$ e (ii) per ogni $g \in G \setminus H$ si ha $H \cap {}^gH = 1$. Il sottogruppo H si chiama *complemento di Frobenius* in G.

Dalle osservazioni precedenti risulta che, se G è un gruppo di permutazioni che soddisfa le condizioni (1), (2) e (3) e $n \geq 2$, ciascuno dei sottogruppi $H = H_i$ soddisfa le condizioni della definizione 5.4. Dunque G è un gruppo di Frobenius e H ne è un complemento di Frobenius. Viceversa, supponiamo che G sia un gruppo di Frobenius con complemento H e consideriamo l'azione di G sull'insieme G/H delle classi laterali sinistre di H. Sappiamo che questa azione è transitiva. Inoltre $a(gH) = gH$ se e solo se $a \in {}^gH$, cosicché $\operatorname{Stab}(gH) = {}^gH$. Il nucleo dell'azione è pertanto $\bigcap_g {}^gH = 1$. Possiamo quindi identificare G con il corrispondente gruppo di permutazioni di G/H. È chiaro che vale (2). La condizione (3) equivale qui all'implicazione $aH \neq bH \Rightarrow {}^aH \neq {}^bH$, che segue dalla condizione (ii) della definizione di gruppo di Frobenius.

Il concetto di gruppo di Frobenius è dunque la versione astratta della situazione considerata inizialmente per i gruppi di permutazioni. Possiamo ora enunciare il seguente teorema.

Teorema di Frobenius. *Sia G un gruppo di Frobenius con complemento di Frobenius H.*

Poniamo

$$K = \{1\} \cup \left(G \setminus \bigcup_{g \in G} {}^{g}H \right). \tag{105}$$

Allora K è un sottogruppo normale di G, $G = KH$ e $K \cap H = 1$.

Dal punto di vista dei gruppi di permutazioni, K è l'unione di $\{1\}$ con l'insieme delle trasformazioni che non fissano alcun $i \in N$. Per la dimostrazione ci occorre il seguente lemma.

Lemma. *Sia G un gruppo di Frobenius con complemento di Frobenius H e sia φ una funzione di classe su H tale che $\varphi(1) = 0$. Allora $(\varphi^G)_H = \varphi$.*

Dimostrazione. Per definizione,

$$\varphi^G(g) = \frac{1}{|H|} \sum_{a \in G} \dot{\varphi}(aga^{-1}). \tag{106}$$

Si ha $\varphi^G(1) = 0$, poiché $\varphi(1) = 0$. Sia ora $h \in H$, $h \neq 1$, e sia $a \in G \setminus H$. Allora $aha^{-1} \notin H$ e $\dot{\varphi}(aha^{-1}) = 0$. Pertanto

$$\varphi^G(h) = \frac{1}{|H|} \sum_{a \in H} \dot{\varphi}(aha^{-1}) = \frac{1}{|H|} \sum_{a \in H} \varphi(aha^{-1}) = \varphi(h).$$

Dunque $(\varphi^G)_H = \varphi$. □

Dimostrazione del teorema di Frobenius. Osserviamo dapprima che, per la definizione di complemento di Frobenius, due coniugati distinti ${}^{g_1}H$ e ${}^{g_2}H$ hanno in comune solo l'elemento neutro e il normalizzatore è $N_G(H) = \{g \mid {}^{g}H = H\} = H$. Il numero dei coniugati è pertanto $[G : N_G(H)] = [G : H]$. Ne segue che $\left|\bigcup_{g \in G} {}^{g}H\right| = [G : H]|H| - [G : H] + 1$ e, per la (105),

$$|K| = [G : H]. \tag{107}$$

Sia ora ψ un carattere complesso irriducibile di H distinto dal carattere unitario ψ_1 e poniamo $\varphi = \psi - \psi(1)\psi_1$. Allora φ è un carattere generalizzato di H con $\varphi(1) = 0$. Per il lemma, φ^G è dunque un carattere generalizzato di G tale che $(\varphi^G)_H = \varphi$. Per la reciprocità di Frobenius,

$$\begin{aligned}(\varphi^G \mid \varphi^G)_G &= (\varphi \mid (\varphi^G)_H)_H = (\varphi \mid \varphi)_H = 1 + \psi(1)^2,\\ (\varphi^G \mid \chi_1)_G &= (\varphi \mid \psi_1)_H = -\psi(1),\end{aligned}$$

dove χ_1 è il carattere unitario di G. Poniamo $\psi^* = \varphi^G + \psi(1)\chi_1$. Allora ψ^* è un carattere generalizzato di G e

$$\begin{aligned}(\psi^* \mid \psi^*)_G &= (\varphi^G \mid \varphi^G)_G + 2\psi(1)(\varphi^G \mid \chi_1)_G + \psi(1)^2\\ &= 1 + \psi(1)^2 - 2\psi(1)^2 + \psi(1)^2 = 1.\end{aligned}$$

Inoltre

$$(\psi^*)_H = (\varphi^G)_H + \psi(1)(\chi_1)_H = \varphi + \psi(1)\psi_1 = \psi.$$

Poiché $(\psi^* \mid \psi^*)_G = 1$ e $\psi^*(1) = \psi(1) > 0$, il carattere generalizzato ψ^* è un carattere complesso irriducibile di G. Abbiamo così definito, per ogni carattere complesso irriducibile $\psi \neq \psi_1$ di H, un carattere complesso irriducibile ψ^* di G che estende ψ. Se ρ^* è una rappresentazione di G di carattere ψ^*, allora $\ker \psi^* = \{g \in G \mid \psi^*(g) = \psi^*(1)\} = \ker \rho^*$ (p. 271). Poniamo

$$K^* = \bigcap_{\psi} \ker \psi^*, \tag{108}$$

dove l'intersezione è presa su tutti i caratteri irriducibili $\psi \neq \psi_1$ di H. Evidentemente K^* è normale in G. Sia $k \neq 1$ in K. Allora $k \notin {}^gH$ per ogni $g \in G$ e $\varphi^G(k) = 0$ per la definizione (106). Quindi $\psi^*(k) = \psi^*(1)$, da cui $K \subseteq K^*$. Sia ora $h \in H \cap K^*$. Si ha $\psi(h) = \psi^*(h) = \psi^*(1) = \psi(1)$, per cui h appartiene al nucleo di ogni carattere irriducibile di H. Per la rappresentazione regolare ρ di H si ha dunque $\rho(h) = 1$, e quindi $h = 1$. Abbiamo ottenuto

$$K^* \triangleleft G, \quad K \subseteq K^*, \quad H \cap K^* = 1, \quad |G| = |H|[G : H] = |H||K|.$$

Pertanto HK^* è un sottogruppo di G e $HK^*/K^* \cong H/(H \cap K^*)$. Ne segue che $|HK^*| = |H||K^*|/|H \cap K^*| = |H||K^*|$ divide $|G| = |H||K|$. Dunque $|K^*|$ divide $|K|$ e, poiché $K^* \supseteq K$, si ha $K = K^*$. Ora $K = K^* \triangleleft G$, $H \cap K = 1$ e $|K| = [G : H]$. Allora $|KH| = |K||H| = |G|$ e quindi $G = KH$. La dimostrazione è conclusa. □

Il sottogruppo K si chiama *nucleo di Frobenius* del gruppo di Frobenius G di complemento H. Osserviamo che non si conosce una dimostrazione del teorema di Frobenius che non faccia uso dei caratteri.

Sia ora A un gruppo di automorfismi di un gruppo finito G. Diremo che A è *senza punti fissi* se nessun $\alpha \neq 1$ in A fissa alcun $g \neq 1$ di G. Metteremo in relazione lo studio delle coppie (G, A), dove G è un gruppo finito e $A \neq 1$ è un gruppo di automorfismi senza punti fissi di G, con lo studio dei gruppi di Frobenius. Ricordiamo che l'*olomorfo* $\operatorname{Hol} G$ di un gruppo G è il gruppo di trasformazioni $G_L \operatorname{Aut} G$, dove G_L è l'insieme delle moltiplicazioni a sinistra $g_L \colon x \mapsto gx$ (BAI, p. 63). Se $\alpha \in \operatorname{Aut} G$, allora $\alpha g_L = (\alpha g)_L \alpha$. Pertanto, per $g_i \in G$ e $\alpha_i \in \operatorname{Aut} G$, si ha

$$(g_{1L}\alpha_1)(g_{2L}\alpha_2) = (g_1\alpha_1(g_2))_L\alpha_1\alpha_2.$$

Sia $\operatorname{Aut} G$ sia G_L sono sottogruppi di $\operatorname{Hol} G$, G_L è normale, $G_L \cap \operatorname{Aut} G = 1$ e $\operatorname{Hol} G = G_L \operatorname{Aut} G$. È chiaro che, se A è un sottogruppo di $\operatorname{Aut} G$, allora $G_L A$ è un sottogruppo dell'olomorfo. Supponiamo che $A \neq 1$ e che A sia senza punti fissi. Per $g \neq 1$ in G,

$${}^{g_L}A = \{(g\alpha(g)^{-1})_L\alpha \mid \alpha \in A\}.$$

Pertanto ${}^{g_L}A \cap A = 1$ e ${}^{u}A \cap A = 1$ per ogni $u \in G_L A \setminus A$. Dunque $G_L A$ è un gruppo di Frobenius con complemento A. È anche chiaro che G_L ne è il nucleo di Frobenius.

Viceversa, sia G un gruppo di Frobenius con complemento H e nucleo K. Il gruppo H agisce su K per coniugio e queste applicazioni sono automorfismi di K. Supponiamo che $h \in H$, $k \in K$ e ${}^hk = k$. Allora $kh = hk$ e ${}^kh = h \in H$. Ne segue che $h = 1$ oppure $k = 1$. Ciò implica che l'omomorfismo di H in $\operatorname{Aut} K$ che associa a h l'applicazione $x \mapsto hxh^{-1}$ è un monomorfismo. Possiamo quindi identificare H con un sottogruppo di $\operatorname{Aut} K$, e questo gruppo di automorfismi è senza punti fissi.

Un risultato a lungo congetturato e dimostrato da Thompson afferma che il nucleo di Frobenius di un gruppo di Frobenius è nilpotente. Le considerazioni precedenti mostrano che ciò equivale al fatto seguente: un gruppo finito che ammette un gruppo non banale di automorfismi senza punti fissi è nilpotente. Per la dimostrazione si veda p. 138 di *Characters of Finite Groups* di W. Feit (si veda la bibliografia).

Esempio. Sia B il sottogruppo di $GSL_2(F)$, con $F = \mathbb{Z}/(p)$ e p primo dispari, costituito dalle matrici della forma

$$\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}. \tag{109}$$

Si ha evidentemente $|B| = p(p-1)$. Il gruppo B contiene i sottogruppi K e D, dove K è l'insieme delle matrici (109) con $a = 1$ e D è l'insieme delle matrici diagonali. Abbiamo $K \triangleleft B$, $B = DK$, $D \cap K = 1$. Inoltre

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-2}b & 1 \end{pmatrix} \tag{110}$$

e

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ ab - a^{-1}b & a^{-1} \end{pmatrix}. \tag{111}$$

Poniamo $G = B/\{1, -1\}$ e indichiamo con $\overline{A}$ l'immagine in G di un sottoinsieme A di B mediante l'omomorfismo canonico di B su G. Possiamo identificare $\overline{K}$ con K. Poiché, per $b \neq 0$, la matrice (111) appartiene a D se e solo se $a = \pm 1$, ne segue che G è un gruppo di Frobenius con complemento $\overline{D}$ e nucleo K.[17]

Vogliamo ottenere la tavola dei caratteri di G. Sia v un generatore del gruppo moltiplicativo ciclico F^* del campo F. Gli elementi di $\overline{D}$ sono allora $\overline{\mathrm{diag}\{v^i, v^{-i}\}}$, con $1 \leq i \leq (p-1)/2$. Due elementi di un complemento in un gruppo di Frobenius sono coniugati nel gruppo se e solo se lo sono nel complemento. Pertanto i $(p-1)/2$ elementi di $\overline{D}$ determinano altrettante classi di coniugio distinte. La classe di $\overline{1}$ ha un solo elemento, mentre quelle degli elementi $\overline{\mathrm{diag}\{v^i, v^{-i}\}}$, $1 \leq i \leq (p-3)/2$, hanno cardinalità p. Dalle formule (110) e (111) si ricavano altre due classi di coniugio, rappresentate da

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$$

(poiché v non è un quadrato in F^*). Ognuna di queste classi contiene $(p-1)/2$ elementi. In tutto abbiamo $(p-1)/2+2 = (p+3)/2$ classi di coniugio e quindi altrettanti caratteri complessi irriducibili.

Poiché $\overline{D}$ è ciclico di ordine $(p-1)/2$, esso ha $(p-1)/2$ caratteri lineari. Mediante l'omomorfismo di G su $G/K \cong \overline{D}$ otteniamo $(p-1)/2$ caratteri lineari di G, che danno la tavola seguente, dove $1 \leq i \leq (p-3)/2$ e $\omega = e^{4\pi \mathrm{i}/(p-1)}$:

	1	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$	$\overline{\begin{pmatrix} v^i & 0 \\ 0 & v^{-i} \end{pmatrix}}$
χ_1	1	1	1	1
χ_2	1	1	1	ω^i
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\chi_{(p-1)/2}$	1	1	1	$\omega^{(p-3)i/2}$

Poiché la classe di $\overline{\mathrm{diag}\{v^i, v^{-i}\}}$ ha cardinalità p, dalla relazione di ortogonalità (60) segue che le restanti voci delle colonne corrispondenti a queste classi sono nulle.

Il sottogruppo K di G è ciclico, generato da $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Abbiamo quindi un omomorfismo σ di K in $\mathbb{C}^*$ che manda il generatore nella radice primitiva p-esima dell'unità $\zeta = e^{2\pi \mathrm{i}/p}$. Esso definisce la rappresentazione $\rho = \sigma^G$ di G. Per la (110),

$$\sigma\left(\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\right) = \zeta^{a^{-2}},$$

[17] Per $p = 3$ il complemento $\overline{D}$ è banale e il gruppo G non rientra nella definizione 5.4. I calcoli dei caratteri che seguono valgono anche in questo caso. [N.d.T.]

dove l'esponente è un intero. Se $a \neq \pm 1$, allora $\zeta^{a^{-2}} \neq \zeta$. Pertanto la rappresentazione di K definita da

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \longmapsto \zeta^{a^{-2}}$$

non è equivalente a σ.[18] Dal corollario 2 del teorema 5.20 (p. 304) segue che $\rho = \sigma^G$ è una rappresentazione irriducibile di G. Se χ è il suo carattere, il grado di ρ è $\chi(1) = (p-1)/2$. Sia χ' il carattere irriducibile rimanente. La relazione

$$\begin{aligned} p(p-1)/2 = |G| &= \sum_{i=1}^{(p-1)/2} \chi_i(1)^2 + \chi(1)^2 + \chi'(1)^2 \\ &= (p-1)/2 + (p-1)^2/4 + \chi'(1)^2 \end{aligned}$$

dà $\chi'(1) = (p-1)/2$. Le ultime due righe della tavola dei caratteri hanno dunque la forma

χ	$(p-1)/2$	c	d	0
χ'	$(p-1)/2$	c'	d'	0

Le relazioni di ortogonalità (60) per la prima e la seconda colonna danno $(p-1)/2 + c(p-1)/2 + c'(p-1)/2 = 0$, perciò $c + c' = -1$. Analogamente $d + d' = -1$. Dall'ortogonalità di χ e χ_1 segue $(p-1)/2 + c(p-1)/2 + d(p-1)/2 = 0$, perciò $c + d = -1$. Queste relazioni implicano $c' = d$, $d' = c$. Le ultime due righe hanno quindi la forma

χ	$(p-1)/2$	c	$-1-c$	0
χ'	$(p-1)/2$	$-1-c$	c	0

e resta da determinare c. Occorre distinguere due casi.

Caso 1. $(-1/p) = 1$, ossia -1 è un residuo quadratico modulo p o, equivalentemente, $p \equiv 1 \pmod 4$ (BAI, p. 133). In questo caso $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ è coniugata a $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^{-1}$. Allora c è reale. La relazione di ortogonalità (60) applicata alla seconda e alla terza colonna dà $(p-1)/2 - 2c(1+c) = 0$, da cui $c = (-1 \pm \sqrt{p})/2$.

Caso 2. $(-1/p) = -1$, ossia -1 non è un quadrato modulo p, perciò $p \equiv 3 \pmod 4$. In questo caso $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ non è coniugata alla sua inversa e quindi $c \notin \mathbb{R}$. Allora $\chi' = \chi^*$, cosicché $\overline{c} = -1 - c$. La relazione di ortogonalità (60) per la seconda e la terza colonna dà $(p-1)/2 + c^2 + (1+c)^2 = 0$, da cui $c = (-1 \pm \sqrt{-p})/2$.

I due casi completano le tavole dei caratteri, sebbene non sappiamo quale scelta del segno dia il carattere χ di $\rho = \sigma^G$. Possiamo riunirli ponendo $p^* = (-1/p)p$. In entrambi i casi abbiamo allora

$$c = (-1 \pm \sqrt{p^*})/2. \tag{112}$$

Applichiamo ora la formula (85) del carattere indotto al carattere χ di ρ. Poiché $\overline{D}$ è un sistema di rappresentanti delle classi laterali di K in G, otteniamo

$$\frac{-1 \pm \sqrt{p^*}}{2} = \chi \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \sum_{x \in S} \zeta^x, \qquad \zeta = e^{2\pi \mathrm{i}/p}, \tag{113}$$

dove S è l'insieme degli interi positivi minori di p che sono quadrati modulo p.

[18] L'esponente a^{-2} è quello della (110). Nella seconda formula di p. 322 l'originale reca $-a^{-2}$. [N.d.T.]

Applichiamo la formula (113) per dimostrare la legge di reciprocità quadratica della teoria elementare dei numeri. Introduciamo la somma di Gauss

$$g = \sum_x \left(\frac{x}{p}\right) \zeta^x, \tag{114}$$

dove $1 \le x \le p-1$. Poiché $1 + \sum_x \zeta^x = 0$ (per la fattorizzazione $\lambda^p - 1 = \prod_{i=0}^{p-1}(\lambda - \zeta^i)$), dalla (113) si ottiene

$$g^2 = p^*. \tag{115}$$

Sia ora q un primo dispari diverso da p. Osserviamo che $(p^*/q) \equiv (p^*)^{(q-1)/2} \pmod q$ (BAI, p. 129, esercizio 13). Lavoriamo nell'anello R degli interi del campo ciclotomico $\mathbb{Q}(\zeta)$ e usiamo le congruenze modulo qR (BAI, pp. 278–281). Abbiamo

$$\left(\frac{p^*}{q}\right) \equiv g^{q-1} \pmod{qR}. \tag{116}$$

Poiché per $u_i \in R$ si ha $(\sum u_i)^q \equiv \sum u_i^q \pmod{qR}$, otteniamo

$$\begin{aligned} g^q &= \left(\sum_x \left(\frac{x}{p}\right)\zeta^x\right)^q \equiv \sum_x \left(\frac{x}{p}\right)\zeta^{xq} \\ &= \left(\frac{q}{p}\right)\sum_x \left(\frac{q}{p}\right)\left(\frac{x}{p}\right)\zeta^{xq} \\ &= \left(\frac{q}{p}\right)\sum_x \left(\frac{xq}{p}\right)\zeta^{xq} \\ &= \left(\frac{q}{p}\right)\sum_x \left(\frac{x}{p}\right)\zeta^{x} = \left(\frac{q}{p}\right) g \pmod{qR}. \end{aligned}$$

Nell'ultima somma abbiamo cambiato la variabile xq in x modulo p.[19] Dunque

$$\left(\frac{p^*}{q}\right) g \equiv g^q \equiv \left(\frac{q}{p}\right) g \pmod{qR}.$$

Ne segue $(p^*/q)g^2 \equiv (q/p)g^2$, e quindi $(p^*/q)p^* \equiv (q/p)p^*$. Poiché la classe di $p^* = (-1/p)p$ è invertibile in R/qR, si ha $(p^*/q) \equiv (q/p)$. Anche la classe di 2 è invertibile, cosicché $(p^*/q) = (q/p)$. Pertanto

$$\begin{aligned} \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) &= \left(\frac{(-1/p)p}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) \\ &= (-1)^{[(q-1)/2][(p-1)/2]}\left(\frac{p}{q}\right). \end{aligned}$$

È questa la legge di reciprocità quadratica, la cui prima dimostrazione fu pubblicata da Gauss nel 1801.

Sono grato a D. R. Corro per avermi segnalato questo esempio di gruppo di Frobenius e la sua applicazione alla legge di reciprocità. La deduzione che segue la formula $g^2 = p^*$ è classica (a quanto pare fu data per la prima volta da Jacobi nel 1827). Si veda *Sechs Beweise des Fundamentaltheorems über quadratische Reste*, di Carl Friedrich Gauss, nei «Klassiker der exacten Wissenschaften» di W. Ostwald, pp. 107–109.

[19] In questo passaggio, a p. 323, l'originale stampa (x/q) al posto di (x/p). [N.d.T.]

Esercizi.

1. Mostrare che, se G è un gruppo di Frobenius con complemento H, il nucleo di Frobenius è l'unico sottogruppo normale K di G che soddisfa $G = KH$, $K \cap H = 1$.

2. Mostrare che, se G è un gruppo diedrale di ordine $2m$, con m dispari, generato da a e b con $a^m = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$, allora G è un gruppo di Frobenius.

3. Un sottoinsieme S di un gruppo G si dice *insieme T.I.* (a intersezione banale) se $S \neq \varnothing$ e, per ogni $g \in G$, si ha ${}^gS = S$ oppure ${}^gS \cap S \subseteq \{1\}$. Mostrare che, se S è T.I., allora $N_G(S) = \{g \in G \mid {}^gS = S\}$ è un sottogruppo contenente S. Mostrare che, se G è un gruppo di Frobenius con complemento di Frobenius H, allora H è un insieme T.I.

4. (Brauer–Suzuki.) Sia S un insieme T.I. in G e sia $N = N_G(S)$. Siano φ e ψ funzioni di classe complesse su N, entrambe nulle fuori di S, con $\varphi(1) = 0$. Mostrare che (i) $\varphi^G(g) = \varphi(g)$ per ogni $g \neq 1$ in S e (ii) $(\varphi \mid \psi)_N = (\varphi^G \mid \psi^G)_G$.

5. (Brauer–Suzuki.) Siano S, G, N come nell'esercizio 4 e siano $\psi_1, \ldots, \psi_m$ caratteri complessi irriducibili di N tali che $\psi_1(1) = \cdots = \psi_m(1)$. Mostrare che esistono un segno $\varepsilon = \pm 1$ e caratteri complessi irriducibili $\chi_1, \ldots, \chi_m$ di G tali che $\chi_i - \chi_j = \varepsilon(\psi_i^G - \psi_j^G)$.

6. Sia G un gruppo di Frobenius con complemento H e nucleo K. Si supponga K abeliano. Servirsi dell'esercizio 8 di BAI, p. 63, per mostrare che, se ρ è una rappresentazione irriducibile di G, allora (i) $K \subseteq \ker \rho$ oppure (ii) ρ è indotta da una rappresentazione di grado uno di K. Concludere che G è un M-gruppo se e solo se H è un M-gruppo. (Il risultato vale anche senza l'ipotesi che K sia abeliano.)

   Traccia della dimostrazione. Supponiamo che (i) non valga. Per il teorema di Clifford esiste allora un costituente irriducibile λ di ρ_K distinto dalla rappresentazione unitaria λ_1 di K. Affermiamo che $T_G(\lambda) = K$. Altrimenti, per il corollario 2 di p. 304, esisterebbe un $x \in G \setminus K$, appartenente a uno dei coniugati ${}^gH$, tale che ${}^x\lambda = \lambda$. Ma H agisce senza punti fissi su K, e lo stesso vale per ${}^gH$ per ogni g (giacché $K \triangleleft G$). Dunque x induce un automorfismo senza punti fissi di K, per cui, in virtù dell'esercizio citato,

   $$K = \{xkx^{-1}k^{-1} \mid k \in K\}.$$

   Allora

   $$\begin{aligned} \lambda(xkx^{-1}k^{-1}) &= \lambda(xkx^{-1})\lambda(k^{-1}) \\ &= {}^x\lambda(k)\lambda(k)^{-1} \\ &= \lambda(k)\lambda(k)^{-1} = 1. \end{aligned}$$

   Pertanto $K \subseteq \ker \lambda$, contro l'ipotesi $\lambda \neq \lambda_1$. Dunque $T_G(\lambda) = K$ e (ii) segue dal corollario 4 di p. 305.

7. Sia F un campo finito con $q = p^m$ elementi, p primo. Definiamo i seguenti sottogruppi di $GL_2(F)$:

   $$T_n = \left\{ \begin{pmatrix} a^n & 0 \\ b & 1 \end{pmatrix} \;\middle|\; a \in F^*,\ b \in F \right\},$$

   $$D_n = \left\{ \begin{pmatrix} a^n & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in F^* \right\},$$

   $$K = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \;\middle|\; b \in F \right\}.$$

Mostrare che, se $D_n \neq 1$, allora T_n è un gruppo di Frobenius con complemento di Frobenius D_n e nucleo di Frobenius K.

Nota. W. Feit si è servito di questi gruppi per ottenere una stima del numero di soluzioni in $F^{(n)}$ di un'equazione della forma $\sum_{i=1}^{n} c_i x_i^{m_i} = 0$, $c_i \in F^*$. Si veda Feit, p. 140, nella bibliografia seguente.

Riferimenti bibliografici

C. W. Curtis e I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley-Interscience, New York, 1962.

W. Feit, *Characters of Finite Groups*, Benjamin, New York, 1967.

I. M. Isaacs, *Character Theory of Finite Groups*, Academic, New York, 1976.

6 Elementi di algebra omologica e applicazioni

Da quando fu introdotta, verso la metà degli anni Quaranta, l'algebra omologica è divenuta un vasto ramo dell'algebra. Il suo primo aspetto, costituito dai gruppi di coomologia e di omologia di un gruppo, nacque da un problema topologico. Witold Hurewicz aveva osservato che i gruppi di omologia di uno spazio connesso per archi, i cui gruppi di omotopia superiori siano banali, sono determinati dal gruppo fondamentale π_1. Si poneva quindi il problema di spiegare il meccanismo di questa dipendenza. Diversi topologi ne diedero soluzioni indipendenti e pressoché contemporanee: Hopf, Eilenberg e MacLane, Freudenthal ed Eckmann [si vedano Cartan ed Eilenberg (1956), p. 137, e MacLane (1963), p. 185, citati in bibliografia]. Tutte queste soluzioni coinvolgevano gruppi di omologia o di coomologia di π_1. Il passo successivo fu definire i gruppi di omologia e di coomologia di un gruppo qualsiasi e studiarli per sé stessi. Nel 1947 Eilenberg e MacLane definirono i gruppi di coomologia a coefficienti in un modulo arbitrario. Nello stesso periodo G. Hochschild introdusse i gruppi di coomologia per le algebre associative. La teoria della coomologia delle algebre di Lie, teoria puramente algebrica corrispondente a quella della coomologia dei gruppi di Lie, fu sviluppata da J. L. Koszul e da Chevalley ed Eilenberg. Queste diverse teorie furono riunite da Cartan ed Eilenberg (1956) in una sintesi organica, fondata sul concetto di funtori derivati dalla categoria dei moduli su un anello alla categoria dei gruppi abeliani. I funtori derivati di cui si servono le teorie della coomologia e dell'omologia sono i funtori Ext e Tor, derivati rispettivamente dal funtore hom e dal funtore prodotto tensoriale.

Sebbene lo sviluppo dell'algebra omologica propriamente detta risalga agli anni della seconda guerra mondiale, alcune importanti anticipazioni sono più antiche. La prima è forse il teorema delle sizigie di Hilbert (1890) in teoria degli invarianti, riguardante le risoluzioni libere di moduli sull'anello dei polinomi in m indeterminate a coefficienti in un campo. Il secondo gruppo di coomologia $H^2(G, \mathbb{C}^*)$, a coefficienti nel gruppo moltiplicativo $\mathbb{C}^*$ dei numeri complessi non nulli, comparve nei lavori di Schur sulle rappresentazioni proiettive dei gruppi (1904). Gruppi di coomologia di grado due più generali comparvero come sistemi di fattori nella teoria delle estensioni di gruppi di Schreier (1926) e nella costruzione delle algebre prodotto incrociato di Emmy Noether (1929). Il terzo gruppo di coomologia apparve per la prima volta in un lavoro di O. Teichmüller (1940).

In questo capitolo giungeremo anzitutto, per la via più breve possibile, alla definizione e ai risultati fondamentali sui funtori derivati. Li applicheremo poi ai casi più importanti, Ext e Tor. Nella seconda metà del capitolo considereremo alcuni temi classici della teoria omologica: la coomologia dei gruppi, la coomologia delle algebre con applicazioni a un teorema di Wedderburn sullo spezzamento del radicale di un'algebra di dimensione finita, la dimensione omologica dei moduli e degli anelli e il teorema delle sizigie di Hilbert. Più avanti, nei §§ 8.4 e 8.5, daremo un'altra applicazione della teoria omologica al gruppo di Brauer e ai prodotti incrociati.

6.1 Categorie additive e abeliane

Una parte considerevole della teoria dei moduli si estende a una classe di categorie dette *abeliane*. In particolare, si può sviluppare l'algebra omologica per categorie abeliane. Benché nella nostra trattazione ci atterremo ai moduli, sarà comodo disporre delle definizioni e delle proprietà più semplici di tali categorie. Ce ne occuperemo dunque in questo paragrafo.

Ricordiamo che un oggetto 0 di una categoria $\mathbf{C}$ è un oggetto zero se, per ogni oggetto A di $\mathbf{C}$, $\hom_{\mathbf{C}}(A, 0)$ e $\hom_{\mathbf{C}}(0, A)$ hanno un solo elemento. Se 0 e $0'$ sono oggetti zero, esiste un unico isomorfismo $0 \to 0'$ (esercizio 3, p. 36 dell'originale). Per $A, B \in \mathrm{ob}\,\mathbf{C}$, definiamo $0_{A,B}$ come il morfismo $0_{0,B}0_{A,0}$, dove $0_{A,0}$ e $0_{0,B}$ sono gli unici elementi rispettivamente di $\hom_{\mathbf{C}}(A, 0)$

e $\hom_{\mathbf{C}}(0, B)$. È facile vedere che tale morfismo è indipendente dalla scelta dell'oggetto zero. Chiamiamo $0_{A,B}$ il *morfismo zero* da A a B. Di solito ne ometteremo gli indici.

Definizione 6.1. Una categoria $\mathbf{C}$ si dice *additiva* se soddisfa le seguenti condizioni.

AC1. $\mathbf{C}$ ha un oggetto zero.

AC2. Per ogni coppia di oggetti (A, B) è definita su $\hom_{\mathbf{C}}(A, B)$ un'operazione binaria $+$ per la quale $(\hom_{\mathbf{C}}(A, B), +, 0_{A,B})$ è un gruppo abeliano.

AC3. Se $A, B, C \in \operatorname{ob}\mathbf{C}$, $f, f_1, f_2 \in \hom_{\mathbf{C}}(A, B)$ e $g, g_1, g_2 \in \hom_{\mathbf{C}}(B, C)$, allora

$$(g_1 + g_2)f = g_1 f + g_2 f, \qquad g(f_1 + f_2) = gf_1 + gf_2.$$

AC4. Per ogni famiglia finita di oggetti $A_1, \dots, A_n$ esistono un oggetto A e morfismi $p_j \colon A \to A_j$, $i_j \colon A_j \to A$, $1 \le j \le n$, tali che

$$p_j i_j = 1_{A_j}, \qquad p_k i_j = 0 \ (j \neq k), \qquad \sum_j i_j p_j = 1_A. \tag{1}$$

La condizione AC2 significa che la struttura di gruppo abeliano di ogni $\hom_{\mathbf{C}}(A, B)$ è un dato della definizione e che il suo zero è l'elemento $0_{A,B}$ definito categorialmente. La AC3 afferma che il prodotto fg, quando è definito, è biadditivo. Ne segue che, per ogni A, $(\hom_{\mathbf{C}}(A, A), +, \cdot, 0, 1_A)$ è un anello. La AC4 implica inoltre che $(A, \{p_j\})$ è un prodotto in $\mathbf{C}$ degli A_j. Infatti, dati $B \in \operatorname{ob}\mathbf{C}$ e $f_j \colon B \to A_j$, poniamo $f = \sum i_j f_j \in \hom_{\mathbf{C}}(B, A)$. Per (1) si ha $p_k f = f_k$. Se $p_k f' = f_k$ per ogni k, ancora per (1) si ha $f' = \sum i_j p_j f' = \sum i_j f_j = f$. Pertanto f è l'unico morfismo da B ad A tale che $p_k f = f_k$ per ogni k, e $(A, \{p_j\})$ è un prodotto degli A_j. Analogamente $(A, \{i_j\})$ è un coprodotto degli A_j.

Non è difficile mostrare che si può sostituire AC4 con una delle due condizioni:

AC4′. $\mathbf{C}$ è una categoria con prodotto, ossia in cui esistono i prodotti di famiglie finite arbitrarie di oggetti.

AC4″. $\mathbf{C}$ è una categoria con coprodotto.

Abbiamo visto che AC4 implica AC4′ e AC4″. Negli esercizi indicheremo come AC1–AC3, insieme ad AC4′ oppure ad AC4″, implichino AC4. Il vantaggio di AC4 è che è autoduale. L'intero sistema di condizioni che definisce una categoria additiva è quindi autoduale: se $\mathbf{C}$ è additiva, anche $\mathbf{C}^{\mathrm{op}}$ lo è. Questo è uno dei principali vantaggi che si hanno nel trattare le categorie additive.

Se R è un anello, R-**mod** e **mod**-R sono categorie additive. Come in questi casi particolari, è naturale supporre che i funtori fra categorie additive siano *additivi*, nel senso che per ogni coppia di oggetti A, B l'applicazione F di $\hom(A, B)$ in $\hom(FA, FB)$ sia un omomorfismo di gruppi. In questo caso la dimostrazione data per i moduli (p. 98 dell'originale) mostra che F conserva i prodotti (e i coprodotti) finiti.

Introduciamo i concetti necessari per definire le categorie abeliane. Sia $\mathbf{C}$ una categoria con un oggetto zero, e sia $f \colon A \to B$ in $\mathbf{C}$. Un *nucleo* di f è un morfismo $k \colon K \to A$ tale che (1) k sia monico, (2) $fk = 0$, (3) per ogni $g \colon G \to A$ tale che $fg = 0$ esista g' con $g = kg'$. Poiché k è monico, g' è unico. La condizione (2) esprime la commutatività del primo diagramma qui sotto; la (3) afferma che, se nel secondo diagramma commuta il triangolo a destra, lo si può completare con una freccia $g' \colon G \to K$ che renda commutativo l'intero diagramma.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle k}\uparrow & \nearrow 0 & \\ K & & \end{array} \qquad\qquad \begin{array}{ccccc} K & \xrightarrow{k} & A & \xrightarrow{f} & B \\ & {\scriptstyle g'}\swarrow & {\scriptstyle g}\uparrow & \nearrow 0 & \\ & & G & & \end{array}$$

Se k, k' sono nuclei di f, esiste evidentemente un unico isomorfismo u tale che $k' = ku$.

Dualmente, un *conucleo* di f è un morfismo $c\colon B \to C$ tale che (1) c sia epico, (2) $cf = 0$, (3) per ogni $h\colon B \to H$ tale che $hf = 0$ esista h' con $h = h'c$:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{c} & C \\ & {\scriptstyle 0}\searrow & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle h'} & \\ & & H & & \end{array}$$

Se $f\colon A \to B$ è in R-**mod**, siano $K = \ker f$ nel senso consueto e k l'inclusione di K in A. Allora k è monico, $fk = 0$, e, se $g\colon G \to A$ è un omomorfismo tale che $fg = 0$, si ha $gG \subseteq K$. Restringendo a K il codominio di g otteniamo quindi g' con $g = kg'$. Dunque k è un nucleo di f. Ora poniamo $C = B/fA$ e sia c l'omomorfismo canonico di B su C. Esso è epico, $cf = 0$, e, se $h\colon B \to H$ soddisfa $hf = 0$, allora $fA \subseteq \ker h$. Esiste dunque un unico omomorfismo $h'\colon C = B/fA \to H$ che renda commutativo il diagramma

$$\begin{array}{ccc} B & \xrightarrow{c} & C = B/fA \\ {\scriptstyle h}\searrow & & \swarrow{\scriptstyle h'} \\ & H & \end{array}$$

Pertanto c è un conucleo di f in R-**mod**.

Definizione 6.2. Una categoria $\mathbf{C}$ è *abeliana* se è additiva e gode delle ulteriori proprietà:

AC5. Ogni morfismo di $\mathbf{C}$ ammette nucleo e conucleo.

AC6. Ogni monomorfismo è un nucleo del proprio conucleo e ogni epimorfismo è un conucleo del proprio nucleo.

AC7. Ogni morfismo si può fattorizzare nella forma $f = me$, con e epico e m monico.

Se R è un anello, abbiamo visto che R-**mod** e **mod**-R sono categorie additive che soddisfano AC5. Lasciamo al lettore la verifica di AC6 e AC7. Si tratta dunque di categorie abeliane.

Esercizi

1. Sia $\mathbf{C}$ una categoria con uno zero. Mostrare che per ogni oggetto A la terna $(A, 1_A, 0)$ è un prodotto e un coprodotto di A e 0.

2. Siano $\mathbf{C}$ una categoria, (A, p_1, p_2) un prodotto di A_1, A_2, (B, q_1, q_2) un prodotto di B_1, B_2 e $h_i\colon B_i \to A_i$. Mostrare che esiste un unico $f\colon B \to A$ tale che $h_i q_i = p_i f$. In particolare, se $\mathbf{C}$ ha uno zero e si prende $(B, q_1, q_2) = (A_1, 1_{A_1}, 0)$, si ottiene un unico $i_1\colon A_1 \to A$ tale che $p_1 i_1 = 1_{A_1}$, $p_2 i_1 = 0$. Analogamente dimostrare che esiste un unico $i_2\colon A_2 \to A$ tale che $p_1 i_2 = 0$, $p_2 i_2 = 1_{A_2}$. Mostrare che $(i_1 p_1 + i_2 p_2) i_1 = i_1$ e $(i_1 p_1 + i_2 p_2) i_2 = i_2$. Concludere che $i_1 p_1 + i_2 p_2 = 1_A$. Dedurne che AC1–AC3 e AC4′ implicano AC4. Passare al duale per provare che AC1–AC3 e AC4″ implicano AC4.

3. Mostrare che, per oggetti A, B di una categoria additiva, $0_{A,B} = 0_{0,B} 0_{A,0}$, dove $0_{A,0}$, $0_{0,B}$, $0_{A,B}$ sono gli zeri dei gruppi abeliani $\hom(A, 0)$, $\hom(0, B)$, $\hom(A, B)$.

4. Sia $(A_1 \prod A_2, p_1, p_2)$ un prodotto di A_1, A_2 in $\mathbf{C}$. Per $f_j\colon B \to A_j$, si indichi con $f_1 \prod f_2$ l'unico $f\colon B \to A_1 \prod A_2$ tale che $p_j f = f_j$. Analogamente, se $(A_1 \coprod A_2, i_1, i_2)$ è un coprodotto e $g_j\colon A_j \to C$, si scriva $g_1 \coprod g_2$ per l'unico $g\colon A_1 \coprod A_2 \to C$ tale che $g i_j = g_j$. Se $\mathbf{C}$ è additiva, con i_j, p_j come in AC4, osservare che $f_1 \prod f_2 = i_1 f_1 + i_2 f_2$ e $g_1 \coprod g_2 = g_1 p_1 + g_2 p_2$. Quindi, quando i_1, i_2, p_1, p_2 sono come in AC4 e $A = A_1 \prod A_2 = A_1 \coprod A_2$, mostrare che, da B a C,
$$(g_1 \coprod g_2)(f_1 \prod f_2) = g_1 f_1 + g_2 f_2.$$

Porre $A_1 = A_2 = C$, $g_1 = g_2 = 1_C$, per ottenere la formula $f_1 + f_2 = (1_C \coprod 1_C)(f_1 \prod f_2)$ per l'addizione in $\hom_{\mathbf{C}}(B, C)$.

5. Usare il risultato dell'esercizio 4 per dimostrare che un funtore F fra categorie additive che conserva prodotti e coprodotti è additivo.

6.2 Complessi e omologia

I concetti fondamentali dell'algebra omologica sono quelli di complesso e di omomorfismo di complessi, che ora definiamo.

Definizione 6.3. Se R è un anello, un *complesso* (C, d) su R è una famiglia $C = \{C_i\}$ di R-moduli indicizzata da $\mathbb{Z}$, insieme con una famiglia $d = \{d_i \mid i \in \mathbb{Z}\}$ di R-omomorfismi $d_i \colon C_i \to C_{i-1}$ tali che $d_{i-1}d_i = 0$ per ogni i. Se $(C, d), (C', d')$ sono R-complessi, un *omomorfismo (di catene)* da C a C' è una famiglia $\alpha = \{\alpha_i \mid i \in \mathbb{Z}\}$ di omomorfismi $\alpha_i \colon C_i \to C'_i$ tali che, per ogni i, commuti il diagramma

$$\begin{array}{ccc} C_i & \xrightarrow{d_i} & C_{i-1} \\ \downarrow{\scriptstyle \alpha_i} & & \downarrow{\scriptstyle \alpha_{i-1}} \\ C'_i & \xrightarrow{d'_i} & C'_{i-1} \end{array} \tag{2}$$

Più brevemente scriveremo $\alpha d = d'\alpha$.

Queste definizioni portano alla categoria R-**comp** dei complessi sull'anello R. I suoi oggetti sono gli R-complessi (C, d) e, per ogni coppia $(C, d), (C', d')$, $\hom(C, C')$ è l'insieme degli omomorfismi di catene da (C, d) a (C', d'). È chiaro che si ottiene una categoria; vedremo che le proprietà principali di R-**mod** si conservano in R-**comp**. Anzitutto $\hom(C, C')$ ha una struttura naturale di gruppo abeliano. Per $\alpha, \beta \in \hom(C, C')$ definiamo $(\alpha + \beta)_i = \alpha_i + \beta_i$. Le relazioni $\alpha_{i-1}d_i = d'_i\alpha_i$, $\beta_{i-1}d_i = d'_i\beta_i$ danno $(\alpha_{i-1} + \beta_{i-1})d_i = d'_i(\alpha_i + \beta_i)$; dunque $\alpha + \beta \in \hom(C, C')$. Poiché $\hom_R(C_i, C'_i)$ è abeliano, lo è anche $\hom(C, C')$. Dal caso dei moduli risultano inoltre le leggi distributive $\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta$ e $(\alpha + \beta)\delta = \alpha\delta + \beta\delta$ ogni volta che questi prodotti di omomorfismi di catene sono definiti.

Per due complessi $(C, d), (C', d')$ si definisce la somma diretta $(C \oplus C', d \oplus d')$ ponendo $(C \oplus C')_i = C_i \oplus C'_i$ e definendo $d_i \oplus d'_i$ per componenti da $C_i \oplus C'_i$ a $C_{i-1} \oplus C'_{i-1}$ mediante $(x_i, x'_i) \mapsto (d_i x_i, d'_i x'_i)$. È chiaro che $(d_{i-1} \oplus d'_{i-1})(d_i \oplus d'_i) = 0$, sicché la somma diretta è un complesso. La costruzione si estende immediatamente a più di due complessi. Poiché tutto si riduce ai moduli, con la struttura di gruppo abeliano appena definita sugli insiemi di morfismi R-**comp** diventa una categoria abeliana.

Incontreremo esempi interessanti di complessi nel § 6.4. Può tuttavia essere utile elencarne già alcuni, anche se i più appariranno piuttosto particolari.

Esempi.

1. Ogni modulo M dà un complesso ponendo $C_i = M$, $i \in \mathbb{Z}$, e $d_i = 0 \colon C_i \to C_{i-1}$.

2. Un *modulo con differenziale* è un R-modulo dotato di un endomorfismo di moduli δ tale che $\delta^2 = 0$. Dato (M, δ), si ottiene un complesso (C, d) ponendo $C_i = 0$ per $i \leq 0$, $C_1 = C_2 = C_3 = M$, $C_j = 0$ per $j > 3$, $d_2 = d_3 = \delta$ e $d_i = 0$ per $i \neq 2, 3$.

3. Sia (M, δ) un modulo con differenziale, $\mathbb{Z}$-graduato nel senso che $M = \bigoplus_{i \in \mathbb{Z}} M_i$, dove gli M_i sono sottomoduli e $\delta(M_i) \subseteq M_{i-1}$ per ogni i. Ponendo $C_i = M_i$, $d_i = \delta|_{M_i}$, si ottiene un R-complesso $C = \{C_i\}$, $d = \{d_i\}$.

4. Ogni successione esatta corta $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ definisce un complesso in cui $C_i = 0$ per $i \leq 0$, $C_1 = M''$, $C_2 = M$, $C_3 = M'$, $C_j = 0$ per $j > 3$, $d_2 = \beta$, $d_3 = \alpha$, $d_i = 0$ per $i \neq 2, 3$.

Definiamo ora per ogni $i \in \mathbb{Z}$ un funtore dalla categoria degli R-complessi a quella degli R-moduli, l'*i-esimo funtore di omologia*. Dato un complesso (C, d), sia $Z_i(C) = \ker d_i$, sottomodulo di C_i i cui elementi si chiamano *i-cicli*. Poiché $d_i d_{i+1} = 0$, l'immagine $d_{i+1}C_{i+1}$ è un sottomodulo di Z_i. La indichiamo con $B_i = B_i(C)$ e chiamiamo i suoi elementi *i-bordi*. Il modulo $H_i = H_i(C) = Z_i/B_i$ è l'*i-esimo modulo di omologia* del complesso. Evidentemente $C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1}$ è esatta se e solo se $H_i(C) = 0$, e quindi la successione infinita

$$\cdots \longleftarrow C_{i-1} \xleftarrow{d_i} C_i \xleftarrow{d_{i+1}} C_{i+1} \longleftarrow \cdots$$

è esatta se e solo se $H_i(C) = 0$ per ogni i.

Sia α un omomorfismo di catene da (C, d) a (C', d'). La commutatività di (2) implica $\alpha_i Z_i \subseteq Z'_i = Z_i(C')$ e $\alpha_i B_i \subseteq B'_i = B_i(C')$. Pertanto $z_i \mapsto \alpha_i z_i + B'_i$ è un omomorfismo da Z_i a $H'_i = H_i(C') = Z'_i/B'_i$ che manda B_i in zero. Ne risulta l'omomorfismo $\widetilde{\alpha}_i$ da $H_i(C)$ a $H_i(C')$ dato da

$$z_i + B_i \longmapsto \alpha_i z_i + B'_i. \tag{3}$$

È immediato verificare che $(C, d) \mapsto H_i(C)$ e $\alpha \mapsto \widetilde{\alpha}_i$ da $\hom(C, C')$ a $\hom(H_i(C), H_i(C'))$ definiscono un funtore da R-**comp** a R-**mod**. Lo chiamiamo l'i-esimo funtore di omologia. È chiaro che $\alpha \mapsto \widetilde{\alpha}_i$ è un omomorfismo di gruppi abeliani: il funtore è quindi additivo.

Nei casi che incontreremo i complessi avranno $C_i = 0$ per $i < 0$, oppure $C_i = 0$ per $i > 0$. Nel primo caso si chiamano *positivi* o *complessi di catene*, nel secondo *negativi* o *complessi di cocatene*. In quest'ultimo caso si scrive di solito $C^i = C_{-i}$, $d^i = d_{-i}$. Omettendo i termini C^{-i} con $i \geq 1$, si ha

$$0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \longrightarrow \cdots.$$

Si scrive allora $Z^i = \ker d^i$ e $B^i = d^{i-1}C^{i-1}$. I loro elementi sono rispettivamente gli *i-cocicli* e gli *i-cobordi*; $H^i = Z^i/B^i$ è l'i-esimo gruppo di coomologia. In grado zero si ha $H^0 = Z^0$. Un complesso di catene ha la forma $0 \leftarrow C_0 \leftarrow C_1 \leftarrow C_2 \leftarrow \cdots$; in questo caso $H_0 = C_0/d_1C_1 = \operatorname{coker} d_1$.

Esercizi

1. Sia α un omomorfismo da (C, d) a (C', d'). Definire $C''_i = C_{i-1} \oplus C'_i$ per $i \in \mathbb{Z}$ e $d''_i(x_{i-1}, x'_i) = (-d_{i-1}x_{i-1}, \alpha_{i-1}x_{i-1} + d'_i x'_i)$ per $x_{i-1} \in C_{i-1}$, $x'_i \in C'_i$. Verificare che (C'', d'') è un complesso.

2. Sia (C, d) un complesso positivo su un campo F, con $\sum \dim C_i < \infty$ (ossia ogni C_i è di dimensione finita e $C_n = 0$ per n abbastanza grande). Posti $r_i = \dim C_i$, $p_i = \dim H_i(C)$, dimostrare che $\sum(-1)^i p_i = \sum(-1)^i r_i$.

3. *Complesso di Amitsur.* Sia S un'algebra commutativa su un anello commutativo K. Poniamo $S^0 = K$, $S^n = S \otimes \cdots \otimes S$ con n fattori e $\otimes = \otimes_K$. Per ogni n abbiamo $n + 1$ omomorfismi di algebre δ^i, $1 \leq i \leq n + 1$, da S^n a S^{n+1}, dati da

$$x_1 \otimes \cdots \otimes x_n \mapsto x_1 \otimes \cdots \otimes x_{i-1} \otimes 1 \otimes x_i \otimes \cdots \otimes x_n.$$

Per ogni anello R sia $U(R)$ il gruppo moltiplicativo delle unità di R. Allora $\delta^i U(S^n) \subseteq U(S^{n+1})$. Definire $d^n\colon U(S^n) \to U(S^{n+1})$, $n \geq 0$, ponendo

$$d^n u = \prod_{i=1}^{n+1} (\delta^i u)^{(-1)^i}$$

(per esempio $d^2 u = (\delta^1 u)^{-1}(\delta^2 u)(\delta^3 u)^{-1}$). Osservare che per $i \geq j$ si ha $\delta^{i+1}\delta^j = \delta^j \delta^i$ e dedurne $d^{n+1}d^n = 0$, ossia l'applicazione $u \mapsto 1$. Concludere che $\{U(S^n), d^n \mid n \geq 0\}$ è un complesso di cocatene.

6.3 La successione esatta lunga di omologia

Svilupperemo uno degli strumenti più importanti dell'algebra omologica: la successione esatta lunga di omologia associata a una successione esatta corta di complessi. Per *successione esatta corta di complessi* intendiamo una successione di complessi e di omomorfismi di catene $C' \xrightarrow{\alpha} C \xrightarrow{\beta} C''$ tale che $0 \to C'_i \xrightarrow{\alpha_i} C_i \xrightarrow{\beta_i} C''_i \to 0$ sia esatta per ogni $i \in \mathbb{Z}$; cioè α_i è iniettivo, β_i suriettivo e $\ker \beta_i = \operatorname{im} \alpha_i$. Diremo allora che $0 \to C' \to C \to C'' \to 0$ è esatta. Abbiamo il diagramma commutativo a righe esatte

$$\begin{array}{ccccccccc}
0 & \to & C'_{i+1} & \xrightarrow{\alpha_{i+1}} & C_{i+1} & \xrightarrow{\beta_{i+1}} & C''_{i+1} & \to & 0 \\
 & & \downarrow{\scriptstyle d'_{i+1}} & & \downarrow{\scriptstyle d_{i+1}} & & \downarrow{\scriptstyle d''_{i+1}} & & \\
0 & \to & C'_i & \xrightarrow{\alpha_i} & C_i & \xrightarrow{\beta_i} & C''_i & \to & 0 \\
 & & \downarrow{\scriptstyle d'_i} & & \downarrow{\scriptstyle d_i} & & \downarrow{\scriptstyle d''_i} & & \\
0 & \to & C'_{i-1} & \xrightarrow{\alpha_{i-1}} & C_{i-1} & \xrightarrow{\beta_{i-1}} & C''_{i-1} & \to & 0.
\end{array}$$

Vogliamo dimostrare il seguente risultato.

Teorema 6.1. *Sia $0 \to C' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \to 0$ una successione esatta di complessi. Per ogni $i \in \mathbb{Z}$ si può definire un omomorfismo di moduli $\Delta_i\colon H_i(C'') \to H_{i-1}(C')$ in modo che la successione infinita dei moduli di omologia*

$$\cdots \to H_i(C') \xrightarrow{\widetilde{\alpha}_i} H_i(C) \xrightarrow{\widetilde{\beta}_i} H_i(C'') \xrightarrow{\Delta_i} H_{i-1}(C') \xrightarrow{\widetilde{\alpha}_{i-1}} H_{i-1}(C) \to \cdots \tag{4}$$

sia esatta.

Dimostrazione. Definiamo anzitutto Δ_i. Sia $z''_i \in Z_i(C'')$, dunque $d''_i z''_i = 0$. Per la suriettività di β_i esiste $c_i \in C_i$ tale che $\beta_i c_i = z''_i$. Allora $\beta_{i-1} d_i c_i = d''_i \beta_i c_i = d''_i z''_i = 0$. Poiché $\ker \beta_{i-1} = \operatorname{im} \alpha_{i-1}$ e α_{i-1} è iniettivo, esiste un unico $z'_{i-1} \in C'_{i-1}$ tale che $\alpha_{i-1} z'_{i-1} = d_i c_i$. Ora $\alpha_{i-2} d'_{i-1} z'_{i-1} = d_{i-1}\alpha_{i-1} z'_{i-1} = d_{i-1} d_i c_i = 0$. L'iniettività di α_{i-2} implica $d'_{i-1} z'_{i-1} = 0$, dunque $z'_{i-1} \in Z_{i-1}(C')$. Il procedimento è descritto dalla formula

$$z'_{i-1} \in \alpha_{i-1}^{-1} d_i(\beta_i^{-1}(z''_i)), \tag{5}$$

dove β_i^{-1} e α_{i-1}^{-1} indicano immagini inverse. Nel primo passo abbiamo scelto $c_i \in \beta_i^{-1}(z''_i)$. Se scegliamo un altro elemento $\bar{c}_i$, da $\beta_i \bar{c}_i = \beta_i c_i$ segue $\bar{c}_i = c_i + \alpha_i c'_i$, con $c'_i \in C'_i$. Quindi

$$\alpha_{i-1}(z'_{i-1} + d'_i c'_i) = d_i c_i + d_i \alpha_i c'_i = d_i(c_i + \alpha_i c'_i) = d_i \bar{c}_i.$$

Sostituire c_i con $\bar{c}_i$ equivale così a sostituire z'_{i-1} con $z'_{i-1} + d'_i c'_i$. La classe $z'_{i-1} + B_{i-1}(C')$ in $H_{i-1}(C')$ è indipendente dalla scelta di c_i, e si ha l'applicazione

$$z''_i \longmapsto z'_{i-1} + B_{i-1}(C') \tag{6}$$

di $Z_i(C'')$ in $H_{i-1}(C')$. Da (5) è chiaro che si tratta di un omomorfismo di moduli. Supponiamo ora $z''_i \in B_i(C'')$, diciamo $z''_i = d''_{i+1}c''_{i+1}$. Scegliamo $c_{i+1} \in C_{i+1}$ tale che $\beta_{i+1}c_{i+1} = c''_{i+1}$. Allora $\beta_i d_{i+1}c_{i+1} = d''_{i+1}\beta_{i+1}c_{i+1} = z''_i$, e per c_i possiamo prendere $d_{i+1}c_{i+1}$. Poiché $d_i d_{i+1} = 0$, in (5) si ha $z'_{i-1} = 0$. Il nucleo di (6) contiene pertanto $B_i(C'')$ e

$$\Delta_i \colon z''_i + B_i(C'') \longmapsto z'_{i-1} + B_{i-1}(C') \tag{7}$$

è un omomorfismo di $H_i(C'')$ in $H_{i-1}(C')$.

Dimostriamo che con questa definizione (4) è esatta. Occorre verificare tre uguaglianze.

I. $\operatorname{im}\widetilde{\alpha}_i = \ker\widetilde{\beta}_i$. È chiaro che $\widetilde{\beta}_i\widetilde{\alpha}_i = 0$, dunque vale l'inclusione $\subseteq$. Sia $z_i \in Z_i(C)$ con $\widetilde{\beta}_i(z_i + B_i(C)) = 0$, ossia $\beta_i z_i = d''_{i+1}c''_{i+1}$. Scegliamo c_{i+1} tale che $\beta_{i+1}c_{i+1} = c''_{i+1}$. Allora $\beta_i(z_i - d_{i+1}c_{i+1}) = d''_{i+1}c''_{i+1} - d''_{i+1}\beta_{i+1}c_{i+1} = 0$. Esiste quindi $z'_i \in C'_i$ con $\alpha_i z'_i = z_i - d_{i+1}c_{i+1}$. Poiché $\alpha_{i-1}d'_i z'_i = d_i\alpha_i z'_i = d_i z_i - d_i d_{i+1}c_{i+1} = 0$, si ha $d'_i z'_i = 0$. Ora $\widetilde{\alpha}_i(z'_i + B_i(C')) = \alpha_i z'_i + B_i(C) = z_i + B_i(C)$. Ne segue l'inclusione inversa e quindi l'uguaglianza.

II. $\operatorname{im}\widetilde{\beta}_i = \ker\Delta_i$. Sia $z_i \in Z_i(C)$ e sia $z''_i = \beta_i z_i$. Allora $\Delta_i(z''_i + B_i(C'')) = 0$ perché $z_i \in \beta_i^{-1}(z''_i)$ e $d_i z_i = 0 = \alpha_{i-1}0$. Dunque $\Delta_i\widetilde{\beta}_i(z_i + B_i(C)) = 0$. Viceversa, se $z''_i \in Z_i(C'')$ e $\Delta_i(z''_i + B_i(C'')) = 0$, scegliamo $c_i \in C_i$ con $\beta_i c_i = z''_i$ e z'_{i-1} con $\alpha_{i-1}z'_{i-1} = d_i c_i$. Allora $z'_{i-1} = d'_i c'_i$ per qualche c'_i. Pertanto $d_i c_i = \alpha_{i-1}d'_i c'_i = d_i\alpha_i c'_i$, onde $d_i(c_i - \alpha_i c'_i) = 0$; inoltre $\beta_i(c_i - \alpha_i c'_i) = z''_i$. Posto $z_i = c_i - \alpha_i c'_i$, si ha $z_i \in Z_i(C)$ e $\widetilde{\beta}_i(z_i + B_i(C)) = z''_i + B_i(C'')$. Segue l'uguaglianza.

III. $\operatorname{im}\Delta_i = \ker\widetilde{\alpha}_{i-1}$. Se $z'_{i-1} + B_{i-1}(C') \in \operatorname{im}\Delta_i$, nella costruzione precedente possiamo rappresentare questa classe scegliendo z''_i e c_i con $\beta_i c_i = z''_i$, $\alpha_{i-1}z'_{i-1} = d_i c_i$. Allora $\widetilde{\alpha}_{i-1}(z'_{i-1} + B_{i-1}(C')) = d_i c_i + B_{i-1}(C) = 0$. Viceversa, se la classe di z'_{i-1} è nel nucleo di $\widetilde{\alpha}_{i-1}$, allora $\alpha_{i-1}z'_{i-1} = d_i c_i$ per qualche c_i. Poniamo $z''_i = \beta_i c_i$. Si ha $d''_i z''_i = \beta_{i-1}d_i c_i = \beta_{i-1}\alpha_{i-1}z'_{i-1} = 0$; dunque z''_i è un ciclo. Per definizione, $\Delta_i(z''_i + B_i(C'')) = z'_{i-1} + B_{i-1}(C')$. Ciò prova l'uguaglianza. □

L'omomorfismo Δ_i si chiama *omomorfismo di connessione* da $H_i(C'')$ a $H_{i-1}(C')$, e (4) è la *successione esatta lunga di omologia* determinata dalla successione esatta corta $0 \to C' \to C \to C'' \to 0$. Una proprietà importante dell'omomorfismo di connessione è la sua naturalità.

Teorema 6.2. *Sia dato un diagramma commutativo di omomorfismi di complessi a righe esatte*

$$\begin{array}{ccccccccc} 0 & \to & C' & \xrightarrow{\alpha} & C & \xrightarrow{\beta} & C'' & \to & 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow f'' & & \\ 0 & \to & D' & \xrightarrow{\gamma} & D & \xrightarrow{\delta} & D'' & \to & 0. \end{array} \tag{8}$$

Allora è commutativo il diagramma

$$\begin{array}{ccc} H_i(C'') & \xrightarrow{\Delta_i} & H_{i-1}(C') \\ \downarrow \widetilde{f}''_i & & \downarrow \widetilde{f}'_{i-1} \\ H_i(D'') & \xrightarrow{\Delta_i} & H_{i-1}(D'). \end{array} \tag{9}$$

La commutatività di (8) significa, naturalmente, che per ogni i commuta

$$\begin{array}{ccccc} C'_i & \xrightarrow{\alpha_i} & C_i & \xrightarrow{\beta_i} & C''_i \\ \downarrow f'_i & & \downarrow f_i & & \downarrow f''_i \\ D'_i & \xrightarrow{\gamma_i} & D_i & \xrightarrow{\delta_i} & D''_i. \end{array}$$

La verifica della commutatività di (9) è diretta ed è lasciata al lettore.

Esercizio

1. *Lemma del serpente.* Sia dato un diagramma commutativo di omomorfismi di moduli con le colonne e le due righe centrali esatte:

$$\begin{array}{ccccccccc}
 & & 0 & \to & 0 & \to & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K' & \xrightarrow{\kappa'} & K & \xrightarrow{\kappa} & K'' & & \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
 & & M' & \xrightarrow{\mu'} & M & \xrightarrow{\mu} & M'' & \to & 0 \\
 & & \downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g''} & & \\
0 & \to & N' & \xrightarrow{\nu'} & N & \xrightarrow{\nu} & N'' & & \\
 & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h''} & & \\
 & & C' & \xrightarrow{\gamma'} & C & \xrightarrow{\gamma} & C'' & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \to & 0 & \to & 0 & &
\end{array}$$

   Dato $x'' \in K''$, sia $y \in M$ tale che $\mu y = f''x''$. Allora $\nu g y = g''\mu y = g''f''x'' = 0$ ed esiste un unico $z' \in N'$ tale che $\nu' z' = gy$. Porre $\Delta x'' = h'z'$. Dimostrare che $\Delta x''$ è indipendente dalla scelta di y e che $\Delta\colon K'' \to C'$ è un omomorfismo di moduli. Verificare l'esattezza di

$$K' \xrightarrow{\kappa'} K \xrightarrow{\kappa} K'' \xrightarrow{\Delta} C' \xrightarrow{\gamma'} C \xrightarrow{\gamma} C''.$$

   Dimostrare che, se μ' è un monomorfismo, anche κ' lo è, e che, se ν è un epimorfismo, anche γ lo è.

6.4 Omotopia

Abbiamo visto che un omomorfismo di catene α da un complesso (C, d) a un complesso (C', d') determina, per ogni $i \in \mathbb{Z}$, un omomorfismo $\widetilde{\alpha}_i$ dall'i-esimo modulo di omologia $H_i(C)$ in $H_i(C')$. Fra gli omomorfismi di catene da (C, d) a (C', d') vi è un'importante relazione che garantisce che i corrispondenti omomorfismi dei moduli di omologia siano identici. La precisiamo con la definizione seguente.

Definizione 6.4. *Siano α e β omomorfismi di catene da un complesso (C, d) a un complesso (C', d'). Si dice che α è* omotopo *a β se esiste una famiglia indicizzata $s = \{s_i\}$ di omomorfismi di moduli $s_i\colon C_i \to C'_{i+1}$, $i \in \mathbb{Z}$, tale che*

$$\alpha_i - \beta_i = d'_{i+1}s_i + s_{i-1}d_i.$$

Indichiamo l'omotopia con $\alpha \sim \beta$.

Se $\alpha \sim \beta$, allora $\widetilde{\alpha}_i = \widetilde{\beta}_i$ per i corrispondenti omomorfismi dei moduli di omologia $H_i(C) \to H_i(C')$. Infatti, se $z_i \in Z_i(C)$, allora $\widetilde{\alpha}_i\colon z_i + B_i \mapsto \alpha_i z_i + B'_i$ e $\widetilde{\beta}_i\colon z_i + B_i \mapsto \beta_i z_i + B'_i$. Quindi

$$\begin{aligned}
\widetilde{\alpha}_i(z_i + B_i) &= \alpha_i z_i + B'_i = (\beta_i + d'_{i+1}s_i + s_{i-1}d_i)z_i + B'_i \\
&= (\beta_i z_i + d'_{i+1}s_i z_i) + B'_i = \beta_i z_i + B'_i = \widetilde{\beta}_i(z_i + B_i).
\end{aligned}$$

È chiaro che l'omotopia è una relazione simmetrica e riflessiva fra omomorfismi di catene. È anche transitiva. Infatti, se $\alpha \sim \beta$ è data da s e $\beta \sim \gamma$ da t, allora

$$\begin{aligned}
\alpha_i - \beta_i &= d'_{i+1}s_i + s_{i-1}d_i, \\
\beta_i - \gamma_i &= d'_{i+1}t_i + t_{i-1}d_i.
\end{aligned}$$

Pertanto

$$\alpha_i - \gamma_i = d'_{i+1}(s_i + t_i) + (s_{i-1} + t_{i-1})d_i.$$

Dunque $s + t = \{s_i + t_i\}$ è un'omotopia fra α e γ.

Le omotopie si possono anche moltiplicare. Supponiamo che $\alpha \sim \beta$ per gli omomorfismi di catene da (C, d) a (C', d') e che $\gamma \sim \delta$ per gli omomorfismi di catene da (C', d') a (C'', d''). Allora $\gamma\alpha \sim \delta\beta$. Scriviamo infatti

$$\alpha_i - \beta_i = d'_{i+1}s_i + s_{i-1}d_i,$$
$$\gamma_i - \delta_i = d''_{i+1}t_i + t_{i-1}d'_i.$$

Moltiplicando la prima uguaglianza a sinistra per γ_i e la seconda a destra per β_i, otteniamo, in virtù della (2),

$$\gamma_i\alpha_i - \gamma_i\beta_i = \gamma_i d'_{i+1}s_i + \gamma_i s_{i-1}d_i = d''_{i+1}\gamma_{i+1}s_i + \gamma_i s_{i-1}d_i,$$
$$\gamma_i\beta_i - \delta_i\beta_i = d''_{i+1}t_i\beta_i + t_{i-1}d'_i\beta_i = d''_{i+1}t_i\beta_i + t_{i-1}\beta_{i-1}d_i.$$

Quindi

$$\gamma_i\alpha_i - \delta_i\beta_i = d''_{i+1}(\gamma_{i+1}s_i + t_i\beta_i) + (\gamma_i s_{i-1} + t_{i-1}\beta_{i-1})d_i.$$

Dunque $\gamma\alpha \sim \delta\beta$ mediante $u = \{u_i\}$, dove $u_i = \gamma_{i+1}s_i + t_i\beta_i$.

6.5 Risoluzioni

Nel prossimo paragrafo raggiungeremo il primo obiettivo principale di questo capitolo, la definizione del funtore derivato di un funtore additivo dalla categoria dei moduli su un anello alla categoria dei gruppi abeliani. La definizione si fonda sul concetto di risoluzione di un modulo, che ora esamineremo.

Definizione 6.5. *Sia M un R-modulo. Per* complesso sopra *M intendiamo un complesso positivo $C = (C, d)$ insieme con un omomorfismo $\varepsilon\colon C_0 \to M$, detto* aumentazione*, tale che $\varepsilon d_1 = 0$. Abbiamo così la successione di omomorfismi*

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0, \tag{10}$$

nella quale il prodotto di due omomorfismi consecutivi è zero. Il complesso C, ε sopra M si dice una risoluzione *di M se la (10) è esatta. Ciò equivale ad avere $H_i(C) = 0$ per $i > 0$ e $H_0(C) = C_0/d_1C_1 = C_0/\ker\varepsilon \simeq M$. Un complesso C, ε sopra M si dice* proiettivo *se ciascun C_i è proiettivo.*

Vale il seguente importante teorema.

Teorema 6.3. *Sia C, ε un complesso proiettivo sopra il modulo M, sia C', ε' una risoluzione del modulo M' e sia μ un omomorfismo di M in M'. Esiste allora un omomorfismo di catene α del complesso C nel complesso C' tale che $\mu\varepsilon = \varepsilon'\alpha_0$. Inoltre, due qualsiasi di tali omomorfismi α e β sono omotopi.*

Dimostrazione. La prima affermazione significa che esistono omomorfismi di moduli α_i, $i \geq 0$, che rendono commutativo il diagramma

$$\begin{array}{ccccccccccc}
\cdots \to & C_n & \xrightarrow{d_n} & C_{n-1} & \xrightarrow{d_{n-1}} & C_{n-2} & \to \cdots \to & C_0 & \xrightarrow{\varepsilon} & M & \to 0 \\
& \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \alpha_{n-1}} & & \downarrow{\scriptstyle \alpha_{n-2}} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \mu} & \\
\cdots \to & C'_n & \xrightarrow[d'_n]{} & C'_{n-1} & \xrightarrow[d'_{n-1}]{} & C'_{n-2} & \to \cdots \to & C'_0 & \xrightarrow[\varepsilon']{} & M' & \to 0
\end{array} \tag{11}$$

Poiché C_0 è proiettivo e $C'_0 \xrightarrow{\varepsilon'} M' \to 0$ è esatta, l'omomorfismo $\mu\varepsilon$ di C_0 in M' si può «sollevare» a un omomorfismo $\alpha_0 \colon C_0 \to C'_0$ tale che $\mu\varepsilon = \varepsilon'\alpha_0$. Supponiamo ora di avere già determinato $\alpha_0, \dots, \alpha_{n-1}$ in modo da avere la commutatività della (11) da C_0 a C_{n-1}. Abbiamo $d'_{n-1}\alpha_{n-1}d_n = \alpha_{n-2}d_{n-1}d_n = 0$. Dunque $\alpha_{n-1}d_nC_n \subseteq \ker d'_{n-1} = \operatorname{im} d'_n = d'_nC'_n$. Possiamo sostituire C'_{n-1} con $d'_nC'_n$, per il quale abbiamo la successione esatta $C'_n \to d'_nC'_n \to 0$. Per la proiettività di C_n esiste un omomorfismo $\alpha_n \colon C_n \to C'_n$ tale che $d'_n\alpha_n = \alpha_{n-1}d_n$. Questo passo induttivo dimostra l'esistenza di α. Siano ora α e β due omomorfismi che soddisfano le condizioni richieste. Poniamo $\gamma = \alpha - \beta$. Abbiamo

$$\begin{aligned} \varepsilon'\gamma_0 &= \varepsilon'\alpha_0 - \varepsilon'\beta_0 = \mu\varepsilon - \mu\varepsilon = 0, \\ d'_n\gamma_n &= \gamma_{n-1}d_n, \qquad n \geq 1. \end{aligned}$$

Abbiamo il diagramma

$$\begin{array}{ccccccc} & & & & C_0 & & \\ & & & & \downarrow{\scriptstyle \gamma_0} & & \\ C'_1 & \xrightarrow{d'_1} & C'_0 & \xrightarrow{\varepsilon'} & M' & \longrightarrow & 0 \end{array}$$

Poiché $\varepsilon'\gamma_0 = 0$, si ha $\gamma_0C_0 \subseteq d'_1C'_1$ e otteniamo il diagramma

$$\begin{array}{ccccc} & & C_0 & & \\ & & \downarrow{\scriptstyle \gamma_0} & & \\ C'_1 & \xrightarrow{d'_1} & d'_1C'_1 & \longrightarrow & 0 \end{array}$$

a riga esatta. Come prima, esiste un omomorfismo $s_0 \colon C_0 \to C'_1$ tale che $\gamma_0 = d'_1s_0$. Supponiamo di aver determinato $s_0, \dots, s_{n-1}$ tali che $s_i \colon C_i \to C'_{i+1}$ e

$$\gamma_i = d'_{i+1}s_i + s_{i-1}d_i, \qquad 0 \leq i \leq n-1.$$

Consideriamo $\gamma_n - s_{n-1}d_n$. Abbiamo

$$\begin{aligned} d'_n(\gamma_n - s_{n-1}d_n) &= \gamma_{n-1}d_n - d'_ns_{n-1}d_n \\ &= (\gamma_{n-1} - d'_ns_{n-1})d_n = s_{n-2}d_{n-1}d_n = 0. \end{aligned}$$

Ne segue, come sopra, che esiste un omomorfismo $s_n \colon C_n \to C'_{n+1}$ tale che $d'_{n+1}s_n = \gamma_n - s_{n-1}d_n$. La successione di omomorfismi $s_0, s_1, \dots$ definisce un'omotopia da α a β. Ciò conclude la dimostrazione. □

L'esistenza di una risoluzione proiettiva di un modulo si dimostra facilmente. Anzi, come ora vedremo, esiste una risoluzione (10) di M che è *libera*, nel senso che i moduli C_i sono liberi. Anzitutto rappresentiamo M come immagine omomorfa di un modulo libero C_0. Ciò significa che abbiamo una successione esatta $\ker\varepsilon \xrightarrow{i} C_0 \xrightarrow{\varepsilon} M \to 0$, dove C_0 è libero e i è l'inclusione di $\ker\varepsilon$. Prendiamo poi un modulo libero C_1 e un epimorfismo π di C_1 su $\ker\varepsilon$. Ponendo $d_1 = i\pi \colon C_1 \to C_0$, abbiamo la successione esatta $C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \to 0$. Iterando questo procedimento otteniamo una successione esatta

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

nella quale i C_i sono liberi. Allora (C, d) ed ε costituiscono una risoluzione libera di M.

Tutto ciò si può dualizzare. Definiamo un *complesso sotto* M come una coppia D, η dove D è un complesso di cocatene e η è un omomorfismo $M \to D^0$ tale che $d^0\eta = 0$. Un tale complesso sotto M si dice una *corisoluzione* di M se la successione

$$0 \longrightarrow M \xrightarrow{\eta} D^0 \xrightarrow{d^0} D^1 \xrightarrow{d^1} D^2 \longrightarrow \cdots \tag{12}$$

è esatta. Nel ğ 3.11 (p. 159) abbiamo mostrato che ogni modulo M si può immergere in un modulo iniettivo, ossia che esiste una successione esatta $0 \to M \xrightarrow{\eta} D^0$, con D^0 iniettivo. Questa si prolunga in $0 \to M \to D^0 \xrightarrow{\pi} \operatorname{coker}\eta$, dove $\operatorname{coker}\eta = D^0/\eta M$ e π è l'omomorfismo canonico sul modulo quoziente. Abbiamo poi un monomorfismo η_1 di $\operatorname{coker}\eta$ in un modulo iniettivo D^1, e quindi la successione esatta $0 \to M \xrightarrow{\eta} D^0 \xrightarrow{d^0} D^1$, dove $d^0 = \eta_1\pi$. Proseguendo così, si ottiene una corisoluzione (12) *iniettiva*, nel senso che ogni D^i è iniettivo. Il teorema principale sulle risoluzioni si può dualizzare nel modo seguente.

Teorema 6.4. *Sia (D, η) un complesso iniettivo sotto M, sia (D', η') una corisoluzione di M' e sia λ un omomorfismo di M' in M. Esiste allora un omomorfismo g del complesso D' nel complesso D tale che $\eta\lambda = g^0\eta'$. Inoltre, due qualsiasi di tali omomorfismi sono omotopi.*

Il diagramma della prima affermazione è

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\eta'} & D'^0 & \xrightarrow{d'^0} & D'^1 & \longrightarrow & \cdots \\ & & \lambda\downarrow & & \downarrow g^0 & & & & \\ 0 & \longrightarrow & M & \xrightarrow[\eta]{} & D^0 & \xrightarrow[d^0]{} & D^1 & \longrightarrow & \cdots \end{array}$$

La dimostrazione di questo teorema si ottiene dualizzando l'argomento usato per il teorema 6.3. Lasciamo i particolari al lettore.

6.6 Funtori derivati

Possiamo ora definire i funtori derivati di un funtore additivo F da una categoria R-**mod** alla categoria **Ab**. Sia M un R-modulo e sia

$$0 \longleftarrow M \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \xleftarrow{d_2} \cdots$$

una risoluzione proiettiva di M. Applicando il funtore F otteniamo una successione di omomorfismi di gruppi abeliani

$$0 \longleftarrow FM \xleftarrow{F(\varepsilon)} FC_0 \xleftarrow{F(d_1)} FC_1 \xleftarrow{F(d_2)} \cdots . \tag{13}$$

Poiché $F(0) = 0$ per l'omomorfismo nullo di un modulo in un altro e F è moltiplicativo, il prodotto di due omomorfismi successivi nella (13) è nullo. Dunque $FC = \{FC_i\}$, $F(d) = \{F(d_i)\}$, con l'aumentazione $F\varepsilon$, è un complesso (positivo) sopra FM. Se F è esatto, ossia conserva l'esattezza, la (13) è esatta e i gruppi di omologia $H_i(FC)$ sono nulli per $i \geq 1$. Ciò può non accadere se F non è esatto, e in un certo senso questi gruppi di omologia misurano quanto F si discosti dall'esattezza. In ogni caso poniamo

$$L_nFM = H_n(FC), \qquad n \geq 0. \tag{14}$$

Da questa definizione segue

$$H_0(FC) = FC_0/F(d_1)FC_1, \tag{15}$$

poiché poniamo $FC_i = 0$ per $i < 0$.

Sia M' un secondo R-modulo e supponiamo di aver scelto una sua risoluzione proiettiva $0 \leftarrow M' \xleftarrow{\varepsilon'} C'_0 \xleftarrow{d'_1} C'_1 \leftarrow \cdots$, dalla quale otteniamo i gruppi abeliani $H_n(FC')$, $n \geq 0$. Sia μ un omomorfismo di moduli di M in M'. Abbiamo visto che si può determinare un omomorfismo α

del complesso (C, d) nel complesso (C', d') tale che $\mu\varepsilon = \varepsilon'\alpha_0$. Diciamo che α è un omomorfismo di catene *sopra* l'omomorfismo dato μ. Poiché F è un funtore additivo, abbiamo l'omomorfismo $F(\alpha)$ del complesso FC nel complesso FC' tale che $F(\mu)F(\varepsilon) = F(\varepsilon')F(\alpha_0)$. Si ha dunque il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longleftarrow & FM & \xleftarrow{F(\varepsilon)} & FC_0 & \xleftarrow{F(d_1)} & FC_1 & \longleftarrow & \cdots \\ & & \downarrow{\scriptstyle F(\mu)} & & \downarrow{\scriptstyle F(\alpha_0)} & & \downarrow{\scriptstyle F(\alpha_1)} & & \\ 0 & \longleftarrow & FM' & \xleftarrow{F(\varepsilon')} & FC'_0 & \xleftarrow{F(d'_1)} & FC'_1 & \longleftarrow & \cdots \end{array}$$

Otteniamo allora l'omomorfismo $\widetilde{F(\alpha_n)}$ di $H_n(FC)$ in $H_n(FC')$. Esso è indipendente dalla scelta di α. Infatti, se β è un secondo omomorfismo di C in C' sopra μ, allora β è omotopo ad α, perciò esistono omomorfismi $s_n\colon C_n \to C'_{n+1}$, $n \geq 0$, tali che $\alpha_n - \beta_n = d'_{n+1}s_n + s_{n-1}d_n$. Per l'additività di F, applicando F a tali relazioni si ha

$$F(\alpha_n) - F(\beta_n) = F(d'_{n+1})F(s_n) + F(s_{n-1})F(d_n).$$

Dunque $F(\alpha) \sim F(\beta)$ e quindi $\widetilde{F(\alpha_n)} = \widetilde{F(\beta_n)}$. Definiamo ora $L_nF(\mu) = \widetilde{F(\alpha_n)}$. Un omomorfismo $\mu\colon M \to M'$ determina dunque un omomorfismo $L_nF(\mu)\colon H_n(FC) \to H_n(FC')$. Lasciamo al lettore la verifica che L_nF, definito da

$$\begin{aligned} (L_nF)M &= H_n(FC), \quad M \in \operatorname{ob} R\text{-}\mathbf{mod}, \\ (L_nF)(\mu) &= \widetilde{F(\alpha_n)}, \qquad \mu \in \hom_R(M, M'), \end{aligned}$$

è un funtore additivo da R-**mod** ad **Ab**. Si chiama *n-esimo funtore derivato sinistro* del funtore dato F.

Osserviamo ora che le nostre definizioni sono essenzialmente indipendenti dalla scelta delle risoluzioni. Sia $\bar{C}$ una seconda risoluzione proiettiva di M. Ponendo $\mu = 1$ nel ragionamento precedente, otteniamo un unico isomorfismo η_n di $H_n(FC)$ su $H_n(F\bar{C})$. Analogamente, un'altra scelta $\bar{C}'$ della risoluzione proiettiva di M' dà un unico isomorfismo η'_n di $H_n(FC')$ su $H_n(F\bar{C}')$, e L_nF viene sostituito da $\eta'_n(L_nF)\eta_n^{-1}$.

D'ora in avanti supporremo di aver scelto, per ogni R-modulo M, una particolare risoluzione proiettiva e di servirci di essa per determinare i funtori L_nF. Ci riserviamo tuttavia di passare da una tale risoluzione a un'altra quando sia conveniente.

Consideriamo ora una successione esatta corta $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$. Mostreremo che a tale successione corrispondono omomorfismi di connessione

$$\Delta_n\colon L_nFM'' \longrightarrow L_{n-1}FM', \qquad n \geq 1,$$

tali che la successione

$$0 \longleftarrow L_0FM'' \xleftarrow{L_0F(\beta)} L_0FM \xleftarrow{L_0F(\alpha)} L_0FM' \xleftarrow{\Delta_1} L_1FM'' \longleftarrow \cdots$$

è esatta. A questo scopo ci occorre l'esistenza di risoluzioni proiettive delle successioni esatte corte di omomorfismi di moduli. Per *risoluzione proiettiva di una tale successione* $0 \to M' \to M \to M'' \to 0$ intendiamo risoluzioni proiettive (C', ε'), (C, ε), (C'', ε'') rispettivamente di M', M e M'', insieme con omomorfismi di catene $i\colon C' \to C$, $p\colon C \to C''$ tali che per ogni n sia esatta $0 \to C'_n \to C_n \to C''_n \to 0$ e sia commutativo il diagramma

$$\begin{array}{ccccc} C'_0 & \xrightarrow{i_0} & C_0 & \xrightarrow{p_0} & C''_0 \\ \downarrow{\scriptstyle \varepsilon'} & & \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \varepsilon''} \\ M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' \end{array} \tag{16}$$

Dimostreremo ora l'esistenza di una risoluzione proiettiva per ogni successione esatta corta di moduli $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$. Partiamo da risoluzioni proiettive (C', ε') e (C'', ε'') rispettivamente di M' e M'':

$$\begin{aligned} \cdots \longrightarrow C'_2 \xrightarrow{d'_2} C'_1 \xrightarrow{d'_1} C'_0 \xrightarrow{\varepsilon'} M' \longrightarrow 0, \\ \cdots \longrightarrow C''_2 \xrightarrow{d''_2} C''_1 \xrightarrow{d''_1} C''_0 \xrightarrow{\varepsilon''} M'' \longrightarrow 0. \end{aligned} \tag{17}$$

Poniamo $C_n = C'_n \oplus C''_n$, $i_n x'_n = (x'_n, 0)$ per $x'_n \in C'_n$ e $p_n x_n = x''_n$ per $x_n = (x'_n, x''_n)$, in ogni grado $n \geq 0$. Allora $0 \to C'_n \to C'_n \oplus C''_n \to C''_n \to 0$ è esatta e C_n è proiettivo. Definiamo

$$\varepsilon x_0 = \alpha\varepsilon' x'_0 + \sigma x''_0, \qquad d_n x_n = (d'_n x'_n + \theta_n x''_n, d''_n x''_n),$$

dove $\sigma\colon C''_0 \to M$ e $\theta_n\colon C''_n \to C'_{n-1}$ vanno determinati in modo che (C, ε) sia una risoluzione proiettiva di M che, insieme a (C', ε') e (C'', ε''), costituisca una risoluzione proiettiva della successione esatta $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$.

Abbiamo $\varepsilon i_0 x'_0 = \varepsilon(x'_0, 0) = \alpha\varepsilon' x'_0$. La commutatività del rettangolo sinistro della (16) è pertanto automatica. Inoltre $\varepsilon'' p_0 x_0 = \varepsilon'' x''_0$ e $\beta\varepsilon x_0 = \beta(\alpha\varepsilon' x'_0 + \sigma x''_0) = \beta\sigma x''_0$. Il rettangolo destro della (16) è quindi commutativo se e soltanto se

$$\varepsilon'' = \beta\sigma. \tag{18}$$

Si ha $\varepsilon d_1 x_1 = \varepsilon(d'_1 x'_1 + \theta_1 x''_1, d''_1 x''_1) = \alpha\varepsilon'\theta_1 x''_1 + \sigma d''_1 x''_1$. Dunque $\varepsilon d_1 = 0$ se e soltanto se

$$\alpha\varepsilon'\theta_1 + \sigma d''_1 = 0. \tag{19}$$

Analogamente, la condizione $d_{n-1} d_n = 0$ equivale a

$$d'_{n-1}\theta_n + \theta_{n-1} d''_n = 0. \tag{20}$$

Consideriamo il diagramma

$$\begin{array}{ccccc} & & C''_0 & & \\ & \overset{\sigma}{\swarrow} & \downarrow{\scriptstyle \varepsilon''} & & \\ M & \xrightarrow[\beta]{} & M'' & \longrightarrow & 0 \end{array}$$

Poiché C''_0 è proiettivo, esiste $\sigma\colon C''_0 \to M$ tale che valga la (18). Consideriamo quindi

$$\begin{array}{ccccc} & & C''_1 & & \\ & \overset{\theta_1}{\swarrow} & \downarrow{\scriptstyle -\sigma d''_1} & & \\ C'_0 & \xrightarrow[\alpha\varepsilon']{} & M & \xrightarrow[\beta]{} & M'' \end{array}$$

Poiché $\varepsilon' C'_0 = M'$, la riga è esatta e, poiché C''_1 è proiettivo e $\beta\sigma d''_1 = \varepsilon'' d''_1 = 0$, esiste $\theta_1\colon C''_1 \to C'_0$ tale che valga la (19) (si veda l'esercizio 4, p. 100). Consideriamo poi

$$\begin{array}{ccccc} & & C''_2 & & \\ & \overset{\theta_2}{\swarrow} & \downarrow{\scriptstyle -\theta_1 d''_2} & & \\ C'_1 & \xrightarrow[d'_1]{} & C'_0 & \xrightarrow[\varepsilon']{} & M' \end{array}$$

Anche qui la riga è esatta, C''_2 è proiettivo e $\varepsilon'\theta_1 d''_2 = 0$, poiché $\alpha\varepsilon'\theta_1 d''_2 = -\sigma d''_1 d''_2 = 0$ e $\ker\alpha = 0$. Esiste dunque $\theta_2 \colon C''_2 \to C'_1$ tale che valga la (20) per $n = 2$.[20] Infine lo stesso ragionamento prova per induzione la (20) per $n > 2$, servendosi del diagramma

$$\begin{array}{ccccc} & & C''_n & & \\ & \overset{\theta_n}{\swarrow} & \downarrow{\scriptstyle -\theta_{n-1}d''_n} & & \\ C'_{n-1} & \xrightarrow[d'_{n-1}]{} & C'_{n-2} & \xrightarrow[d'_{n-2}]{} & C'_{n-3} \end{array}$$

Resta da dimostrare che $\cdots \to C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \to 0$ è una risoluzione. A questo scopo consideriamo tale successione di moduli e di omomorfismi come un complesso $\bar{C}$ e, analogamente, i moduli e gli omomorfismi della (17) come complessi $\bar{C}'$ e $\bar{C}''$. Abbiamo allora una successione esatta di complessi $0 \to \bar{C}' \to \bar{C} \to \bar{C}'' \to 0$. Poiché $H_i(\bar{C}') = 0 = H_i(\bar{C}'')$, dalla (4) segue che $H_i(\bar{C}) = 0$. Pertanto $\bar{C}$ fornisce una risoluzione di M che, insieme alle risoluzioni di M' e M'', dà una risoluzione proiettiva di $0 \to M' \to M \to M'' \to 0$.

Possiamo ora dimostrare il seguente teorema.

Teorema 6.5. *Sia F un funtore additivo da R-**mod** ad **Ab**. Per ogni successione esatta corta di R-moduli $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ e per ogni $n = 1, 2, 3, \ldots$ esiste un omomorfismo di connessione $\Delta_n \colon L_nFM'' \to L_{n-1}FM'$ tale che*

$$0 \longleftarrow L_0FM'' \xleftarrow{L_0F(\beta)} L_0FM \xleftarrow{L_0F(\alpha)} L_0FM' \xleftarrow{\Delta_1} L_1FM'' \longleftarrow \cdots \tag{21}$$

sia esatta.

Dimostrazione. Costruiamo una risoluzione proiettiva (C', ε'), (C, ε), (C'', ε''), i, p per la successione esatta corta di moduli data. Per ogni $n \geq 0$ abbiamo la successione esatta corta di moduli proiettivi $0 \to C'_n \xrightarrow{i_n} C_n \xrightarrow{p_n} C''_n \to 0$. Poiché C''_n è proiettivo, questa successione si spezza, e di conseguenza $0 \to FC'_n \xrightarrow{F(i_n)} FC_n \xrightarrow{F(p_n)} FC''_n \to 0$ è esatta spezzata. Abbiamo dunque una successione esatta corta di complessi $0 \to F(C') \xrightarrow{F(i)} F(C) \xrightarrow{F(p)} F(C'') \to 0$. Il teorema segue applicando la successione esatta lunga di omologia a questa successione esatta corta di complessi. □

Quanto abbiamo fatto si può trasportare alle corisoluzioni e si ottengono così la definizione e risultati analoghi per i funtori derivati destri. Ne daremo ora un cenno, lasciando al lettore i particolari.

Sia ancora F un funtore da R-**mod** ad **Ab**. Per un dato R-modulo M scegliamo una corisoluzione iniettiva $0 \to M \xrightarrow{\eta} D^0 \xrightarrow{d^0} D^1 \xrightarrow{d^1} D^2 \to \cdots$. Applicando F, otteniamo

$$0 \longrightarrow FM \xrightarrow{F(\eta)} FD^0 \xrightarrow{F(d^0)} FD^1 \xrightarrow{F(d^1)} FD^2 \longrightarrow \cdots$$

e quindi il complesso $FD = \{FD^i\}$, $F(d) = \{F(d^i)\}$. Poniamo $(R^nF)M = H^n(FD)$, $n \geq 0$. Se M' è un secondo R-modulo e (D', η') una sua corisoluzione, per ogni omomorfismo $\lambda \colon M' \to M$ otteniamo un omomorfismo $R^nF(\lambda) \colon (R^nF)M' \to (R^nF)M$. Si definisce così il *funtore derivato destro* del funtore dato F. Si trasportano a questo caso i risultati ottenuti per i funtori derivati sinistri. In particolare, si ha un analogo della successione esatta lunga del teorema 6.5. Omettiamo i particolari.

[20] A pp. 344–345 dell'originale il codominio di σ è stampato M' anziché M, il primo termine della riga nel diagramma per θ_1 è stampato C'_1 anziché C'_0 e il rinvio per $n = 2$ è alla (19). Qui le notazioni seguono le identità (18)–(20).

Esercizi

1. Dimostrare che, se M è proiettivo, $L_0FM = FM$ e $L_nFM = 0$ per $n > 0$.

2. Dimostrare che, se F è esatto a destra, F e L_0F sono naturalmente equivalenti.

6.7 Ext

In questo paragrafo e nel successivo considereremo i più importanti esempi di funtori derivati. Cominciamo dal funtore controvariante $\hom(-, N)$ definito da un modulo fissato N. Dobbiamo però indicare prima le modifiche che il procedimento precedente richiede quando si passa a funtori additivi controvarianti da R-**mod** ad **Ab**. Un tale funtore è un funtore (covariante) dalla categoria opposta $(R\text{-}\mathbf{mod})^{\mathrm{op}}$ ad **Ab**, e poiché nel passaggio alla categoria opposta si invertono le frecce, bisogna scambiare i ruoli dei moduli iniettivi e proiettivi. Per definire il funtore derivato destro di un funtore controvariante G da R-**mod** ad **Ab** partiamo dunque da una risoluzione proiettiva $0 \leftarrow M \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \leftarrow \cdots$ del modulo dato M. Ne risultano la successione $0 \to GM \xrightarrow{G(\varepsilon)} GC_0 \xrightarrow{G(d_1)} GC_1 \to \cdots$ e il complesso di cocatene $(GC, G(d))$, dove $GC = \{GC_i\}$ e $G(d) = \{G(d_i)\}$. Definiamo $(R^nG)M = H^n(GC)$. In particolare si ha $(R^0G)M = \ker(GC_0 \to GC_1)$. Per ogni $\mu \in \hom_R(M', M)$ otteniamo un omomorfismo $(R^nG)(\mu)\colon (R^nG)M \to (R^nG)M'$ e così otteniamo l'*n-esimo funtore derivato destro* R^nG di G, che è additivo e controvariante. A una successione esatta corta $0 \to M' \to M \to M'' \to 0$ corrisponde la successione esatta lunga di coomologia

$$0 \to R^0GM'' \to R^0GM \to R^0GM' \to R^1GM'' \to R^1GM \to R^1GM' \to \cdots, \tag{22}$$

dove $R^nGM' \to R^{n+1}GM''$ è un omomorfismo di connessione. La dimostrazione è quasi identica a quella del teorema 6.5 e pertanto la omettiamo.

Poniamo ora $G = \hom(-, N)$, il funtore hom controvariante determinato da un R-modulo fissato N. Ricordiamone la definizione. Se $M \in \operatorname{ob} R\text{-}\mathbf{mod}$, allora $\hom(-, N)M = \hom_R(M, N)$ e, se $\alpha \in \hom_R(M, M')$, $\hom(-, N)(\alpha)$ è l'applicazione α^* di $\hom_R(M', N)$ in $\hom_R(M, N)$ che manda ogni β del primo insieme in $\beta\alpha \in \hom_R(M, N)$. Il gruppo $\hom(-, N)M$ è abeliano e α^* è un omomorfismo di gruppi. Dunque $\hom(-, N)$ è additivo. Poiché $(\alpha_1\alpha_2)^* = \alpha_2^*\alpha_1^*$, il funtore $\hom(-, N)$ è controvariante. Ricordiamo inoltre che questo funtore è esatto a sinistra, ossia, se $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ è esatta, è esatta anche $0 \to \hom(M'', N) \xrightarrow{\beta^*} \hom(M, N) \xrightarrow{\alpha^*} \hom(M', N)$ (p. 105).

L'n-esimo funtore derivato destro di $\hom(-, N)$ si indica con $\operatorname{Ext}^n(-, N)$. Il suo valore nel modulo M è $\operatorname{Ext}^n(M, N)$ (o $\operatorname{Ext}^n_R(M, N)$, se si desidera indicare R). Se (C, ε) è una risoluzione proiettiva di M, l'esattezza di $C_1 \to C_0 \xrightarrow{\varepsilon} M \to 0$ implica quella di $0 \to \hom(M, N) \xrightarrow{\varepsilon^*} \hom(C_0, N) \to \hom(C_1, N)$. Poiché $\operatorname{Ext}^0(M, N)$ è il nucleo dell'omomorfismo di $\hom(C_0, N)$ in $\hom(C_1, N)$, è chiaro che

$$\operatorname{Ext}^0(M, N) \cong \hom(M, N) \tag{23}$$

mediante l'applicazione ε^*.

Sia ora $0 \to M' \to M \to M'' \to 0$ una successione esatta corta. Otteniamo allora la successione esatta lunga

$$\begin{aligned} 0 &\to \operatorname{Ext}^0(M'', N) \to \operatorname{Ext}^0(M, N) \to \operatorname{Ext}^0(M', N) \\ &\to \operatorname{Ext}^1(M'', N) \to \operatorname{Ext}^1(M, N) \to \cdots. \end{aligned} \tag{24}$$

Adoperando l'isomorfismo (23), otteniamo un'immersione della successione esatta $0 \to \hom(M'', N) \to \hom(M, N) \to \hom(M', N)$ in una successione esatta lunga

$$\begin{aligned} 0 \to \hom(M'', N) \to \hom(M, N) \to \hom(M', N) \\ \to \operatorname{Ext}^1(M'', N) \to \operatorname{Ext}^1(M, N) \to \cdots . \end{aligned} \tag{25}$$

Possiamo ora dimostrare il seguente teorema.

Teorema 6.6. *Per un modulo M le condizioni seguenti sono equivalenti.*

(1) *M è proiettivo.*

(2) *$\operatorname{Ext}^n(M, N) = 0$ per ogni $n \geq 1$ e ogni modulo N.*

(3) *$\operatorname{Ext}^1(M, N) = 0$ per ogni N.*

Dimostrazione. (1) $\Rightarrow$ (2). Se M è proiettivo, allora $0 \leftarrow M \xleftarrow{1_M} C_0 = M \leftarrow 0 \leftarrow \cdots$ è una risoluzione proiettiva. Il complesso corrispondente per il calcolo di $\operatorname{Ext}^n(M, N)$ è $0 \to \hom(M, N) \to \hom(M, N) \to 0 \to \cdots$. Dunque $\operatorname{Ext}^n(M, N) = 0$ per ogni $n \geq 1$. L'implicazione (2) $\Rightarrow$ (3) è chiara. (3) $\Rightarrow$ (1). Sia M un modulo qualsiasi e sia $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ una successione esatta corta con P proiettivo. La (25) e il fatto che $\operatorname{Ext}^1(P, N) = 0$ danno allora l'esattezza di

$$0 \to \hom(M, N) \to \hom(P, N) \to \hom(K, N) \to \operatorname{Ext}^1(M, N) \to 0. \tag{26}$$

Supponiamo ora $\operatorname{Ext}^1(M, N) = 0$. Abbiamo allora l'esattezza di $0 \to \hom(M, N) \to \hom(P, N) \to \hom(K, N) \to 0$, il che implica che l'applicazione η^* di $\hom(P, N)$ in $\hom(K, N)$ è suriettiva. Prendiamo ora $N = K$. La suriettività di η^* su $\hom(K, K)$ implica che esiste $\zeta \in \hom(P, K)$ tale che $1_K = \zeta\eta$. Ciò implica che la successione esatta corta $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ si spezza. Allora M è un addendo diretto di un modulo proiettivo, perciò M è proiettivo. □

Applicando la successione esatta (24) al caso in cui $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ è esatta, M è arbitrario e P è proiettivo, otteniamo la seguente formula per $\operatorname{Ext}^1(M, N)$:

$$\operatorname{Ext}^1(M, N) = \operatorname{coker} \eta^* = \hom(K, N)/\operatorname{im}(\hom(P, N)). \tag{27}$$

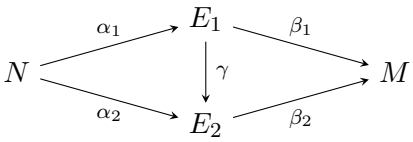
Useremo questa formula per porre in relazione $\operatorname{Ext}^1(M, N)$ con le estensioni del modulo M mediante il modulo N. Da questa connessione deriva il nome Ext del funtore.

Se M e N sono moduli, definiamo un'*estensione di M mediante N* come una successione esatta corta

$$0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0. \tag{28}$$

Per brevità parleremo dell'«estensione E». Due estensioni E_1 ed E_2 si dicono *equivalenti* se esiste un isomorfismo $\gamma\colon E_1 \to E_2$ tale che sia commutativo il diagramma

(29)



Si vede facilmente che, se γ è un omomorfismo dall'estensione E_1 in E_2 che rende commutativo il diagramma (29), allora γ è necessariamente un isomorfismo. L'equivalenza di estensioni è

effettivamente una relazione di equivalenza. È anche chiaro che esistono estensioni di M mediante N. Possiamo infatti costruire l'*estensione spezzata*

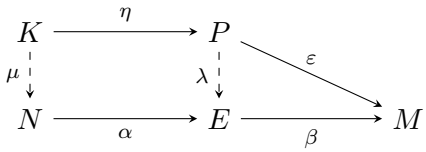
$$0 \to N \xrightarrow{i} M \oplus N \xrightarrow{p} M \to 0, \tag{30}$$

con le consuete i e p.

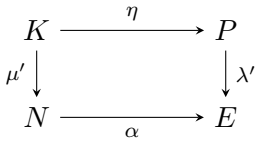
Definiremo ora una biiezione fra la classe $E(M,N)$ delle classi di equivalenza di estensioni di M mediante N e l'insieme $\operatorname{Ext}^1(M,N)$. Più precisamente, definiremo una biiezione di $E(M,N)$ su $\operatorname{coker}\eta^*$, dove $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ è una presentazione proiettiva di M e η^* è la corrispondente applicazione $\hom(P,N) \to \hom(K,N)$, data da $\eta^*(\lambda) = \lambda\eta$. In virtù dell'isomorfismo della (27), si otterrà così la biiezione fra $E(M,N)$ ed $\operatorname{Ext}^1(M,N)$.

Sia $0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0$ un'estensione di M mediante N. Abbiamo allora il diagramma

(31)



senza le frecce tratteggiate. Poiché P è proiettivo, esiste un omomorfismo $\lambda\colon P \to E$ che rende commutativo il triangolo. Scelto così λ, esiste un unico omomorfismo $\mu\colon K \to N$ che rende commutativo il rettangolo. Infatti, se $x \in K$, si ha $\beta\lambda\eta x = \varepsilon\eta x = 0$. Dunque $\lambda\eta x \in \ker\beta$ ed esiste un unico $y \in N$ tale che $\alpha y = \lambda\eta x$. Definiamo μ ponendo $x \mapsto y$. È allora chiaro che μ è un omomorfismo di K in N che rende commutativo il rettangolo e che μ è unico. Sia ora λ' un secondo omomorfismo di P in E tale che $\beta\lambda' = \varepsilon$. Allora $\beta(\lambda' - \lambda) = 0$, il che implica che esiste un omomorfismo $\tau\colon P \to N$ tale che $\lambda' - \lambda = \alpha\tau$. Si ha dunque $\lambda'\eta = (\lambda + \alpha\tau)\eta = \alpha(\mu + \tau\eta)$. Pertanto $\mu' = \mu + \tau\eta$ rende commutativo il diagramma



Poiché $\tau \in \hom(P,N)$, si ha $\tau\eta \in \operatorname{im}\eta^*$. Di conseguenza μ e μ' determinano lo stesso elemento di $\operatorname{coker}\eta^*$ e abbiamo l'applicazione che manda l'estensione E nell'elemento $\mu + \operatorname{im}\eta^*$ di $\operatorname{coker}\eta^*$. Tracciando un diagramma si vede facilmente che sostituendo E con un'estensione equivalente E' si ottiene lo stesso elemento $\mu + \operatorname{im}\eta^*$. Abbiamo quindi un'applicazione di $E(M,N)$ in $\operatorname{coker}\eta^*$.

Viceversa, sia $\mu \in \hom(K,N)$. Formiamo il pushout di η e μ (esercizio 8, p. 37). Esplicitamente, formiamo $N \oplus P$ e sia I il sottomodulo degli elementi $(-\mu(x), \eta(x))$, $x \in K$. Poniamo $E = (N \oplus P)/I$ e sia α l'omomorfismo di N in E tale che $\alpha(y) = (y,0) + I$. Abbiamo inoltre l'omomorfismo di $N \oplus P$ in M dato da $(y,z) \mapsto \varepsilon(z)$, $y \in N$, $z \in P$. Questo manda I in zero e quindi definisce un omomorfismo β di $E = (N \oplus P)/I$ in M tale che $(y,z) + I \mapsto \varepsilon(z)$. Affermiamo che $0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0$ è esatta. In primo luogo, se $\alpha(y) = (y,0) + I = 0$, allora $(y,0) = (-\mu(x), \eta(x))$, $x \in K$, e dunque $\eta(x) = 0$, $x = 0$ e $y = 0$. Perciò α è iniettivo. Si ha poi $\beta\alpha y = \beta((y,0) + I) = \varepsilon(0) = 0$, cosicché $\beta\alpha = 0$. Inoltre, se $\beta((y,z) + I) = 0$, allora $\varepsilon(z) = 0$ e quindi $z = \eta(x)$ per qualche $x \in K$. Si ha dunque $(y,z) + I = (y + \mu(x), 0) + I = \alpha(y + \mu(x))$. Pertanto $\ker\beta = \operatorname{im}\alpha$. Infine β è suriettivo, poiché, se $u \in M$, si ha $u = \varepsilon(z)$ con $z \in P$, e $\beta((0,z) + I) = \varepsilon(z) = u$. Ponendo $\lambda(z) = (0,z) + I$ otteniamo la commutatività del diagramma (31). Ne segue che l'elemento di $\operatorname{coker}\eta^*$ associato alla classe di equivalenza dell'estensione E è $\mu + \operatorname{im}\eta^*$. Ciò mostra che la nostra applicazione è suriettiva. Essa è anche iniettiva. Sia infatti

E una qualsiasi estensione la cui classe abbia per immagine la classe laterale $\mu + \operatorname{im}\eta^*$. Possiamo allora supporre che $E \mapsto \mu$ nell'applicazione originaria che abbiamo definito. Formando il pushout E' di μ e η, otteniamo un'estensione tale che $E' \mapsto \mu$. Ora, poiché E' è un pushout, abbiamo un diagramma commutativo (29) con $E_1 = E'$ ed $E_2 = E$. Dunque E ed E' sono isomorfe. Ciò implica evidentemente l'iniettività.

Enunciamo questo risultato nel modo seguente.

Teorema 6.7. *Esiste una biiezione fra* $\operatorname{Ext}^1(M,N)$ *e l'insieme* $E(M,N)$ *delle classi di equivalenza di estensioni di* M *mediante* N.

Studieremo ora la dipendenza di $\operatorname{Ext}^n(M,N)$ dall'argomento N. Ciò ci porterà a definire un funtore $\operatorname{Ext}^n(M,-)$ e un bifuntore Ext^n. Siano M, N, N' degli R-moduli e sia β un omomorfismo di N in N'. Come prima, sia $C = \{C_i\}$, ε, una risoluzione proiettiva di M. Si ha allora il diagramma

$$\begin{array}{ccccccc} 0 & \longrightarrow & \hom(M,N) & \longrightarrow & \hom(C_0,N) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \hom(M,N') & \longrightarrow & \hom(C_0,N') & \longrightarrow & \cdots \end{array} \tag{32}$$

dove le applicazioni orizzontali sono quelle di prima e le verticali sono le moltiplicazioni a sinistra β_L per β. È chiaro che il diagramma (32) è commutativo. Abbiamo quindi omomorfismi dal complesso $\hom(C,N)$ nel complesso $\hom(C,N')$ e, di conseguenza, per ogni $n \geq 0$ abbiamo un omomorfismo $\widetilde{\beta}^n$ fra i gruppi di coomologia corrispondenti. Si ha dunque l'omomorfismo $\widetilde{\beta}^n\colon \operatorname{Ext}^n(M,N) \to \operatorname{Ext}^n(M,N')$. È chiaro che ciò definisce un funtore additivo e covariante $\operatorname{Ext}^n(M,-)$ da R-**mod** ad **Ab**.

Se $\alpha \in \hom(M',M)$, si ha il diagramma commutativo

$$\begin{array}{ccc} \hom(M,N) & \longrightarrow & \hom(M',N) \\ \downarrow & & \downarrow \\ \hom(M,N') & \longrightarrow & \hom(M',N') \end{array}$$

da cui si ottiene il diagramma commutativo

$$\begin{array}{ccc} \operatorname{Ext}^n(M,N) & \longrightarrow & \operatorname{Ext}^n(M',N) \\ \downarrow & & \downarrow \\ \operatorname{Ext}^n(M,N') & \longrightarrow & \operatorname{Ext}^n(M',N') \end{array}$$

Ne segue, come nel caso del funtore hom, che si può definire un bifuntore Ext^n da R-**mod** ad **Ab** (p. 38).

Supponiamo ora di avere una successione esatta corta $0 \to N' \to N \to N'' \to 0$. Come nella (32), abbiamo la successione di omomorfismi di complessi $\hom(C,N') \to \hom(C,N) \to \hom(C,N'')$. Poiché C_i è proiettivo e $0 \to N' \to N \to N'' \to 0$ è esatta, la successione $0 \to \hom(C_i,N') \to \hom(C_i,N) \to \hom(C_i,N'') \to 0$ è esatta per ogni i. Dunque $0 \to \hom(C,N') \to \hom(C,N) \to \hom(C,N'') \to 0$ è esatta. Possiamo quindi applicare il teorema 6.1 e l'isomorfismo di $\hom(M,N)$ con $\operatorname{Ext}^0(M,N)$ per ottenere una seconda successione esatta lunga di funtori Ext:

$$\begin{aligned} &0 \to \hom(M,N') \to \hom(M,N) \to \hom(M,N'') \to \operatorname{Ext}^1(M,N') \\ &\quad \to \operatorname{Ext}^1(M,N) \to \operatorname{Ext}^1(M,N'') \to \cdots . \end{aligned} \tag{33}$$

Chiameremo le due successioni (24) e (33) rispettivamente *successione esatta lunga nella prima variabile* e *nella seconda variabile* per Ext.

Possiamo ora dimostrare il seguente analogo della caratterizzazione dei moduli proiettivi data nel teorema 6.6.

Teorema 6.8. *Per un modulo N le condizioni seguenti sono equivalenti.*

(1) *N è iniettivo.*

(2) $\mathrm{Ext}^n(M,N)=0$ *per ogni $n\geq 1$ e ogni modulo M.*

(3) $\mathrm{Ext}^1(M,N)=0$ *per ogni M.*

Dimostrazione. (1) $\Rightarrow$ (2). Se N è iniettivo, l'esattezza di $0\leftarrow M\leftarrow C_0\leftarrow C_1\leftarrow\cdots$ implica quella di $0\to\hom(M,N)\to\hom(C_0,N)\to\hom(C_1,N)\to\cdots$. Ne segue $\mathrm{Ext}^n(M,N)=0$ per ogni $n\geq 1$. L'implicazione (2) $\Rightarrow$ (3) è immediata e la (3) $\Rightarrow$ (1) si ottiene come nella dimostrazione del teorema 6.6, servendosi di una successione esatta corta $0\to N\to Q\to L\to 0$ con Q iniettivo. Lasciamo al lettore il compito di completare il ragionamento. □

I funtori $\mathrm{Ext}^n(M,-)$ che abbiamo definito partendo dai funtori $\mathrm{Ext}^n(-,N)$ si possono anche definire direttamente come funtori derivati destri di $\hom(M,-)$. Per il momento indichiamo con $\overline{\mathrm{Ext}}^n(M,N)$ il valore di questo funtore nel modulo N. Per determinare questo gruppo scegliamo una corisoluzione iniettiva $0\to N\xrightarrow{\eta} D^0\xrightarrow{d^0} D^1\to\cdots$ e otteniamo il complesso di cocatene $\hom(M,D)\colon 0\to\hom(M,D^0)\to\hom(M,D^1)\to\cdots$. Allora $\overline{\mathrm{Ext}}^n(M,N)$ è l'n-esimo gruppo di coomologia di $\hom(M,D)$. I risultati ottenuti per Ext si stabiliscono facilmente per $\overline{\mathrm{Ext}}$. In particolare, si può dimostrare che $\overline{\mathrm{Ext}}^0(M,N)\cong\hom(M,N)$ e si hanno per $\overline{\mathrm{Ext}}$ le due successioni esatte lunghe analoghe alle (24) e (33). Omettiamo le dimostrazioni di questi risultati. Si può ora dimostrare che i bifuntori Ext^n e $\overline{\mathrm{Ext}}^n$ sono naturalmente equivalenti. Non lo dimostreremo e ci limiteremo a provare il risultato più debole che segue.

Teorema 6.9. $\mathrm{Ext}^n(M,N)\cong\overline{\mathrm{Ext}}^n(M,N)$ *per ogni n, M e N.*

Dimostrazione. Se $n=0$, abbiamo $\mathrm{Ext}^0(M,N)\cong\hom(M,N)\cong\overline{\mathrm{Ext}}^0(M,N)$. Sia ora $0\to K\to P\to M\to 0$ una successione esatta corta con P proiettivo. Usando la successione esatta lunga nella prima variabile per $\overline{\mathrm{Ext}}$ e la relazione $\overline{\mathrm{Ext}}^1(P,N)=0$, otteniamo la successione esatta $0\to\hom(M,N)\to\hom(P,N)\to\hom(K,N)\to\overline{\mathrm{Ext}}^1(M,N)\to 0$. Ciò implica che $\overline{\mathrm{Ext}}^1(M,N)\cong\hom(K,N)/\operatorname{im}\hom(P,N)$. Nella (27) abbiamo mostrato che $\mathrm{Ext}^1(M,N)\cong\hom(K,N)/\operatorname{im}\hom(P,N)$. Pertanto $\mathrm{Ext}^1(M,N)\cong\overline{\mathrm{Ext}}^1(M,N)$. Sia ora $n>1$ e supponiamo valido il risultato per $n-1$. Ricorriamo di nuovo alla successione esatta lunga nella prima variabile per Ext e otteniamo

$$0=\mathrm{Ext}^{n-1}(P,N)\to\mathrm{Ext}^{n-1}(K,N)\to\mathrm{Ext}^n(M,N)\to\mathrm{Ext}^n(P,N)=0,$$

da cui deduciamo che $\mathrm{Ext}^n(M,N)\cong\mathrm{Ext}^{n-1}(K,N)$. Quindi $\mathrm{Ext}^n(M,N)\cong\mathrm{Ext}^{n-1}(K,N)\cong\overline{\mathrm{Ext}}^{n-1}(K,N)$. Lo stesso ragionamento dà $\overline{\mathrm{Ext}}^n(M,N)\cong\overline{\mathrm{Ext}}^{n-1}(K,N)$. Pertanto $\mathrm{Ext}^n(M,N)\cong\overline{\mathrm{Ext}}^n(M,N)$. □

Esercizi

1. Sia $R=D$ un dominio commutativo a ideali principali. Sia $M=D/(a)$, cosicché si ha la presentazione proiettiva $0\to D\to D\to M\to 0$ in cui la prima applicazione è la moltiplicazione per a e la seconda è l'omomorfismo canonico sul modulo quoziente. Usare la (27) e l'isomorfismo di $\hom_D(D,N)$ con N che manda η in $\eta 1$ per dimostrare che $\mathrm{Ext}^1(M,N)\cong N/aN$. Dimostrare che, se $N=D/(b)$, si ha $\mathrm{Ext}^1(M,N)\cong D/(a,b)$, dove (a,b) è un massimo comun divisore di a e b. Usare questi risultati e il teorema fondamentale

di struttura dei moduli finitamente generati su un dominio a ideali principali (BAI, p. 187) per ottenere una formula per $\mathrm{Ext}^1(M,N)$ per due moduli finitamente generati qualsiasi su D.

2. Dimostrare l'equivalenza di $\mathrm{Ext}^n(M,-)$ e $\overline{\mathrm{Ext}}^n(M,-)$.

3. Dimostrare che, nella corrispondenza del teorema 6.7 fra le classi di equivalenza di estensioni di M mediante N e l'insieme $\mathrm{Ext}^1(M,N)$, la classe di equivalenza dell'estensione spezzata corrisponde all'elemento 0 di $\mathrm{Ext}^1(M,N)$.

4. Siano $N \xrightarrow{\alpha_i} E_i \xrightarrow{\beta_i} M$, $i = 1, 2$, due estensioni di M mediante N. Formare $E_1 \oplus E_2$ e sia F il suo sottomodulo costituito dalle coppie (z_1, z_2), $z_i \in E_i$, tali che $\beta_1 z_1 = \beta_2 z_2$. Sia K il sottoinsieme di $E_1 \oplus E_2$ degli elementi della forma $(\alpha_1 y, -\alpha_2 y)$, $y \in N$. Osservare che K è un sottomodulo di F. Porre $E = F/K$ e definire applicazioni $\alpha\colon N \to E$, $\beta\colon E \to M$ mediante

$$\alpha y = (\alpha_1 y, 0) + K = (0, \alpha_2 y) + K, \qquad \beta((z_1, z_2) + K) = \beta_1 z_1 = \beta_2 z_2.$$

Nell'originale compare $(0, -\alpha_2 y) + K$; il segno positivo qui riportato segue dalla definizione di K. Dimostrare che α e β sono omomorfismi di moduli e che $0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0$ è esatta, cosicché abbiamo un'estensione di M mediante N. Essa si chiama *somma di Baer* delle estensioni $N \xrightarrow{\alpha_i} E_i \xrightarrow{\beta_i} M$. Dimostrare che l'elemento di $\mathrm{Ext}^1(M,N)$ corrispondente alla somma di Baer è la somma degli elementi corrispondenti alle estensioni date. Usare questo fatto e l'esercizio 3 per concludere che le classi di equivalenza di estensioni di M mediante N formano un gruppo rispetto alla composizione data dalla somma di Baer, con elemento zero la classe dell'estensione spezzata.

6.8 Tor

Se $M \in \mathbf{mod}\text{-}R$, la categoria dei moduli destri sull'anello R, allora $M \otimes_R$ è il funtore da R-**mod** ad **Ab** che manda un R-modulo sinistro N nel gruppo $M \otimes_R N$ e un elemento η di $\hom_R(N, N')$ in $1 \otimes \eta$. Il funtore $M \otimes_R$ è additivo ed esatto a destra. La seconda condizione significa che, se $N' \to N \to N'' \to 0$ è esatta, anche $M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$ è esatta. L'n-esimo funtore derivato sinistro di $M\otimes$ $(= M \otimes_R)$ si indica con $\mathrm{Tor}_n(M, -)$ (o $\mathrm{Tor}_n^R(M, -)$). Per ottenere $\mathrm{Tor}_n(M,N)$ scegliamo una risoluzione proiettiva $0 \leftarrow N \xleftarrow{\varepsilon} C_0 \leftarrow \cdots$ di N e formiamo il complesso di catene $M \otimes C = \{M \otimes C_i\}$. Allora $\mathrm{Tor}_n(M,N)$ è l'n-esimo gruppo di omologia $H_n(M \otimes C)$ di $M \otimes C$. Per definizione, $\mathrm{Tor}_0(M,N) = (M \otimes C_0)/\operatorname{im}(M \otimes C_1)$. Poiché $M\otimes$ è esatto a destra, la successione $M \otimes C_1 \to M \otimes C_0 \to M \otimes N \to 0$ è esatta e dunque

$$M \otimes N \cong (M \otimes C_0)/\operatorname{im}(M \otimes C_1) = \mathrm{Tor}_0(M,N).$$

L'isomorfismo $\mathrm{Tor}_0(M,N) \cong M \otimes N$ e la successione esatta lunga di omologia implicano che, se $0 \to N' \to N \to N'' \to 0$ è esatta, è esatta anche

$$\begin{aligned} 0 \leftarrow M \otimes N'' \leftarrow M \otimes N \leftarrow M \otimes N' &\leftarrow \mathrm{Tor}_1(M, N'') \\ &\leftarrow \mathrm{Tor}_1(M,N) \leftarrow \cdots . \end{aligned} \tag{34}$$

Ricordiamo che un modulo destro M è piatto se e solo se il funtore tensoriale $M\otimes$ dalla categoria dei moduli sinistri alla categoria dei gruppi abeliani è esatto (p. 154). Possiamo ora caratterizzare la piattezza mediante il funtore Tor. Il risultato è il seguente analogo del teorema 6.6 sul funtore Ext.

Teorema 6.10. *Per un modulo destro M le condizioni seguenti sono equivalenti.*

1. *M è piatto.*
2. *$\mathrm{Tor}_n(M,N)=0$ per ogni $n\geq 1$ e ogni modulo (sinistro) N.*
3. *$\mathrm{Tor}_1(M,N)=0$ per ogni N.*

Dimostrazione. (1) implica (2). Se M è piatto e $0\leftarrow N\leftarrow C_0\leftarrow C_1\leftarrow\cdots$ è una risoluzione proiettiva di N, allora $0\leftarrow M\otimes N\leftarrow M\otimes C_0\leftarrow M\otimes C_1\leftarrow\cdots$ è esatta. Perciò $\mathrm{Tor}_n(M,N)=0$ per ogni $n\geq 1$. È chiaro che (2) implica (3). Infine (3) implica (1). Sia esatta $0\to N'\to N\to N''\to 0$. Allora l'ipotesi $\mathrm{Tor}_1(M,N'')=0$ implica che $0\to M\otimes N'\to M\otimes N\to M\otimes N''\to 0$ è esatta. Quindi M è piatto. □

Consideriamo ora la dipendenza di $\mathrm{Tor}_n(M,N)$ da M. Il ragionamento è identico a quello usato per Ext^n. Sia α un omomorfismo del modulo destro M nel modulo destro M' e sia, come prima, $0\leftarrow N\leftarrow C_0\leftarrow C_1\leftarrow\cdots$ una risoluzione proiettiva del modulo sinistro N. Si ha il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \leftarrow & M\otimes N & \leftarrow & M\otimes C_0 & \leftarrow & M\otimes C_1 & \leftarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \leftarrow & M'\otimes N & \leftarrow & M'\otimes C_0 & \leftarrow & M'\otimes C_1 & \leftarrow & \cdots \end{array} \tag{35}$$

in cui le applicazioni verticali sono $\alpha\otimes 1_N, \alpha\otimes 1_{C_0}, \alpha\otimes 1_{C_1},\ldots$. Dunque abbiamo un omomorfismo del complesso $\{M\otimes C_i\}$ nel complesso $\{M'\otimes C_i\}$ e un corrispondente omomorfismo del gruppo di omologia $\mathrm{Tor}_n(M,N)$ in $\mathrm{Tor}_n(M',N)$. In questo modo otteniamo un funtore $\mathrm{Tor}_n(-,N)$ da **mod**-R, la categoria dei moduli destri su R, alla categoria **Ab**, additivo e covariante.

Supponiamo ora di avere una successione esatta corta di moduli destri $0\to M'\to M\to M''\to 0$ e sia C,ε, come prima, una risoluzione proiettiva del modulo sinistro N. Poiché i C_i sono proiettivi, $0\to M'\otimes C_i\to M\otimes C_i\to M''\otimes C_i\to 0$ è esatta per ogni i. Per il teorema 6.1 e per l'isomorfismo di $\mathrm{Tor}_0(M,N)$ con $M\otimes N$, otteniamo quindi la successione esatta lunga di Tor nella prima variabile:

$$\begin{aligned} 0\leftarrow M''\otimes N\leftarrow M\otimes N\leftarrow M'\otimes N\leftarrow{}& \\ \mathrm{Tor}_1(M'',N)\leftarrow \mathrm{Tor}_1(M,N)\leftarrow{}& \mathrm{Tor}_1(M',N)\leftarrow\cdots . \end{aligned} \tag{36}$$

Osserviamo infine che, come per Ext, possiamo definire funtori $\overline{\mathrm{Tor}}_n(M,N)$ usando una risoluzione proiettiva del primo argomento M. Inoltre si può dimostrare che $\mathrm{Tor}_n(M,N)\cong\overline{\mathrm{Tor}}_n(M,N)$. Il ragionamento è simile a quello svolto per Ext e $\overline{\mathrm{Ext}}$ ed è lasciato al lettore.

Esercizi.

1. Determinare $\mathrm{Tor}_1^{\mathbb{Z}}(M,N)$ se M,N sono gruppi ciclici.
2. Mostrare che $\mathrm{Tor}_1^{\mathbb{Z}}(M,N)$ è un gruppo di torsione per ogni coppia di gruppi abeliani M,N.

6.9 Coomologia dei gruppi

Nel resto del capitolo esamineremo alcuni dei più importanti casi particolari dell'algebra omologica, insieme con le loro applicazioni a problemi classici, alcuni dei quali diedero impulso allo sviluppo della teoria astratta.

Cominciamo con la coomologia dei gruppi. Daremo dapprima la definizione originaria dei gruppi di coomologia di un gruppo, che, a differenza della definizione dei funtori derivati, è del tutto concreta. Ci occorre la nozione di G-modulo, strettamente connessa con una nozione fondamentale della teoria delle rappresentazioni dei gruppi. Se G è un gruppo, un *G-modulo* A è un gruppo abeliano (scritto additivamente) su cui G agisce mediante endomorfismi. Ciò significa che abbiamo un'applicazione

$$(g, x) \longmapsto gx \tag{37}$$

di $G \times A$ in A tale che

$$\begin{aligned} g(x+y) &= gx + gy, \\ (g_1 g_2)x &= g_1(g_2 x), \\ 1x &= x \end{aligned} \tag{38}$$

per $g, g_1, g_2 \in G$ e $x, y \in A$. Come nella teoria delle rappresentazioni, possiamo ricondurci a una nozione più familiare introducendo l'anello del gruppo $\mathbb{Z}[G]$, che è il $\mathbb{Z}$-modulo libero di base G, con moltiplicazione definita da

$$\left(\sum_g \alpha_g g\right)\left(\sum_h \beta_h h\right) = \sum_{g,h} \alpha_g \beta_h gh, \tag{39}$$

dove $\alpha_g, \beta_h \in \mathbb{Z}$. Se A è un G-modulo, diventa uno $\mathbb{Z}[G]$-modulo ponendo

$$\left(\sum_g \alpha_g g\right) x = \sum_g \alpha_g (gx). \tag{40}$$

La verifica è immediata ed è lasciata al lettore. Viceversa, se A è uno $\mathbb{Z}[G]$-modulo, diventa un G-modulo ponendo $gx = (1g)x$.

Un caso particolare di G-modulo si ottiene prendendo per A un qualsiasi gruppo abeliano e ponendo $gx = x$ per ogni $g \in G$, $x \in A$. Questa azione di G si chiama *azione banale*. Un altro esempio è il *G-modulo regolare* $A = \mathbb{Z}[G]$, in cui l'azione è $h(\sum_g \alpha_g g) = \sum_g \alpha_g hg$.

Sia ora A un G-modulo. Per $n = 0, 1, 2, 3, \ldots$ indichiamo con $C^n(G, A)$ l'insieme delle funzioni di n variabili in G con valori nel modulo A. Dunque, se $n > 0$, $C^n(G, A)$ è l'insieme delle applicazioni di $G \times G \times \cdots \times G$ in A, e se $n = 0$ un'applicazione si riduce a un elemento di A. L'insieme $C^n(G, A)$ è un gruppo abeliano con le consuete definizioni di addizione e di zero. Per $f, f' \in C^n(G, A)$ si ha

$$\begin{aligned} (f + f')(g_1, \ldots, g_n) &= f(g_1, \ldots, g_n) + f'(g_1, \ldots, g_n), \\ 0(g_1, \ldots, g_n) &= 0. \end{aligned}$$

Nel caso $C^0(G, A) = A$ la struttura di gruppo è quella di A.

Definiamo ora un'applicazione δ $(= \delta_n)$ di $C^n(G, A)$ in $C^{n+1}(G, A)$. Per $f \in C^n(G, A)$ definiamo δf mediante

$$\begin{aligned} (\delta f)(g_1, \ldots, g_{n+1}) &= g_1 f(g_2, \ldots, g_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n). \end{aligned} \tag{41}$$

Per $n = 0$, f è un elemento di A e

$$(\delta f)(g_1) = g_1 f - f. \tag{42}$$

Per $n = 1$ si ha

$$(\delta f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1), \tag{43}$$

e per $n = 2$

$$(\delta f)(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2). \tag{44}$$

È chiaro che δ è un omomorfismo di $C^n(G, A)$ in $C^{n+1}(G, A)$. Indichiamo con $Z^n(G, A)$ il suo nucleo e con $B^{n+1}(G, A)$ la sua immagine in $C^{n+1}(G, A)$. Si può verificare che $\delta^2 f = 0$ per ogni $f \in C^n(G, A)$. Tralasciamo il calcolo, poiché l'uguaglianza si dedurrà più semplicemente da un risultato che vedremo fra poco. Da $\delta(\delta f) = 0$ segue $Z^n(G, A) \supseteq B^n(G, A)$. Possiamo perciò formare il gruppo quoziente $H^n(G, A) = Z^n(G, A)/B^n(G, A)$, detto *n-esimo gruppo di coomologia di G a coefficienti in A*.

La definizione precedente è concreta ma un po' artificiosa. I casi particolari $H^1(G, A)$ e $H^2(G, A)$ sono emersi nello studio di alcune questioni naturali della teoria dei gruppi, che esamineremo nel prossimo paragrafo. La definizione generale è stata suggerita da questi casi particolari e dalla definizione dei gruppi di coomologia di un complesso simpliciale. Daremo ora un'altra definizione di $H^n(G, A)$, di carattere funtoriale. A tale scopo consideriamo $\mathbb{Z}$ come G-modulo banale e, per un dato G-modulo A, consideriamo $\mathrm{Ext}^n(\mathbb{Z}, A)$. Otteniamo una particolare realizzazione di questo gruppo scegliendo una risoluzione proiettiva

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \longleftarrow \cdots \tag{45}$$

di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo banale. Si ottiene il complesso di cocatene

$$0 \longrightarrow \hom(C_0, A) \longrightarrow \hom(C_1, A) \longrightarrow \cdots, \tag{46}$$

il cui n-esimo gruppo di omologia è una realizzazione di $\mathrm{Ext}^n(\mathbb{Z}, A)$.

Costruiremo ora la particolare risoluzione proiettiva (45) che ci permetterà di identificare $\mathrm{Ext}^n(\mathbb{Z}, A)$ con l'n-esimo gruppo di coomologia $H^n(G, A)$ definito sopra. Poniamo

$$C_n = \underbrace{\mathbb{Z}[G] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[G]}_{n+1 \text{ fattori}}. \tag{47}$$

Poiché $\mathbb{Z}[G]$ è uno $\mathbb{Z}$-modulo libero di base G, C_n è uno $\mathbb{Z}$-modulo libero di base $g_0 \otimes g_1 \otimes \cdots \otimes g_n$, $g_i \in G$. Su C_n è definita un'azione di G mediante

$$g(x_0 \otimes \cdots \otimes x_n) = g x_0 \otimes x_1 \otimes \cdots \otimes x_n, \tag{48}$$

che fa di C_n uno $\mathbb{Z}[G]$-modulo libero con base

$$(g_1, \ldots, g_n) \equiv 1 \otimes g_1 \otimes \cdots \otimes g_n, \qquad g_i \in G. \tag{49}$$

Definiamo uno $\mathbb{Z}[G]$-omomorfismo d_n di C_n in C_{n-1} specificandone l'azione sulla base $\{(g_1, \ldots, g_n)\}$:

$$\begin{aligned} d_n(g_1, \ldots, g_n) &= g_1(g_2, \ldots, g_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i (g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_n) \\ &\quad + (-1)^n (g_1, \ldots, g_{n-1}). \end{aligned} \tag{50}$$

Per $n = 1$ si intende $d_1(g_1) = g_1 - 1 \in C_0 = \mathbb{Z}[G]$. Definiamo anche uno $\mathbb{Z}[G]$-omomorfismo ε di C_0 in $\mathbb{Z}$ ponendo $\varepsilon(1) = 1$. Allora $\varepsilon(g) = \varepsilon(g1) = g1 = 1$ e $\varepsilon(\sum_g \alpha_g g) = \sum_g \alpha_g$. Mostriamo che $0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \leftarrow \cdots$ è una risoluzione proiettiva di $\mathbb{Z}$. Poiché i C_i sono $\mathbb{Z}[G]$-moduli liberi, la proiettività è evidente. Rimane da provare l'esattezza della successione di $\mathbb{Z}[G]$-omomorfismi. A tale scopo definiamo una successione di *omomorfismi di contrazione*

$$\mathbb{Z} \xrightarrow{s_{-1}} C_0 \xrightarrow{s_0} C_1 \xrightarrow{s_1} C_2 \longrightarrow \cdots .$$

Con ciò intendiamo che gli s_i sono omomorfismi di gruppi tali che

$$\begin{aligned} \varepsilon s_{-1} = 1_{\mathbb{Z}}, \qquad & d_1 s_0 + s_{-1}\varepsilon = 1_{C_0}, \\ & d_{n+1}s_n + s_{n-1}d_n = 1_{C_n} \qquad (n \geq 1). \end{aligned} \tag{51}$$

Osserviamo che $\{1\}$ è una $\mathbb{Z}$-base di $\mathbb{Z}$, G è una $\mathbb{Z}$-base di $C_0 = \mathbb{Z}[G]$ e $\{g_0(g_1, \ldots, g_n) = g_0 \otimes g_1 \otimes \cdots \otimes g_n \mid g_i \in G\}$ è una $\mathbb{Z}$-base di C_n per $n \geq 1$. Vi sono perciò unici omomorfismi di gruppi $s_{-1} \colon \mathbb{Z} \to C_0$, $s_n \colon C_n \to C_{n+1}$ tali che

$$\begin{aligned} s_{-1}1 = 1, \qquad & s_0 g_0 = (g_0), \\ s_n g_0(g_1, \ldots, g_n) = (g_0, g_1, \ldots, g_n) \qquad & (n > 0). \end{aligned} \tag{52}$$

Se $n > 0$, abbiamo

$$\begin{aligned} d_{n+1}s_n g_0(g_1, \ldots, g_n) &= d_{n+1}(g_0, g_1, \ldots, g_n) \\ &= g_0(g_1, \ldots, g_n) \\ &\quad + \sum_{i=0}^{n-1} (-1)^{i+1}(g_0, \ldots, g_i g_{i+1}, \ldots, g_n) \\ &\quad + (-1)^{n+1}(g_0, \ldots, g_{n-1}), \end{aligned}$$

e

$$\begin{aligned} s_{n-1}d_n g_0(g_1, \ldots, g_n) &= s_{n-1}g_0 d_n(g_1, \ldots, g_n) \\ &= s_{n-1}g_0 g_1(g_2, \ldots, g_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i s_{n-1}g_0(g_1, \ldots, g_i g_{i+1}, \ldots, g_n) \\ &\quad + (-1)^n s_{n-1}g_0(g_1, \ldots, g_{n-1}) \\ &= (g_0 g_1, g_2, \ldots, g_n) \\ &\quad + \sum_{i=1}^{n-1} (-1)^i (g_0, g_1, \ldots, g_i g_{i+1}, \ldots, g_n) \\ &\quad + (-1)^n (g_0, g_1, \ldots, g_{n-1}). \end{aligned}$$

Dunque $d_{n+1}s_n g_0(g_1, \ldots, g_n) + s_{n-1}d_n g_0(g_1, \ldots, g_n) = g_0(g_1, \ldots, g_n)$. Questo dimostra la terza uguaglianza in (51). Le altre due si verificano in modo analogo.

Possiamo ora mostrare che gli $\mathbb{Z}[G]$-omomorfismi ε, d_n soddisfano $\varepsilon d_1 = 0$, $d_n d_{n+1} = 0$ per $n \geq 1$. Per (49), C_1 è libero di base $\{(g) = 1 \otimes g \mid g \in G\}$. Poiché $\varepsilon d_1(g) = \varepsilon(g - 1) = 1 - 1 = 0$, vale la prima uguaglianza. Ponendo $\varepsilon = d_0$, abbiamo quindi $d_n d_{n+1} = 0$ per $n = 0$. Osserviamo inoltre che per $n > 0$ l'immagine $s_n C_n$ contiene l'insieme dei generatori $\{(g_0, g_1, \ldots, g_n)\}$ di C_{n+1} come $\mathbb{Z}[G]$-modulo. Basta dunque mostrare che $d_n d_{n+1} s_n = 0$ per $n > 0$, e possiamo supporre $d_{n-1}d_n = 0$. Allora

$$\begin{aligned} d_n d_{n+1} s_n &= d_n(1 - s_{n-1}d_n) = d_n - (1 - s_{n-2}d_{n-1})d_n \\ &= s_{n-2}d_{n-1}d_n = 0. \end{aligned}$$

Possiamo considerare (45) come uno $\mathbb{Z}$-complesso e la successione $s_{-1}, s_0, s_1, \ldots$ come un'omotopia fra l'omomorfismo di catene del complesso in sé che è l'identità su ogni C_i e l'omomorfismo di catene nullo su ogni C_i. Questi due omomorfismi di catene inducono gli stessi omomorfismi sui gruppi di omologia. Ne segue che i gruppi di omologia dello $\mathbb{Z}$-complesso (45) sono tutti nulli. Ciò significa che (45) è esatta, e abbiamo così provato il teorema seguente.

Teorema 6.11. *Sia $C_n = \mathbb{Z}[G] \otimes \cdots \otimes \mathbb{Z}[G]$ (con $n+1$ fattori), $n \geq 0$, e siano $\varepsilon\colon C_0 \to \mathbb{Z}$ lo $\mathbb{Z}[G]$-omomorfismo tale che $\varepsilon 1 = 1$ e $d_n\colon C_n \to C_{n-1}$ lo $\mathbb{Z}[G]$-omomorfismo definito da (50). Allora $C = \{C_n\}$, insieme con ε, costituisce una risoluzione libera di $\mathbb{Z}$ considerato come G-modulo banale.*

Per calcolare $\mathrm{Ext}^n(\mathbb{Z}, A)$ per un qualsiasi $\mathbb{Z}[G]$-modulo A, possiamo servirci della risoluzione C, ε. Allora $\mathrm{Ext}^n(\mathbb{Z}, A)$ è l'n-esimo gruppo di omologia del complesso

$$0 \longrightarrow \hom(C_0, A) \longrightarrow \hom(C_1, A) \longrightarrow \cdots . \tag{53}$$

Poiché $\{(g_1, \ldots, g_n) \mid g_i \in G\}$ è una $\mathbb{Z}[G]$-base di C_n, abbiamo una biiezione di $\hom(C_n, A)$ sull'insieme $C^n(G, A)$ delle funzioni di n variabili in G a valori in A. Essa associa a ogni $f \in \hom(C_n, A)$ la sua restrizione alla base $\{(g_1, \ldots, g_n)\}$. L'applicazione $\hom(C_n, A) \to \hom(C_{n+1}, A)$ è la moltiplicazione a destra per d_{n+1}. Ossia, se f è uno $\mathbb{Z}[G]$-omomorfismo di C_n in A, la sua immagine è l'omomorfismo $x \mapsto f(d_{n+1}x)$. Prendendo per x l'elemento $(g_1, \ldots, g_{n+1})$ di C_{n+1}, questa applicazione manda $(g_1, \ldots, g_{n+1})$ in

$$\begin{aligned} f\Big(g_1(g_2, \ldots, g_{n+1}) &+ \sum_{i=1}^{n} (-1)^i (g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1}(g_1, \ldots, g_n)\Big) \\ = g_1 f(g_2, \ldots, g_{n+1}) &+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n) \\ = (\delta f)(g_1, \ldots, g_{n+1}). & \end{aligned}$$

Abbiamo quindi il diagramma commutativo

$$\begin{array}{ccc} \hom(C_n, A) & \longrightarrow & \hom(C_{n+1}, A) \\ \downarrow & & \downarrow \\ C^n(G, A) & \xrightarrow{\delta} & C^{n+1}(G, A) \end{array} \tag{54}$$

in cui le frecce verticali sono isomorfismi di gruppi. Poiché il prodotto di $\hom(C_{n-1}, A) \to \hom(C_n, A)$ e $\hom(C_n, A) \to \hom(C_{n+1}, A)$ è nullo, si ha $\delta^2 = 0$. Pertanto $0 \to C^0(G, A) \xrightarrow{\delta} C^1(G, A) \xrightarrow{\delta} C^2(G, A) \to \cdots$ è un complesso di cocatene ed è isomorfo al complesso di cocatene $0 \to \hom(C_0, A) \to \hom(C_1, A) \to \hom(C_2, A) \to \cdots$. Ne segue che i due complessi hanno gruppi di omologia isomorfi. Abbiamo quindi il seguente teorema.

Teorema 6.12. *$B^n(G, A)$ è un sottogruppo di $Z^n(G, A)$ e $H^n(G, A) = Z^n(G, A)/B^n(G, A) \cong \mathrm{Ext}^n(\mathbb{Z}, A)$.*

Dalla definizione originaria dei gruppi di coomologia di G a coefficienti in A passiamo ora ai gruppi $\mathrm{Ext}^n(\mathbb{Z}, A)$. D'ora innanzi useremo $\mathrm{Ext}^n(\mathbb{Z}, A)$ come definizione dell'n-esimo gruppo di coomologia di G a coefficienti in A. Questa definizione ha il vantaggio di rendere disponibili i

risultati funtoriali su Ext nello studio dei gruppi di coomologia di un gruppo. Offre inoltre una flessibilità assai maggiore, poiché ci permette di sostituire alla risoluzione di $\mathbb{Z}$ qui impiegata altre risoluzioni. Alcuni esempi si troveranno negli esercizi.

Esaminiamo ora $H^n(G, A)$ per $n = 0, 1, 2$. Dimostriamo anzitutto il teorema seguente.

Teorema 6.13. *$H^0(G, A) = A^G$, il sottogruppo di A formato dagli elementi x tali che $gx = x$ per ogni $g \in G$.*

Dimostrazione. Ricordiamo che $\mathrm{Ext}^0(M, N) \cong \hom(M, N)$. Dunque $H^0(G, A) \cong \hom_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, il gruppo degli $\mathbb{Z}[G]$-omomorfismi di $\mathbb{Z}$ in A. Un tale omomorfismo η è determinato da $\eta(1)$ e, se $\eta(1) = x \in A$, allora $x = \eta(1) = \eta(g1) = g\eta(1) = gx$ per ogni $g \in G$. Viceversa, se $x \in A$ soddisfa $gx = x$ per ogni $g \in G$, l'applicazione η tale che $\eta(n) = nx$ è uno $\mathbb{Z}[G]$-omomorfismo di $\mathbb{Z}$ in A. Ne segue che $\hom(\mathbb{Z}, A)$ è isomorfo ad A^G mediante $\eta \mapsto \eta(1)$. □

Osserviamo che questa proposizione si può dimostrare facilmente anche usando le definizioni di $Z^0(G, A)$, $B^0(G, A)$ e $Z^0(G, A)/B^0(G, A)$. Lasciamo al lettore questa dimostrazione.

Se A è un G-modulo, un'applicazione f di G in A si chiama *omomorfismo incrociato* di G in A se

$$f(gh) = gf(h) + f(g), \qquad g, h \in G. \tag{55}$$

Se $x \in A$, l'applicazione f definita da

$$f(g) = gx - x \tag{56}$$

è un omomorfismo incrociato di G in A, poiché

$$gf(h) + f(g) = g(hx - x) + gx - x = ghx - x = f(gh).$$

Un omomorfismo incrociato definito dalla (56) si dice *principale*. È chiaro che gli omomorfismi incrociati formano un gruppo abeliano rispetto all'addizione di applicazioni e che quelli principali formano un sottogruppo. Il confronto con (42) e (43) mostra che il primo gruppo è $Z^1(G, A)$ e il secondo è $B^1(G, A)$. Il gruppo quoziente è dunque (isomorfo a) il primo gruppo di coomologia di G a coefficienti in A.

In teoria di Galois abbiamo già incontrato gli omomorfismi incrociati studiando le equazioni di Speiser e il loro analogo additivo (*BAI*, pp. 297–299). Ricordiamo questi risultati, il primo dei quali costituiva una generalizzazione del *Satz* 90 di Hilbert. Sia E un'estensione di Galois di dimensione finita del campo F, con gruppo di Galois G. Allora G è finito e $|G| = [E : F]$. Abbiamo le azioni naturali di G sul gruppo additivo di E e sul gruppo moltiplicativo E^* degli elementi non nulli di E. Consideriamo il gruppo additivo di E come G-modulo. Un omomorfismo incrociato è un'applicazione f di G in E tale che $f(gh) = f(g) + gf(h)$. Il teorema 4.32 di *BAI* (p. 297) afferma che ogni tale omomorfismo incrociato è principale. Abbiamo così il risultato $H^1(G, E) = 0$, ossia il primo gruppo di coomologia del gruppo di Galois G di E/F a coefficienti in E è nullo. Consideriamo ora l'azione di G su E^*. Poiché la composizione in E^* è la moltiplicazione, un omomorfismo incrociato di G in E^* è un'applicazione f di G in E^* tale che

$$f(gh) = (gf(h))f(g). \tag{57}$$

Queste sono le equazioni di Speiser date nella (75), p. 297 di *BAI*. Il teorema di Speiser afferma che una tale f è principale, ossia ha la forma $f(g) = (gu)u^{-1}$ per un opportuno $u \in E^*$. Il teorema di Speiser equivale dunque al risultato omologico $H^1(G, E^*) = 1$ (in notazione moltiplicativa).

Se G è un gruppo e A è un gruppo abeliano scritto moltiplicativamente su cui G agisce per automorfismi, $C^2(G,A)$ è il gruppo delle funzioni di due variabili in G a valori in A, con la moltiplicazione come legge di composizione. Il sottogruppo $Z^2(G,A)$ è formato dalle $f \in C^2(G,A)$ tali che

$$f(g,h)f(gh,k) = (gf(h,k))f(g,hk), \qquad g,h,k \in G. \tag{58}$$

Ciò segue immediatamente dalla (44). Una tale applicazione si chiama *sistema di fattori*. Il sottogruppo $B^2(G,A)$ è formato dalle applicazioni f della forma $f(g,h) = u(g)\,gu(h)\,u(gh)^{-1}$, dove u è un'applicazione di G in A. Il gruppo $Z^2(G,A)/B^2(G,A)$ è il secondo gruppo di coomologia di G a coefficienti in A. Nel prossimo paragrafo daremo un'interpretazione di questo gruppo.

Concludiamo il paragrafo dimostrando il seguente risultato sui gruppi di coomologia dei gruppi finiti.

Teorema 6.14. *Se G è un gruppo finito e A è un G-modulo, ogni elemento di $H^n(G,A)$, per $n > 0$, ha ordine finito divisore di $|G|$.*

Dimostrazione. Sia $f \in C^n(G,A)$ e consideriamo la formula (41) per δf. Facciamo variare g_{n+1} in G e sommiamo le formule corrispondenti. Indichiamo $\sum_{g\in G} f(g_1,\dots,g_{n-1},g)$ con $u(g_1,\dots,g_{n-1})$. Poiché $\sum_{g\in G} f(g_1,\dots,g_{n-1},g_ng) = u(g_1,\dots,g_{n-1})$, otteniamo

$$\begin{aligned}\sum_{g\in G}(\delta f)(g_1,\dots,g_n,g) &= g_1u(g_2,\dots,g_n)\\ &\quad+\sum_{i=1}^{n-1}(-1)^i u(g_1,\dots,g_ig_{i+1},\dots,g_n)\\ &\quad+(-1)^n u(g_1,\dots,g_{n-1})+(-1)^{n+1}|G|f(g_1,\dots,g_n)\\ &= (\delta u)(g_1,\dots,g_n)+(-1)^{n+1}|G|f(g_1,\dots,g_n).\end{aligned}$$

Quindi, se $\delta f = 0$, si ha $|G|f(g_1,\dots,g_n) = \pm(\delta u)(g_1,\dots,g_n)$, ossia $|G|f \in B^n(G,A)$. Dunque $|G|Z^n(G,A) \subseteq B^n(G,A)$ e perciò $|G|H^n(G,A) = 0$, come si voleva. □

Una conseguenza immediata di questo risultato è il seguente corollario.

Corollario. *Sia G un gruppo finito e sia A un G-modulo finito tale che $(|G|,|A|) = 1$. Allora $H^n(G,A) = 0$ per ogni $n > 0$.*

Ciò è chiaro, poiché $|A|f = 0$ per ogni $f \in C^n(G,A)$.

Esercizi.

1. Sia B un modulo destro su $\mathbb{Z}[G]$. Si definisca l'*n-esimo gruppo di omologia di G a coefficienti in B*, $n \geq 0$, ponendo $H_n(G,B) = \mathrm{Tor}_n(B,\mathbb{Z})$, con $\mathbb{Z}$ considerato come G-modulo banale. Mostrare che $H_0(G,B) = B/B_G$, dove B_G è il sottogruppo di B generato dagli elementi $xg - x$, $x \in B$, $g \in G$.

2. Sia ε l'omomorfismo di $\mathbb{Z}[G]$ in $\mathbb{Z}$ definito nel testo e sia $I = \ker\varepsilon$. Mostrare che I è uno $\mathbb{Z}$-modulo libero di base $\{g-1 \mid g \in G,\ g \neq 1\}$.

3. Siano A, B due G-moduli. Mostrare che $A \otimes_{\mathbb{Z}} B$ è un G-modulo con l'azione tale che $g(x\otimes y) = gx \otimes gy$.

4. Sia A un G-modulo e si indichi con A_t il gruppo abeliano A munito dell'azione banale di G. Mostrare che $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ e $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A_t$ sono isomorfi come G-moduli. (*Suggerimento.* Mostrare che esiste un isomorfismo di moduli di $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ su $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A_t$ tale che $g \otimes x \mapsto g \otimes g^{-1}x$, $g \in G,\ x \in A$.)

5. Servirsi dell'esercizio 4 per provare che, se A è un G-modulo libero su $\mathbb{Z}$, allora $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ è libero su $\mathbb{Z}[G]$.

6. Sia $I = \ker \varepsilon$, con $\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ come nel testo, e si ponga $I^n = I \otimes_{\mathbb{Z}} I \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} I$ (n fattori). Mostrare che la successione esatta corta $0 \to I \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$, in cui la prima applicazione è l'inclusione, dà luogo a una successione esatta corta $0 \to I^{n+1} \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} I^n \to I^n \to 0$. Sia d_n l'omomorfismo di $\mathbb{Z}[G] \otimes_{\mathbb{Z}} I^n$ in $\mathbb{Z}[G] \otimes_{\mathbb{Z}} I^{n-1}$ ottenuto componendo $\mathbb{Z}[G] \otimes_{\mathbb{Z}} I^n \to I^n$ con $I^n \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} I^{n-1}$. Osservare che

$$d_n\big(g_0 \otimes (g_1 - 1) \otimes \cdots \otimes (g_n - 1)\big) = (g_1 - 1) \otimes \cdots \otimes (g_n - 1),$$

con $g_i \in G$. Mostrare che

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}[G] \xleftarrow{d_1} \mathbb{Z}[G] \otimes I \xleftarrow{d_2} \mathbb{Z}[G] \otimes I^2 \longleftarrow \cdots$$

è una risoluzione libera di $\mathbb{Z}$.

7. Sia $G = \langle g \rangle$ il gruppo ciclico di ordine finito m generato da g. Osservare che $\mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^m - 1)$, con t indeterminata. Siano $D = g - 1$, $N = 1 + g + \cdots + g^{m-1}$, e siano D', N' le moltiplicazioni per D, N, rispettivamente, in $\mathbb{Z}[G]$. Mostrare che

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}[G] \xleftarrow{D'} \mathbb{Z}[G] \xleftarrow{N'} \mathbb{Z}[G] \xleftarrow{D'} \cdots$$

è una risoluzione libera di $\mathbb{Z}$.

8. Servirsi dell'esercizio 7 per mostrare che, se A è un G-modulo per il gruppo ciclico di ordine $m < \infty$, allora

$$H^{2n}(G, A) = A^G/NA, \qquad n > 0,$$
$$H^{2n+1}(G, A) = (\operatorname{Ann}_A N)/DA, \quad n \geq 0,$$

dove $\operatorname{Ann}_A N = \{x \in A \mid Nx = 0\}$.

6.10 Estensioni di gruppi

Per *estensione di un gruppo G mediante un gruppo A* intenderemo una successione esatta corta

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1. \tag{59}$$

Dunque i è iniettivo, p è suriettivo e $\ker p = iA$. Pertanto $iA \triangleleft E$. Se $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ è una seconda estensione di G mediante A, diremo che essa è *equivalente* alla (59) se esiste un omomorfismo $h\colon E \to E'$ che rende commutativo il diagramma

(60)
$$\begin{array}{ccccccc} & & & & E & & \\ & & & \overset{i}{\nearrow} & & \overset{p}{\searrow} & \\ 1 & \to & A & & \downarrow h & & G \to 1 \\ & & & \underset{i'}{\searrow} & & \underset{p'}{\nearrow} & \\ & & & & E' & & \end{array}$$

Come per i moduli (p. 348), si vede facilmente che in tal caso h è un isomorfismo.

Limitiamo la nostra attenzione alle estensioni di un gruppo G mediante un gruppo abeliano. A una tale estensione possiamo associare un'azione di G su A per automorfismi e un elemento del gruppo di coomologia $H^2(G, A)$, dove A è considerato come G-modulo mediante l'azione che definiremo. Nel seguito sarà utile denotare gli elementi di G con lettere greche minuscole e quelli di A e di E con lettere latine minuscole.

Definiamo anzitutto l'azione di G su A. Siano $\sigma \in G$, $x \in A$. Scegliamo un elemento $s \in E$ tale che $ps = \sigma$ e consideriamo l'elemento $s(ix)s^{-1}$. Poiché $iA \triangleleft E$, si ha $s(ix)s^{-1} \in iA$ e, poiché i è iniettivo, esiste un unico elemento $y \in A$ tale che $s(ix)s^{-1} = iy$. Per ottenere y abbiamo scelto un elemento $s \in E$ tale che $ps = \sigma$. Sia s' un secondo elemento tale che $ps' = \sigma$. Allora $p(s's^{-1}) = 1$, e quindi $s's^{-1} = ia$, con $a \in A$, e $s' = (ia)s$. Poiché iA è abeliano,

$$s'(ix)s'^{-1} = (ia)s(ix)s^{-1}(ia)^{-1} = s(ix)s^{-1}.$$

L'elemento y è dunque indipendente dalla scelta di s e possiamo porre $\sigma x = y$. La nostra definizione è pertanto

$$\sigma x = y, \qquad \text{dove } ps = \sigma, \quad s(ix)s^{-1} = iy. \tag{61}$$

Si verifica direttamente che la definizione di σx dà un'azione di G su A per automorfismi, ossia

$$(\sigma_1\sigma_2)x = \sigma_1(\sigma_2 x), \qquad 1x = x, \qquad \sigma(xy) = (\sigma x)(\sigma y).$$

A parte il fatto che A è scritto moltiplicativamente, abbiamo definito su A una struttura di G-modulo. D'ora in avanti lo chiameremo un G-modulo, pur conservando in A la notazione moltiplicativa.

Scegliamo ora per ogni $\sigma \in G$ un elemento $s_\sigma \in E$ tale che $ps_\sigma = \sigma$. Abbiamo così un'applicazione $s\colon G \to E$, $\sigma \mapsto s_\sigma$, tale che $ps_\sigma = \sigma$ per ogni σ, ossia $ps = 1_G$. Siano $\sigma, \tau \in G$ e consideriamo l'elemento $s_\sigma s_\tau s_{\sigma\tau}^{-1}$ di E. La sua immagine mediante p è 1. Vi è dunque un unico elemento $k_{\sigma,\tau} \in A$ tale che $s_\sigma s_\tau s_{\sigma\tau}^{-1} = ik_{\sigma,\tau}$, ossia

$$s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}. \tag{62}$$

Se anche $\rho \in G$, si ha

$$\begin{aligned} s_\rho(s_\sigma s_\tau) &= s_\rho(ik_{\sigma,\tau})s_{\sigma\tau} = s_\rho(ik_{\sigma,\tau})s_\rho^{-1}s_\rho s_{\sigma\tau} = i(\rho k_{\sigma,\tau})s_\rho s_{\sigma\tau} \\ &= i(\rho k_{\sigma,\tau})i(k_{\rho,\sigma\tau})s_{\rho\sigma\tau} = i\big((\rho k_{\sigma,\tau})k_{\rho,\sigma\tau}\big)s_{\rho\sigma\tau}. \end{aligned}$$

Analogamente, $(s_\rho s_\sigma)s_\tau = i(k_{\rho,\sigma}k_{\rho\sigma,\tau})s_{\rho\sigma\tau}$. Dunque la legge associativa in E implica

$$k_{\rho,\sigma}k_{\rho\sigma,\tau} = (\rho k_{\sigma,\tau})k_{\rho,\sigma\tau}. \tag{63}$$

Queste relazioni mostrano che l'applicazione $k\colon G \times G \to A$, $(\sigma, \tau) \mapsto k_{\sigma,\tau}$, è un elemento di $Z^2(G, A)$, come nella definizione classica di $H^2(G, A)$ data all'inizio del § 6.9.

Vediamo ora come cambia k se si sostituisce s con una seconda applicazione s' tale che $ps' = 1_G$. Per ogni $\sigma \in G$ abbiamo $p(s'_\sigma s_\sigma^{-1}) = (ps'_\sigma)(ps_\sigma)^{-1} = \sigma\sigma^{-1} = 1$. Esiste quindi un unico $u_\sigma \in A$ tale che $s'_\sigma s_\sigma^{-1} = iu_\sigma$, ossia $s'_\sigma = (iu_\sigma)s_\sigma$. Abbiamo così un'applicazione $u\colon \sigma \mapsto u_\sigma$ da G in A tale che

$$s'_\sigma = (iu_\sigma)s_\sigma, \qquad \sigma \in G. \tag{64}$$

Viceversa, se u è una qualsiasi applicazione di G in A, l'applicazione s' definita dalla (64) soddisfa $ps' = 1_G$. Per la (64) si ha

$$\begin{aligned} s'_\sigma s'_\tau &= (iu_\sigma)s_\sigma(iu_\tau)s_\tau = i\big(u_\sigma(\sigma u_\tau)\big)s_\sigma s_\tau \\ &= i\big(u_\sigma(\sigma u_\tau)k_{\sigma,\tau}\big)s_{\sigma\tau} = i\big(u_\sigma(\sigma u_\tau)k_{\sigma,\tau}u_{\sigma\tau}^{-1}\big)s'_{\sigma\tau}. \end{aligned}$$

Dunque a k si sostituisce k' con

$$k'_{\sigma,\tau} = u_\sigma(\sigma u_\tau)u_{\sigma\tau}^{-1}k_{\sigma,\tau}. \tag{65}$$

Ciò mostra che k' e k determinano lo stesso elemento di $H^2(G,A)$. Pertanto l'estensione determina un unico elemento di $H^2(G,A)$.

Segue direttamente dalle definizioni che, se le estensioni $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ e $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ sono equivalenti, esse determinano la stessa azione di G su A e lo stesso elemento di $H^2(G,A)$. Per provare il viceversa, mostreremo che la moltiplicazione in E è determinata dall'azione di G su A e dall'applicazione k. Sia $e \in E$ e poniamo $\sigma = pe \in G$, $f = e(s_\sigma)^{-1}$. Allora $pf = (pe)(ps_\sigma)^{-1} = \sigma\sigma^{-1} = 1$. Dunque $f = ix$ per un elemento $x \in A$ univocamente determinato. Otteniamo la fattorizzazione

$$e = (ix)s_\sigma, \qquad x \in A, \quad \sigma \in G. \tag{66}$$

È chiaro che gli elementi $x \in A$ e $\sigma \in G$ sono univocamente determinati dall'elemento e dato. Sia $(iy)s_\tau$, con $y \in A$ e $\tau \in G$, un secondo elemento di E. Allora

$$(ix)s_\sigma(iy)s_\tau = i\big(x(\sigma y)\big)s_\sigma s_\tau = i\big(x(\sigma y)k_{\sigma,\tau}\big)s_{\sigma\tau}. \tag{67}$$

Supponiamo ora che le estensioni $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ e $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ determinino la stessa struttura di modulo e lo stesso elemento di $H^2(G,A)$. Possiamo allora scegliere le applicazioni s e s' di G rispettivamente in E e in E' in modo che $ps = 1_G$, $p's' = 1_G$ e, per ogni $\sigma, \tau \in G$, si abbia $s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}$ e $s'_\sigma s'_\tau = (i'k_{\sigma,\tau})s'_{\sigma\tau}$. Valgono allora la (67) e la relazione $(i'x)s'_\sigma(i'y)s'_\tau = i'(x(\sigma y)k_{\sigma,\tau})s'_{\sigma\tau}$. Ne segue che l'applicazione $h\colon (ix)s_\sigma \mapsto (i'x)s'_\sigma$ è un omomorfismo di E in E' che rende commutativo il diagramma (60). Le estensioni sono quindi equivalenti.

Possiamo ora enunciare il seguente teorema fondamentale.

Teorema 6.15. *Due estensioni di G mediante un gruppo abeliano A sono equivalenti se e soltanto se determinano la stessa azione di G su A e lo stesso elemento di $H^2(G,A)$. Sia G un gruppo, sia A un G-modulo e sia M l'insieme delle estensioni di G mediante A che hanno il G-modulo dato A come modulo associato. Si ha allora una corrispondenza biunivoca fra l'insieme delle classi di equivalenza delle estensioni di G mediante A contenute in M e gli elementi di $H^2(G,A)$.*

Dimostrazione. La prima affermazione è stata dimostrata. Per provare la seconda basta mostrare che, dati un G-modulo A e un'applicazione k di $G \times G$ in A che soddisfa la (63), esiste un'estensione $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ per la quale l'azione associata di G su A è quella data e l'elemento associato di $H^2(G,A)$ è quello determinato da k. Poniamo $E = A \times G$, l'insieme delle coppie (x,σ), $x \in A$, $\sigma \in G$, e definiamo in E una moltiplicazione ponendo

$$(x,\sigma)(y,\tau) = \big(x(\sigma y)k_{\sigma,\tau}, \sigma\tau\big). \tag{68}$$

Dalla (63) è immediato che questa moltiplicazione è associativa. Se poniamo $\rho = \sigma = 1$ nella (63), otteniamo $k_{1,1}k_{1,\tau} = k_{1,\tau}k_{1,\tau}$. Quindi $k_{1,\tau} = k_{1,1}$. Allora

$$(k_{1,1}^{-1}, 1)(y,\tau) = (k_{1,1}^{-1}yk_{1,\tau}, \tau) = (y,\tau),$$

sicché $\mathbf{1} = (k_{1,1}^{-1}, 1)$ è un'unità sinistra in E. Per dimostrare che E è un gruppo con elemento neutro $\mathbf{1}$, basta mostrare che ogni elemento (x,σ) di E ha un inverso sinistro rispetto a $\mathbf{1}$ (BAI, p. 36, esercizio 10). Ciò segue da

$$\begin{aligned}&(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}(\sigma^{-1}x^{-1}), \sigma^{-1})(x,\sigma)\\ &\quad = \big(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}(\sigma^{-1}x^{-1})(\sigma^{-1}x)k_{\sigma^{-1},\sigma}, 1\big) = (k_{1,1}^{-1}, 1).\end{aligned}$$

Dunque E è un gruppo. Siano $i\colon x \mapsto (xk_{1,1}^{-1}, 1)$ e $p\colon (x,\sigma) \mapsto \sigma$. Allora i è un omomorfismo di A in E e p è un omomorfismo di E in G. È chiaro che i è iniettivo e p è suriettivo. Inoltre $iA = \ker p$. Quindi $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ è un'estensione di G mediante A. Per determinare l'azione di G su A data dall'estensione, osserviamo che $p(1,\sigma) = \sigma$. Occorre dunque calcolare

$$\begin{aligned}(1,\sigma)(ix)(1,\sigma)^{-1} &= (1,\sigma)(xk_{1,1}^{-1},1)(1,\sigma)^{-1}\\ &= (1,\sigma)(xk_{1,1}^{-1},1)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1},\sigma^{-1}).\end{aligned}$$

Abbiamo visto che $k_{1,\rho} = k_{1,1}$. Se poniamo $\sigma = \tau = 1$ nella (63), otteniamo $k_{\rho,1}k_{\rho,1} = (\rho k_{1,1})k_{\rho,1}$. Quindi $k_{\rho,1} = \rho k_{1,1}$. Poniamo ora $\sigma = \rho^{-1}$, $\tau = \rho$ nella (63). Otteniamo $k_{\rho,\rho^{-1}}k_{1,\rho} = (\rho k_{\rho^{-1},\rho})k_{\rho,1}$, e quindi $k_{\rho,\rho^{-1}}k_{1,1} = (\rho k_{\rho^{-1},\rho})k_{\rho,1}$. Abbiamo così

$$\begin{gathered}k_{1,\rho} = k_{1,1}, \qquad k_{\rho,1} = \rho k_{1,1},\\ k_{\rho,\rho^{-1}}k_{1,1} = (\rho k_{\rho^{-1},\rho})k_{\rho,1}.\end{gathered} \tag{69}$$

Ora $(1,\sigma)(k_{1,1}^{-1}x,1) = ((\sigma k_{1,1}^{-1})(\sigma x)k_{\sigma,1},\sigma) = (\sigma x,\sigma)$ e

$$\begin{aligned}&(\sigma x,\sigma)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1},\sigma^{-1})\\ &\quad= \big((\sigma x)(\sigma k_{1,1})^{-1}(\sigma k_{\sigma^{-1},\sigma})^{-1}k_{\sigma,\sigma^{-1}},1\big)\\ &\quad= \big((\sigma x)k_{\sigma,1}^{-1}(\sigma k_{\sigma^{-1},\sigma})^{-1}k_{\sigma,\sigma^{-1}},1\big) = \big((\sigma x)k_{1,1}^{-1},1\big)\end{aligned}$$

per la (69). Dunque l'azione sul modulo è quella data. Sia ora s l'applicazione $\sigma \mapsto (1,\sigma)$, così che $ps = 1_G$. Abbiamo $(1,\sigma)(1,\tau) = (k_{\sigma,\tau},\sigma\tau) = (k_{1,1}^{-1}k_{\sigma,\tau},1)(1,\sigma\tau)$, e quindi $s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}$. L'elemento di $H^2(G,A)$ associato a questa estensione è pertanto quello determinato da k. Ciò conclude la dimostrazione. □

Il risultato precedente è classico, in una forma leggermente diversa. Fu dimostrato da Schreier, che per primo considerò il problema delle estensioni come quello di descrivere tutti i gruppi che hanno un dato sottogruppo normale A (non necessariamente commutativo) con gruppo quoziente dato G.

Un'estensione (59) si dice *spezzata* se esiste un omomorfismo di gruppi $s\colon G \to E$ tale che $ps = 1_G$. Si ha allora $(s_\sigma)(s_\tau) = s_{\sigma\tau}$ per ogni $\sigma,\tau \in G$ e quindi il $k_{\sigma,\tau}$ determinato dalla (62) è 1. L'elemento di $H^2(G,A)$ associato a un'estensione spezzata è dunque 1. Viceversa, se ciò accade, esiste un'applicazione $s\colon G \to E$ che soddisfa $ps = 1_G$ e per la quale tutti i $k_{\sigma,\tau}$ sono 1, il che significa che s è un omomorfismo. Le estensioni spezzate sono dunque quelle per le quali l'elemento associato di $H^2(G,A)$ è 1. Evidentemente ne segue che $H^2(G,A) = 1$ se e soltanto se si spezzano tutte le estensioni di G mediante A che danno la struttura di G-modulo fissata su A. Per il corollario al teorema 6.14 (p. 361) ciò accade se G e A sono finiti e $(|G|,|A|) = 1$.

Se $A \lhd E$ ed $E/A = G$, con A qualsiasi (anche non abeliano), abbiamo l'estensione $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$, dove i è l'inclusione di A in E e p è l'omomorfismo naturale di E su G. Dalla definizione si vede subito che questa estensione si spezza se e soltanto se esiste un sottogruppo S di E tale che $E = SA$ e $S \cap A = 1$. In tal caso si dice che E è il *prodotto semidiretto* di S e di A. Il risultato appena enunciato afferma che, se A è abeliano e A e G sono finiti con $(|A|,|G|) = 1$, allora $E = SA$ e $S \cap A = 1$ per un sottogruppo S di E. Completando questo risultato, ottenuto con metodi omologici, con un po' di teoria dei gruppi, si può dimostrare il seguente teorema dovuto a H. Zassenhaus.

Teorema 6.16. *Sia E un gruppo finito e sia A un sottogruppo normale di E tale che $(|A|,|E/A|) = 1$. Allora E è un prodotto semidiretto di A e di un sottogruppo S.*

Dimostrazione. Siano $|A| = m$, $|E/A| = n$. Basta mostrare che esiste un sottogruppo S tale che $|S| = n$. Infatti, per un tale sottogruppo S, l'ordine di $S \cap A$ divide sia $|S| = n$ sia $|A| = m$.

Quindi $S \cap A = 1$. Inoltre, poiché $A \lhd E$, SA è un sottogruppo il cui ordine è multiplo di $|S|$ e di $|A|$, e quindi di $mn = |E|$. Sia p un divisore primo di m e sia H un p-sottogruppo di Sylow di A. Allora H è anche un p-sottogruppo di Sylow di E. L'insieme Syl_p dei p-sottogruppi di Sylow di E è $\{gHg^{-1} \mid g \in E\}$ (BAI, p. 80). Poiché $A \lhd E$, questo è anche l'insieme dei p-sottogruppi di Sylow di A. Se N è il normalizzante di H in E, si ha quindi $|\,\mathrm{Syl}_p\,| = [E : N] = [A : N \cap A]$. Dunque

$$|E|/|N| = |A|/|N \cap A|$$

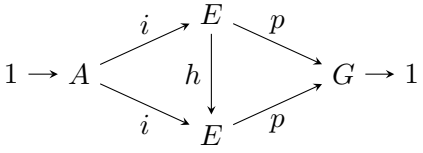
e pertanto

$$n = [E : A] = |E|/|A| = |N|/|N \cap A| = [N : N \cap A].$$

D'altra parte $|N \cap A| \mid |A|$, perciò $(|N \cap A|, |N/(N \cap A)|) = 1$. Se $|N| < |E|$, possiamo procedere per induzione sull'ordine per concludere che N, e quindi E, contiene un sottogruppo di ordine n. Supponiamo ora che $|N| = |E|$. Allora $N = E$ e $H \lhd E$. Il centro Z di H non è banale (BAI, p. 76). Poiché Z è un sottogruppo caratteristico di H, si ha $Z \lhd E$ e $A/Z \lhd E/Z$. Poiché $(E/Z)/(A/Z) \simeq E/A$, possiamo applicare l'induzione per concludere che E/Z contiene un sottogruppo L/Z di ordine n. Poiché Z è abeliano e $|Z|$ è una potenza di p, il risultato che abbiamo stabilito mediante l'omologia implica che L contiene un sottogruppo S di ordine n. Ciò conclude la dimostrazione. □

Esercizi

1. Sia $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ un'estensione di G mediante il gruppo abeliano A e sia H l'insieme delle equivalenze h di questa estensione, ossia degli automorfismi di E che rendono commutativo il diagramma



   Mostrare che H è un sottogruppo di $\mathrm{Aut}\, E$ che contiene gli automorfismi interni indotti dagli elementi di iA. Mostrare che questi ultimi formano un sottogruppo normale J di H e che $H/J \simeq H^1(G, A)$.

2. (Schreier, Eilenberg e MacLane.) Sia $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ un'estensione di G mediante il gruppo A (non necessariamente abeliano) e sia Z il centro di A. Sia s un'applicazione $\sigma \mapsto s_\sigma$ di G in E tale che $ps_\sigma = \sigma$ e sia $\varphi(s_\sigma)$ l'automorfismo $x \mapsto y$ di A tale che $s_\sigma(ix)s_\sigma^{-1} = iy$. Mostrare che, se s' è una seconda applicazione di G in E che soddisfa $ps'_\sigma = \sigma$ per $\sigma \in G$, allora $\varphi(s'_\sigma) \in (\mathrm{Inaut}\, A)\varphi(s_\sigma)$ e $\varphi(s'_\sigma)|Z = \varphi(s_\sigma)|Z$. Mostrare che $\bar{\varphi}\colon \sigma \mapsto (\mathrm{Inaut}\, A)\varphi(s_\sigma)$ è un omomorfismo di G in $\mathrm{Aut}\, A/\,\mathrm{Inaut}\, A$ e che $\sigma c = \varphi(s_\sigma)c$, $c \in Z$, definisce un'azione di G su Z per automorfismi.

   Mostrare che, se $\sigma, \tau \in G$, si ha $s_\sigma s_\tau = i(k_{\sigma,\tau})s_{\sigma\tau}$, dove $k_{\sigma,\tau}$ è un elemento univocamente determinato di A. Mostrare che, ponendo $\varphi(\sigma) = \varphi(s_\sigma)$, si ha

   (70) $$\varphi(\sigma)\varphi(\tau) = I_{k_{\sigma,\tau}}\varphi(\sigma\tau),$$

   dove $I_{k_{\sigma,\tau}}$ è l'automorfismo interno $x \mapsto k_{\sigma,\tau}xk_{\sigma,\tau}^{-1}$ di A. Mostrare che

   (71) $$k_{\rho,\sigma}k_{\rho\sigma,\tau} = (\varphi(\rho)k_{\sigma,\tau})k_{\rho,\sigma\tau}$$

   e che

   (72) $$\varphi(1) = I_{k_{1,1}}.$$

Viceversa, siano G e A gruppi, k un'applicazione di $G \times G$ in A e φ un'applicazione di G in $\operatorname{Aut} A$ tali che valgano le (70)–(72). Sia $E = A \times G$ e si definisca in E un prodotto mediante

$$(x, \sigma)(y, \tau) = \big(x(\varphi(\sigma)y)k_{\sigma,\tau}, \sigma\tau\big). \tag{73}$$

Mostrare che E è un gruppo con elemento neutro $(k_{1,1}^{-1}, 1)$ e che, se i è l'applicazione $x \mapsto (xk_{1,1}^{-1}, 1)$ e p è l'applicazione $(x, \sigma) \mapsto \sigma$, allora $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ è un'estensione di G mediante A.

Siano $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ e $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ estensioni di G mediante A tali che gli omomorfismi associati di G in $\operatorname{Aut} A/\operatorname{Inaut} A$, e quindi le azioni associate di G su Z, siano gli stessi. Mostrare che le applicazioni s e s' (di G in E ed E', rispettivamente) si possono scegliere in modo che $\varphi(s_\sigma) = \varphi'(s'_\sigma)$, dove φ' è definita analogamente a φ. Sia $k'_{\sigma,\tau}$ definito da $s'_\sigma s'_\tau = i'(k'_{\sigma,\tau})s'_{\sigma\tau}$ e si ponga $f(\sigma, \tau) = k'_{\sigma,\tau}k_{\sigma,\tau}^{-1}$. Mostrare che $f(\sigma, \tau) \in Z$ e che $f\colon (\sigma, \tau) \mapsto f(\sigma, \tau)$ è un 2-cociclo di G a valori in Z, con l'azione di G definita sopra. Usare questo fatto per stabilire una corrispondenza biunivoca tra l'insieme delle classi di equivalenza delle estensioni di G mediante A aventi tutte lo stesso omomorfismo associato fissato da G in $\operatorname{Aut} A/\operatorname{Inaut} A$ e $H^2(G, Z)$.

3. Sia G finito e sia $H^2(G, \mathbb{C}^*)$ il secondo gruppo di coomologia di G a coefficienti nel gruppo moltiplicativo $\mathbb{C}^*$ degli elementi non nulli di $\mathbb{C}$, dove l'azione di G su $\mathbb{C}^*$ è banale. Il gruppo $H^2(G, \mathbb{C}^*)$ si chiama *moltiplicatore di Schur* di G. Usare il teorema 6.14 per mostrare che, se $[\gamma]$ è un elemento qualsiasi di $H^2(G, \mathbb{C}^*)$, si può scegliere per rappresentante un cociclo γ i cui valori siano radici n-esime dell'unità, con $n = |G|$. Dedurne che $H^2(G, \mathbb{C}^*)$ è un gruppo finito.

4. Sia ρ una rappresentazione proiettiva di un gruppo G. Per definizione, ρ è un omomorfismo di G nel gruppo lineare proiettivo $\mathrm{PGL}(V)$ di uno spazio vettoriale V/F di dimensione finita (esercizio 4, p. 256). Come nell'esercizio citato, per ogni $g \in G$ sia $\mu(g)$ un rappresentante della classe laterale $\rho(g) \in \mathrm{PGL}(V)$, sicché $\mu(g_1g_2) = \gamma_{g_1,g_2}\mu(g_1)\mu(g_2)$, con $\gamma_{g_1,g_2} \in F^*$, il gruppo moltiplicativo di F. Mostrare che $\gamma\colon (g_1, g_2) \mapsto \gamma_{g_1,g_2}$ è un 2-cociclo di G a coefficienti in F^*, con l'azione banale di G su F^*. Mostrare che, se scegliamo una seconda famiglia di rappresentanti $\mu'(g) \in \mathrm{GL}(V)$ per i $\rho(g)$, $g \in G$, il 2-cociclo γ' che ne risulta determina lo stesso elemento di $H^2(G, F^*)$ di γ. Mostrarne come conseguenza che a ρ possiamo associare un unico elemento $[\gamma]$ di $H^2(G, F^*)$. Osservare che, se $[\gamma] = 1$, possiamo prendere $\gamma_{g_1,g_2} = 1$ per $g_i \in G$. Allora $\mu(g_1g_2) = \mu(g_1)\mu(g_2)$, cosicché ρ è essenzialmente una rappresentazione ordinaria. In tal caso diremo che ρ *si spezza*.

5. Con le notazioni dell'esercizio precedente, sia A un sottogruppo di F^* contenente i γ_{g_1,g_2} per una particolare scelta del cociclo γ. Costruire, come nel testo, l'estensione E di G mediante A corrispondente a γ. Scrivere gli elementi di E come (g, a), $g \in G$, $a \in A$. Si ha allora $(g_1, a_1)(g_2, a_2) = (g_1g_2, \gamma_{g_1,g_2}a_1a_2)$. Osservare che $iA = \{(1, a) \mid a \in A\}$ è contenuto nel centro di E. Mostrare che $\widetilde{\mu}(g, a) = a\mu(g)$ definisce una rappresentazione di E su V tale che $\widetilde{\mu}(g, 1) = \mu(g)$.[21]

6. Sia E un'estensione di G mediante A tale che $iA \subseteq Z(E)$, il centro di E. Sia $\widetilde{\mu}$ una rappresentazione di E su uno spazio vettoriale V di dimensione finita su un campo alge-

[21] Con la convenzione dell'esercizio 4, $\mu(g_1g_2) = \gamma_{g_1,g_2}\mu(g_1)\mu(g_2)$, quest'ultima affermazione richiede γ_{g_1,g_2}^{-1} nella legge di prodotto. La legge qui riportata dall'originale corrisponde invece alla convenzione $\mu(g_1)\mu(g_2) = \gamma_{g_1,g_2}\mu(g_1g_2)$. [N.d.T.]

bricamente chiuso F. Per $g \in G$, si definisca $\rho(g)$ come l'elemento di $\mathrm{PGL}(V)$ avente per rappresentante $\widetilde{\mu}(g,1) \in L(V)$. Mostrare che ρ è una rappresentazione proiettiva di G.[22]

Nota. Gli esercizi 3–6 danno un primo cenno dei numerosi legami fra il moltiplicatore di Schur e le rappresentazioni proiettive di un gruppo finito. Schur sviluppò l'argomento in tre lavori. Per un'esposizione della teoria di Schur, con riferimenti bibliografici, il lettore può consultare *Endliche Gruppen* di Huppert, Springer-Verlag, Berlino–Heidelberg–New York, 1967, pp. 628–641.

6.11 Coomologia delle algebre

Le definizioni dei moduli di omologia e coomologia di un'algebra (associativa), dovute a Hochschild, si fondano sulla nozione di bimodulo su un'algebra. Sia A un'algebra su un anello commutativo K. Abbiamo definito un modulo (sinistro) M su A, considerata come K-algebra, come un gruppo abeliano scritto additivamente che sia al tempo stesso un K-modulo e un A-modulo nell'usuale senso degli anelli e tale che $k(ax) = (ka)x = a(kx)$ per $k \in K$, $a \in A$, $x \in M$ (p. 211). La definizione di modulo destro sull'algebra A è analoga: M è un K-modulo e un A-modulo destro nel senso usuale, con $k(xa) = (kx)a = x(ka)$. Siano ora A e B algebre su K. Un A-B-bimodulo (nel senso delle algebre) è un A-modulo sinistro e un B-modulo destro M le cui strutture di K-modulo, indotte da A e da B, coincidono, e per il quale $(ax)b = a(xb)$ per $a \in A$, $b \in B$, $x \in M$.

Un semplice accorgimento riconduce lo studio degli A-B-bimoduli a quello dei moduli su un'altra algebra. Sia B^{op} l'algebra opposta di B e formiamo $A \otimes B^{\mathrm{op}}$, dove $\otimes$ sta per $\otimes_K$. Se M è un A-B-bimodulo e $x \in M$, l'applicazione $(a,b) \mapsto axb$ da $A \times B$ in M è K-bilineare e induce quindi un'applicazione K-lineare da $A \otimes B$ in M che manda $\sum a_i \otimes b_i$ in $\sum a_i x b_i$. Il punto essenziale è che per ogni $\sum a_i \otimes b_i \in A \otimes B^{\mathrm{op}}$ e per ogni $x \in M$ il prodotto $(\sum a_i \otimes b_i)x = \sum a_i x b_i \in M$ è ben definito. Si verifica direttamente che questo fa di M un modulo sull'algebra $A \otimes B^{\mathrm{op}}$. Viceversa, se M è un tale modulo, ponendo $ax = (a \otimes 1)x$, $xb = (1 \otimes b)x$ e mantenendo l'azione kx per $a \in A$, $b \in B$, $k \in K$, si ottiene un A-B-bimodulo nel senso delle algebre. Si può quindi passare liberamente da un punto di vista all'altro.

Se M, N sono moduli sull'algebra A, un omomorfismo $\eta : M \to N$ è un omomorfismo di gruppi abeliani tale che $\eta(kx) = k(\eta x)$, $\eta(ax) = a(\eta x)$, per $k \in K$, $a \in A$. Poiché $kx = (k1)x$, la prima condizione è superflua. Si ritrova dunque la nozione di omomorfismo di moduli sull'anello A. D'altra parte viene naturale dare a $\hom_A(M,N)$ una struttura di K-modulo che estenda quella di gruppo abeliano finora considerata. Basta definire $(k\eta)x = k(\eta x)$ per $k \in K$, $\eta \in \hom(M,N)$. In questo modo $\hom(M,N)$ diviene evidentemente un K-modulo. Analogamente, dati un modulo destro M e un modulo sinistro N sull'algebra A, $M \otimes_A N$ è un K-modulo. Gli usuali funtori $\hom_A(M,-)$, $\hom_A(-,N)$, $- \otimes_A N$, ecc., a valori nei gruppi abeliani, danno così funtori a valori nei K-moduli. Oltre a essere additivi, essi sono K-lineari, nel senso che le applicazioni fra i K-moduli che intervengono nelle definizioni sono K-omomorfismi. Osservazioni analoghe valgono per i funtori derivati. Tutto ciò è immediato, e sarebbe tedioso precisare ogni dettaglio. Nel seguito sostituiremo senz'altro i gruppi abeliani con moduli quando sarà opportuno.

Consideriamo ora una sola algebra A e la categoria degli A-A-bimoduli, i cui morfismi sono gli A-A-omomorfismi. Equivalentemente si ha la categoria dei moduli su $A \otimes_K A^{\mathrm{op}}$. Scriveremo A^e per $A \otimes A^{\mathrm{op}}$. L'algebra A è essa stessa un A-A-bimodulo rispetto alle moltiplicazioni sinistra

[22] L'originale indica il centro di E con $Z(G)$. Per la discesa a $\mathrm{PGL}(V)$ occorre inoltre che iA agisca mediante scalari, condizione soddisfatta, ad esempio, se $\widetilde{\mu}$ è irriducibile, per il lemma di Schur. [N.d.T.]

e destra in A. Dunque A è un A^e-modulo in cui, per $a_i, x \in A$, $b_i \in A^{\mathrm{op}}$,

$$\Big(\sum a_i \otimes b_i\Big)x = \sum a_i x b_i. \tag{74}$$

Il modulo è ciclico con generatore 1, e si ha quindi un A^e-omomorfismo di A^e su A dato da

$$\varepsilon : \sum a_i \otimes b_i \longmapsto \Big(\sum a_i \otimes b_i\Big)1 = \sum a_i b_i. \tag{75}$$

Siamo ora in grado di definire i moduli di omologia e di coomologia di un'algebra A. Sia M un A-A-bimodulo, ossia un A^e-modulo. Definiamo l'*n-esimo modulo di coomologia di A a coefficienti in M* ponendo $H^n(A, M) = \mathrm{Ext}^n_{A^e}(A, M)$, e l'*$n$-esimo modulo di omologia di A a coefficienti in M* ponendo $H_n(A, M) = \mathrm{Tor}^{A^e}_n(A, M)$. In entrambi i casi si considera A come modulo su A^e nel senso indicato sopra.

Supponiamo ora A libera su K (basterebbe proiettiva). Definiremo una risoluzione libera di A come A^e-modulo tale che il calcolo di $H^n(A, M)$ mediante questa risoluzione si identifichi con la definizione originaria data da Hochschild per le algebre su campi. Siano $X_0 = A \otimes_K A$, $X_1 = A \otimes_K A \otimes_K A$ e, in generale, $X_n = A \otimes_K \cdots \otimes_K A$ con $n+2$ fattori. Se M, N sono A-A-bimoduli, anche $M \otimes_K N$ lo è, con $a(x \otimes y) = ax \otimes y$, $(x \otimes y)a = x \otimes ya$ per $a \in A$, $x \in M$, $y \in N$ (proposizione 3.6, p. 135). Ne segue che X_n è un A-A-bimodulo in cui

$$\begin{aligned} a(x_0 \otimes \cdots \otimes x_{n+1}) &= ax_0 \otimes x_1 \otimes \cdots \otimes x_{n+1}, \\ (x_0 \otimes \cdots \otimes x_{n+1})a &= x_0 \otimes \cdots \otimes x_n \otimes x_{n+1}a. \end{aligned} \tag{76}$$

Dalle definizioni è chiaro che, come A^e-moduli, $X_0 = A \otimes_K A \cong A^e$, $X_1 = A \otimes_K A \otimes_K A \cong A^e \otimes A$ e, per $n > 1$, $X_n \cong A^e \otimes X_{n-2}$. L'isomorfismo $A^e \otimes X_{n-2} \to X_n$ manda $(a \otimes b) \otimes x$ in $a \otimes x \otimes b$, $x \in X_{n-2}$. Poiché A è libera su K, i moduli X_n sono liberi su K. Perciò $X_0 \cong A^e$, $X_1 \cong A^e \otimes A$ e $X_n \cong A^e \otimes X_{n-2}$ sono liberi su A^e.

Il consueto argomento sui prodotti tensoriali dà un unico K-omomorfismo $d_n : X_n \to X_{n-1}$ tale che

$$d_n(x_0 \otimes \cdots \otimes x_{n+1}) = \sum_{i=0}^{n} (-1)^i x_0 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_{n+1}. \tag{77}$$

Per la definizione delle azioni sinistra e destra di A si tratta di un omomorfismo di A-A-bimoduli, dunque di un A^e-omomorfismo da X_n in X_{n-1}. Unendo l'aumentazione $\varepsilon : X_0 \to A$ otteniamo la successione di A^e-omomorfismi

$$0 \longleftarrow A \xleftarrow{\varepsilon} X_0 \xleftarrow{d_1} X_1 \longleftarrow \cdots . \tag{78}$$

Ne mostreremo l'esattezza, provando così che (78) è una risoluzione libera di A come A^e-modulo. La dimostrazione è simile a quella per il complesso impiegato nel caso dei gruppi (p. 357). Definiamo un'omotopia contraente

$$A \xrightarrow{s_{-1}} X_0 \xrightarrow{s_0} X_1 \longrightarrow \cdots , \tag{79}$$

ossia una successione di K-omomorfismi s_i tali che

$$\varepsilon s_{-1} = 1_A, \quad d_1 s_0 + s_{-1}\varepsilon = 1_{X_0}, \quad d_{n+1}s_n + s_{n-1}d_n = 1_{X_n} \quad (n \geq 1). \tag{80}$$

Definiamo s_n, $n \geq -1$, come il K-omomorfismo tale che

$$s_n(x_0 \otimes \cdots \otimes x_{n+1}) = 1 \otimes x_0 \otimes \cdots \otimes x_{n+1}. \tag{81}$$

Dalla definizione segue direttamente (80). Come nel caso dei gruppi (p. 358), ciò implica che (78) è esatta e dunque è una risoluzione libera di A con aumentazione ε.

Per un dato A-A-bimodulo M si ha ora il complesso di cocatene

$$0 \longrightarrow \hom_{A^e}(X_0, M) \longrightarrow \hom_{A^e}(X_1, M) \longrightarrow \cdots, \tag{82}$$

i cui gruppi di coomologia sono i gruppi di coomologia di A a coefficienti in M. Abbiamo la catena di isomorfismi

$$\begin{aligned}\hom_{A^e}(X_n, M) &\cong \hom_{A^e}(A^e \otimes X_{n-2}, M) \cong \hom_{A^e}(X_{n-2} \otimes A^e, M)\\ &\cong \hom_K(X_{n-2}, \hom_{A^e}(A^e, M)) \cong \hom_K(X_{n-2}, M)\end{aligned}$$

(si veda p. 136). Possiamo identificare quest'ultimo modulo con il K-modulo delle applicazioni n-lineari da $A \times \cdots \times A$ (n volte) in M. Una tale applicazione ha dominio $A \times \cdots \times A$, codominio M ed è un K-omomorfismo da A in M quando si fissano tutti gli argomenti tranne uno. L'isomorfismo precedente diviene quindi un isomorfismo sul K-modulo $C^n(A, M)$ delle applicazioni n-lineari f da $A \times \cdots \times A$ in M. Per $f \in C^n(A, M)$ definiamo $\delta f \in C^{n+1}(A, M)$ mediante

$$\begin{aligned}(\delta f)(x_1, \ldots, x_{n+1}) &= x_1 f(x_2, \ldots, x_{n+1})\\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1})\\ &\quad + (-1)^{n+1} f(x_1, \ldots, x_n) x_{n+1},\end{aligned} \tag{83}$$

con $x_i \in A$. Si verifica allora la commutatività del diagramma

$$\begin{array}{ccc}\hom_{A^e}(X_n, M) & \longrightarrow & \hom_{A^e}(X_{n+1}, M)\\ \downarrow & & \downarrow\\ C^n(A, M) & \xrightarrow[\delta]{} & C^{n+1}(A, M)\end{array} \tag{84}$$

dove le applicazioni verticali sono gli isomorfismi indicati. Ne segue che

$$0 \longrightarrow C^0(A, M) \xrightarrow{\delta} C^1(A, M) \longrightarrow \cdots \tag{85}$$

è un complesso di cocatene isomorfo a (82), con gli stessi gruppi di coomologia. Otteniamo pertanto il seguente teorema.

Teorema 6.17. *Sia A una K-algebra libera su K, sia M un A-A-bimodulo e sia $C^n(A, M)$, $n \geq 0$, il K-modulo delle applicazioni n-lineari da $A \times \cdots \times A$ (n volte) in M. Per $f \in C^n(A, M)$ si definisca $\delta f \in C^{n+1}(A, M)$ mediante (83). Siano $Z^n(A, M)$ il nucleo di δ su $C^n(A, M)$ e $B^n(A, M) = \delta C^{n-1}(A, M)$. Allora $B^n(A, M)$ è un sottomodulo di $Z^n(A, M)$ e $Z^n(A, M)/B^n(A, M) \cong H^n(A, M)$, l'$n$-esimo modulo di coomologia di A a coefficienti in M.*

Benché alcuni dei risultati che ora indicheremo valgano anche senza tale restrizione, continuiamo a supporre A libera su K. Come nel caso dei gruppi, consideriamo ora $H^n(A, M)$ per $n = 0, 1, 2$, usando il calcolo del teorema 6.17.

Come al solito identifichiamo $C^0(A, M)$ con M. Per $u \in M$, la definizione dà $(\delta u)(x) = xu - ux$ per $x \in A$. Dunque $Z^0(A, M)$ è il sottomodulo degli $u \in M$ per cui $ux = xu$ per ogni $x \in A$. Poiché $C^{-1}(A, M) = 0$, $H^0(A, M)$ è isomorfo a questo sottomodulo.

Sia ora $f \in C^1(A, M)$. Allora $(\delta f)(x, y) = xf(y) - f(xy) + f(x)y$ per $x, y \in A$, e $\delta f = 0$ se e solo se f è un K-omomorfismo da A in M tale che

$$f(xy) = xf(y) + f(x)y. \tag{86}$$

È naturale chiamare una tale f una *derivazione* di A nell'A-A-bimodulo M. Ogni $u \in M$ determina la *derivazione interna* δu data da

$$(\delta u)(x) = xu - ux. \tag{87}$$

Le derivazioni interne formano un sottomodulo $\mathrm{Inder}(A, M)$ del modulo $\mathrm{Der}(A, M)$ delle derivazioni da A in M. Il caso $n = 1$ del teorema 6.17 dà l'isomorfismo

$$H^1(A, M) \cong \mathrm{Der}(A, M)/\mathrm{Inder}(A, M). \tag{88}$$

Se $f \in C^2(A, M)$, si ha $(\delta f)(x, y, z) = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y)z$, e $\delta f = 0$ se e solo se

$$xf(y, z) + f(x, yz) = f(xy, z) + f(x, y)z, \qquad x, y, z \in A. \tag{89}$$

Le $f \in C^2(A, M)$ che soddisfano questa condizione costituiscono $Z^2(A, M)$. Questo contiene il sottomodulo delle applicazioni δg, $g \in C^1(A, M)$, con $(\delta g)(x, y) = xg(y) - g(xy) + g(x)y$. Il quoziente di $Z^2(A, M)$ per questo sottomodulo è isomorfo a $H^2(A, M)$.

Il secondo gruppo di coomologia di un'algebra, nella forma $Z^2(A, M)/B^2(A, M)$, comparve per la prima volta nella letteratura nelle dimostrazioni date da J. H. C. Whitehead e da Hochschild di un classico teorema di struttura sulle algebre di dimensione finita su un campo, il cosiddetto *teorema principale di Wedderburn*. Ne daremo la traccia di una dimostrazione coomologica, lasciando al lettore il compito di completarne i dettagli nella successione di esercizi che segue.

Sia A un'algebra di dimensione finita su un campo F, e sia $N = \mathrm{rad}\, A$. Allora N è un ideale nilpotente di A e $\bar{A} = A/N$ è semiprimitiva. Il teorema principale di Wedderburn afferma che, se $\bar{A}$ è separabile, nel senso che $\bar{A}_E$ è semiprimitiva per ogni estensione E/F, allora A contiene una sottoalgebra S tale che $A = S + N$ e $S \cap N = 0$. La somma diretta $A = S \oplus N$ si intende come somma di spazi vettoriali su F, non di algebre.

La dimostrazione si riduce anzitutto al caso $N^2 = 0$. Si introduce $B = A/N^2$ (N^2 è un ideale), il cui radicale è N/N^2 e soddisfa $(N/N^2)^2 = 0$. Se $N^2 \neq 0$, si ha $[B : F] < [A : F]$ e si può supporre il teorema valido per B. Ne segue facilmente che vale anche per A.

Supponiamo ora $N^2 = 0$. Possiamo scegliere un sottospazio V di A tale che $A = V \oplus N$. Ciò equivale a scegliere un'applicazione lineare $s : \bar{A} \to A$ con $ps = 1_{\bar{A}}$, dove p è l'applicazione canonica $x \mapsto x + N$ da A su $\bar{A}$. Allora $V = s\bar{A}$ e s è iniettiva. Ogni elemento di A si scrive in modo unico come $s(a) + x$, con $a \in \bar{A}$, $x \in N$. Poiché N è un ideale e $N^2 = 0$, la moltiplicazione è data da

$$(s(a) + x)(s(b) + y) = s(a)s(b) + s(a)y + xs(b). \tag{90}$$

Ponendo $ax = s(a)x$, $xa = xs(a)$, si fa di N un $\bar{A}$-$\bar{A}$-bimodulo. Poiché $p(s(a)s(b)) = p(s(a))p(s(b)) = ab$ e $p(s(ab)) = ab$, abbiamo

$$s(a)s(b) = s(ab) + f(a, b), \qquad f(a, b) \in N. \tag{91}$$

L'applicazione f appartiene a $Z^2(\bar{A}, N)$. Sostituire s con un'applicazione lineare $t : \bar{A} \to A$ con $pt = 1_{\bar{A}}$ equivale a sostituire f con un cociclo coomologo. Inoltre, se in (91) si ha $f = 0$, allora $S = s(\bar{A})$ è una sottoalgebra e $A = S \oplus N$. Per ottenere il teorema principale di Wedderburn basta dunque provare che $H^2(\bar{A}, N) = 0$ per ogni algebra separabile $\bar{A}$ e ogni $\bar{A}$-$\bar{A}$-bimodulo N. Una dimostrazione è indicata nei seguenti esercizi.

Esercizi.

1. Completare i dettagli del ragionamento precedente: la riduzione al caso $N^2 = 0$ e, in questo caso, la riduzione alla dimostrazione che $H^2(\bar{A}, N) = 0$.

2. Sia A un'algebra separabile di dimensione finita su un campo F. Mostrare che esiste un'estensione E/F tale che $A_E = M_{n_1}(E) \oplus M_{n_2}(E) \oplus \cdots \oplus M_{n_s}(E)$. (Il modo più semplice consiste nell'usare la chiusura algebrica $\bar{F}$ di F definita nel §8.1, ma se ne può fare a meno.)

3. Usare l'esercizio 2 per mostrare che $A^e = A \otimes_F A^{\mathrm{op}}$ è semisemplice di dimensione finita.

4. Mostrare che ogni modulo su un anello artiniano semisemplice è proiettivo.

5. Usare gli esercizi 3 e 4 per mostrare che, se A è separabile di dimensione finita, allora A è un A^e-modulo proiettivo. Dedurre dal teorema 6.6 (p. 347) che $H^n(A, M) = 0$ per ogni $n \geq 1$ e per ogni M. (Ciò completa la dimostrazione del teorema.)

6. (A. I. Malcev.) Sia $A = S \oplus N$, dove $N = \operatorname{rad} A$ e S è una sottoalgebra separabile di A. Sia T una sottoalgebra separabile di A. Dimostrare che esiste $z \in N$ tale che $(1 - z)T(1 - z)^{-1} \subseteq S$.

7. Sia A un'algebra arbitraria e sia $J = \ker \varepsilon$, con $\varepsilon : A^e \to A$ l'aumentazione definita sopra. Mostrare che J è l'ideale sinistro di A^e generato dagli elementi $a \otimes 1 - 1 \otimes a$.

8. Mostrare che A è proiettivo su A^e se e solo se esiste un idempotente $e \in A^e$ tale che $(a \otimes 1)e = (1 \otimes a)e$ per ogni $a \in A$.[23]

6.12 Dimensione omologica

Sia M un modulo (sinistro) su un anello R. Le risoluzioni proiettive di M permettono di definire in modo naturale una dimensione omologica per M. Diremo che M ha *dimensione omologica finita* se ammette una risoluzione proiettiva C, ε per la quale $C_n = 0$ per ogni n sufficientemente grande. In tal caso il più piccolo intero n per cui M ammette una risoluzione proiettiva

$$\cdots 0 \longrightarrow 0 \longrightarrow C_n \longrightarrow \cdots \longrightarrow C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

si chiama *dimensione omologica* di M e si indica con $\mathrm{h.dim}\, M$. Dalla definizione segue che M è proiettivo se e solo se $\mathrm{h.dim}\, M = 0$. Ricordiamo che tali moduli sono caratterizzati dalla proprietà $\mathrm{Ext}^n(M, N) = 0$ per ogni modulo N e ogni $n \geq 1$. Il risultato seguente generalizza questo criterio.

Teorema 6.18. *Le condizioni seguenti su un modulo M sono equivalenti.*

1. $\mathrm{h.dim}\, M \leq n$.

2. $\mathrm{Ext}^{n+1}(M, N) = 0$ *per ogni modulo* N.

3. *Data una successione esatta* $0 \to C_n \to C_{n-1} \to \cdots \to C_0 \to M \to 0$ *in cui ogni* C_k *con* $k < n$ *è proiettivo, anche* C_n *è proiettivo.*

[23] Nell'enunciato a stampa manca la condizione di normalizzazione $\varepsilon(e) = 1$, necessaria per escludere in particolare la soluzione banale $e = 0$. Con tale condizione $a \mapsto (a \otimes 1)e$ è una sezione A^e-lineare dell'aumentazione. [N.d.T.]

Dimostrazione. (1) $\Rightarrow$ (2). Per ipotesi abbiamo una risoluzione proiettiva $\cdots 0 \to 0 \to C_n \to \cdots \to C_0 \to M \to 0$. Otteniamo allora il complesso

$$0 \to \hom(C_0, N) \to \hom(C_1, N) \to \cdots \to \hom(C_n, N) \to 0 \to \cdots .$$

I gruppi di coomologia di questo complesso di cocatene sono i termini della successione $\mathrm{Ext}^0(M,N), \mathrm{Ext}^1(M,N), \ldots$. È evidente che $\mathrm{Ext}^{n+1}(M,N) = 0$ e ciò vale per ogni N.

(2) $\Rightarrow$ (3). Da una successione esatta con le proprietà indicate in (3) ricaviamo la successione di omomorfismi

$$0 \to C_n \to D_n \to C_{n-1} \to D_{n-1} \to \cdots \to C_0 \to D_0 \to 0,$$

dove $D_k = \mathrm{im}(C_k \to C_{k-1})$ per $k > 0$ e $D_0 = \mathrm{im}(C_0 \to M) = M$. La freccia $C_k \to D_k$ si ottiene da $C_k \to C_{k-1}$ restringendo il codominio, mentre $D_k \to C_{k-1}$ è un'iniezione. Dunque $0 \to D_k \to C_{k-1} \to D_{k-1} \to 0$ è esatta. Dalla successione esatta lunga per Ext nella prima variabile segue l'esattezza di

$$\begin{aligned}\mathrm{Ext}^i(C_{k-1}, N) \to \mathrm{Ext}^i(D_k, N) &\to \mathrm{Ext}^{i+1}(D_{k-1}, N) \\ &\to \mathrm{Ext}^{i+1}(C_{k-1}, N)\end{aligned}$$

per $i = 1, 2, \ldots$, $1 \le k \le n$. Essendo C_{k-1} proiettivo, il primo e l'ultimo termine sono nulli. Quindi $\mathrm{Ext}^i(D_k, N) \cong \mathrm{Ext}^{i+1}(D_{k-1}, N)$ e pertanto

$$\mathrm{Ext}^1(D_n, N) \cong \mathrm{Ext}^2(D_{n-1}, N) \cong \cdots \cong \mathrm{Ext}^{n+1}(D_0, N).$$

Per (2), $\mathrm{Ext}^{n+1}(D_0, N) = 0$, dunque $\mathrm{Ext}^1(D_n, N) = 0$. Poiché $0 \to C_n \to C_{n-1} \to \cdots$ è esatta, $D_n \cong C_n$. Ne segue $\mathrm{Ext}^1(C_n, N) = 0$ per ogni N, e quindi C_n è proiettivo.

(3) $\Rightarrow$ (1). Al passo $(n-1)$-esimo, la costruzione di una risoluzione proiettiva di M dà una successione esatta $0 \leftarrow M \leftarrow C_0 \leftarrow \cdots \leftarrow C_{n-1}$ in cui tutti i C_i sono proiettivi. Poniamo $C_n = \ker(C_{n-1} \to C_{n-2})$. Abbiamo allora la successione esatta $0 \leftarrow M \leftarrow C_0 \leftarrow \cdots \leftarrow C_n \leftarrow 0$. Per (3), C_n è proiettivo. Allora $0 \leftarrow M \leftarrow C_0 \leftarrow \cdots \leftarrow C_n \leftarrow 0 \leftarrow 0 \cdots$ è una risoluzione proiettiva, e ciò dimostra che $\mathrm{h.dim}\, M \le n$. □

Osservazioni. La dimostrazione dell'implicazione (1) $\Rightarrow$ (2) mostra anche che, se $\mathrm{h.dim}\, M \le n$, allora $\mathrm{Ext}^k(M,N) = 0$ per ogni $k > n$ e per ogni modulo N. In modo analogo questa condizione implica che $\mathrm{Tor}_k(M,N) = 0$ per ogni $k > n$ e ogni N. È pure chiaro che, se $\mathrm{h.dim}\, M = n$, per ogni $k \le n$ esiste un modulo N tale che $\mathrm{Ext}^k(M,N) \neq 0$.

Dal fatto che $\mathrm{Ext}^k(-,N)$ è un funtore additivo da R-**mod** in **Ab** segue che $\mathrm{Ext}^k(M' \oplus M'', N) \cong \mathrm{Ext}^k(M',N) \oplus \mathrm{Ext}^k(M'',N)$. Da questa relazione e dal teorema 6.18 discende immediatamente che $M = M' \oplus M''$ ha dimensione omologica finita se e solo se l'hanno sia M' sia M''. In tal caso $\mathrm{h.dim}\, M$ è la maggiore delle due dimensioni $\mathrm{h.dim}\, M'$ e $\mathrm{h.dim}\, M''$. Consideriamo, più in generale, le relazioni fra le dimensioni omologiche dei termini di una successione esatta corta $0 \to M' \to M \to M'' \to 0$. Per ogni modulo N abbiamo la successione esatta lunga

$$\cdots \to \mathrm{Ext}^k(M'', N) \to \mathrm{Ext}^k(M, N) \to \mathrm{Ext}^k(M', N) \to \mathrm{Ext}^{k+1}(M'', N) \to \cdots .$$

Supponiamo $\mathrm{h.dim}\, M \le n$. Allora per $k > n$ si ha $\mathrm{Ext}^k(M,N) = 0$ e quindi $\mathrm{Ext}^k(M',N) \cong \mathrm{Ext}^{k+1}(M'',N)$. Analogamente, se $\mathrm{h.dim}\, M' \le n$, si ha $\mathrm{Ext}^{k+1}(M'',N) \cong \mathrm{Ext}^{k+1}(M,N)$ per $k > n$, e se $\mathrm{h.dim}\, M'' \le n$, si ha $\mathrm{Ext}^k(M,N) \cong \mathrm{Ext}^k(M',N)$ per $k > n$. Da queste relazioni segue, anzitutto, che, se due qualsiasi dei tre moduli M, M', M'' hanno dimensione omologica finita, anche il terzo ha dimensione omologica finita. Supponiamo di trovarci in questo caso e poniamo $\mathrm{h.dim}\, M = n$, $\mathrm{h.dim}\, M' = n'$, $\mathrm{h.dim}\, M'' = n''$. Dalle relazioni osservate fra gli Ext si vede subito che si verifica una delle seguenti possibilità.

I. $n \leq n', n''$. Allora o $n = n' = n''$, oppure $n \leq n'$ e $n'' = n' + 1$.

II. $n' \leq n''$, $n' < n$. Allora $n = n''$.

III. $n'' \leq n'$, $n'' < n$. Allora $n = n'$.

Ne segue che, se $n > n'$, allora $n'' = n$, se $n < n'$, allora $n'' = n' + 1$, e se $n = n'$, allora $n'' \leq n' + 1$. Enunciamo i risultati ottenuti.

Teorema 6.19. *Sia* $0 \to M' \to M \to M'' \to 0$ *esatta. Se due qualsiasi delle dimensioni* $\mathrm{h.dim}\, M', \mathrm{h.dim}\, M, \mathrm{h.dim}\, M''$ *sono finite, anche la terza è finita. Inoltre* $\mathrm{h.dim}\, M'' = \mathrm{h.dim}\, M$ *se* $\mathrm{h.dim}\, M' < \mathrm{h.dim}\, M$, $\mathrm{h.dim}\, M'' = \mathrm{h.dim}\, M' + 1$ *se* $\mathrm{h.dim}\, M < \mathrm{h.dim}\, M'$, *e* $\mathrm{h.dim}\, M'' \leq \mathrm{h.dim}\, M + 1$ *se* $\mathrm{h.dim}\, M = \mathrm{h.dim}\, M'$.

La nozione di dimensione omologica di un modulo porta a definire dimensioni omologiche per un anello. Chiamiamo *dimensione globale sinistra (destra)* di R l'estremo superiore delle $\mathrm{h.dim}\, M$ al variare di M tra i moduli sinistri (destri) su R. La dimensione globale sinistra (destra) è dunque zero se e solo se ogni R-modulo sinistro (destro) è proiettivo. Questo accade se e solo se si spezza ogni successione esatta corta di moduli sinistri (destri) $0 \to M' \to M \to M'' \to 0$ (p. 150), ossia se e solo se ogni modulo sinistro (destro) su R è completamente riducibile. Pertanto R ha dimensione globale sinistra (destra) zero se e solo se è artiniano semisemplice (p. 208). Dunque R ha dimensione globale sinistra zero se e solo se ha dimensione globale destra zero. Al di fuori di questo caso, in generale non vi è alcun legame fra le dimensioni globali sinistra e destra di un anello. Ci interesseremo soprattutto degli anelli commutativi, per i quali, naturalmente, i moduli sinistri e destri si identificano ed esiste una sola nozione di dimensione globale.

Un dominio (commutativo) a ideali principali R che non sia un campo ha dimensione globale uno. Infatti ogni sottomodulo di un R-modulo libero è libero (esercizio 4, p. 155). Per ogni R-modulo M si ha dunque una successione esatta $0 \to K \to F \to M \to 0$ in cui F e K sono liberi. Quindi $\mathrm{h.dim}\, M \leq 1$ per ogni M e la dimensione globale di R è al più uno. D'altra parte non è zero, perché altrimenti R sarebbe artiniano semisemplice e quindi somma diretta di un numero finito di campi. Poiché R non ha divisori dello zero non nulli, dovrebbe essere esso stesso un campo, contro l'ipotesi.

Esercizio. 1. Sia M un modulo su un anello commutativo K, e sia L una K-algebra commutativa e libera come K-modulo. Dimostrare che $\mathrm{h.dim}_K M = \mathrm{h.dim}_L M_L$ (con $\mathrm{h.dim}_K M$ si intende la dimensione omologica come K-modulo).

6.13 Il complesso di Koszul e il teorema delle sizigie di Hilbert

Consideriamo ora le proprietà omologiche dell'anello $R = F[x_1, \ldots, x_m]$ dei polinomi nelle indeterminate x_i a coefficienti in un campo F. Il nostro obiettivo principale è un teorema di Hilbert sui moduli graduati per l'anello R, graduato nel modo consueto per componenti omogenee. Consideriamo dapprima la decomposizione $R = F \oplus J$, dove J è l'ideale di R costituito dai polinomi con termine costante nullo o, equivalentemente, che si annullano in 0. Questa decomposizione permette di definire su F una struttura di R-modulo ponendo $(a + f)b = ab$ per $a, b \in F$, $f \in J$. Si noti che questo modulo è isomorfo a R/J. Uno strumento importante nello studio delle proprietà omologiche di R è una particolare risoluzione di F come R-modulo, introdotta da Koszul in un contesto più generale che si applica allo studio dell'omologia delle algebre di Lie (si veda, dell'autore, *Lie Algebras*, pp. 174–185).

Il complesso di Koszul, che fornisce una risoluzione di F, si basa sull'algebra esterna $E(M)$ di un modulo libero M di rango m su $R = F[x_1, \dots, x_m]$. Occorre richiamare le definizioni e le proprietà elementari delle algebre esterne ottenute nel capitolo 3 (p. 141). Siano K un anello commutativo arbitrario, M un K-modulo ed $E(M)$ l'algebra esterna definita da M. Ricordiamo che M è immerso in $E(M)$ e che $E(M)$ è graduata, con $E(M) = K \oplus M \oplus M^2 \oplus \cdots$. Ricordiamo anche la proprietà universale fondamentale di $E(M)$: si ha $x^2 = 0$ per ogni $x \in M$ e, se f è un K-omomorfismo di M in un'algebra A su K tale che $f(x)^2 = 0$, allora f si estende in uno e un solo modo a un omomorfismo di K-algebre di $E(M)$ in A. In particolare, l'applicazione $x \mapsto -x$ in M ha un'unica estensione a un omomorfismo ι di $E(M)$ in sé e, poiché applicando due volte $x \mapsto -x$ si ottiene l'identità, $\iota^2 = 1_{E(M)}$.

Diremo che un K-endomorfismo D di $E(M)$ è un'*antiderivazione* se

$$D(ab) = (Da)b + \bar{a}(Db), \qquad \bar{a} = \iota a. \tag{92}$$

Ci occorre il seguente lemma.

Lemma 1. *Sia D un K-omomorfismo di M in $E(M)$ tale che*

$$x(Dx) = (Dx)x, \qquad x \in M. \tag{93}$$

Allora D si estende in uno e un solo modo a un'antiderivazione di $E(M)$.

Dimostrazione. Consideriamo l'applicazione

$$f\colon x \longmapsto \begin{pmatrix} x & 0 \\ Dx & -x \end{pmatrix}$$

di M nell'algebra $A = M_2(E(M))$. La condizione su D implica che f è un K-omomorfismo tale che $f(x)^2 = 0$. Pertanto f ha un'unica estensione a un omomorfismo di algebre di $E(M)$ in A. È chiaro che l'estensione ha la forma

$$f\colon a \longmapsto \begin{pmatrix} a & 0 \\ Da & \bar{a} \end{pmatrix}, \qquad a \in E(M),$$

dove $\bar{a} = \iota a$ e D è un K-endomorfismo di $E(M)$ che estende il D dato. La condizione $f(ab) = f(a)f(b)$ implica che D è un'antiderivazione. L'unicità dell'estensione segue dai fatti seguenti, di immediata verifica.

1. La differenza di due antiderivazioni è un'antiderivazione.
2. Il sottoinsieme su cui un'antiderivazione è nulla è una sottoalgebra.
3. M genera $E(M)$.

Ora, se D_1 e D_2 sono antiderivazioni tali che $D_1|_M = D_2|_M = D$, allora $D_1 - D_2$ è un'antiderivazione tale che $(D_1 - D_2)|_M = 0$. Poiché M genera $E(M)$, si ha $D_1 - D_2 = 0$ e $D_1 = D_2$. □

Un caso particolare in cui si applica il lemma è quello in cui $D = d \in M^*$, il K-modulo dei K-omomorfismi di M in K (il modulo duale di M). Poiché $K \subseteq E(M)$, possiamo considerare d come un K-omomorfismo di M in $E(M)$. Poiché K è contenuto nel centro di $E(M)$, è chiaro che la condizione $(dx)x = x(dx)$ del lemma è soddisfatta. Abbiamo dunque un'estensione d che è un'antiderivazione di $E(M)$. Poiché $dM \subseteq K$ e d è un'antiderivazione, si può dimostrare per

induzione che $dM^i \subseteq M^{i-1}$, $i \geq 1$. Dimostriamo ora che, se $d \in M^*$, l'antiderivazione d che la estende soddisfa il

Lemma 2. $d^2 = 0$.

Dimostrazione. Dalla regola dell'antiderivazione risulta che $D1 = 0$ per ogni antiderivazione. Quindi $dk = 0$ per $k \in K$. Allora $d^2M = 0$, poiché $dM \subseteq K$. Osserviamo poi che $\overline{dx} = dx = -d\bar{x}$ per $x \in M$ e che, se $a \in E(M)$ soddisfa $\overline{da} = -d\bar{a}$, dal fatto che d è un'antiderivazione segue $\overline{d(ax)} = -d(\overline{ax})$. Pertanto $\overline{da} = -d\bar{a}$ per ogni a. Per induzione su i, questa relazione implica $d^2M^i = 0$. Dunque $d^2 = 0$. □

Abbiamo ora il complesso di catene

$$0 \longleftarrow K \xleftarrow{d} M \xleftarrow{d} M^2 \longleftarrow \cdots \tag{94}$$

determinato dall'elemento $d \in M^*$. Ci occorrerà anche un risultato sul cambiamento dell'anello base per le algebre esterne.

Lemma 3. *Siano M un modulo su un anello commutativo K, L un'algebra commutativa su K ed $E(M)$ l'algebra esterna su M. Allora $E(M)_L = E(M_L)$.*

Dimostrazione. Poiché M è un addendo diretto di $E(M)$, possiamo identificare M_L con il sottoinsieme di $E(M)_L$ degli elementi $\sum l_i \otimes x_i$, $l_i \in L$, $x_i \in M \subseteq E(M)$. Si ha $x_i^2 = 0$, e quindi $x_ix_j + x_jx_i = (x_i + x_j)^2 - x_i^2 - x_j^2 = 0$ per $x_i, x_j \in M$. Ne segue che $(\sum l_i \otimes x_i)^2 = 0$ per ogni $\sum l_i \otimes x_i \in M_L$. Sia $\tilde{f}$ un L-omomorfismo di M_L in un'algebra $\widetilde{A}/L$ tale che $\tilde{f}(\tilde{x})^2 = 0$, $\tilde{x} \in M_L$. Allora $\widetilde{A}$ diventa un'algebra su K se definiamo $k\tilde{a}$, $k \in K$, $\tilde{a} \in \widetilde{A}$, come $(k1)\tilde{a}$, con $k1 \in L$. Per $x \in M$, $f\colon x \mapsto \tilde{f}(1 \otimes x)$ è un K-omomorfismo di M in $\widetilde{A}/K$ tale che $f(x)^2 = 0$. Esso si estende dunque a un K-omomorfismo f di $E(M)$ in $\widetilde{A}/K$. Abbiamo allora l'omomorfismo $1 \otimes f$ di $E(M)_L$ in $(\widetilde{A}/K)_L$ e l'omomorfismo di L-algebre di $(\widetilde{A}/K)_L$ in $\widetilde{A}/L$ dato da $l \otimes \tilde{a} \mapsto l\tilde{a}$. Componendoli otteniamo un omomorfismo di L-algebre di $E(M)_L$ in $\widetilde{A}/L$. Esso manda l'elemento $1 \otimes x$, $x \in M$, in $f(x) = \tilde{f}(1 \otimes x)$. Coincide dunque su M_L con l'L-omomorfismo $\tilde{f}$ assegnato. Abbiamo così ottenuto un'estensione di $\tilde{f}$ a un omomorfismo di algebre di $E(M)_L$ in $\widetilde{A}/L$. Poiché M genera $E(M)$, M_L genera $E(M)_L$. L'estensione è dunque unica. Abbiamo quindi mostrato che $E(M)_L$ possiede la proprietà universale che caratterizza $E(M_L)$ e possiamo perciò identificare le due algebre. □

Specializziamo ora K a $R = F[x_1, \ldots, x_m]$, dove F è un campo e le x_i sono indeterminate. Sia V uno spazio vettoriale su F di dimensione m, sia $(y_1, \ldots, y_m)$ una base di V/F ed $E(V)$ l'algebra esterna determinata da V. Allora $E(V) = F1 \oplus V \oplus \cdots \oplus V^m$, $V^{m+1} = 0$, e V^r ha per base i $\binom{m}{r}$ elementi $y_{i_1} \cdots y_{i_r}$ con $i_1 < i_2 < \cdots < i_r$ (*BA I*, p. 415). Sia $M = V_R$. Per il lemma 3, $E(M) = R1 \oplus M \oplus \cdots \oplus M^m$, dove M^r ha per base su R gli elementi $y_{i_1} \cdots y_{i_r}$. Questo modulo è dunque libero di rango $\binom{m}{r}$ su R. (Ciò si può vedere anche direttamente, con lo stesso metodo usato nel caso di V/F.) Sia d l'elemento di $M^* = \hom_R(M, R)$ tale che $dy_i = x_i$, $1 \leq i \leq m$, e indichiamo ancora con d l'antiderivazione di $E(M)$ che lo estende. Abbiamo allora il complesso di catene (94) e vogliamo mostrare che, se ε è l'omomorfismo canonico di R in F ottenuto valutando un polinomio in $(0, \ldots, 0)$, allora

$$0 \longleftarrow F \xleftarrow{\varepsilon} R \xleftarrow{d} M \longleftarrow \cdots \longleftarrow M^m \longleftarrow 0 \longleftarrow \cdots \tag{95}$$

è una risoluzione di F come R-modulo con aumentazione ε. Poiché $F \subseteq R \subseteq E(M)$ e $E(M)$ è uno spazio vettoriale su F, possiamo estendere ε a una trasformazione lineare ε di $E(M)/F$ ponendo $\varepsilon(M^i) = 0$, $i \geq 1$. Allora $\varepsilon E(M) = \varepsilon R = F$ e perciò $d\varepsilon = 0$. Inoltre, poiché $dE(M) \subseteq dM + \sum_{i \geq 1} M^i$ e dM è l'ideale di R generato dagli elementi $x_i = dy_i$, si ha $\varepsilon dM = 0$,

e dunque $\varepsilon dE(M) = 0$. Abbiamo così

$$\varepsilon d = 0 = d\varepsilon. \tag{96}$$

Inoltre, poiché $\sum_{i\geq 1} M^i$ è un ideale di $E(M)$ e $\varepsilon|_R$ è un omomorfismo di F-algebre di R in F, si ha

$$\varepsilon(ab) = (\varepsilon a)(\varepsilon b) \tag{97}$$

per $a, b \in E(M)$. Dunque ε è un omomorfismo di F-algebre di $E(M)$.

La dimostrazione che la (95) è esatta è simile ad altre due dimostrazioni di esattezza già date (p. 359 e p. 373). Essa si basa sul seguente lemma.

Lemma 4. *Esiste una trasformazione lineare s di $E(M)/F$ tale che*

$$sd + ds = 1 - \varepsilon. \tag{98}$$

Dimostrazione. Procediamo per induzione su m. Se $m = 1$, allora $M = Ry$ ed $E(M) = R1 \oplus Ry$. Poiché $(1, x, x^2, \ldots)$ è una base di $R = F[x]$ su F, $(1, x, x^2, \ldots, y, xy, x^2y, \ldots)$ è una base di $E(M)/F$. Si ha $dx^i = 0$, $d(x^iy) = x^{i+1}$, $i \geq 0$, e $\varepsilon 1 = 1$, $\varepsilon x^{i+1} = 0$, $\varepsilon(x^iy) = 0$. Sia s la trasformazione lineare di $E(M)/F$ tale che $s1 = 0$, $sx^i = x^{i-1}y$ per $i \geq 1$, $s(x^iy) = 0$. Si verifica subito che vale la (98). Notiamo inoltre che

$$s\varepsilon = 0 = \varepsilon s, \qquad \iota\varepsilon = \varepsilon = \varepsilon\iota, \qquad s\iota + \iota s = 0, \tag{99}$$

dove ι è l'automorfismo definito in precedenza. Supponiamo ora il lemma vero per $m - 1 > 0$. Sia E_1 l'F-sottospazio di $E(M)$ generato dagli elementi $x_1^k, x_1^k y_1$, $k \geq 0$, ed E_2 l'F-sottospazio generato dagli elementi $x_2^{k_2} \cdots x_m^{k_m} y_{i_1} \cdots y_{i_r}$ con $k_j \geq 0$ e $2 \leq i_1 < i_2 < \cdots < i_r \leq m$. Esaminando le basi si vede allora che E_1 è una sottoalgebra isomorfa a $E(M_1)$, con $M_1 = Ry_1$, ed E_2 è una sottoalgebra isomorfa a $E(M_2)$, con $M_2 = \sum_{j=2}^m Ry_j$, e che $u \otimes v \mapsto uv$ è un isomorfismo di spazi vettoriali (non di algebre) da $E_1 \otimes_F E_2$ su $E(M)$. Osserviamo inoltre che ι e d lasciano stabili E_1 ed E_2 e che le applicazioni indotte sono quelle definite in $E(M)$. Per induzione abbiamo in E_2 una trasformazione lineare s_2 tale che $s_2d + ds_2 = 1 - \varepsilon$. Sia s_1 la trasformazione lineare di E_1 definita all'inizio della dimostrazione. Poiché $E(M) \simeq E_1 \otimes_F E_2$, esiste un'unica trasformazione lineare s di $E(M)$ tale che

$$s(uv) = (s_1u)v + (\varepsilon u)(s_2v) \tag{100}$$

per $u \in E_1$, $v \in E_2$. Allora

$$\begin{aligned}
ds(uv) &= (ds_1u)v + (\iota s_1u)(dv) + (d\varepsilon u)(s_2v) + (\iota\varepsilon u)(ds_2v) \\
&= (ds_1u)v + (\iota s_1u)(dv) + (\varepsilon u)(ds_2v), \\
sd(uv) &= s\big((du)v + (\iota u)dv\big) \\
&= (s_1du)v + (\varepsilon du)(s_2v) + (s_1\iota u)(dv) + (\varepsilon\iota u)(s_2dv) \\
&= (s_1du)v + (s_1\iota u)(dv) + (\varepsilon u)(s_2dv).
\end{aligned}$$

Quindi

$$\begin{aligned}
(ds + sd)(uv) &= ((1 - \varepsilon)u)v + (\varepsilon u)((1 - \varepsilon)v) \\
&= uv - (\varepsilon u)v + (\varepsilon u)v - (\varepsilon u)(\varepsilon v) \\
&= (1 - \varepsilon)(uv),
\end{aligned}$$

poiché ε è un omomorfismo di algebre. La dimostrazione è completa. □

Possiamo ora provare che la successione (95) è esatta. Sappiamo anzitutto che ε è suriettivo, dunque $R \to F \to 0$ è esatta. Abbiamo anche visto che dM è l'ideale di R generato dalle x_i. Poiché questo è l'ideale dei polinomi che si annullano in $(0, 0, \dots, 0)$, si ha $dM = J = \ker \varepsilon$. Dunque $M \xrightarrow{d} R \to F \to 0$ è esatta. Resta da mostrare che, se $z_i \in M^i$, $i \geq 1$, e $dz_i = 0$, esiste $w_{i+1} \in M^{i+1}$ tale che $dw_{i+1} = z_i$. Si ha $z_i = 1z_i = (1 - \varepsilon)z_i = (sd + ds)z_i = d(sz_i) = dw$, dove $w = sz_i$. Possiamo scrivere $w = \sum_{j=0}^{m} w_j$, $w_j \in M^j$. Allora $dw_j \in M^{j-1}$ per $j \geq 1$, e quindi $dw = z_i$ dà $dw_{i+1} = z_i$. La (95) è dunque esatta. Riassumiamo i risultati nel

Teorema 6.20. *Sia $R = F[x_1, \dots, x_m]$, con x_i indeterminate ed F un campo, e sia M l'R-modulo libero di base $(y_1, \dots, y_m)$, $E(M)$ l'algebra esterna definita da M. Sia d l'antiderivazione di $E(M)$ tale che $dy_i = x_i$, $1 \leq i \leq m$, ed ε l'omomorfismo di anelli da R in F tale che $\varepsilon f = f(0, \dots, 0)$. Allora $dM^i \subseteq M^{i-1}$ e*

$$0 \longleftarrow F \xleftarrow{\varepsilon} R \xleftarrow{d} M \longleftarrow \cdots \longleftarrow M^m \longleftarrow 0 \longleftarrow \cdots$$

è una risoluzione libera di F come R-modulo.

Chiamiamo questa risoluzione la *risoluzione di Koszul* di F come R-modulo e il complesso $M^0 (= R) \leftarrow M^1 \leftarrow M^2 \leftarrow \cdots$ il *complesso di Koszul* per R.

Poiché $M^k = 0$ per $k > m$, si ha evidentemente $\mathrm{h.dim}\, F \leq m$. Affermiamo che in realtà $\mathrm{h.dim}\, F = m$. Ciò seguirà da una delle osservazioni successive al teorema 6.18, mostrando che $\mathrm{Tor}_m^R(F, F) \neq 0$. Più in generale, determiniamo $\mathrm{Tor}_r^R(F, F)$ utilizzando la risoluzione di Koszul del secondo F. Otteniamo il complesso

$$0 \longleftarrow F \otimes_R R \longleftarrow F \otimes_R M \longleftarrow F \otimes_R M^2 \longleftarrow \cdots, \tag{101}$$

i cui gruppi di omologia danno $\mathrm{Tor}_0^R(F, F), \mathrm{Tor}_1^R(F, F), \dots$. Ora $M^r \simeq R \otimes_F V^r$, dove V è lo spazio vettoriale di dimensione m su F considerato sopra, e

$$F \otimes_R M^r \simeq F \otimes_R (R \otimes_F V^r) \simeq (F \otimes_R R) \otimes_F V^r \simeq F \otimes_F V^r \simeq V^r.$$

Se, come prima, usiamo per M^r, $1 \leq r \leq m$, la base $\{y_{i_1} \cdots y_{i_r} \mid i_1 < i_2 < \cdots < i_r\}$, possiamo seguire la catena degli isomorfismi e vedere che l'isomorfismo di $F \otimes_R M^r$ su V^r/F manda $\alpha \otimes f y_{i_1} \cdots y_{i_r}$, per $\alpha \in F$, $f \in R$, in $\alpha(\varepsilon f) y_{i_1} \cdots y_{i_r}$, con $\varepsilon f = f(0, \dots, 0)$. La definizione di d dà

$$d(y_{i_1} \cdots y_{i_r}) = \sum_{j=1}^{r} (-1)^{j+1} x_{i_j} y_{i_1} \cdots y_{i_{j-1}} y_{i_{j+1}} \cdots y_{i_r}. \tag{102}$$

Quindi $(1 \otimes d)(\alpha \otimes 1 y_{i_1} \cdots y_{i_r})$ va in 0 mediante il nostro isomorfismo. Pertanto gli operatori bordo nella (101) sono tutti nulli e l'isomorfismo $F \otimes_R M^r \to V^r$ dà l'F-isomorfismo

$$\mathrm{Tor}_r^R(F, F) \simeq V^r. \tag{103}$$

In particolare, $\mathrm{Tor}_m^R(F, F) \simeq V^m \simeq F$.

Il risultato appena dimostrato, $\mathrm{h.dim}\, F = m$, implica che $R = F[x_1, \dots, x_m]$ ha dimensione globale maggiore o uguale a m. Non è difficile completare questo risultato e dimostrare che la dimensione globale di R è esattamente m. Ne daremo un'indicazione negli esercizi. Nel resto del paragrafo considereremo un risultato in qualche modo analogo, dovuto a Hilbert, sulle risoluzioni libere dei moduli graduati per R. Naturalmente Hilbert dovette enunciare il suo teorema in una forma più rudimentale di quella a noi consentita, perché non disponeva dei concetti che utilizzeremo.

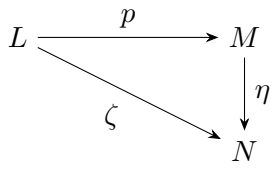
Ricordiamo anzitutto la graduazione consueta di $R = F[x_1, \ldots, x_m]$:

$$F[x_1, \ldots, x_m] = R^{(0)}\,(= F1) \oplus R^{(1)} \oplus R^{(2)} \oplus \cdots , \tag{104}$$

dove $R^{(i)}$ è il sottospazio su F delle forme di grado i, ossia delle combinazioni F-lineari di monomi di grado totale i nelle x. Si ha $R^{(i)}R^{(j)} \subseteq R^{(i+j)}$.

Se R è un anello graduato, con graduazione data dai sottogruppi $R^{(i)}$ del gruppo additivo ($R = R^{(0)} \oplus R^{(1)} \oplus \cdots$, $R^{(i)}R^{(j)} \subseteq R^{(i+j)}$), si dice che un R-modulo M è *graduato* dai sottogruppi $M^{(i)}$, $i = 0, 1, \ldots$, del suo gruppo additivo se $M = M^{(0)} \oplus M^{(1)} \oplus M^{(2)} \oplus \cdots$ e $R^{(i)}M^{(j)} \subseteq M^{(i+j)}$ per ogni i, j. Gli elementi di $M^{(i)}$ si dicono *omogenei di grado i*. Un sottomodulo N di M si dice *omogeneo* se $N = \sum_i (N \cap M^{(i)})$ o, equivalentemente, se, da $v = \sum v^{(i)} \in N$ con $v^{(i)} \in M^{(i)}$, segue $v^{(i)} \in N$ per ogni i. Allora N è graduato dalle componenti $N^{(i)} = N \cap M^{(i)}$. Inoltre M/N è graduato dai sottogruppi $(M^{(i)} + N)/N$, e $(M^{(i)} + N)/N \simeq M^{(i)}/(M^{(i)} \cap N)$. Se M e N sono R-moduli graduati, un *omomorfismo di moduli graduati* η (di grado 0) è un omomorfismo nel senso consueto degli R-moduli tale che $\eta M^{(i)} \subseteq N^{(i)}$ per ogni i. L'immagine $\eta(M)$ è allora un sottomodulo omogeneo di N e $\ker \eta$ è un sottomodulo omogeneo di M.

Se M è un modulo graduato per l'anello graduato R, possiamo scegliere un sistema di generatori $\{u_\alpha\}$ di M in modo che ogni u_α sia omogeneo (per esempio, $\{u_\alpha\} = \bigcup_i M^{(i)}$). Sia $\{e_\alpha\}$ un insieme di elementi indicizzati dallo stesso insieme $I = \{\alpha\}$ di $\{u_\alpha\}$, e sia L un R-modulo libero di base $\{e_\alpha\}$. Si ha allora l'omomorfismo ε di L su M che manda e_α in u_α. Sia $L^{(i)}$ l'insieme delle somme di elementi della forma $a^{(j)}e_\alpha$, dove $a^{(j)} \in R^{(j)}$ e $j + \deg u_\alpha = i$. Si vede subito che L è graduato dagli $L^{(i)}$ e che l'epimorfismo ε è un omomorfismo di moduli graduati. Si vede anche facilmente che, se N è un modulo graduato e $\eta\colon M \to N$ è un omomorfismo (di moduli graduati), esiste un omomorfismo ζ che rende commutativo il diagramma



Supponiamo ora che M sia un modulo graduato per $R = F[x_1, \ldots, x_m]$. Sia $L = L_0$ un modulo graduato libero per cui si ha un epimorfismo ε di L_0 su M e sia $K_0 = \ker \varepsilon$. Allora K_0 è graduato e possiamo quindi determinare un modulo graduato libero L_1 con un epimorfismo ε_1 di L_1 su K_0. Componendo con l'iniezione di K_0 in L_0 otteniamo $d_1\colon L_1 \to L_0$. Sia ancora $K_1 = \ker d_1$ e siano L_2, ε_2 un modulo graduato libero e un epimorfismo di L_2 su K_1; sia d_2 il composto di quest'ultimo con l'iniezione di K_1 in L_1. Si prosegue in questo modo. Il teorema delle sizigie di Hilbert afferma che in al più m passi si ottiene un nucleo K_i che è esso stesso libero, cosicché non occorre proseguire. In una forma leggermente diversa possiamo enunciare il

Teorema delle sizigie di Hilbert. *Sia M un modulo graduato per $R = F[x_1, \ldots, x_m]$, l'anello dei polinomi in m indeterminate a coefficienti in un campo F. Sia*

$$0 \longleftarrow M \xleftarrow{\varepsilon} L_0 \xleftarrow{d_1} L_1 \longleftarrow \cdots \longleftarrow L_{m-1} \xleftarrow{d_m} K_m$$

una successione esatta di omomorfismi di moduli graduati nella quale tutti gli L_i sono liberi. Allora K_m è libero.

La dimostrazione si baserà sul risultato $\mathrm{h.dim}\, F \leq m$ e su altri due risultati che ricaveremo ora. Come prima, F è considerato come R-modulo in cui $JF = 0$, dove J è l'ideale dei polinomi che si annullano in $(0, \ldots, 0)$. Poiché $J = \sum_{i>0} R^{(i)}$, F diventa un R-modulo graduato se poniamo $F^{(0)} = F$, $F^{(i)} = 0$ per $i \geq 1$. Dimostriamo ora il

Lemma 5. *Se M è un R-modulo graduato e $M \otimes_R F = 0$, allora $M = 0$.*

Dimostrazione. Abbiamo la successione esatta $0 \to J \to R \to F \to 0$. Essa dà la successione esatta $M \otimes_R J \to M \otimes_R R \to M \otimes_R F \to 0$. Poiché $M \otimes_R R \simeq M$ e, per ipotesi, $M \otimes_R F = 0$, otteniamo l'esattezza di $M \otimes_R J \to M \to 0$. L'applicazione manda un elemento $\sum u_i \otimes f_i$ in $\sum f_i u_i$, cosicché l'esattezza significa che ogni elemento di M può essere scritto nella forma $\sum f_i u_i$, con $u_i \in M$ e $f_i \in J$. Ne segue che $M = 0$. In caso contrario, infatti, sia u un elemento non nullo di M di grado minimo (il grado è il massimo dei gradi delle componenti omogenee). Allora $u = \sum f_i u_i$, con $f_i \in J$, $u_i \in M$ e f_i, u_i omogenei. Poiché i gradi degli f_i sono positivi, esiste un $u_i \neq 0$ con $\deg u_i < \deg u$, contrariamente alla scelta di u. Dunque $M = 0$. □

Il risultato essenziale per dimostrare il teorema di Hilbert è il seguente.

Teorema 6.21. *Se M è un modulo graduato tale che $\operatorname{Tor}_1^R(M, F) = 0$, allora M è libero.*

Dimostrazione. Possiamo considerare $M \otimes_R F$ come spazio vettoriale su F restringendo a F l'azione di R. Allora, se $\alpha, \beta \in F$ e $u \in M$, si ha $\alpha(u \otimes \beta) = \alpha u \otimes \beta = u \otimes \alpha\beta$. Ne segue che gli elementi della forma $u \otimes 1$, con $u \in M$ omogeneo, generano $M \otimes_R F$ come spazio vettoriale su F, e quindi possiamo scegliere una base di $M \otimes_R F$ della forma $\{u_i \otimes 1 \mid u_i \in M\}$. Sia L un R-modulo libero di base $\{b_i\}$. Dimostreremo che M è libero di base $\{u_i\}$ mostrando che l'omomorfismo η di L in M tale che $\eta b_i = u_i$ è un isomorfismo. Sia C il conucleo di η. Si ha allora la successione esatta $L \xrightarrow{\eta} M \xrightarrow{p} C \to 0$ e quindi la successione esatta

$$L \otimes_R F \xrightarrow{\eta \otimes 1} M \otimes_R F \xrightarrow{p \otimes 1} C \otimes_R F \longrightarrow 0.$$

L'applicazione $\eta \otimes 1$ manda $b_i \otimes 1$ in $u_i \otimes 1$ e, poiché $\{u_i \otimes 1\}$ è una base di $M \otimes_R F$, $\eta \otimes 1$ è un isomorfismo. Quindi $C \otimes_R F = 0$ e, per il lemma 5, $C = 0$. Ciò significa che η è suriettivo e che $L \xrightarrow{\eta} M \to 0$ è esatta. Sia ora $K = \ker \eta$. Abbiamo la successione esatta $0 \to K \to L \to M \to 0$, che dà la successione esatta

$$\operatorname{Tor}_1^R(M, F) \longrightarrow K \otimes_R F \longrightarrow L \otimes_R F \xrightarrow{\eta \otimes 1} M \otimes_R F.$$

Per ipotesi $\operatorname{Tor}_1^R(M, F) = 0$ e abbiamo visto che $\eta \otimes 1$ è un isomorfismo. Quindi $K \otimes_R F = 0$ e, ancora per il lemma 5, $K = 0$. Allora $\ker \eta = 0$ ed η è un isomorfismo. □

Poiché ogni modulo proiettivo soddisfa l'ipotesi $\operatorname{Tor}_1^R(M, F) = 0$ (teorema 6.10, p. 354), dal teorema 6.21 si ottiene la conseguenza seguente.

Corollario. *Ogni R-modulo proiettivo graduato, per $R = F[x_1, \ldots, x_m]$, è libero.*

Possiamo ora dare la *dimostrazione del teorema delle sizigie di Hilbert.* L'argomento usato nella dimostrazione dell'implicazione (2) ⇒ (3) del teorema 6.18, p. 376, mostra che $\operatorname{Tor}_1^R(K_m, F) \simeq \operatorname{Tor}_{m+1}^R(M, F)$. Poiché $\text{h.dim}\, F \leq m$, si ha $\operatorname{Tor}_{m+1}^R(M, F) = 0$ per una delle osservazioni successive al teorema 6.18. Quindi $\operatorname{Tor}_1^R(K_m, F) = 0$ e K_m è libero per il teorema 6.21. □

Esercizi.

1. Sia K un anello commutativo di dimensione globale finita m e sia $K[x]$ l'anello dei polinomi in un'indeterminata x su K. Sia M un $K[x]$-modulo e sia $\widetilde{M} = K[x] \otimes_K M$. Si osservi che ogni elemento di $\widetilde{M}$ si può scrivere in uno e un solo modo nella forma $1 \otimes u_0 + x \otimes u_1 + x^2 \otimes u_2 + \cdots$, $u_i \in M$. Si osservi che esiste un $K[x]$-omomorfismo η di $\widetilde{M}$ su M tale che $f(x) \otimes u \mapsto f(x)u$ per $f(x) \in K[x]$, $u \in M$. Mostrare che $N = \ker \eta$ è l'insieme degli elementi
$$(x \otimes u_0 - 1 \otimes x u_0) + (x^2 \otimes u_1 - 1 \otimes x^2 u_1) + \cdots$$
$$+ (x^n \otimes u_{n-1} - 1 \otimes x^n u_{n-1}) + \cdots$$

e che l'applicazione

$$\begin{aligned} 1 \otimes u_0 + x \otimes u_1 + x^2 \otimes u_2 + \cdots \\ \longmapsto (x \otimes u_0 - 1 \otimes x u_0) + (x^2 \otimes u_1 - 1 \otimes x^2 u_1) + \cdots \end{aligned}$$

è un $K[x]$-isomorfismo, sicché si ha una successione esatta di $K[x]$-omomorfismi $0 \to \widetilde{M} \to \widetilde{M} \to M \to 0$. Per l'esercizio 1 di p. 378, $\mathrm{h.\,dim}_{K[x]} \widetilde{M} = \mathrm{h.\,dim}_K M \leq m$. Pertanto, per il teorema 6.19, $\mathrm{h.\,dim}_{K[x]} M \leq m + 1$ e la dimensione globale di $K[x]$ è minore o uguale a $m + 1$.

2. Dimostrare che, se F è un campo e le x_j sono indeterminate, la dimensione globale di $F[x_1, \ldots, x_m]$ è m.

Riferimenti bibliografici.

- D. Hilbert, «Über die Theorie der Algebraischen Formen», *Mathematische Annalen*, vol. 36 (1890), pp. 473–534.
- H. Cartan e S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, N.J., 1956.
- S. MacLane, *Homology*, Springer, New York, 1963.
- P. J. Hilton e U. Stammbach, *A Course in Homological Algebra*, Springer, New York, 1970.

7 Teoria degli ideali negli anelli commutativi: teoria generale e anelli noetheriani

La teoria degli ideali degli anelli commutativi ebbe origine quando Dedekind, introducendo gli ideali, riuscì a «ristabilire» l'unicità della fattorizzazione negli anelli degli interi algebrici dei campi di numeri. Alcuni di questi anelli, ad esempio $\mathbb{Z}[\sqrt{-5}]$, non sono fattoriali, ossia non vi vale l'unicità della fattorizzazione degli elementi in elementi irriducibili (si veda BAI, pp. 141–142). Dedekind mostrò tuttavia che in tali anelli ogni ideale si fattorizza in modo unico come prodotto di ideali primi (per la definizione, si veda il ğ 7.1). Un secondo tipo di teoria degli ideali, introdotto all'inizio del Novecento da E. Lasker e F. S. Macaulay, riguarda gli ideali degli anelli di polinomi in più indeterminate. È evidente l'interesse di questa teoria per la geometria algebrica. Fra i risultati principali della teoria di Lasker e Macaulay vi è un teorema di decomposizione degli ideali degli anelli di polinomi come intersezioni di ideali detti primari (definiti a p. 434 dell'originale), con proprietà di unicità relativamente deboli. Nel 1921 Emmy Noether ricavò questi risultati con un ragionamento estremamente semplice per anelli commutativi arbitrari che soddisfano la condizione della catena ascendente per gli ideali. Quel lavoro, che con un efficace impiego dei metodi concettuali impresse all'algebra una nuova direzione, fu uno dei più influenti pubblicati in algebra nel corso del Novecento.

In questo capitolo ci occuperemo della teoria degli ideali, un tempo detta *teoria additiva degli ideali*, sviluppatasi dalla teoria di Lasker, Macaulay e Noether. Negli ultimi anni l'accento si è in parte spostato dalle decomposizioni primarie ad altri metodi, in particolare alla localizzazione, all'uso dello spettro primo di un anello e allo studio degli anelli locali. Le applicazioni alla geometria algebrica hanno continuato a fornire la motivazione principale. Hanno però esercitato la loro influenza anche altri sviluppi, come lo studio delle algebre su anelli commutativi, e naturalmente la disciplina ha progredito anche per impulso proprio.

Tratteremo la teoria degli ideali di Dedekind nel capitolo 10, dopo aver sviluppato la teoria della struttura dei campi e la teoria delle valutazioni, che logicamente la precedono.

In tutto questo capitolo, e nei successivi, gli anelli si intendono commutativi salvo esplicita indicazione contraria. Di tanto in tanto, soprattutto negli esercizi, indicheremo applicazioni ed estensioni agli anelli non commutativi. I primi nove paragrafi riguardano gli anelli commutativi arbitrari. Gli argomenti principali sono la localizzazione, il metodo che permette di ricondurre questioni su anelli arbitrari agli anelli locali localizzando rispetto ai complementari degli ideali primi, lo spettro primo di un anello, il rango dei moduli proiettivi e il gruppo delle classi proiettive. Nei ğğ 7.10–7.18 si sviluppa la teoria degli ideali degli anelli e dei moduli noetheriani. Fra gli esempi importanti di anelli noetheriani vi figurano gli anelli di polinomi e gli anelli di serie formali su anelli noetheriani. Daremo inoltre un'introduzione alla geometria algebrica affine comprendente il *Nullstellensatz* di Hilbert. Le decomposizioni primarie sono trattate nel ğ 7.13. Considereremo poi alcune proprietà fondamentali degli anelli noetheriani, in particolare il teorema d'intersezione di Krull, la funzione di Hilbert di un modulo graduato, la teoria della dimensione e il teorema dell'ideale principale di Krull. Il capitolo si chiude con un paragrafo sulle topologie J-adiche e sui completamenti.

7.1 Ideali primi. Nilradicale

Ricordiamo che un elemento p di un dominio D si dice *primo* se p non è invertibile e se $p \mid ab$ in D implica $p \mid a$ oppure $p \mid b$ in D. Ciò suggerisce la seguente definizione.

Definizione 7.1. *Un ideale P di un anello (commutativo) R si chiama primo se $P \neq R$ e, per $a, b \in R$, da $ab \in P$ segue $a \in P$ oppure $b \in P$.*

In altri termini, un ideale P è primo se e solo se il suo complementare $P' = R - P$ è chiuso rispetto alla moltiplicazione e contiene 1, ossia se P' è un sottomonoide del monoide moltiplicativo di R. Nella notazione delle congruenze, la seconda condizione della definizione 7.1 dice che $ab \equiv 0 \pmod{P}$ implica $a \equiv 0 \pmod{P}$ oppure $b \equiv 0 \pmod{P}$. La prima condizione dice che l'anello $\bar{R} = R/P$ è diverso da zero. È dunque chiaro che P è primo se e solo se R/P è un dominio. Poiché un ideale M di un anello commutativo R è massimale se e solo se R/M è un campo e ogni campo è un dominio, ogni ideale massimale di R è primo. È anche chiaro che un elemento p è primo nel senso consueto se e solo se l'ideale principale $(p) = pR$ è primo. Vale inoltre la pena di osservare che, se P è primo e A, B sono ideali di R con $AB \subset P$, allora $A \subset P$ oppure $B \subset P$. In caso contrario esisterebbero $a \in A$, $a \notin P$, e $b \in B$, $b \notin P$. Si avrebbe $ab \in AB \subset P$, contro la primalità di P. Per induzione è chiaro che, se P è primo e $a_1 a_2 \cdots a_n \in P$, allora $a_i \in P$ per qualche i e che, se $A_1 A_2 \cdots A_n \subset P$ per ideali A_i, allora $A_i \subset P$ per qualche i.

Ricordiamo il risultato elementare di teoria dei gruppi secondo cui un gruppo non può essere l'unione di due suoi sottogruppi propri (esercizio 14, p. 36 di BAI). Lo si può rafforzare nel modo seguente: se G_1, G_2, H sono sottogruppi di G e $H \subset G_1 \cup G_2$, allora $H \subset G_1$ oppure $H \subset G_2$. Il seguente risultato ne è un'utile estensione agli ideali primi di un anello.

Proposizione 7.1. *Siano $A, I_1, \ldots, I_n$ ideali di un anello e si supponga che al più due degli I_j non siano primi. Se $A \subset \bigcup_{j=1}^{n} I_j$, allora $A \subset I_j$ per qualche j.*

Dimostrazione. Procediamo per induzione su n. Il risultato è evidente per $n = 1$. Supponiamo dunque $n > 1$. Se $A \subset I_1 \cup \cdots \cup \widehat{I_k} \cup \cdots \cup I_n$ per qualche k, la tesi segue dall'ipotesi induttiva. Supponiamo perciò che A non sia contenuto in tale unione per alcun $k = 1, \ldots, n$, e mostriamo che se ne ricava una contraddizione. Per ogni k esiste un $a_k \in A$ che non appartiene a $I_1 \cup \cdots \cup \widehat{I_k} \cup \cdots \cup I_n$. Poiché $A \subset \bigcup I_j$, si ha $a_k \in I_k$. Per $n = 2$ si vede subito, come nell'argomento di teoria dei gruppi, che $a_1 + a_2 \in A$ ma $a_1 + a_2 \notin I_1 \cup I_2$, contro l'ipotesi. Se $n > 2$, almeno uno degli I_j è primo. Possiamo supporre che sia I_1. Si vede allora subito che

$$a_1 + a_2 a_3 \cdots a_n$$

appartiene ad A ma non a $\bigcup I_j$. Ancora una volta abbiamo una contraddizione, il che prova il risultato. □

Il risultato si enuncia di solito sotto l'ipotesi più restrittiva che tutti gli I_j siano primi. La forma più forte che abbiamo dimostrato è dovuta a N. McCoy, che la rafforzò ulteriormente sostituendo l'ipotesi che A sia un ideale con la condizione che A sia un sottoanello, non necessariamente con unità, di R (BAI, p. 155). È chiaro che la dimostrazione appena data vale anche in questo caso. Nel seguito ci riferiremo alla proposizione 7.1 come al «lemma di evitamento degli ideali primi». La terminologia si giustifica con l'enunciato contrapposto: se $A, I_1, \ldots, I_n$ sono ideali, $A \not\subset I_j$ per ogni j e al più due degli I_j non sono primi, allora esiste $a \in A$ tale che $a \notin \bigcup I_j$.

Vi è un importante procedimento per ottenere ideali primi dai sottomonoidi del monoide moltiplicativo di R. Esso si basa sul seguente risultato.

Proposizione 7.2. *Sia S un sottomonoide del monoide moltiplicativo di R e sia P un ideale di R tale che (1) $P \cap S = \varnothing$ e (2) P è massimale rispetto alla proprietà (1), nel senso che ogni ideale $P' \supsetneq P$ soddisfa $P' \cap S \neq \varnothing$. Allora P è primo.*

Dimostrazione. Siano $a, b \in R$ con $a \notin P$ e $b \notin P$. Gli ideali $(a) + P$ e $(b) + P$ contengono propriamente P e quindi incontrano S. Esistono pertanto $p_1, p_2 \in P$, $x_1, x_2 \in R$ e $s_1, s_2 \in S$ tali che $s_1 = x_1 a + p_1$ e $s_2 = x_2 b + p_2$. Allora $s_1 s_2 \in S$ e

$$s_1 s_2 = x_1 x_2 ab + x_1 a p_2 + x_2 b p_1 + p_1 p_2.$$

Se $ab \in P$, ne segue $s_1 s_2 \in P$, contro $P \cap S = \varnothing$. Pertanto $ab \notin P$, e abbiamo provato che $a \notin P$, $b \notin P$ implicano $ab \notin P$. Dunque P è primo. □

Se S è un sottomonoide che non contiene 0, l'ideale nullo soddisfa $0 \cap S = \varnothing$. Sia ora A un ideale qualsiasi tale che $A \cap S = \varnothing$ e sia $\mathcal{A}$ l'insieme degli ideali B di R tali che $B \supset A$ e $B \cap S = \varnothing$. Dal lemma di Zorn segue immediatamente che $\mathcal{A}$ ha elementi massimali. Ciascuno di essi è un ideale $P \supset A$ che soddisfa le ipotesi della proposizione 7.2. Da questa proposizione segue dunque il risultato seguente.

Proposizione 7.3. *Sia S un sottomonoide del monoide moltiplicativo di R e sia A un ideale di R tale che $S \cap A = \varnothing$. Allora A è contenuto in un ideale primo P tale che $S \cap P = \varnothing$.*

Sia N l'insieme degli elementi nilpotenti di R. Se $z \in N$, cosicché $z^n = 0$ per qualche n, e se a è un elemento qualsiasi di R, allora $(az)^n = a^n z^n = 0$. Quindi $az \in N$. Se $z_i \in N$, $i = 1, 2$, e n_i è un intero tale che $z_i^{n_i} = 0$, per il teorema binomiale, con $n = n_1 + n_2 - 1$, abbiamo $(z_1 + z_2)^n = \sum_{i=0}^{n} \binom{n}{i} z_1^i z_2^{n-i}$. La somma è nulla: per $i < n_1$ si ha $n - i \geq n_2$, sicché $z_1^i z_2^{n-i} = 0$, e per $i \geq n_1$ è evidente che $z_1^i z_2^{n-i} = 0$. Quindi N è un ideale. Lo chiamiamo *nilradicale* dell'anello R e lo indichiamo con $\operatorname{nilrad} R$. Se $\bar{z} = z + N$ appartiene al nilradicale di $\bar{R} = R/N$, con $N = \operatorname{nilrad} R$, allora $z^n \in N$ per qualche n, e dunque $z^{mn} = 0$ per qualche multiplo mn. Allora $z \in N$ e $\bar{z} = 0$. Quindi $\operatorname{nilrad} \bar{R} = 0$. Ricordiamo che ogni ideale nil di un anello è contenuto nel radicale (di Jacobson) $\operatorname{rad} R$ (p. 192 dell'originale). Ricordiamo inoltre che $\operatorname{rad} R$ è l'intersezione degli ideali sinistri massimali di R (p. 193). Per un anello commutativo $\operatorname{rad} R$ è pertanto l'intersezione dei suoi ideali massimali. Per il nilradicale vale il risultato analogo seguente.

Teorema 7.1 (Krull). *Il nilradicale di R è l'intersezione degli ideali primi di R.*

Dimostrazione. Sia $N = \operatorname{nilrad} R$ e sia $N' = \bigcap P$, dove l'intersezione è estesa a tutti gli ideali primi di R. Se $z \in N$, si ha $z^n = 0$ per qualche intero n. Ne segue $z^n \in P$ per ogni ideale primo P e quindi $z \in P$. Dunque $N \subset P$ per ogni primo P, e $N \subset N'$. Sia ora $s \notin N$; s non è nilpotente e $S = \{s^n \mid n = 0, 1, 2, \ldots\}$ è un sottomonoide del monoide moltiplicativo di R tale che $S \cap \{0\} = \varnothing$. Per la proposizione 7.3, applicata ad $A = 0$, esiste un ideale primo P con $P \cap S = \varnothing$. Allora $s \notin P$ e $s \notin N'$. Ciò implica che $N' \subset N$, sicché $N = N' = \bigcap P$. □

Se A è un ideale di R, definiamo il *nilradicale di A*, $\operatorname{nilrad} A$ (talvolta indicato con $\sqrt{A}$), come l'insieme degli elementi z di R nilpotenti modulo A, nel senso che $z^n \in A$ per qualche intero positivo n. È precisamente l'insieme degli elementi z tali che $\bar{z} = z + A$ appartenga al nilradicale di $\bar{R} = R/A$. Si ha dunque

$$\operatorname{nilrad} A = \nu^{-1}(\operatorname{nilrad} \bar{R}), \tag{1}$$

dove ν è l'omomorfismo canonico di R su $\bar{R}$. Ne segue (o lo si vede direttamente) che $\operatorname{nilrad} A$ è un ideale di R contenente A. È chiaro anche che iterando la formazione del nilradicale di un ideale non si ottiene nulla di nuovo: $\operatorname{nilrad}(\operatorname{nilrad} A) = \operatorname{nilrad} A$.

Abbiamo la biiezione $B \mapsto \bar{B} = B/A$ dell'insieme degli ideali di R contenenti A sull'insieme degli ideali di $\bar{R} = R/A$. Inoltre $\bar{R}/\bar{B} \cong R/B$ (BAI, p. 107). Pertanto B è primo in R se e solo se $\bar{B}$ è primo in $\bar{R}$. L'insieme degli ideali primi di $\bar{R}$ è dunque l'insieme degli ideali $\bar{P} = P/A$ con P ideale primo di R contenente A. Poiché $\bigcap(P/A) = (\bigcap P)/A$ (BAI, p. 67, esercizio 2) e l'intersezione di tutti gli ideali primi di $\bar{R}$ è il nilradicale di $\bar{R}$, abbiamo

$$(\bigcap P)/A = \bigcap(P/A) = \bigcap \bar{P} = \operatorname{nilrad} \bar{R} = \operatorname{nilrad}(R/A). \tag{2}$$

Quindi $\operatorname{nilrad} A = \bigcap P$, dove P varia fra gli ideali primi di R contenenti A. Enunciamo il risultato.

Teorema 7.2. *Il nilradicale di un ideale A è l'intersezione degli ideali primi di R che contengono A.*

Esercizi

1. Siano A_i, $1 \leq i \leq n$, ideali e sia P un ideale primo. Mostrare che, se $P \supset \bigcap_i A_i$, allora $P \supset A_i$ per qualche i, e che, se $P = \bigcap_i A_i$, allora $P = A_i$ per qualche i.

2. Mostrare che, se P è un ideale primo, allora $S = R - P$ è un sottomonoide del monoide moltiplicativo di R ed è saturo nel senso che contiene i divisori di ogni $s \in S$. Più in generale, mostrare che, se $\{P_\alpha\}$ è un insieme di ideali primi, $S = R - \bigcup P_\alpha$ è un sottomonoide saturo del monoide moltiplicativo di R. Viceversa, mostrare che ogni sottomonoide saturo del monoide moltiplicativo di R ha la forma $R - \bigcup P_\alpha$, con $\{P_\alpha\}$ insieme di ideali primi di R.

3. Mostrare che l'insieme dei divisori dello zero di R è un'unione di ideali primi.

4. (McCoy.) Mostrare che gli elementi invertibili dell'anello dei polinomi $R[x]$, con x indeterminata, sono i polinomi $a_0 + a_1x + \cdots + a_nx^n$ in cui a_0 è invertibile in R e ogni a_i con $i > 0$ è nilpotente. (Suggerimento: considerare dapprima il caso in cui R è un dominio. Dedurne il caso generale mediante il teorema di Krull.)

I due esercizi seguenti portano a un importante risultato di S. Amitsur sul radicale di un anello di polinomi. In essi R può non essere commutativo.

5. Sia $f(x) \in R[x]$ con termine costante nullo e si supponga che $f(x)$ sia quasi-regolare con quasi-inverso $g(x)$ (p. 194 dell'originale). Mostrare che i coefficienti di $g(x)$ appartengono al sottoanello generato dai coefficienti di $f(x)$.

6. (Amitsur.) Mostrare che $R[x]$ è semiprimitivo se R non ha ideali nil diversi da 0. (Suggerimento: supporre $\operatorname{rad} R[x] \neq 0$ e scegliere in quest'ideale un elemento non nullo con il minimo numero di coefficienti non nulli. Mostrare che questi coefficienti sono contenuti in un sottoanello commutativo B di R. Applicare gli esercizi 4 e 5.)

7.2 Localizzazione degli anelli

Lo strumento della localizzazione, che ora introdurremo, è uno dei più efficaci dell'algebra commutativa. Esso generalizza la ben nota costruzione del campo delle frazioni di un dominio (BAI, pp. 115–119). Possiamo considerare questa generalizzazione dal punto di vista di una costruzione universale che risolve il problema seguente.

Dati un anello (commutativo) R e un sottoinsieme S di R, costruire un anello R_S e un omomorfismo λ_S di R in R_S tali che ogni $\lambda_S(s)$, $s \in S$, sia invertibile in R_S e che la coppia (R_S, λ_S) sia universale fra le coppie di questo tipo. Ciò significa che, se η è un qualsiasi omomorfismo di R in un anello R' tale che ogni $\eta(s)$ sia invertibile, esiste un unico omomorfismo $\bar{\eta}\colon R_S \to R'$ che rende commutativo il diagramma

(3)
$$\begin{array}{ccc} R & \xrightarrow{\lambda_S} & R_S \\ {\scriptstyle\eta}\downarrow & \swarrow_{\bar{\eta}} & \\ R' & & \end{array}$$

Prima di procedere alla soluzione del problema, che è facile, facciamo alcune osservazioni.

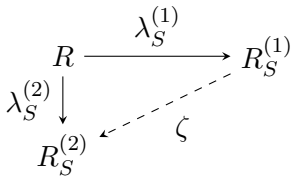
1. Poiché il prodotto di due elementi di un anello commutativo è invertibile se e soltanto se sono invertibili entrambi gli elementi, non si perde generalità supponendo che S sia un sottomonoide del monoide moltiplicativo di R. La soluzione del problema per un insieme arbitrario S si riconduce al caso in cui S è un monoide sostituendo l'insieme S con il sottomonoide $\langle S\rangle$ da esso generato. Ad esempio, se S è un singoletto $\{s\}$, lo possiamo sostituire con $\langle s\rangle = \{s^n \mid n = 0, 1, 2, \ldots\}$.

2. Il caso particolare del campo delle frazioni è quello in cui R è un dominio e $S = R^*$ è il sottomonoide degli elementi non nulli di R. In questo caso nulla cambia se nell'enunciato del problema si considerano come anelli R' soltanto i campi. Ciò è chiaro perché l'immagine di un campo mediante un omomorfismo è o l'anello banale costituito da un solo elemento, o un campo.

3. Poiché un divisore dello zero in un anello diverso da $\{0\}$ non è invertibile, non possiamo aspettarci che λ_S sia iniettivo se S contiene divisori dello zero.

4. Se gli elementi di S sono invertibili in R, basta prendere $R_S = R$ e $\lambda_S = 1_R$, l'applicazione identica di R. È allora chiaro che $\bar{\eta} = \eta$ soddisfa la condizione del problema.

5. Se esiste una soluzione, essa è unica nel senso forte seguente. Se $(R_S^{(1)}, \lambda_S^{(1)})$ e $(R_S^{(2)}, \lambda_S^{(2)})$ soddisfano la condizione per l'anello R e il sottoinsieme S, esiste un unico isomorfismo $\zeta\colon R_S^{(1)} \to R_S^{(2)}$ che rende commutativo il diagramma



(si veda p. 44).

Passiamo ora alla costruzione di una coppia (R_S, λ_S) per un qualsiasi anello R e un qualsiasi sottomonoide S del suo monoide moltiplicativo. Come nel caso particolare di un dominio R e del suo monoide $S = R^*$ degli elementi non nulli, cominciamo con il prodotto cartesiano $R \times S$ delle coppie (a, s), $a \in R$, $s \in S$. Poiché il monoide S può contenere divisori dello zero, occorre modificare un poco la definizione di equivalenza fra le coppie (a, s) che abbiamo usato nella costruzione del campo delle frazioni di un dominio. Definiamo una relazione binaria $\sim$ su $R \times S$ ponendo $(a_1, s_1) \sim (a_2, s_2)$ se esiste $s \in S$ tale che

$$s(s_2 a_1 - s_1 a_2) = 0 \tag{4}$$

(ossia $ss_2a_1 = ss_1a_2$). Se R è un dominio e S non contiene 0, la (4) si può sostituire con la condizione più semplice $s_2a_1 = s_1a_2$. Nel caso generale si verifica facilmente che $\sim$ è una relazione di equivalenza. Denotiamo con R_S l'insieme quoziente definito da questa relazione e con a/s la classe di equivalenza di (a, s).

Definiamo l'addizione e la moltiplicazione nell'insieme R_S ponendo

$$a_1/s_1 + a_2/s_2 = (s_2a_1 + s_1a_2)/(s_1s_2) \tag{5}$$

e

$$(a_1/s_1)(a_2/s_2) = (a_1a_2)/(s_1s_2). \tag{6}$$

È un po' laborioso, ma immediato, verificare che queste operazioni sono ben definite e che, ponendo $0 = 0/1$ (uguale a $0/s$ per ogni $s \in S$) e $1 = 1/1$ (uguale a s/s per $s \in S$), $(R_S, +, \cdot, 0, 1)$ è un anello. Lasciamo le verifiche al lettore.

Definiamo ora un'applicazione λ_S (o λ_S^R) di R in R_S mediante

$$\lambda_S \colon a \longmapsto a/1. \tag{7}$$

Dalle (5) e (6) e dalla definizione di 1 in R_S risulta che λ_S è un omomorfismo di R in R_S. Inoltre, se $s \in S$, l'elemento $\lambda_S(s) = s/1$ ha inverso $1/s$, poiché $(s/1)(1/s) = s/s = 1$. Sia ora η un omomorfismo di R in R' tale che $\eta(s)$ sia invertibile per ogni $s \in S$. Si verifica facilmente che

$$\bar{\eta} \colon a/s \longmapsto \eta(a)\eta(s)^{-1} \tag{8}$$

è ben definita ed è un omomorfismo di R_S in R'. Inoltre $\bar{\eta}\lambda_S(a) = \bar{\eta}(a/1) = \eta(a)$. Il diagramma (3) è dunque commutativo. Anche l'unicità di $\bar{\eta}$ è chiara, poiché $a/s = (a/1)(1/s) = (a/1)(s/1)^{-1}$, e quindi qualsiasi $\bar{\eta}$ che soddisfi la condizione di commutatività verifica

$$\bar{\eta}(a/s) = \bar{\eta}(\lambda_S(a)\lambda_S(s)^{-1}) = \eta(a)\eta(s)^{-1}.$$

Dunque $\bar{\eta}$ è l'applicazione definita nella (8) e (R_S, λ_S) è una soluzione del problema formulato all'inizio. Chiameremo (R_S, λ_S) (o semplicemente R_S) la *localizzazione di R rispetto a S*.

Studieremo ora le relazioni fra R_S e $R_{S'}$, dove S' è un sottomonoide del monoide S. Osserviamo anzitutto che $\lambda_S(s')$ è invertibile in R_S per $s' \in S'$. Esiste quindi un unico omomorfismo $\zeta_{S',S} \colon R_{S'} \to R_S$ tale che $\lambda_S = \zeta_{S',S}\lambda_{S'}$. Supponiamo ora che $\lambda_{S'}(s)$ sia invertibile in $R_{S'}$ per $s \in S$. Esiste allora anche un unico omomorfismo $\zeta_{S,S'} \colon R_S \to R_{S'}$ tale che $\lambda_{S'} = \zeta_{S,S'}\lambda_S$. Ne segue che $\zeta_{S,S'}\zeta_{S',S} = 1_{R_{S'}}$ e $\zeta_{S',S}\zeta_{S,S'} = 1_{R_S}$. Quindi $\zeta_{S',S}$ e $\zeta_{S,S'}$ sono isomorfismi. Mostreremo ora che, in generale, se $S' \subseteq S$, R_S è in effetti una localizzazione di $R_{S'}$. Enunciamo il risultato in forma un po' imprecisa come segue.

Proposizione 7.4. *Sia S' un sottomonoide di S e sia $S/S' = \{s/s' \mid s \in S,\ s' \in S'\}$. Allora S/S' è un sottomonoide del monoide moltiplicativo di $R_{S'}$ e vi sono isomorfismi canonici fra R_S e $(R_{S'})_{\lambda_{S'}(S)}$ e fra $(R_{S'})_{\lambda_{S'}(S)}$ e $(R_{S'})_{S/S'}$.*

Dimostrazione. Otterremo il primo isomorfismo mostrando che $(R_{S'})_{\lambda_{S'}(S)}$ gode della proprietà universale di R_S. Anzitutto abbiamo l'omomorfismo composto $\lambda_{\lambda_{S'}(S)}\lambda_{S'}$ di R in $(R_{S'})_{\lambda_{S'}(S)}$ dato dalla successione

$$R \xrightarrow{\lambda_{S'}} R_{S'} \xrightarrow{\lambda_{\lambda_{S'}(S)}} (R_{S'})_{\lambda_{S'}(S)}.$$

Sia ora η un omomorfismo di R in R' tale che $\eta(s)$ sia invertibile per $s \in S$. Poiché $S' \subseteq S$, esiste un unico omomorfismo $\bar{\eta}'$ di $R_{S'}$ in R' tale che $\bar{\eta}'\lambda_{S'} = \eta$. Se $s \in S$, allora $\bar{\eta}'(\lambda_{S'}(s)) = \eta(s)$ è invertibile in R'. Pertanto, per la proprietà universale di $(R_{S'})_{\lambda_{S'}(S)}$, esiste un unico omomorfismo $\bar{\eta}$ di $(R_{S'})_{\lambda_{S'}(S)}$ in R' tale che $\bar{\eta}\lambda_{\lambda_{S'}(S)} = \bar{\eta}'$. Si ha allora $\bar{\eta}\lambda_{\lambda_{S'}(S)}\lambda_{S'} = \bar{\eta}'\lambda_{S'} = \eta$. Inoltre $\bar{\eta}$ è l'unico omomorfismo di $(R_{S'})_{\lambda_{S'}(S)}$ in R' che soddisfi $\bar{\eta}(\lambda_{\lambda_{S'}(S)}\lambda_{S'}) = \eta$. Infatti questa condizione implica $(\bar{\eta}\lambda_{\lambda_{S'}(S)})\lambda_{S'} = \bar{\eta}'\lambda_{S'}$, da cui $\bar{\eta}\lambda_{\lambda_{S'}(S)} = \bar{\eta}'$ per l'universalità di $(R_{S'}, \lambda_{S'})$. L'unicità di $\bar{\eta}$ segue poi dall'universalità di $((R_{S'})_{\lambda_{S'}(S)}, \lambda_{\lambda_{S'}(S)})$. Dunque $((R_{S'})_{\lambda_{S'}(S)}, \lambda_{\lambda_{S'}(S)}\lambda_{S'})$ gode della proprietà universale di (R_S, λ_S) e si ha l'isomorfismo richiesto.

Per vedere l'isomorfismo di $(R_{S'})_{\lambda_{S'}(S)}$ e $(R_{S'})_{S/S'}$ basta osservare che $\lambda_{S'}(S)$ è un sottomonoide di S/S'. Abbiamo quindi l'omomorfismo canonico di $(R_{S'})_{\lambda_{S'}(S)}$ in $(R_{S'})_{S/S'}$. Se $s \in S$, $s' \in S'$, allora $s/s' = (s/1)(s'/1)^{-1}$ in $R_{S'}$ e $\lambda_{\lambda_{S'}(S)}(s/1)$ e $\lambda_{\lambda_{S'}(S)}(s'/1)$ sono invertibili in $(R_{S'})_{\lambda_{S'}(S)}$. È quindi invertibile $\lambda_{\lambda_{S'}(S)}(s/s')$. Dal risultato ottenuto prima segue che l'omomorfismo canonico di $(R_{S'})_{\lambda_{S'}(S)}$ in $(R_{S'})_{S/S'}$ è un isomorfismo. □

Esercizi

1. Siano S e T sottomonoidi del monoide moltiplicativo di R. Osservare che $ST = \{st \mid s \in S,\ t \in T\}$ è il sottomonoide generato da S e T. Mostrare che $R_{ST} \simeq (R_S)_{\lambda_S(T)}$.

2. Siano $a, b \in R$. Mostrare che $(R_{\langle a\rangle})_{\langle b/1\rangle} \simeq R_{\langle ab\rangle}$.

3. Sia S un sottomonoide del monoide moltiplicativo di R. Per $a, b \in S$, porre $\langle a\rangle \leq \langle b\rangle$ se $a \mid b$ in S. In tal caso esiste un unico omomorfismo $\zeta_{\langle a\rangle,\langle b\rangle}\colon R_{\langle a\rangle} \to R_{\langle b\rangle}$ tale che $\lambda_{\langle b\rangle} = \zeta_{\langle a\rangle,\langle b\rangle}\lambda_{\langle a\rangle}$. Mostrare che $R_S = \varinjlim R_{\langle a\rangle}$ rispetto alle ζ.

7.3 Localizzazione dei moduli

È importante estendere agli R-moduli il concetto di localizzazione. Sia M un modulo su R e sia S un sottomonoide del monoide moltiplicativo di R. Costruiremo un R_S-modulo M_S in maniera simile a quella usata per costruire R_S. Consideriamo il prodotto cartesiano $M \times S$ delle coppie (x, s), $x \in M$, $s \in S$, e introduciamo in esso una relazione $\sim$ ponendo $(x_1, s_1) \sim (x_2, s_2)$ se esiste $s \in S$ tale che

$$s(s_2x_1 - s_1x_2) = 0. \tag{9}$$

Gli stessi calcoli fatti nel caso degli anelli mostrano che $\sim$ è una relazione di equivalenza. Indichiamo con M_S l'insieme quoziente e con x/s la classe di equivalenza di (x, s). Possiamo fare di M_S un R_S-modulo definendo l'addizione con

$$x_1/s_1 + x_2/s_2 = (s_2x_1 + s_1x_2)/(s_1s_2) \tag{10}$$

e l'azione di R_S su M_S con

$$(a/s)(x/t) = ax/(st). \tag{11}$$

Come nel caso degli anelli, si può verificare che le (10) e (11) sono ben definite, che con $+$ e $0 = 0/s$ si ottiene un gruppo abeliano e che la (11) definisce su M_S un'azione di R_S che ne fa un modulo. Chiameremo l'R_S-modulo M_S la *localizzazione di M rispetto a S*, o la *S-localizzazione di M*.

Benché in generale M_S ci interessi come R_S-modulo, possiamo considerarlo anche come R-modulo definendo l'azione di R con $a(x/s) = (a/1)(x/s) = ax/s$. Poiché $a \mapsto a/1$ è un omomorfismo di anelli, è chiaro che si ottiene un'azione di modulo. Abbiamo un'applicazione λ_S (o λ_S^M, se occorre indicare M) da M in M_S definita da $x \mapsto x/1$. Essa è un omomorfismo di R-moduli. Il nucleo di λ_S è l'insieme degli $x \in M$ per i quali esiste $s \in S$ tale che $sx = 0$. In altri termini, se $\operatorname{ann} x$ denota l'ideale annullatore di x in R, si ha $\operatorname{ann} x \cap S \neq \varnothing$. È chiaro che λ_S può non essere iniettivo. Per esempio, se M è uno $\mathbb{Z}$-modulo e $S = \mathbb{Z} \setminus \{0\}$, il sottomodulo di torsione di M è mandato in zero da λ_S. È chiaro che, se S contiene 0, allora $M_S = 0$ e $\ker \lambda_S = M$. Un'altra osservazione utile è la seguente.

Proposizione 7.5. *Se M è un modulo finitamente generato, allora $M_S = 0$ se e soltanto se esiste $s \in S$ tale che $sM = 0$.*

Dimostrazione. Se $sM = 0$, ogni x/t è uguale a $0 = 0/1$, poiché $s(1x) = s(t0) = 0$. Viceversa, supponiamo $M_S = 0$ e sia $\{x_1, \ldots, x_n\}$ un insieme di generatori di M. Da $x_i/1 = 0$ segue che esiste $s_i \in S$ tale che $s_ix_i = 0$. Se $s = \prod_{i=1}^n s_i$, allora $sx_i = 0$ per ogni i, e quindi $sx = 0$ per ogni $x = \sum r_ix_i$, $r_i \in R$. Dunque $sM = 0$. □

Sia $f\colon M \to N$ un omomorfismo di R-moduli. Esiste allora un corrispondente R_S-omomorfismo f_S di M_S in N_S definito da

$$f_S(x/t) = f(x)/t. \tag{12}$$

Lasciamo ancora al lettore le verifiche. Le applicazioni $M \mapsto M_S$, $f \mapsto f_S$ definiscono un funtore, il *funtore di S-localizzazione*, dalla categoria degli R-moduli alla categoria degli R_S-moduli. Mostreremo ora che questo funtore è naturalmente isomorfo al funtore $R_S \otimes_R -$ da R-**mod** a R_S-**mod**. Si ha dunque la seguente proposizione.

Proposizione 7.6. *Per ogni R-modulo M si può definire un R_S-isomorfismo η_M di M_S su $R_S \otimes_R M$ naturale in M.*

Dimostrazione. Mostriamo anzitutto che esiste un'applicazione η_M di M_S in $R_S \otimes_R M$ tale che

$$x/s \longmapsto (1/s) \otimes x. \tag{13}$$

Supponiamo $x_1/s_1 = x_2/s_2$. Ciò significa che esiste $s \in S$ tale che $ss_2x_1 = ss_1x_2$. Allora

$$\begin{aligned}(1/s_1) \otimes x_1 &= (ss_2/(ss_2s_1)) \otimes x_1 = ss_2(1/(ss_2s_1)) \otimes x_1 \\ &= (1/(ss_2s_1)) \otimes ss_2x_1 = (1/(ss_2s_1)) \otimes ss_1x_2 \\ &= ss_1(1/(ss_2s_1)) \otimes x_2 = (ss_1/(ss_2s_1)) \otimes x_2 \\ &= (1/s_2) \otimes x_2.\end{aligned}$$

Dunque la (13) è ben definita. Una verifica diretta mostra che η_M è un omomorfismo di gruppi. Osserviamo poi che esiste un'applicazione ben definita del prodotto cartesiano $R_S \times M$ in M_S tale che

$$(a/s, x) \longmapsto ax/s. \tag{14}$$

Per verificarlo dobbiamo mostrare che, se $a_1/s_1 = a_2/s_2$ in R_S, allora $a_1x/s_1 = a_2x/s_2$. Se $a_1/s_1 = a_2/s_2$, esiste $s \in S$ tale che $sa_1s_2 = sa_2s_1$. Allora $sa_1s_2x = sa_2s_1x$, da cui segue l'uguaglianza richiesta $a_1x/s_1 = a_2x/s_2$. Una verifica diretta mostra che la (14) soddisfa le condizioni per un prodotto bilanciato degli R-moduli R_S e M. Abbiamo quindi un omomorfismo di gruppi η'_M di $R_S \otimes_R M$ in M_S che manda $(a/s) \otimes x$ in ax/s. Applicando poi η_M otteniamo $(1/s) \otimes ax = (a/s) \otimes x$. D'altra parte, applicando η_M a x/s otteniamo $(1/s) \otimes x$, e applicando a questo η'_M si riottiene x/s. Ne segue che $\eta_M\eta'_M$ è l'applicazione identica di $R_S \otimes_R M$ e $\eta'_M\eta_M$ è l'identità di M_S. Pertanto η_M è un isomorfismo di gruppi, e così pure $\eta'_M = \eta_M^{-1}$. Direttamente dalle definizioni si verifica che η_M, e quindi anche η_M^{-1}, è un'applicazione R_S-lineare, dunque un R_S-isomorfismo. Resta da provare la naturalità, ossia la commutatività del diagramma

$$\begin{array}{ccc} M_S & \xrightarrow{\eta_M} & R_S \otimes_R M \\ {\scriptstyle f_S}\downarrow & & \downarrow{\scriptstyle 1 \otimes f} \\ N_S & \xrightarrow[\eta_N]{} & R_S \otimes_R N \end{array}$$

per un R-omomorfismo $f\colon M \to N$ dato. Ciò segue dal calcolo

$$\begin{aligned}(1 \otimes f)\eta_M(x/s) = (1 \otimes f)((1/s) \otimes x) = (1/s) \otimes f(x), \\ \eta_N f_S(x/s) = \eta_N(f(x)/s) = (1/s) \otimes f(x),\end{aligned}$$

che conclude la dimostrazione. □

Questo risultato permette di passare utilmente dai prodotti tensoriali alla localizzazione e viceversa. Ricordiamo anzitutto che il funtore $N \otimes_R -$ è esatto a destra, ossia che dall'esattezza di $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ segue quella di

$$N \otimes_R M' \xrightarrow{1\otimes f} N \otimes_R M \xrightarrow{1\otimes g} N \otimes_R M'' \longrightarrow 0.$$

Applicando questo fatto con $N = R_S$, insieme con la proposizione 7.6, si vede che $M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S \to 0$ è esatta. Dimostriamo ora direttamente che, se $0 \to M' \xrightarrow{f} M$ è esatta, allora $0 \to M'_S \xrightarrow{f_S} M_S$ è esatta. Supponiamo $f_S(x'/s) = 0$, ossia $f(x')/s = 0$. Esiste allora $t \in S$ tale che $tf(x') = 0$. Quindi $f(tx') = 0$ e, poiché f è iniettivo, $tx' = 0$, da cui $x'/s = 0$. Pertanto $\ker f_S = 0$ e la successione $0 \to M'_S \xrightarrow{f_S} M_S$ è esatta. Possiamo ora applicare la proposizione 7.6 e concludere che è esatta la successione

$$0 \longrightarrow R_S \otimes_R M' \xrightarrow{1\otimes f} R_S \otimes_R M.$$

Ricordiamo che questa è la definizione di piattezza di R_S come R-modulo (p. 153). Abbiamo dunque l'importante proposizione seguente.

Proposizione 7.7. *R_S è un R-modulo piatto.*

Osserviamo inoltre che abbiamo dimostrato che, se $0 \to M' \to M \to M'' \to 0$ è una successione esatta di R-moduli, allora $0 \to M'_S \to M_S \to M''_S \to 0$ è una successione esatta di R_S-moduli. Pertanto il funtore di S-localizzazione da R-**mod** a R_S-**mod** è esatto.

Sia ora N un sottomodulo di M. Dalla successione esatta $0 \to N \xrightarrow{i} M$, dove i è l'inclusione, si ottiene la successione esatta $0 \to N_S \xrightarrow{i_S} M_S$ e la definizione mostra che i_S è l'inclusione di N_S. Si ha la successione esatta $0 \to N \xrightarrow{i} M \xrightarrow{\nu} M/N \to 0$, dove ν è l'omomorfismo canonico. Abbiamo quindi la successione esatta $0 \to N_S \xrightarrow{i_S} M_S \xrightarrow{\nu_S} (M/N)_S \to 0$, che mostra che $M_S/N_S \simeq (M/N)_S$. Più precisamente, tale esattezza mostra che l'applicazione

$$x/s + N_S \longmapsto (x+N)/s \tag{15}$$

è un isomorfismo di M_S/N_S su $(M/N)_S$.

Se M e N sono R-moduli e $f\colon M \to N$ è un omomorfismo, abbiamo la successione esatta

$$0 \longrightarrow \ker f \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{\nu} \operatorname{coker} f \longrightarrow 0,$$

dove $\operatorname{coker} f = N/f(M)$. Abbiamo quindi la successione esatta

$$0 \longrightarrow (\ker f)_S \xrightarrow{i_S} M_S \xrightarrow{f_S} N_S \xrightarrow{\nu_S} (\operatorname{coker} f)_S \longrightarrow 0. \tag{16}$$

Ciò implica che $(\ker f)_S$ è $\ker f_S$. Inoltre

$$(\operatorname{coker} f)_S = (N/f(M))_S \simeq N_S/f(M)_S = N_S/f_S(M_S) = \operatorname{coker} f_S.$$

Ricordiamo poi che vi è un R_S-isomorfismo di $R_S \otimes_R (M \otimes_R N)$ su $(R_S \otimes_R M) \otimes_{R_S} (R_S \otimes_R N)$ che manda $1 \otimes_R (x \otimes_R y)$ in $(1 \otimes_R x) \otimes_{R_S} (1 \otimes_R y)$ (esercizio 13, p. 148). Per la proposizione 7.6 esiste dunque un R_S-isomorfismo di $(M \otimes_R N)_S$ su $M_S \otimes_{R_S} N_S$ tale che

$$(x \otimes_R y)/1 \longmapsto (x/1) \otimes_{R_S} (y/1). \tag{17}$$

Sia ora M un R_S-modulo. Allora M diventa un R-modulo definendo $ax = (a/1)x$ per $a \in R$. È chiaro che, se f è un omomorfismo di M come R_S-modulo, f è un R-omomorfismo. Consideriamo ora M_S, dove M è considerato come R-modulo. Poiché $s/1$ è invertibile in R_S per $s \in S$, da $sx = (s/1)x = 0$ per $x \in M$ segue $x = 0$. Dunque l'omomorfismo $\lambda_S\colon x \mapsto x/1$ da M in M_S è un monomorfismo. Poiché $x/s = (1/s)(x/1)$, λ_S è suriettivo. Così possiamo identificare l'R_S-modulo M con la S-localizzazione M_S di M considerato come R-modulo.

7.4 Localizzazione rispetto al complementare di un ideale primo. Relazioni locali e globali

Ricordiamo che un ideale P di R è primo se e soltanto se il complementare $R \setminus P$ di P in R è un sottomonoide del monoide moltiplicativo di R. Le localizzazioni rispetto a tali monoidi rivestono particolare importanza. Scriveremo abitualmente M_P per $M_{R\setminus P}$, f_P per $f_{R\setminus P}$ e così via, e chiameremo M_P la *localizzazione di M nell'ideale primo P*.

Consideriamo anzitutto una corrispondenza fra gli ideali di R e quelli di R_P. Cominceremo considerando più in generale gli ideali di R e di R_S per un sottomonoide S qualsiasi. Sia A' un ideale di R_S. Allora

$$j(A') = \{a \in R \mid a/s \in A' \text{ per qualche } s \in S\} \tag{18}$$

è un ideale di R. È chiaro che $(j(A'))_S = A'$. Se invece partiamo da un ideale A di R, si vede facilmente che $A_S = R_S$ se e soltanto se A contiene un elemento di S. Per questo motivo è naturale limitare la nostra attenzione agli ideali A di R che non incontrano S.

Osserviamo poi che, se P è un ideale primo di R tale che $P \cap S = \varnothing$, allora $j(P_S) = P$. Sia infatti $a \in j(P_S)$. Esistono un elemento $p \in P$ ed elementi $s, t \in S$ tali che $a/s = p/t$. Esiste quindi $u \in S$ tale che $uat = ups \in P$. Poiché $ut \in S$ e $S \cap P = \varnothing$, ne segue $a \in P$. Dunque $j(P_S) \subseteq P$. Poiché l'inclusione opposta $j(A_S) \supseteq A$ vale per ogni ideale A, si ha $j(P_S) = P$. Si verificano direttamente altri due fatti. Se P è un ideale primo di R tale che $P \cap S = \varnothing$, allora P_S è un ideale primo di R_S. Se P' è un ideale primo di R_S, allora $j(P')$ è un ideale primo di R che non incontra S. Lasciamo le verifiche al lettore. Mettendo insieme questi risultati otteniamo la seguente proposizione.

Proposizione 7.8. *L'applicazione $P \mapsto P_S$ è una biiezione che conserva l'ordine dall'insieme degli ideali primi di R che non incontrano S all'insieme degli ideali primi di R_S. L'applicazione inversa è $P' \mapsto j(P')$, definita dalla (18).*

Consideriamo ora il caso importante della localizzazione in un ideale primo P. Poiché $Q \cap (R \setminus P) = \varnothing$ significa $Q \subseteq P$, il risultato precedente si specializza come segue.

Proposizione 7.9. *L'applicazione $Q \mapsto Q_P$ è una biiezione che conserva l'ordine dall'insieme degli ideali primi Q contenuti in P all'insieme degli ideali primi di R_P. L'applicazione inversa è $P' \mapsto j(P')$.*

È chiaro che P_P contiene ogni ideale primo di R_P. È anche chiaro che gli elementi fuori di P_P sono invertibili in R_P e che, essendo $R_P \neq P_P$, nessun elemento di P_P è invertibile. Dunque P_P è l'insieme degli elementi non invertibili di R_P e quindi R_P è un anello locale il cui unico ideale massimale è $\operatorname{rad} R_P = P_P$. Ripetiamo l'enunciato di questo risultato.

Proposizione 7.10. *R_P è un anello locale il cui unico ideale massimale è* $\operatorname{rad} R_P = P_P$.

Questo fatto spiega l'importanza centrale della localizzazione. Essa permette spesso di ricondurre questioni sugli anelli commutativi e sui moduli su tali anelli al caso degli anelli locali, perché in molti casi importanti un risultato è valido per R se vale per ogni R_P, con P ideale primo di R. Il risultato seguente dà alcune proprietà fondamentali dei moduli che valgono se e soltanto se valgono per tutte le localizzazioni negli ideali primi.

Proposizione 7.11. *(1) Sia M un R-modulo. Se $M = 0$, allora $M_S = 0$ per ogni localizzazione. Se $M_P = 0$ per ogni ideale massimale P, allora $M = 0$.*

(2) Siano M e N due R-moduli e sia f un omomorfismo di M in N. Se f è iniettivo (rispettivamente, suriettivo), f_S è iniettivo (rispettivamente, suriettivo) per la localizzazione rispetto a qualsiasi S. D'altra parte, se f_P è iniettivo (rispettivamente, suriettivo) per ogni ideale massimale P, allora f è iniettivo (rispettivamente, suriettivo).

(3) Se M è piatto, ogni M_S è piatto. Se M_P è piatto per ogni ideale massimale P, allora M è piatto.

Dimostrazione. (1) Evidentemente $M = 0$ implica $M_S = 0$. Supponiamo ora $M \neq 0$ e sia x un elemento non nullo di M. Allora $\operatorname{ann} x \neq R$, sicché questo ideale è contenuto in un ideale massimale P di R. Affermiamo che $x/1 \neq 0$ in M_P, e quindi $M_P \neq 0$. Ciò è chiaro poiché $x/1$ è l'immagine di x mediante l'omomorfismo canonico di M in M_P, e da $x/1 = 0$ seguirebbe $\operatorname{ann} x \cap (R \setminus P) \neq \varnothing$. Questo è escluso da $\operatorname{ann} x \subseteq P$.

(2) Sia $f\colon M \to N$. Abbiamo visto che $\ker f_S = (\ker f)_S$ e $\operatorname{coker} f_S \simeq (\operatorname{coker} f)_S$ per ogni sottomonoide S del monoide moltiplicativo di R. Poiché un omomorfismo è iniettivo (rispettivamente, suriettivo) se e soltanto se il suo nucleo (rispettivamente, conucleo) è nullo, la (2) è conseguenza immediata della (1).

(3) Supponiamo che M sia un R-modulo piatto e che $0 \to N' \xrightarrow{f} N$ sia una successione esatta di R_S-moduli. Considerando N' e N come R-moduli, vediamo che $0 \to M \otimes_R N' \to M \otimes_R N$ è esatta. È quindi esatta anche

$$0 \longrightarrow (M \otimes_R N')_S \xrightarrow{(1\otimes f)_S} (M \otimes_R N)_S,$$

e, per l'isomorfismo (17), è esatta

$$0 \longrightarrow M_S \otimes_{R_S} N'_S \xrightarrow{1\otimes f_S} M_S \otimes_{R_S} N_S.$$

Abbiamo visto che N'_S e N_S si possono identificare rispettivamente con N' e N. Dunque $0 \to M_S \otimes_{R_S} N' \xrightarrow{1\otimes f} M_S \otimes_{R_S} N$ è esatta e M_S è piatto su R_S. Supponiamo ora che M sia un R-modulo tale che M_P sia piatto su R_P per ogni ideale massimale P di R. Sia $0 \to N' \xrightarrow{f} N$ una successione esatta di R-moduli e consideriamo

$$M \otimes_R N' \xrightarrow{1\otimes f} M \otimes_R N.$$

Poiché M_P è piatto e $0 \to N'_P \xrightarrow{f_P} N_P$ è esatta, è esatta

$$0 \longrightarrow M_P \otimes_{R_P} N'_P \xrightarrow{1\otimes f_P} M_P \otimes_{R_P} N_P.$$

Allora $0 \to (M \otimes_R N')_P \xrightarrow{(1\otimes f)_P} (M \otimes_R N)_P$ è esatta. Poiché questo vale per ogni P massimale, dalla (2) segue che $0 \to M \otimes_R N' \xrightarrow{1\otimes f} M \otimes_R N$ è esatta. Pertanto M è piatto. □

Esercizi

1. Mostrare che il nilradicale di R_S è $(\operatorname{nilrad} R)_S$.

2. Mostrare che, se P è un ideale primo di R, R_P/P_P è isomorfo al campo delle frazioni del dominio R/P.

3. Mostrare che, se R è un dominio fattoriale (BAI, p. 141) e S è un sottomonoide del monoide moltiplicativo di R che non contiene 0, allora R_S è un dominio fattoriale.

4. Sia $\{P_i \mid 1 \leq i \leq n\}$ un insieme di ideali primi di R e sia $S = \bigcap_{i=1}^{n}(R \setminus P_i)$. Mostrare che ogni ideale primo di R_S ha la forma P_S, dove P è un ideale primo contenuto in uno dei P_i.

7.5 Lo spettro primo di un anello commutativo

Sia R un anello commutativo e indichiamo con $X = X(R)$ l'insieme degli ideali primi di R. Vi è un modo naturale di introdurre su X una topologia che permette di impiegare idee geometriche nello studio dell'anello R. Definiamo questa topologia.

Per ogni sottoinsieme A di R denotiamo con $V(A)$ il sottoinsieme di X formato dagli ideali primi P contenenti A. Evidentemente $V(A) = V(I(A))$, dove $I(A)$ è l'ideale generato da A, e poiché il nilradicale di un ideale I è l'intersezione degli ideali primi contenenti I, è chiaro che $V(I) = V(\operatorname{nilrad} I)$. Inoltre, se P è un ideale primo contenente $I_1 I_2$, con I_1, I_2 ideali, allora $P \supseteq I_1$ oppure $P \supseteq I_2$. Pertanto $V(I_1 I_2) = V(I_1) \cup V(I_2)$. Possiamo ora verificare che gli insiemi $V(A)$, con A sottoinsieme di R, soddisfano gli assiomi per i chiusi di uno spazio topologico.

(1) $\varnothing$ e X sono chiusi, poiché $\varnothing = V(\{1\})$ e $X = V(\{0\})$.

(2) L'intersezione di una famiglia qualsiasi di chiusi è chiusa. Infatti, se $\{A_\alpha\}$ è una famiglia di sottoinsiemi di R, si ha
$$\bigcap_\alpha V(A_\alpha) = V\Big(\bigcup_\alpha A_\alpha\Big).$$

(3) L'unione di due chiusi è chiusa, poiché possiamo scriverli nella forma $V(I_1)$ e $V(I_2)$, con I_j ideali, e allora $V(I_1) \cup V(I_2) = V(I_1 I_2)$.

Chiameremo X munito di questa topologia lo *spettro primo* di R e lo indicheremo con $\operatorname{Spec} R$. Il sottoinsieme $X_{\max}$ di X formato dagli ideali massimali di R, con la topologia indotta, si chiama *spettro massimale* e si indica con $\operatorname{Maxspec} R$. Topologie di questo tipo furono introdotte da M. H. Stone per gli anelli booleani e furono considerate dall'autore per gli ideali primitivi di un anello arbitrario. Nel caso di anelli commutativi questa topologia si chiama *topologia di Zariski* di X.

Gli aperti di $X = \operatorname{Spec} R$ sono i complementari
$$X - V(A) = X - \bigcap_{a \in A} V(\{a\}) = \bigcup_{a \in A} (X - V(\{a\})).$$

Per $a \in R$ denotiamo con X_a l'insieme $X - V(\{a\})$. Esso è precisamente l'insieme degli ideali primi P che non contengono a, ossia dei P tali che $\bar{a} = a + P \neq 0$ in R/P. Poiché ogni aperto è unione di insiemi X_a, questi sottoinsiemi aperti di X costituiscono una base degli aperti di $\operatorname{Spec} R$. Conviene elencare le seguenti proprietà dell'applicazione $a \mapsto X_a$ di R nell'insieme degli aperti di $\operatorname{Spec} R$.

(1) $X_{ab} = X_a \cap X_b$.

(2) $X_a = \varnothing$ se e soltanto se a è nilpotente (poiché $\operatorname{nilrad} R$ è l'intersezione degli ideali primi di R).

(3) $X_a = X$ se e soltanto se a è invertibile in R.

Se Y è un sottoinsieme di X, poniamo $\Delta_Y = \bigcap_{P \in Y} P$. Questo è un ideale di R e $V(\Delta_Y)$ è un chiuso contenente Y. D'altra parte, se $V(A) \supseteq Y$, allora $P \supseteq A$ per ogni $P \in Y$, cosicché $\Delta_Y \supseteq A$ e $V(A) \supseteq V(\Delta_Y)$. Dunque $V(\Delta_Y)$ è la chiusura di Y, ossia il più piccolo chiuso di X contenente Y. In particolare, la chiusura di un punto P è l'insieme degli ideali primi contenenti P. Se R è un dominio, 0 è un ideale primo di R e la sua chiusura è dunque l'intero spazio X.

Esempi

1. $R = \mathbb{Z}$. Come abbiamo osservato, la chiusura dell'ideale primo 0 è l'intero spazio $X(\mathbb{Z})$. Dunque $\operatorname{Spec}\mathbb{Z}$ non è uno spazio T_1 (uno spazio in cui i punti sono chiusi). Consideriamo ora $\operatorname{Maxspec}\mathbb{Z}$. Gli ideali massimali di $\mathbb{Z}$ sono gli ideali primi $(p) \neq 0$. La chiusura di $(p) \neq 0$ si riduce perciò a (p) e $\operatorname{Maxspec}\mathbb{Z}$ è uno spazio T_1. Sia Y un insieme infinito di ideali primi $(p) \neq 0$ di $\mathbb{Z}$. Evidentemente $\bigcap_{(p)\in Y}(p) = 0$, perciò $V(\Delta_Y) = X$. Dunque la chiusura di ogni sottoinsieme infinito di $\operatorname{Maxspec}\mathbb{Z}$ è l'intero spazio. I chiusi di $\operatorname{Maxspec}\mathbb{Z}$ sono pertanto i sottoinsiemi finiti (compreso $\varnothing$) e l'intero spazio. È evidente che $\operatorname{Maxspec}\mathbb{Z}$ non soddisfa l'assioma di separazione di Hausdorff.

2. $R = F[x_1, \ldots, x_r]$, con F campo e x_i indeterminate. Per $r = 1$, la discussione di Spec e di Maxspec è simile a quella per l'anello $\mathbb{Z}$. Per r arbitrario, osserviamo che $F[x_1, \ldots, x_r]/(x_1) \cong F[x_2, \ldots, x_r]$, cosicché gli ideali primi di $F[x_1, \ldots, x_r]$ contenenti (x_1) sono in corrispondenza biunivoca con gli ideali primi di $F[x_2, \ldots, x_r]$. La chiusura di (x_1) in $\operatorname{Spec} F[x_1, \ldots, x_r]$ è quindi in corrispondenza biunivoca con $\operatorname{Spec} F[x_2, \ldots, x_r]$.

Dedurremo ora alcune proprietà fondamentali dello spettro primo. Dimostriamo anzitutto la seguente proposizione.

Proposizione 7.12. $\operatorname{Spec} R$ *è quasi compatto.*

Dimostrazione. Ciò significa che, data una famiglia di aperti O_α tale che $\bigcup O_\alpha = X$, esistono fra gli O_α un numero finito di aperti $O_{\alpha_1}, \ldots, O_{\alpha_n}$ tali che $\bigcup_i O_{\alpha_i} = X$. (Seguiamo l'uso corrente che riserva «compatto» a «quasi compatto e di Hausdorff».) Poiché gli insiemi X_a formano una base, basta mostrare che, se $\bigcup_{a\in A} X_a = X$, si ha $\bigcup_i X_{a_i} = X$ per un opportuno sottoinsieme finito $\{a_i\}$ di A. La condizione $\bigcup_{a\in A} X_a = X$ dà $X - V(A) = X$, quindi $V(A) = \varnothing$. Si ha allora $V(I(A)) = \varnothing$ per l'ideale $I(A)$ generato da A e perciò $I(A) = R$. Esistono dunque $a_i \in A$ e $x_i \in R$ tali che $\sum_{i=1}^n a_i x_i = 1$. Ripercorrendo i passaggi a ritroso, vediamo che $V(\{a_i\}) = \varnothing$ e $\bigcup_i X_{a_i} = X$. □

Siano $N = \operatorname{nilrad} R$, $\bar{R} = R/N$, e sia ν l'omomorfismo canonico $a \mapsto a + N$ di R su $\bar{R}$. Ogni ideale primo P di R contiene N e $\nu(P)$ è un ideale primo di $\bar{R}$. Inoltre ogni ideale primo di $\bar{R}$ ha la forma $\nu(P)$ con P ideale primo di R. Abbiamo il seguente risultato.

Proposizione 7.13. *L'applicazione* $P \mapsto \nu(P)$ *è un omeomorfismo di* $\operatorname{Spec} R$ *su* $\operatorname{Spec}\bar{R}$.

Dimostrazione. L'applicazione è iniettiva poiché $P \supseteq N$ per ogni ideale primo P, e abbiamo visto che è suriettiva. Ora, se $a \in R$, si ha $\nu(a) \in \nu(P)$ se e soltanto se $a \in P$. Ne segue che, se A è un sottoinsieme di R, l'immagine del chiuso $V(A)$ di $\operatorname{Spec} R$ è $V(\nu(A))$ in $\operatorname{Spec}\bar{R}$ e, se $\bar{A}$ è un sottoinsieme di $\bar{R}$, la controimmagine del chiuso $V(\bar{A})$ è $V(\nu^{-1}(\bar{A}))$. Pertanto $P \mapsto \nu(P)$ è un omeomorfismo. □

Ricordiamo che uno spazio X è sconnesso se contiene un sottoinsieme aperto e chiuso diverso da $\varnothing$ e da X. Mostreremo che $\operatorname{Spec} R$ è sconnesso se e soltanto se R contiene un idempotente diverso da 0 e da 1. Ciò seguirà da un risultato assai più forte che dà una biiezione fra l'insieme degli idempotenti di R e l'insieme dei sottoinsiemi aperti e chiusi di $\operatorname{Spec} R$. Per ottenerlo avremo bisogno del seguente risultato sul sollevamento degli idempotenti, che presenta anche un interesse autonomo.

Proposizione 7.14. *Sia R un anello non necessariamente commutativo, sia N un ideale nil di R e sia $\bar{u} = u + N$ un elemento idempotente di $\bar{R} = R/N$. Esiste allora un idempotente e di R tale che $\bar{e} = \bar{u}$. Inoltre e è unico se R è commutativo.*

Dimostrazione. Si ha $u^2 - u = z$, dove $z \in N$ è nilpotente, diciamo $z^n = 0$. Allora $(u(1-u))^n =$

$u^n v^n = 0$, con $v = 1 - u$. Da $u + v = 1$ otteniamo

$$1 = 1^{2n-1} = (u + v)^{2n-1} = e + f,$$

dove e è la somma dei termini $u^i v^{2n-1-i}$ per i quali $n \leq i \leq 2n-1$, ed f è la somma dei termini per i quali $0 \leq i \leq n-1$, ciascuno contato con la sua molteplicità nello sviluppo. Poiché $u^n v^n = 0$, ogni termine di e annulla ogni termine di f. Pertanto $ef = 0 = fe$. Essendo $e+f = 1$, si ricava $e^2 = e$, $f^2 = f$. Ogni termine di e, tranne u^{2n-1}, contiene il fattore $uv = -z$. Dunque $u^{2n-1} \equiv e \pmod{N}$. Poiché $u \equiv u^2 \equiv u^3 \equiv \cdots \equiv u^{2n-1} \pmod{N}$, abbiamo $e \equiv u \pmod{N}$. Si è così provata la prima affermazione.

Supponiamo ora R commutativo. L'unicità di e seguirà se mostreremo che, dato un idempotente e, l'unico idempotente della forma $e+z$, con z nilpotente, è e. La condizione $(e+z)^2 = e+z$ dà $(1-2e)z = z^2$. Allora $z^3 = (1-2e)z^2 = (1-2e)^2 z$ e per induzione $(1-2e)^n z = z^{n+1}$. Poiché $(1-2e)^2 = 1 - 4e + 4e = 1$, ciò implica $z = 0$, e quindi $e + z = e$. □

Se e ed f sono idempotenti di R, lo sono anche $e' = 1 - e$, ef ed $e \circ f = 1 - (1-e)(1-f) = e + f - ef$. Si verifica facilmente che l'insieme E degli idempotenti di R è un'algebra di Boole per le operazioni $e \wedge f = ef$ ed $e \vee f = e \circ f$ (esercizio 1, p. 479 di BAI). Osserviamo poi che i sottoinsiemi aperti e chiusi di uno spazio topologico X costituiscono una sottoalgebra dell'algebra di Boole dei sottoinsiemi di X. Possiamo ora dimostrare il seguente teorema.

Teorema 7.3. *Se e è un idempotente di R, allora X_e è un sottospazio aperto e chiuso di* Spec R *e l'applicazione $e \mapsto X_e$ è un isomorfismo dell'algebra di Boole E sull'algebra di Boole dei sottoinsiemi aperti e chiusi di* Spec R.

Dimostrazione. Sia $e = e^2 \in R$. Allora $e(1-e) = 0$, perciò ogni ideale primo P di R contiene uno e uno solo degli elementi e, $1-e$. Dunque $X_e \cup X_{1-e} = X$ e $X_e \cap X_{1-e} = \varnothing$, sicché X_e è aperto e chiuso. Sia ora Y un sottoinsieme aperto e chiuso di X, e sia $Y' = X - Y$. Siano $\bar{R} = R/N$, $N = \operatorname{nilrad} R$, e sia ν l'omomorfismo canonico di R su $\bar{R}$. Dall'omeomorfismo $P \mapsto \nu(P)$ di $X = \operatorname{Spec} R$ con $\bar{X} = \operatorname{Spec} \bar{R}$ concludiamo che $\nu(Y)$ è un sottoinsieme aperto e chiuso di $\bar{X}$ e che $\nu(Y')$ ne è il complementare. Consideriamo $\Delta_{\nu(Y)}$ e $\Delta_{\nu(Y')}$ come definiti a p. 404. Sono ideali di $\bar{R}$ e $V(\Delta_{\nu(Y)}) = \nu(Y)$, $V(\Delta_{\nu(Y')}) = \nu(Y')$, poiché $\nu(Y)$ e $\nu(Y')$ sono aperti e chiusi in $\bar{X}$. Se $\bar{P}$ è un ideale primo di $\bar{R}$ contenente $\Delta_{\nu(Y)} + \Delta_{\nu(Y')}$, allora $\bar{P} \supseteq \Delta_{\nu(Y)}$ e $\bar{P} \supseteq \Delta_{\nu(Y')}$, cosicché $\bar{P} \in \nu(Y) \cap \nu(Y')$. Poiché $\nu(Y) \cap \nu(Y') = \varnothing$, un tale $\bar{P}$ non esiste, e quindi $\Delta_{\nu(Y)} + \Delta_{\nu(Y')} = \bar{R}$. Se $\bar{P}$ è un qualunque ideale primo di $\bar{R}$, allora $\bar{P} \supseteq \Delta_{\nu(Y)}$ oppure $\bar{P} \supseteq \Delta_{\nu(Y')}$, e quindi $\bar{P} \supseteq \Delta_{\nu(Y)} \cap \Delta_{\nu(Y')}$. Poiché ciò vale per tutti i $\bar{P}$ e $\bar{R}$ non ha elementi nilpotenti diversi da zero, $\Delta_{\nu(Y)} \cap \Delta_{\nu(Y')} = 0$. Dunque $\bar{R} = \Delta_{\nu(Y)} \oplus \Delta_{\nu(Y')}$. Sia $\bar{e}$ l'elemento unità di $\Delta_{\nu(Y')}$ e sia e l'idempotente di R tale che $\nu(e) = \bar{e}$. Ora, per un ideale primo P di R, la condizione $P \ni e$ equivale a $\nu(P) \ni \bar{e}$, che equivale a sua volta a $\nu(P) \supseteq \Delta_{\nu(Y')}$, ossia a $\nu(P) \in \nu(Y')$ e a $P \in Y'$. Quindi $X_e = Y$, il che mostra che l'applicazione $e \mapsto X_e$ è suriettiva.

Per vedere che è iniettiva, sia e un idempotente dato in R, $\bar{e} = \nu(e)$. Allora $\bar{R} = \bar{R}\bar{e} \oplus \bar{R}(\bar{1} - \bar{e})$ e $\bar{R}\bar{e}$, $\bar{R}(\bar{1} - \bar{e})$ sono ideali. Ora $\nu(X_e)$ è l'insieme degli ideali primi di $\bar{R}$ che contengono $\bar{1} - \bar{e}$, e quindi $\bar{R}(\bar{1} - \bar{e})$, e $\nu(X_{1-e})$ è l'insieme degli ideali primi contenenti $\bar{R}\bar{e}$. Abbiamo mostrato che $\bar{R} = \Delta_{\nu(X_e)} \oplus \Delta_{\nu(X_{1-e})}$. Poiché $\Delta_{\nu(X_e)} \supseteq \bar{R}(\bar{1} - \bar{e})$, $\Delta_{\nu(X_{1-e})} \supseteq \bar{R}\bar{e}$ e $\bar{R} = \bar{R}\bar{e} \oplus \bar{R}(\bar{1} - \bar{e})$, si ha $\Delta_{\nu(X_e)} = \bar{R}(\bar{1} - \bar{e})$. Per la proposizione 7.14, $1-e$ è l'unico idempotente nella classe laterale $\bar{1} - \bar{e}$, il che implica l'iniettività di $e \mapsto X_e$. Se e ed f sono idempotenti, allora $X_{ef} = X_e \cap X_f$. Inoltre $X_{1-e} = X - X_e$, $X_1 = X$ e $X_0 = \varnothing$. Queste relazioni implicano che $e \mapsto X_e$ è un isomorfismo di algebre di Boole. □

Dal teorema si ricava immediatamente la seguente conseguenza.

Corollario. Spec R *è connesso se e soltanto se R non contiene idempotenti diversi da* 0 *e da* 1.

In virtù di questo risultato, un anello commutativo R si dice *connesso* se i suoi soli idempotenti

sono 0 e 1.

Sia f un omomorfismo di R in un secondo anello R'. Se P' è un ideale primo di R', allora $P = f^{-1}(P')$ è un ideale primo di R. Infatti, se $ab \in P$, si ha $f(a)f(b) = f(ab) \in P'$. Quindi $f(a) \in P'$ oppure $f(b) \in P'$ e, di conseguenza, $a \in P$ oppure $b \in P$. Ciò permette di definire un'applicazione

$$f^*\colon P' \longmapsto f^{-1}(P')$$

di $X' = \operatorname{Spec} R'$ in $X = \operatorname{Spec} R$. Se $a \in R$, un ideale primo P' di R' non contiene $a' = f(a)$ se e soltanto se $P = f^*(P')$ non contiene a. Pertanto

$$(f^*)^{-1}(X_a) = X'_{f(a)}.$$

Ne segue che la controimmagine mediante f^* di ogni aperto di $\operatorname{Spec} R$ è aperta in $\operatorname{Spec} R'$, cosicché f^* è un'applicazione continua di $\operatorname{Spec} R'$ in $\operatorname{Spec} R$. È chiaro che, se $R' = R$ e $f = 1_R$, si ha $f^* = 1_{\operatorname{Spec} R}$ e che, se g è un omomorfismo di R' in R'', si ha $(g \circ f)^* = f^* \circ g^*$. Dunque la coppia di applicazioni $R \mapsto \operatorname{Spec} R$, $f \mapsto f^*$ definisce un funtore controvariante dalla categoria degli anelli commutativi (con gli omomorfismi come morfismi) nella categoria degli spazi topologici (con le applicazioni continue come morfismi).

Esercizi

1. Sia f un omomorfismo di R in R' e sia f^* la corrispondente applicazione continua di $\operatorname{Spec} R'$ in $\operatorname{Spec} R$. Dimostrare che, se f è suriettivo, $f^*(\operatorname{Spec} R')$ è il chiuso $V(\ker f)$ di $\operatorname{Spec} R$. Dimostrare anche che f^* è un omeomorfismo di $\operatorname{Spec} R'$ con il chiuso $V(\ker f)$.

2. Con le notazioni dell'esercizio 1, dimostrare che $f^*(\operatorname{Spec} R')$ è denso in $\operatorname{Spec} R$ se e soltanto se $\operatorname{nilrad} R \supseteq \ker f$. Osservare che ciò vale quando f è iniettivo.

3. Dare un esempio di omomorfismo f di R in R' per cui, per qualche ideale massimale M' di R', $f^{-1}(M')$ non sia massimale in R.

4. (D. Lazard.) Dimostrare che, se P è un ideale primo di R e I è l'ideale di R generato dagli idempotenti di R contenuti in P, allora R/I non contiene idempotenti diversi da 0 e da 1. Dimostrare che l'insieme degli ideali primi $P' \supseteq I$ è la componente connessa di $\operatorname{Spec} R$ contenente P (il più grande sottoinsieme connesso contenente P). *Suggerimento.* Sia $\bar{u} = u + I$ un idempotente di $\bar{R} = R/I$. Allora $u(1-u) \in I \subseteq P$ e possiamo supporre $u \in P$. Dimostrare che esiste $f \in I$ tale che $f^2 = f$ e $f(u-u^2) = u-u^2$. Allora $(1-f)u = g$ è un idempotente contenuto in P, perciò $g \in I$. Quindi $u = g + fu \in I$ e $\bar{u} = 0$.

Negli esercizi 5 e 6 l'anello R non è necessariamente commutativo.

5. Sia N un ideale nil di R e siano $\bar{u}_1, \ldots, \bar{u}_n$ elementi idempotenti ortogonali di $\bar{R} = R/N$ ($\bar{u}_i^2 = \bar{u}_i$, $\bar{u}_i\bar{u}_j = 0$ se $i \neq j$). Dimostrare che esistono idempotenti ortogonali e_i in R tali che $\bar{e}_i = \bar{u}_i$, $1 \leq i \leq n$. Dimostrare anche che, se $\sum_{i=1}^n \bar{u}_i = 1$, necessariamente $\sum_i e_i = 1$.

6. Siano $R, N, \bar{R}$ come nell'esercizio 5 e siano $\bar{u}_{ij}$, $1 \leq i, j \leq n$, elementi di $\bar{R}$ tali che $\bar{u}_{ij}\bar{u}_{kl} = \delta_{jk}\bar{u}_{il}$, $\sum_i \bar{u}_{ii} = 1$. Dimostrare che esistono $e_{ij} \in R$ tali che $e_{ij}e_{kl} = \delta_{jk}e_{il}$, $\sum_i e_{ii} = 1$, $\bar{e}_{ij} = \bar{u}_{ij}$, $1 \leq i, j \leq n$.[24]

[24] Nel secondo prodotto l'originale stampa $\delta_{lk}e_{ij}$. Si è ripristinata la relazione fra unità matriciali enunciata nella prima parte dell'esercizio.

7.6 Dipendenza intera

In BAI, pp. 278–281, abbiamo introdotto il concetto di elemento di un campo E intero su un sottoanello R di E. Il concetto e i risultati elementari ottenuti in BAI si estendono al caso generale in cui E è un anello commutativo arbitrario. Diamo la seguente definizione.

Definizione 7.2. *Se E è un anello commutativo e R è un suo sottoanello, un elemento $u \in E$ si dice intero su R se esiste un polinomio monico $f(x) \in R[x]$, con x indeterminata, tale che $f(u) = 0$.*

Se $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$, con $a_i \in R$, abbiamo la relazione $u^n = a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$, da cui deduciamo che, se $M = R1 + Ru + \cdots + Ru^{n-1}$, si ha $uM \subseteq M$. Evidentemente M è un R-sottomodulo finitamente generato di E contenente 1. Poiché $uM \subseteq M$, M è un $R[u]$-sottomodulo di E, e poiché $1 \in M$, M è fedele come $R[u]$-modulo. Abbiamo dunque l'implicazione $1 \Rightarrow 2$ nel risultato seguente.

Lemma. *Le seguenti condizioni per un elemento $u \in E$ sono equivalenti. 1. u è intero su R. 2. Esiste un $R[u]$-sottomodulo fedele di E che è finitamente generato come R-modulo.*

Dimostrazione. Supponiamo ora che valga la condizione 2. Esistono allora $u_i \in M$ tali che $M = Ru_1 + Ru_2 + \cdots + Ru_n$. Abbiamo le relazioni $uu_i = \sum_{j=1}^{n} a_{ij}u_j$, $1 \le i \le n$, con $a_{ij} \in R$. Otteniamo quindi il sistema

$$\begin{aligned}
(u - a_{11})u_1 - a_{12}u_2 - \cdots - a_{1n}u_n &= 0,\\
-a_{21}u_1 + (u - a_{22})u_2 - \cdots - a_{2n}u_n &= 0,\\
&\vdots\\
-a_{n1}u_1 - a_{n2}u_2 - \cdots + (u - a_{nn})u_n &= 0.
\end{aligned}$$

Se moltiplichiamo l'i-esima equazione per il cofattore dell'elemento (i, j) della matrice $u1 - (a_{ij})$ e sommiamo le equazioni ottenute, ricaviamo $f(u)u_j = 0$, $1 \le j \le n$, dove $f(x)$ è il polinomio caratteristico della matrice (a_{ij}). Poiché gli u_j generano M e M è fedele come $R[u]$-modulo, si ha $f(u) = 0$. Dunque u è una radice del polinomio monico $f(x)$ e perciò $2 \Rightarrow 1$. □

Osserviamo che il ragionamento appena usato differisce leggermente da quello dato nel caso dei campi in BAI, p. 279. Se M e N sono R-sottomoduli di E finitamente generati su R, lo stesso vale per $MN = \{\sum_i m_i n_i \mid m_i \in M,\ n_i \in N\}$. Inoltre, se $1 \in M$ e $1 \in N$, si ha $1 \in MN$ e, se $uM \subseteq M$ oppure $uN \subseteq N$, si ha $uMN \subseteq MN$. Queste osservazioni e il lemma precedente si possono usare esattamente come in BAI, pp. 279–280, per dimostrare il seguente teorema.

Teorema 7.4. *Se E è un anello commutativo e R è un sottoanello, il sottoinsieme R' degli elementi di E interi su R è un sottoanello contenente R. Inoltre, ogni elemento di E intero su R' è intero su R e quindi appartiene a R'.*

Il sottoanello R' di E si chiama *chiusura intera* di R in E. Se $R' = E$, ossia se ogni elemento di E è intero su R, diciamo che E è *intero su R* (oppure che E è un'*estensione intera* di R).

Se A è un ideale di un anello E, evidentemente $R \cap A$ è un ideale del sottoanello R di E. Lo chiamiamo *contrazione* di A a R e lo indichiamo con A^c. Abbiamo inoltre il sottoanello $(R + A)/A$ di E/A e l'isomorfismo canonico di questo anello con l'anello $R/A^c = R/(R \cap A)$. Si identifica di solito $(R + A)/A$ con R/A^c mediante l'isomorfismo canonico e si considera così E/A come un'estensione di R/A^c. In questo senso vale quanto segue.

Proposizione 7.15. *Se E è intero su R e A è un ideale di E, allora $\bar{E} = E/A$ è intero su $\bar{R} = R/A^c$.*

Dimostrazione. Sia $\bar{u} = u + A$ un elemento di $\bar{E}$. Esistono $a_i \in R$, $0 \le i \le n - 1$, tali che $u^n = a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$. Allora $\bar{u}^n = \bar{a}_0 + \bar{a}_1\bar{u} + \cdots + \bar{a}_{n-1}\bar{u}^{n-1}$, dove $\bar{a}_i = a_i + A$.

Dunque $\bar{u}$ è intero su $(R+A)/A$, e pertanto su $\bar{R} = R/A^c$. □

Supponiamo ora che S sia un sottomonoide del monoide moltiplicativo di R. Allora la localizzazione E_S contiene come sottoanello la localizzazione R_S. Vale inoltre la seguente proposizione.

Proposizione 7.16. *Sia R un sottoanello di E, sia R' la chiusura intera di R in E e sia S un sottomonoide del monoide moltiplicativo di R. Allora R'_S è la chiusura intera di R_S in E_S.*

Dimostrazione. Ogni elemento di R'_S ha la forma u/s, con $u \in R'$, $s \in S$. Abbiamo una relazione $u^n = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$, $a_i \in R$. Quindi

$$(u/s)^n = a_0/s^n + (a_1/s^{n-1})(u/s) + \cdots + (a_{n-1}/s)(u/s)^{n-1}.$$

Dunque u/s è intero su R_S. Viceversa, supponiamo che u/s sia intero su R_S, con $u \in E$, $s \in S$. Per mostrare che $u/s = v/t$, con $v \in R'$, $t \in S$, basta mostrare che esiste $s' \in S$ tale che $us' \in R'$. Infatti $u/s = us'/ss'$ ha la forma richiesta. Ora, dal fatto che u/s è intero su R_S segue che $u/1$ è intero su R_S, poiché $s/1 \in R_S$ e $u/1 = (u/s)(s/1)$. Abbiamo perciò una relazione della forma

$$(u/1)^n = a_0/s_0 + (a_1/s_1)(u/1) + \cdots + (a_{n-1}/s_{n-1})(u/1)^{n-1}$$

con $a_i \in R$, $s_i \in S$. Moltiplicando per $t_1^n/1$, dove $t_1 = \prod_{i=0}^{n-1} s_i$, otteniamo

$$(t_1 u/1)^n = a'_0/1 + (a'_1/1)(t_1 u/1) + \cdots + (a'_{n-1}/1)(t_1 u/1)^{n-1},$$

con $a'_i \in R$. Dunque $[(t_1 u)^n - a'_0 - a'_1(t_1 u) - \cdots - a'_{n-1}(t_1 u)^{n-1}]/1 = 0$. Esiste allora $t_2 \in S$ tale che $t_2[(t_1 u)^n - a'_0 - \cdots - a'_{n-1}(t_1 u)^{n-1}] = 0$. Moltiplicando questa relazione per t_2^{n-1} vediamo che $s'u \in R'$ per $s' = t_1 t_2$. □

Dimostriamo ora il risultato seguente.

Proposizione 7.17. *Se E è un dominio intero sul sottodominio R, allora E è un campo se e soltanto se R è un campo.*

Dimostrazione. Supponiamo anzitutto che R sia un campo e sia $u \neq 0$ un elemento di E. Abbiamo una relazione $u^n + a_1 u^{n-1} + \cdots + a_n = 0$ con $a_i \in R$, e poiché u non è un divisore dello zero in E, possiamo supporre $a_n \neq 0$. Allora a_n^{-1} esiste in R e si ha $u(u^{n-1} + a_1 u^{n-2} + \cdots + a_{n-1})(-a_n^{-1}) = 1$. Pertanto u è invertibile ed E è un campo. Viceversa, supponiamo che E sia un campo e sia $a \in R$, $a \neq 0$. Allora a^{-1} esiste in E e abbiamo una relazione $(a^{-1})^n + a_1(a^{-1})^{n-1} + \cdots + a_n = 0$ con $a_i \in R$. Moltiplicando per a^{n-1} otteniamo $a^{-1} = -(a_1 + a_2 a + \cdots + a_n a^{n-1}) \in R$. Dunque a è invertibile in R e R è un campo. □

Una conseguenza immediata di questo risultato e della proposizione 7.15 è il seguente corollario.

Corollario 1. *Sia E un anello commutativo, sia R un sottoanello tale che E sia intero su R e sia P un ideale primo di E. Allora $P^c = P \cap R$ è massimale in R se e soltanto se P è massimale in E.*

Dimostrazione. $\bar{E} = E/P$ è un dominio e per la proposizione 7.15 $\bar{E}$ è intero su $\bar{R} = R/P^c$. Per la proposizione 7.17, $\bar{E}$ è un campo se e soltanto se $\bar{R}$ è un campo. Pertanto P è massimale in E se e soltanto se P^c è massimale in R. □

Si ha inoltre il seguente corollario.

Corollario 2. *Siano E e R come nel corollario 1 e siano P_1 e P_2 ideali primi di E tali che $P_1 \supsetneq P_2$. Allora $P_1^c \supsetneq P_2^c$.*[25]

Dimostrazione. Abbiamo $P_1^c \supseteq P_2^c$. Supponiamo ora $p = P_1^c = P_2^c$. Consideriamo la localizzazione E_S per $S = R - p$. Per la proposizione 7.16, E_S è intero su R_S. Poiché $P_i \cap R = p$, si

[25] Nell'enunciato originale si legge «ideals in R». La dimostrazione considera ideali primi di E, che è l'ipotesi del corollario di incomparabilità.

ha $P_i \cap S = \varnothing$. Allora, per la proposizione 7.8, $P_{1S} \supsetneq P_{2S}$. D'altra parte P_{iS} contiene p_S, che è l'ideale massimale dell'anello locale R_S. Poiché E_S è intero su R_S, dal corollario 1 segue che P_{iS} è massimale in E_S. Ciò contraddice $P_{1S} \supsetneq P_{2S}$. Dunque $P_1^c \supsetneq P_2^c$. □

Se P è un ideale primo di E, è chiaro che P^c è un ideale primo di R. Abbiamo pertanto un'applicazione $P \mapsto P^c$ di $\operatorname{Spec} E$ in $\operatorname{Spec} R$. Essa è suriettiva, in virtù del seguente teorema.

Teorema 7.5 (teorema del *lying-over*). *Sia E un anello commutativo e sia R un suo sottoanello tale che E sia intero su R. Allora ogni ideale primo p di R è la contrazione P^c di un ideale primo P di E.*

Dimostrazione. Supponiamo anzitutto che R sia locale e p sia l'ideale massimale di R. Sia P un ideale massimale di E. Per il corollario precedente, P^c è un ideale massimale di R. Poiché p è l'unico ideale massimale di R, abbiamo $p = P^c$.

Sia ora R arbitrario e consideriamo le localizzazioni R_p ed E_p. L'anello R_p è locale ed E_p è intero su R_p (proposizione 7.16). Esiste dunque un ideale primo P' di E_p la cui contrazione $P'^c = P' \cap R_p$ è p_p, l'ideale massimale di R_p. Per la proposizione 7.8 (p. 401), $P' = P_p$ per un ideale primo P di E tale che $P \cap (R - p) = \varnothing$ o, equivalentemente, $P \cap R \subseteq p$. Sempre per la proposizione 7.8,

$$P = j(P_p) = \{u \in E \mid u/s \in P_p \text{ per qualche } s \in R - p\}.$$

Ora $p \subseteq j(p_p) \subseteq j(P_p) = P$. Dunque $P \cap R = p$. □

Esercizi

1. Sia E un anello commutativo e sia R un sottoanello tale che (1) E sia intero su R e (2) E sia finitamente generato come R-algebra. Dimostrare che E è finitamente generato come R-modulo.

2. (Teorema del *going-up*.) Sia E un anello commutativo e sia R un sottoanello tale che E sia intero su R. Siano p_1, p_2 ideali primi di R tali che $p_1 \supseteq p_2$ e sia P_2 un ideale primo di E tale che $P_2^c = p_2$. Dimostrare che esiste un ideale primo P_1 di E tale che $P_1 \supseteq P_2$ e $P_1^c = p_1$.

3. Sia R un sottoanello di un anello commutativo E, sia R' la chiusura intera di R in E, sia I un ideale di R e sia $I^e = IR'$ il suo esteso in R'. Un elemento $a \in E$ si dice *intero su* I se soddisfa un'equazione $f(a) = 0$ dove $f(\lambda) = \lambda^m + b_1\lambda^{m-1} + \cdots + b_m$, con $b_i \in I$. Il sottoinsieme I' di E degli elementi interi su I si chiama *chiusura intera di I in E*.

   Dimostrare che $I' = \operatorname{nilrad} I^e$ in R'. *Traccia della dimostrazione.* Se $a \in E$ e $a^m + b_1 a^{m-1} + \cdots + b_m = 0$ con $b_i \in I$, allora $a \in R'$ e $a^m \in I^e$. Dunque $a \in \operatorname{nilrad} I^e$ in R'. Viceversa, sia $a \in \operatorname{nilrad} I^e$ in R'. Allora $a \in R'$ e $a^m = \sum_{i=1}^n a_i b_i$ per qualche $m > 0$, con $a_i \in R'$, $b_i \in I$. Sia A la R-sottoalgebra di E generata dagli a_i. Per l'esercizio 1, A ammette un insieme finito di generatori $a_1, \ldots, a_q$, $q \geq n$, come R-modulo. Allora $a^m a_j = \sum_{k=1}^q b_{jk} a_k$, $1 \leq j \leq q$, con $b_{jk} \in I$. Come nella dimostrazione del lemma a p. 408, ciò implica che a^m, e quindi a, è intero su I.

   Osservazioni. (i) I' è un sottoanello di E (nel senso di BAI, ossia I' è un sottogruppo del gruppo additivo chiuso rispetto alla moltiplicazione). (ii) Se R è integralmente chiuso in E ($R' = R$), allora $I' = \operatorname{nilrad} I$ in R.

4. (Proprietà fondamentali della contrazione e dell'estensione di ideali.) Sia R un sottoanello di un anello commutativo E. Per ogni ideale I di E, $I^c = I \cap R$ è un ideale di R, e per

ogni ideale i di R, $i^e = iE$ è un ideale di E. Osservare che

$$I_1 \supseteq I_2 \implies I_1^c \supseteq I_2^c, \qquad i_1 \supseteq i_2 \implies i_1^e \supseteq i_2^e,$$
$$i^{ec} \supseteq i, \qquad I^{ce} \subseteq I.$$

Deducerne che $i^{ece} = i^e$, $I^{cec} = I^c$ per ogni coppia di ideali i e I. Osservare che da ciò segue che un ideale i di R è la contrazione di un ideale di E se e soltanto se $i = i^{ec}$, e un ideale I di E è l'esteso di un ideale di R se e soltanto se $I = I^{ce}$.

7.7 Domini integralmente chiusi

Un'importante proprietà dei domini, che incontreremo specialmente nello studio dei domini di Dedekind (si veda il capitolo 10), è espressa dalla definizione seguente.

Definizione 7.3. *Un dominio D si dice integralmente chiuso se è integralmente chiuso nel suo campo delle frazioni.*

Si vede facilmente che $\mathbb{Z}$ è integralmente chiuso. Più generalmente, ogni dominio fattoriale è integralmente chiuso (esercizio 1, qui sotto). In questo breve paragrafo il nostro scopo principale è dimostrare un teorema di discesa (teorema 7.6) per i domini integralmente chiusi, che ci servirà più avanti (nella dimostrazione del teorema 8.37). Per dimostrare questo teorema ci occorre il seguente risultato.

Proposizione 7.18. *Sia D un sottodominio integralmente chiuso di un dominio E, sia F il campo delle frazioni di D e sia I un ideale di D. Sia $a \in E$ intero su I. Allora a è algebrico su F e il suo polinomio minimo $m(\lambda) = \lambda^m - b_1\lambda^{m-1} + \cdots + (-1)^m b_m$ su F ha i coefficienti $(-1)^j b_j \in \operatorname{nilrad} I$, $1 \leq j \leq m$.*

Dimostrazione. La prima affermazione è chiara. Per la seconda, sia S un campo di spezzamento di $m(\lambda)$ su F e sia $m(\lambda) = (\lambda - a_1)\cdots(\lambda - a_m)$ in $S[\lambda]$, con $a_1 = a$. Per ogni i esiste un automorfismo di S/F che manda a in a_i. Poiché esso stabilizza I, ne segue che ogni a_i è intero su I. Poiché b_j, $1 \leq j \leq m$, è un polinomio simmetrico elementare negli a_i, dall'osservazione (i) che segue l'esercizio 3 del ğ 7.6 si ricava che b_j è intero su I. Allora, per l'osservazione (ii), $b_j \in \operatorname{nilrad} I$. □

Ci occorre anche il seguente criterio affinché un ideale sia la contrazione di un ideale primo.

Proposizione 7.19. *Sia R un sottoanello di un anello commutativo E e sia p un ideale primo di R. Allora $p = P^c = P \cap R$ per un ideale primo P di E se e soltanto se $p^{ec} = Ep \cap R = p$.*

Dimostrazione. Se $p = P^c$, si ha $p^{ec} = p$ per l'esercizio 4 del ğ 7.6. Supponiamo ora che questa uguaglianza valga per un ideale primo p di R. Consideriamo il sottomonoide $S = R - p$ del monoide moltiplicativo di E. Poiché $p^{ec} = p$, si ha $Ep \cap R = p$, e quindi $Ep \cap S = \varnothing$. Essendo Ep un ideale di E con $Ep \cap S = \varnothing$, l'esteso $(Ep)_S$ è un ideale proprio della localizzazione E_S di E rispetto al monoide S. Allora $(Ep)_S$ è contenuto in un ideale massimale Q di E_S e $P = j(Q)$, definito dalla (18), è un ideale primo di E tale che $P \cap (R - p) = P \cap S = \varnothing$. Dunque $P \cap R \subseteq p$. Poiché $P = j(Q) \supseteq j((Ep)_S) \supseteq p$, si ha $P^c = P \cap R = p$. □

Possiamo ora dimostrare il seguente teorema.

Teorema 7.6 (teorema di discesa, *going-down*). *Sia D un sottodominio integralmente chiuso di un dominio E intero su D. Siano p_1, p_2 ideali primi di D tali che $p_1 \supseteq p_2$ e sia P_1 un ideale primo di E tale che $P_1^c = p_1$. Allora esiste un ideale primo P_2 di E tale che $P_2^c = p_2$ e $P_2 \subseteq P_1$.*

Dimostrazione. Consideriamo la localizzazione E_{P_1} $(= E_{E-P_1})$. Basta mostrare che $p_2 E_{P_1} \cap D = p_2$. Infatti, se vale questa uguaglianza, per la proposizione 7.19 esiste un ideale primo Q di E_{P_1}

tale che $D \cap Q = p_2$. Allora $P_2 = j(Q)$ è un ideale primo di E contenuto in P_1 e

$$P_2 \cap D = j(Q) \cap D = j(Q) \cap E \cap D = Q \cap D = p_2.$$

Dimostriamo dunque che $p_2E_{P_1} \cap D = p_2$. Sia $a \in p_2E_{P_1}$. Allora $a = b/s$, con $b \in Ep_2$ e $s \in E - P_1$. Per l'esercizio 3 del § 7.6, b è intero su p_2 e quindi, per la proposizione 7.18, il polinomio minimo di b sul campo delle frazioni F di D ha la forma $\lambda^m - b_1\lambda^{m-1} + \cdots + (-1)^m b_m$, con $b_i \in p_2$, $1 \leq i \leq m$.

Supponiamo $a = b/s \in p_2E_{P_1} \cap D$. Possiamo limitarci al caso $a \neq 0$. Allora $s = b/a$ e il polinomio minimo di s su F è $\lambda^m - (b_1/a)\lambda^{m-1} + \cdots + (-1)^m(b_m/a^m)$. Poiché s è intero su D, ponendo $I = D$ nella proposizione 7.18 vediamo che ogni b_i/a^i appartiene a D. Allora $(b_i/a^i)a^i \in p_2$, con b_i/a^i e a^i in D. Supponiamo ora $a \notin p_2$. Poiché p_2 è primo in D, si ha $b_i/a^i \in p_2$ per $1 \leq i \leq m$. Dunque s è intero su p_2 e quindi su p_1. Di nuovo per l'esercizio 3, $s \in \text{nilrad}(p_1E) \subseteq P_1$, in contraddizione con $s \in E - P_1$. Ciò mostra che $a \in p_2$, cosicché $p_2E_{P_1} \cap D \subseteq p_2$. Poiché l'inclusione inversa è chiara, si ha $p_2E_{P_1} \cap D = p_2$. □

Esercizi

1. Dimostrare che ogni dominio fattoriale è integralmente chiuso.

2. Sia D un dominio e sia F il suo campo delle frazioni. Dimostrare che, se D è integralmente chiuso, D_S è integralmente chiuso per ogni sottomonoide S del monoide moltiplicativo di D per cui si definisce la localizzazione nel campo delle frazioni. Viceversa, dimostrare che, se D_P è integralmente chiuso per ogni ideale massimale P di D, allora D è integralmente chiuso. *Suggerimento.* Usare la proposizione 7.11 a p. 402.

7.8 Rango dei moduli proiettivi

Abbiamo mostrato in *BAI*, p. 171, che se R è un anello commutativo e M è un R-modulo con una base di n elementi, allora ogni base ha cardinalità n. Il numero n, detto *rango* di M, è quindi un invariante. Ripetiamo il ragionamento in una forma leggermente migliorata. Sia $\{e_i \mid 1 \leq i \leq n\}$ una base di M e sia $\{f_j \mid 1 \leq j \leq m\}$ un insieme di generatori. Allora $f_j = \sum_{i=1}^n a_{ji}e_i$ ed $e_i = \sum_{k=1}^m b_{ik}f_k = \sum_{k,j} b_{ik}a_{kj}e_j$, da cui $\sum_{k=1}^m b_{ik}a_{kj} = \delta_{ij}$ per $1 \leq i, j \leq n$. Supponiamo $n \geq m$ e consideriamo le matrici $n \times n$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ & & 0 & \end{bmatrix}, \qquad B = \begin{bmatrix} b_{11} & \cdots & b_{1m} & \\ b_{21} & \cdots & b_{2m} & \\ \vdots & & \vdots & 0 \\ b_{n1} & \cdots & b_{nm} & \end{bmatrix}.$$

Si ha $BA = 1_n$, la matrice identità $n \times n$. Essendo R commutativo, ne segue $AB = 1_n$ (*BAI*, p. 97), impossibile se $n > m$. Dunque $n = m$. Se M ha una base di n elementi, ogni insieme di generatori contiene pertanto almeno n elementi. Ne segue che due basi qualsiasi hanno la stessa cardinalità. Il ragionamento mostra inoltre che ogni insieme di n generatori $f_j = \sum_i a_{ji}e_i$, $1 \leq j \leq n$, è una base. Infatti la matrice $A = (a_{ij})$ è in tal caso invertibile in $M_n(R)$, e ciò implica che l'unica relazione della forma $\sum_i c_i f_i = 0$ si ha con tutti i $c_i = 0$. Riassumiamo i risultati nella proposizione seguente.

Proposizione 7.20. *Sia M un modulo libero su un anello commutativo, con una base di n elementi. Allora (1) ogni base ha cardinalità n, (2) ogni insieme di generatori contiene almeno n elementi, e (3) ogni insieme di n generatori è una base.*

Daremo ora un metodo, basato sulla localizzazione, per estendere la nozione di rango ai moduli proiettivi finitamente generati su anelli commutativi R. Mostreremo anzitutto che, se R è locale, tali moduli sono liberi. A tal fine ci occorre un importante lemma per anelli arbitrari, noto come

Lemma di Nakayama. *Sia M un modulo su un anello R (non necessariamente commutativo). Supponiamo che (1) M sia finitamente generato e (2) $(\operatorname{rad} R)M = M$. Allora $M = 0$.*

Dimostrazione. Sia m il minimo intero tale che M sia generato da m elementi $x_1, x_2, \dots, x_m$. Se $M \neq 0$, allora $m > 0$. La condizione $(\operatorname{rad} R)M = M$ implica $x_m = r_1 x_1 + \cdots + r_m x_m$ con $r_i \in \operatorname{rad} R$. Quindi

$$(1 - r_m)x_m = r_1 x_1 + \cdots + r_{m-1} x_{m-1}.$$

Poiché $r_m \in \operatorname{rad} R$, $1 - r_m$ è invertibile in R. Applicando $(1 - r_m)^{-1}$ alla relazione, si vede che x_m si esprime mediante $x_1, \dots, x_{m-1}$. Allora $x_1, \dots, x_{m-1}$ generano M, contro la scelta di m. □

Ricordiamo che, se B è un ideale di un anello R e M un R-modulo, allora BM è un sottomodulo e il modulo M/BM è annullato da B, sicché si può considerare naturalmente come R/B-modulo. Ciò vale in particolare per $B = \operatorname{rad} R$. In questo caso il lemma di Nakayama ha la seguente conseguenza.

Corollario. *Sia M un R-modulo finitamente generato. Allora $x_1, \dots, x_m \in M$ generano M se e solo se le classi $\bar{x}_1 = x_1 + (\operatorname{rad} R)M, \dots, \bar{x}_m = x_m + (\operatorname{rad} R)M$ generano $M/(\operatorname{rad} R)M$ come modulo su $R/\operatorname{rad} R$.*

Dimostrazione. Se $x_1, \dots, x_m$ generano M, è evidente che $\bar{x}_1, \dots, \bar{x}_m$ generano $\bar{M} = M/(\operatorname{rad} R)M$ come R-modulo e, equivalentemente, come modulo su $\bar{R} = R/\operatorname{rad} R$. Viceversa, supponiamo che i $\bar{x}_i$ generino $\bar{M}$ come $\bar{R}$-modulo, dunque come R-modulo. Allora $M = (\operatorname{rad} R)M + N$, dove $N = \sum_i Rx_i$. Abbiamo $(\operatorname{rad} R)(M/N) = M/N$ e M/N è finitamente generato. Il lemma di Nakayama implica $M/N = 0$, onde $M = N = \sum_i Rx_i$. □

Possiamo ora dimostrare il teorema seguente.

Teorema 7.7. *Se R è un anello locale (commutativo), ogni modulo proiettivo finitamente generato su R è libero.*

Dimostrazione. Possiamo supporre che M sia un addendo diretto di un modulo libero $F = R^{(n)}$, cioè $F = M \oplus N$ con M, N sottomoduli. Allora $(\operatorname{rad} R)F = (\operatorname{rad} R)M + (\operatorname{rad} R)N$, con $(\operatorname{rad} R)M \subseteq M$ e $(\operatorname{rad} R)N \subseteq N$. Dunque $\bar{F} = F/(\operatorname{rad} R)F = \bar{M} \oplus \bar{N}$, dove

$$\bar{M} = \frac{M + (\operatorname{rad} R)F}{(\operatorname{rad} R)F}, \qquad \bar{N} = \frac{N + (\operatorname{rad} R)F}{(\operatorname{rad} R)F}.$$

Ora $\bar{R} = R/\operatorname{rad} R$ è un campo, $\bar{F}$ è chiaramente uno spazio vettoriale di dimensione n su $\bar{R}$, e $\bar{M}, \bar{N}$ ne sono sottospazi. Possiamo scegliere $y_1, \dots, y_n$ in modo che $y_1, \dots, y_r \in M$, $y_{r+1}, \dots, y_n \in N$ e, posto $\bar{y}_i = y_i + (\operatorname{rad} R)F$, l'insieme $\{\bar{y}_1, \dots, \bar{y}_n\}$ sia una base di $\bar{F}$ su $\bar{R}$. Per il corollario del lemma di Nakayama, $y_1, \dots, y_n$ generano F e, per la proposizione 7.20, ne formano una base. Allora $\{y_1, \dots, y_r\}$ è una base di M, sicché M è libero. □

Consideriamo ora i moduli proiettivi finitamente generati su un anello arbitrario R e proviamo anzitutto la proposizione seguente.

Proposizione 7.21. *Se M è un R-modulo libero di rango n, per ogni sottomonoide S del monoide moltiplicativo di R il modulo M_S è libero di rango n su R_S. Se M è proiettivo con n generatori su R, allora M_S è proiettivo con n generatori su R_S.*

Dimostrazione. Per la prima asserzione ricordiamo che la localizzazione rispetto a S è un funtore da R-**mod** a R_S-**mod**. Quindi una relazione $M \cong M_1 \oplus \cdots \oplus M_s$ fra R-moduli implica $M_S \cong M_{1S} \oplus \cdots \oplus M_{sS}$ fra R_S-moduli. Da $M \cong R \oplus \cdots \oplus R$ (n copie) segue $M_S \cong R_S \oplus \cdots \oplus R_S$ (n copie). Supponiamo ora che M sia proiettivo con n generatori. Ciò equivale a supporre che M sia isomorfo a un addendo diretto del modulo libero $R^{(n)}$. Allora M_S è proiettivo con n generatori su R_S. □

In particolare, se M è proiettivo con n generatori, per ogni ideale primo P il modulo M_P è proiettivo con n generatori sull'anello locale R_P. Dunque M_P è libero su R_P e ha rango $n_P \leq n$. Chiameremo n_P il *P-rango* di M e diremo che M *ha rango* se $n_P = n_Q$ per ogni coppia di ideali primi P, Q di R. In tal caso il valore comune dei ranghi locali n_P si chiama *rango* del modulo proiettivo finitamente generato M. Mostreremo che $P \mapsto n_P$ è un'applicazione continua di $\operatorname{Spec} R$ in $\mathbb{Z}$ munito della topologia discreta. Ne seguirà che, se $\operatorname{Spec} R$ è connesso, ossia, equivalentemente, R non ha idempotenti diversi da $0, 1$, allora M ha rango.

La continuità che vogliamo dimostrare seguirà facilmente dalla proposizione seguente.

Proposizione 7.22. *Siano M un R-modulo proiettivo finitamente generato e P un ideale primo di R. Esiste allora $a \notin P$ tale che $M_{\langle a \rangle}$ è libero come $R_{\langle a \rangle}$-modulo.*

Dimostrazione. M_P è un R_P-modulo libero di rango finito. Sia $(x_1/s_1, \ldots, x_n/s_n)$, con $x_i \in M$ e $s_i \in R - P$, una base di M_P. Poiché gli $s_i/1$ sono unità di R_P, anche $(x_1/1, \ldots, x_n/1)$ è una base. Consideriamo l'R-omomorfismo f di $R^{(n)}$ in M tale che $(a_1, \ldots, a_n) \mapsto \sum_i a_i x_i$. Abbiamo la successione esatta

$$0 \longrightarrow \ker f \xrightarrow{i} R^{(n)} \xrightarrow{f} M \xrightarrow{p} \operatorname{coker} f \longrightarrow 0.$$

Localizzando in P si ottiene la successione esatta

$$0 \longrightarrow \ker f_P \longrightarrow R_P^{(n)} \xrightarrow{f_P} M_P \longrightarrow \operatorname{coker} f_P \longrightarrow 0.$$

Poiché M_P è libero con base $(x_1/1, \ldots, x_n/1)$, f_P è un isomorfismo, onde $\ker f_P = 0$ e $\operatorname{coker} f_P = 0$. Insieme con M è finitamente generata anche la sua immagine omomorfa $\operatorname{coker} f$ e, poiché $\operatorname{coker} f_P = (\operatorname{coker} f)_P$, per la proposizione 7.5 esiste $b \notin P$ tale che $b(\operatorname{coker} f) = 0$. Allora $(\operatorname{coker} f)_{\langle b \rangle} = 0$ e abbiamo la successione esatta

$$0 \longrightarrow \ker f_{\langle b \rangle} \longrightarrow R_{\langle b \rangle}^{(n)} \xrightarrow{f_{\langle b \rangle}} M_{\langle b \rangle} \longrightarrow 0.$$

Poiché $M_{\langle b \rangle}$ è proiettivo, la successione si spezza, sicché $\ker f_{\langle b \rangle}$ è isomorfo a un'immagine omomorfa di $R_{\langle b \rangle}^{(n)}$ ed è quindi finitamente generato. Poiché $\langle b \rangle$ è un sottomonoide di $R - P$, il modulo $0 = (\ker f)_P = \ker f_P$ si ottiene localizzando $(\ker f)_{\langle b \rangle}$ (proposizione 7.4). Essendo $(\ker f)_{\langle b \rangle}$ finitamente generato, esiste $c/1$, con $c \notin P$, tale che $(c/1)(\ker f)_{\langle b \rangle} = 0$. Allora $\ker f_{\langle bc \rangle} = 0$. Dunque, posto $a = bc$, abbiamo $a \notin P$ e

$$0 \longrightarrow R_{\langle a \rangle}^{(n)} \xrightarrow{f_{\langle a \rangle}} M_{\langle a \rangle} \longrightarrow 0.$$

Ne segue che $M_{\langle a \rangle} \cong R_{\langle a \rangle}^{(n)}$ è libero. □

Teorema 7.8. *L'applicazione* $r_M\colon P \mapsto n_P(M)$ *di* $\operatorname{Spec} R$ *in* $\mathbb{Z}$ *(con la topologia discreta) è continua.*

Dimostrazione. Sia P un punto qualsiasi di $\operatorname{Spec} R$. Dobbiamo mostrare che esiste un aperto O contenente P tale che $n_Q = n_P$ per ogni $Q \in O$. Prendiamo $O = X_a$ con a come nella proposizione 7.22. Allora $P \in X_a$ e, se $Q \in X_a$, M_Q è una localizzazione di $M_{\langle a\rangle}$, che è un $R_{\langle a\rangle}$-modulo libero di rango n. Il rango di M_Q è dunque n, ossia $n_Q = n = n_P$. □

Se $\operatorname{Spec} R$ è connesso, la continuità di r_M implica $n_P = n_Q$ per ogni $P, Q \in \operatorname{Spec} R$. Segue il corollario.

Corollario. *Se* R *è connesso, ossia non ha idempotenti diversi da* $0, 1$*, il rango è definito per ogni* R*-modulo proiettivo finitamente generato.*

Sia ancora M un modulo proiettivo finitamente generato e consideriamo l'applicazione continua r_M di $\operatorname{Spec} R$ in $\mathbb{Z}$. Poiché $\mathbb{Z}$ ha la topologia discreta, ogni singoletto $\{n\}$ è aperto e chiuso in $\mathbb{Z}$, e $r_M^{-1}(n)$ è aperto e chiuso in $\operatorname{Spec} R$. Inoltre $\operatorname{Spec} R$ è l'unione disgiunta di questi insiemi. Poiché è quasi-compatto, solo un numero finito degli $r_M^{-1}(n)$ è non vuoto. Esistono dunque interi $n_1, \dots, n_s$ tali che $r_M^{-1}(n_i) \neq \varnothing$ e $X = \operatorname{Spec} R = \bigcup_i r_M^{-1}(n_i)$. Per il teorema 7.3 l'aperto e chiuso $r_M^{-1}(n_i)$ è della forma X_{e_i}, con $e_i \in R$ idempotente. Poiché $r_M^{-1}(n_i) \cap r_M^{-1}(n_j) = \varnothing$ per $i \neq j$, abbiamo $e_i e_j = 0$ per $i \neq j$, e poiché $\bigcup_i r_M^{-1}(n_i) = X$, abbiamo $\sum_i e_i = 1$. Gli e_i sono quindi idempotenti ortogonali di R di somma 1, onde $R = R_1 \oplus \cdots \oplus R_s$ con $R_i = Re_i$, e $M = M_1 \oplus \cdots \oplus M_s$ con $M_i = e_i M = R_i M$. Dal lemma della base duale (proposizione 3.11, p. 152) è chiaro che M_i è un R_i-modulo proiettivo finitamente generato.

Affermiamo che M_i ha rango su R_i e che tale rango è n_i. Sia P_i un ideale primo di R_i. Allora $P = P_i + \sum_{j\neq i} R_j$ è un ideale primo di R che non contiene e_i, sicché $P \in X_{e_i}$, e P contiene ogni e_j per $j \neq i$. Abbiamo $R_P = R_{1P} \oplus \cdots \oplus R_{sP}$ e, poiché $e_i \notin P$ ed $e_i R_j = 0$ per $j \neq i$, $R_P = R_{iP}$. Analogamente $M_P = M_{iP}$. Il rango di M_{iP} su R_{iP} è dunque n_i. L'omomorfismo $r \mapsto re_i$ di R in R_i manda gli elementi di $R - P$ in $R_i - P_i$. Componendolo con l'omomorfismo canonico di R_i in R_{iP_i}, otteniamo un omomorfismo di R in R_{iP_i} che manda gli elementi di $R - P$ in elementi invertibili. Ne segue un omomorfismo di R_P in R_{iP_i}, mediante il quale possiamo considerare R_{iP_i} come R_P-modulo. Allora $M_{iP_i} = R_{iP_i} \otimes_{R_P} M_{iP}$ e, poiché M_{iP} è un R_{iP}-modulo libero di rango n_i, M_{iP_i} è un R_{iP_i}-modulo libero di rango n_i. Poiché ciò vale per ogni ideale primo P_i di R_i, il rango di M_i su R_i è n_i. Possiamo enunciare parte di quanto dimostrato nel modo seguente.

Teorema 7.9. *Sia* M *un modulo proiettivo finitamente generato su un anello commutativo* R*. I ranghi* $n_P(M)$*, al variare dell'ideale primo* P *di* R*, assumono soltanto un numero finito di valori. Se questi sono* $n_1, \dots, n_s$*, allora* $R = R_1 \oplus \cdots \oplus R_s$*, dove gli* R_i *sono ideali tali che* $R_i M$ *è proiettivo finitamente generato di rango* n_i *su* R_i*.*

Esercizi.

1. Sia M un modulo proiettivo finitamente generato sull'anello commutativo R e sia P un ideale massimale di R. Mostrare che, se M ha rango su R, questo è la dimensione di M/PM come spazio vettoriale sul campo R/P.

2. Siano M, R come nell'esercizio 1 e si supponga che R sia un'algebra su R', proiettiva e finitamente generata come modulo su R'. Supponiamo che M abbia rango su R e R abbia rango su R'. Mostrare che M ha rango su R' e che

$$\operatorname{rg}(M/R') = \operatorname{rg}(M/R)\operatorname{rg}(R/R').$$

3. Mostrare che, se D è un dominio, ogni modulo proiettivo finitamente generato M su D ha rango, e questo coincide con la dimensione di $F \otimes_D M$ su F, dove F è il campo delle frazioni di D.

7.9 Gruppo delle classi proiettive

Ritorniamo alla teoria di Morita. Ricordiamo che, se R', R sono anelli, un R'-R-bimodulo M si dice *invertibile* se esiste un R-R'-bimodulo M' tale che $M' \otimes_{R'} M \cong R$ come R-R-bimodulo e $M \otimes_R M' \cong R'$ come R'-R'-bimodulo. Ciò avviene se e solo se M è un progeneratore di **mod**-R (R'-**mod**). Allora $R' \cong \operatorname{End} M_R$ come anelli e $M' = \hom(M_R, R_R)$ come R-R'-bimodulo. Se $R' = R$, le classi di isomorfismo dei bimoduli invertibili formano un gruppo $\operatorname{Pic} R$ in cui la moltiplicazione è data dal prodotto tensoriale. Supponiamo ora R commutativo. Limitiamoci agli R-R-bimoduli in cui l'azione sinistra coincide con quella destra. In effetti stiamo considerando gli R-moduli (sinistri). Le classi di isomorfismo dei moduli invertibili costituiscono un sottogruppo di $\operatorname{Pic} R$, detto *gruppo delle classi proiettive* dell'anello commutativo R. Il risultato seguente identifica i moduli le cui classi di isomorfismo costituiscono tale gruppo.

Teorema 7.10. *Siano R un anello commutativo e M un R-modulo. Allora M è invertibile se e solo se è fedele, proiettivo, finitamente generato e di rango* 1.

Dimostrazione. Supponiamo che M sia invertibile e che M' sia un R-modulo tale che $M \otimes_R M' \cong R$. Allora M e M' sono proiettivi finitamente generati. Sia P un ideale primo di R. Da $M \otimes_R M' \cong R$ segue $M_P \otimes_{R_P} M'_P \cong R_P$. Poiché questi moduli sono liberi di rango finito sull'anello locale R_P, la relazione implica $\operatorname{rg}(M_P/R_P) = 1$. Ciò vale per ogni P, quindi M ha rango 1.

Viceversa, supponiamo che M soddisfi le condizioni enunciate e sia $M^* = \hom_R(M, R)$. Poiché M è fedele, proiettivo e finitamente generato, è un progeneratore per il teorema 3.22. Come nella teoria di Morita, abbiamo l'isomorfismo ρ di $M \otimes_R M^*$ su $\operatorname{End}_R M$ che manda $x \otimes y^*$, con $x \in M$, $y^* \in M^*$, nell'applicazione $y \mapsto y^*(y)x$. Poiché R è commutativo, ogni $r \in R$ determina un R-endomorfismo $y \mapsto ry$. Possiamo identificare R con questo insieme di endomorfismi, sicché $\operatorname{End}_R M \supseteq R$. Per mostrare che $M \otimes_R M^* \cong R$ basta dunque provare che $\operatorname{End}_R M = R$. Ciò seguirà se mostriamo che $(\operatorname{End}_R M)_P = R_P$ per ogni ideale primo P. Ora $(\operatorname{End}_R M)_P \cong R_P \otimes_R \operatorname{End}_R M$. Essendo M proiettivo finitamente generato, si vede facilmente che $R_P \otimes_R \operatorname{End}_R M \cong \operatorname{End}_{R_P} M_P$ (si veda la dimostrazione della proposizione 3.14, p. 154). Se M è un modulo libero di rango n su un anello commutativo R, $\operatorname{End}_R M$ è un modulo libero di rango n^2 su R (è isomorfo a $M_n(R)$). Per ipotesi M_P ha rango 1 su R_P, dunque $\operatorname{End}_{R_P} M_P$ ha rango 1 su R_P. Ne segue che $(\operatorname{End}_R M)_P$ ha rango 1 su R_P, e quindi $(\operatorname{End}_R M)_P = R_P$ per ogni P. La dimostrazione è conclusa. □

Per ora non daremo esempi di gruppi delle classi proiettive. Più avanti (ğ 10.6) vedremo come, nel caso di un campo di numeri algebrici, questo gruppo si identifichi con un gruppo classico della teoria dei numeri.

7.10 Anelli noetheriani

Nel resto del capitolo ci interesseremo principalmente degli anelli e dei moduli noetheriani. Ricordiamo che la condizione noetheriana, secondo cui un modulo soddisfa la condizione della catena ascendente per i sottomoduli, equivale alla condizione del massimo, secondo cui ogni insieme non vuoto di sottomoduli contiene elementi massimali nell'insieme, e alla «condizione della base finita», secondo cui ogni sottomodulo ammette un insieme finito di generatori (p. 103,

esercizio 1). Ricordiamo inoltre che un anello (commutativo) è noetheriano se è noetheriano come modulo su sé stesso. Ciò significa che ogni catena strettamente ascendente di ideali dell'anello è finita, che ogni insieme non vuoto di ideali contiene elementi massimali e che ogni ideale ammette un insieme finito di generatori. Ognuna di queste condizioni implica le altre due. Nel 1890 Hilbert fondò la dimostrazione di un teorema fondamentale della teoria degli invarianti sul seguente risultato.

Teorema della base di Hilbert. *Se R è un campo oppure l'anello degli interi, ogni ideale dell'anello dei polinomi $R[x_1, x_2, \ldots, x_r]$, con le x_i indeterminate, ha un insieme finito di generatori.*

La dimostrazione di Hilbert consente l'immediata estensione seguente.

Teorema (generalizzato) della base di Hilbert. *Se R è un anello in cui ogni ideale è finitamente generato, ogni ideale di $R[x_1, \ldots, x_r]$ è finitamente generato.*

Dimostrazione. Per induzione è chiaro che basta dimostrare il teorema per una sola indeterminata x. Dobbiamo mostrare che un qualsiasi ideale B di $R[x]$ ha un insieme finito di generatori. Per $j = 0, 1, 2, \ldots$ sia $I_j = I_j(B)$ l'insieme degli elementi $b_j \in R$ per i quali esiste un elemento della forma

$$f_j = b_j x^j + a_{j-1}x^{j-1} + \cdots + a_0 \in B.$$

È evidente che I_j è un ideale di R e, poiché da $f_j \in B$ segue $xf_j = b_j x^{j+1} + \cdots \in B$, è chiaro che $I_j \subseteq I_{j+1}$. Dunque $I = \bigcup_j I_j$ è un ideale di R. Esso ha un insieme finito di generatori, che possiamo supporre contenuti in uno degli ideali I_m. Siano $b_m^{(1)}, \ldots, b_m^{(k)}$ tali generatori. Abbiamo polinomi $f_m^{(i)} = b_m^{(i)} x^m + g_m^{(i)} \in B$, dove $\deg g_m^{(i)} < m$. Analogamente, poiché ciascun I_j, $j < m$, è finitamente generato, abbiamo polinomi $f_j^{(i)} = b_j^{(i)} x^j + g_j^{(i)} \in B$ con $\deg g_j^{(i)} < j$, $1 \leq i \leq k_j$, corrispondenti a generatori di I_j. Affermiamo che l'insieme finito di polinomi

$$\{f_0^{(1)}, \ldots, f_0^{(k_0)}, f_1^{(1)}, \ldots, f_1^{(k_1)}, \ldots, f_m^{(1)}, \ldots, f_m^{(k)}\}$$

genera B. Sia $f \in B$. Dimostriamo per induzione su $n = \deg f$ che $f = \sum_{i,j} h_{ij} f_j^{(i)}$ per opportuni $h_{ij} \in R[x]$. Ciò è chiaro per $f = 0$ o $\deg f = 0$. Supponiamo quindi $f = b_n x^n + f_1$, con $b_n \neq 0$, $\deg f_1 < n$. Allora $b_n \in I_n \subseteq I$. Se $n \geq m$, si ha $b_n = \sum_i a_i b_m^{(i)}$, con $a_i \in R$, e $\sum_i a_i x^{n-m} f_m^{(i)} \in B$ ha lo stesso coefficiente direttivo di f. Quindi $\deg(f - \sum_i a_i x^{n-m} f_m^{(i)}) < n$. Poiché questo polinomio appartiene a B, il risultato segue per induzione. Se $n < m$, abbiamo $b_n = \sum_i a_i b_n^{(i)}$, con $a_i \in R$, e $\deg(f - \sum_i a_i f_n^{(i)}) < n$. Anche in questo caso si conclude per induzione. □

Una formulazione alternativa del teorema di Hilbert è che, se R è noetheriano, anche l'anello dei polinomi $R[x_1, \ldots, x_r]$ è noetheriano. Vale inoltre il seguente risultato più forte.

Corollario. *Sia R noetheriano e sia R' un anello estensione di R, finitamente generato come algebra su R. Allora R' è noetheriano.*

Dimostrazione. Per ipotesi $R' = R[u_1, \ldots, u_r]$ per opportuni $u_i \in R'$. Allora R' è un'immagine omomorfa di $R[x_1, \ldots, x_r]$, con x_i indeterminate. Poiché $R[x_1, \ldots, x_r]$ è noetheriano, anche R' lo è. □

Un'altra importante classe di esempi di anelli noetheriani è costituita dagli anelli di serie formali di potenze su anelli noetheriani. Per un anello arbitrario R possiamo definire l'anello

$R[[x]]$ delle *serie formali di potenze* su R come l'insieme delle successioni arbitrarie

$$a = (a_0, a_1, a_2, \ldots), \tag{19}$$

con $a_i \in R$, addizione per componenti, $0 = (0, 0, \ldots)$, $1 = (1, 0, 0, \ldots)$. Il prodotto ab, con a come sopra e $b = (b_0, b_1, \ldots)$, è $c = (c_0, c_1, \ldots)$, dove

$$c_i = \sum_{j+k=i} a_j b_k. \tag{20}$$

Si verifica facilmente che $R[[x]]$ è un anello (esercizio 7, p. 127 di *BAI*). È chiaro che R si identifica con il sottoanello degli elementi $(a_0, 0, 0, \ldots)$ di $R[[x]]$ e $R[x]$ con il sottoanello delle successioni $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$, cioè con un numero finito di termini non nulli (*BAI*, pp. 116–118).

Per le serie formali di potenze la nozione di *ordine* di una serie prende il posto del grado di un polinomio. Se $a = (a_0, a_1, \ldots)$, definiamo l'ordine $o(a)$ mediante

$$o(a) = \begin{cases} \infty & \text{se } a = 0, \\ k & \text{se } a_0 = \cdots = a_{k-1} = 0,\ a_k \neq 0. \end{cases} \tag{21}$$

Si ha allora

$$o(ab) \geq o(a) + o(b) \tag{22}$$

e

$$o(a + b) \geq \min(o(a), o(b)). \tag{23}$$

Se R è un dominio, nella (22) vale anzi l'uguaglianza $o(ab) = o(a) + o(b)$. In ogni caso, se poniamo

$$|a| = 2^{-o(a)} \tag{24}$$

(con la convenzione $2^{-\infty} = 0$), l'applicazione $a \mapsto |a|$ di $R[[x]]$ in $\mathbb{R}$ gode delle seguenti proprietà.

(i) $|a| \geq 0$, e $|a| = 0$ se e solo se $a = 0$.

(ii) $|a + b| \leq \max(|a|, |b|)$.

(iii) $|ab| \leq |a||b|$.

La seconda implica $|a+b| \leq |a|+|b|$. Dunque (i) e (ii) implicano che $R[[x]]$ è uno spazio metrico con distanza $d(a, b) = |a - b|$. Possiamo perciò introdurre le consuete nozioni di convergenza di successioni e serie, di successione di Cauchy e così via.

Diciamo che la successione $\{a^{(i)}\}$, con $a^{(i)} \in R[[x]]$, $i = 1, 2, 3, \ldots$, converge ad $a \in R[[x]]$ se per ogni reale $\varepsilon > 0$ esiste un intero $N = N(\varepsilon)$ tale che $|a - a^{(i)}| < \varepsilon$ per ogni $i \geq N$. Scriviamo allora $\lim a^{(i)} = a$. La successione $\{a^{(i)}\}$ si dice *di Cauchy* se per ogni $\varepsilon > 0$ esiste un intero N tale che $|a^{(i)} - a^{(j)}| < \varepsilon$ per ogni $i, j \geq N$. Lo spazio $R[[x]]$ è completo rispetto alla sua metrica, nel senso che ogni successione di Cauchy di elementi di $R[[x]]$ converge. Sia infatti $\{a^{(i)}\}$ una tale successione. Per ogni intero $n \geq 0$ esiste un N tale che $o(a^{(i)} - a^{(j)}) > n$ per ogni $i, j \geq N$. Sia a_n il termine che occupa il posto $n + 1$ in $a^{(N)}$. Allora ogni $a^{(i)}$, $i \geq N$, ha lo stesso termine al posto $n + 1$. È facile vedere che, posto $a = (a_0, a_1, a_2, \ldots)$, si ha $\lim a^{(i)} = a$.

Possiamo definire anche la convergenza delle serie nel modo consueto. Diciamo che $a^{(1)} + a^{(2)} + \cdots = a$ se la successione delle somme parziali $a^{(1)}, a^{(1)} + a^{(2)}, \ldots$ converge ad a.

Ponendo $x = (0, 1, 0, \ldots)$, la potenza x^i ha un 1 al posto $i+1$ e tutti gli altri termini nulli. Quindi, se $a = (a_0, a_1, a_2, \ldots)$ e identifichiamo a_j con $(a_j, 0, 0, \ldots)$, possiamo scrivere

$$(a_0, a_1, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots . \tag{25}$$

È chiaro che se R è un dominio anche $R[[x]]$ lo è. È pure facile determinare le unità di $R[[x]]$. Infatti $\sum_{i=0}^{\infty} a_i x^i$ è un'unità se e solo se a_0 è un'unità in R. La condizione è evidentemente necessaria. Per provarne la sufficienza scriviamo $\sum_i a_i x^i = a_0(1-z)$, con $z = \sum_{j=1}^{\infty} b_j x^j$ e $b_j = -a_0^{-1} a_j$. Allora $o(z) \geq 1$ e $o(z^k) \geq k$. Quindi esiste $1 + z + z^2 + \cdots$ e si vede subito che

$$(1-z)(1 + z + z^2 + \cdots) = 1. \tag{26}$$

Dunque $\sum_{i=0}^{\infty} a_i x^i = a_0(1-z)$ è un'unità con inverso $a_0^{-1}(\sum_{k=0}^{\infty} z^k)$. È anche chiaro che l'insieme delle serie $\sum_{i=0}^{\infty} a_i x^i$ di ordine > 0 è un ideale di $R[[x]]$. Una conseguenza immediata è la proposizione seguente.

Proposizione 7.23. *Se F è un campo, $F[[x]]$ è un anello locale.*

Dimostrazione. Gli elementi $\sum_{i=0}^{\infty} a_i x^i$ che non sono unità sono precisamente quelli con $a_0 = 0$. Essi formano un ideale. Poiché i non invertibili costituiscono un ideale, $F[[x]]$ è locale. □

È pure facile vedere che se R è locale anche $R[[x]]$ è locale. Lasciamo la dimostrazione al lettore. Dimostreremo ora il seguente importante teorema.

Teorema 7.11. *Se R è noetheriano, anche $R[[x]]$ è noetheriano.*

Dimostrazione. La dimostrazione è molto simile a quella del teorema della base di Hilbert. Sia B un ideale. Per ogni $j = 0, 1, 2, \ldots$, sia I_j l'insieme dei $b_j \in R$ per i quali esiste un elemento $f_j = b_j x^j + g_j \in B$ con $o(g_j) > j$. Allora I_j è un ideale di R e $I_0 \subseteq I_1 \subseteq \cdots$, sicché $I = \bigcup I_j$ è un ideale di R. Essendo R noetheriano, I ha un insieme finito di generatori, tutti contenuti in I_m per un opportuno m. Siano $b_m^{(1)}, \ldots, b_m^{(k)}$ tali generatori. Da (22) e (23) è chiaro che gli elementi di $R[[x]]$ di ordine $\geq m$ formano un ideale. L'intersezione con B è un ideale B_m di $R[[x]]$ che contiene gli elementi $f_m^{(i)}$, $1 \leq i \leq k$. Sia ora $f \in B_m$ e supponiamo $f = b_n x^n + g$ con $b_n \in R$, $n \geq m$ e $o(g) > n$. Allora $b_n = \sum_i a_i b_m^{(i)}$ per opportuni $a_i \in R$, e

$$o\left(f - \sum_i a_i x^{n-m} f_m^{(i)}\right) > n.$$

Iterando si ottiene una successione di interi $n_1 = n - m < n_2 < n_3 < \cdots$ ed elementi $a_{ij} \in R$, $1 \leq i \leq k$, $j = 1, 2, \ldots$, tali che

$$o\left(f - \sum_{i=1}^{k} \left(\sum_{j=1}^{r} a_{ij} x^{n_j}\right) f_m^{(i)}\right) > m + n_r, \qquad r = 1, 2, \ldots .$$

Allora $a_i = \sum_{j=1}^{\infty} a_{ij} x^{n_j}$ è ben definito e $f = \sum_{i=1}^{k} a_i f_m^{(i)}$. Consideriamo ora gli ideali I_j per $0 \leq j < m$. Scegliamo per I_j un insieme di generatori $b_j^{(1)}, \ldots, b_j^{(k_j)}$ e scegliamo $f_j^{(i)} = b_j^{(i)} x^j + p_j^{(i)} \in B$ con $o(p_j^{(i)}) > j$. Come nel caso dei polinomi, l'insieme

$$\{f_0^{(1)}, \ldots, f_0^{(k_0)}, \ldots, f_m^{(1)}, \ldots, f_m^{(k)}\}$$

genera B. □

Possiamo iterare la costruzione delle serie formali di potenze ottenendo $R[[x,y]] = (R[[x]])[[y]]$, ecc. Possiamo anche combinarla con quella delle estensioni polinomiali. Partendo da un anello R noetheriano e applicando queste costruzioni un numero finito di volte, si ottengono anelli noetheriani.

Un'altra costruzione che conserva la proprietà noetheriana è descritta nel teorema seguente.

Teorema 7.12. *Sia R noetheriano e sia S un sottomonoide del monoide moltiplicativo di R. La localizzazione R_S è noetheriana.*

Dimostrazione. Sia B' un ideale di R_S. Come a p. 401 sia $j(B')$ l'insieme degli elementi $b \in R$ tali che $b/s \in B'$ per qualche $s \in S$. Allora $j(B')$ è un ideale di R e $j(B')_S = B'$. Poiché R è noetheriano, $j(B')$ ha un insieme finito di generatori $\{b_1, \dots, b_m\}$. Allora $\{b_1/1, \dots, b_m/1\}$ è contenuto in B' e lo genera. □

Esercizi.

1. Mostrare che, se I è un ideale di un anello commutativo R tale che I non è finitamente generato mentre ogni ideale che lo contiene propriamente è finitamente generato, allora I è primo. Dedurne che, se ogni ideale primo di R è finitamente generato, R è noetheriano.

2. Se R è un anello, definiamo l'*anello delle serie formali di Laurent* $R((x))$ su R come l'insieme delle successioni (a_i), $-\infty < i < \infty$, $a_i \in R$, per le quali esiste un intero n (dipendente dalla successione) tale che $a_i = 0$ per $i < n$. Definire addizione e moltiplicazione come per le serie di potenze. Mostrare che $R((x))$ è una localizzazione di $R[[x]]$ e dunque è noetheriano se R è noetheriano. Mostrare che, se R è un campo, anche $R((x))$ è un campo e contiene il campo $R(x)$ delle espressioni razionali in x.

3. (*Teorema di finitezza di Emmy Noether sugli invarianti di un gruppo finito.*) Sia $E = F[u_1, \dots, u_m]$ un'algebra finitamente generata sul campo F e sia G un gruppo finito di automorfismi di E/F. Sia $\operatorname{Inv} G = \{y \in E \mid sy = y,\ s \in G\}$. Mostrare che $\operatorname{Inv} G$ è un'algebra finitamente generata su F. (*Traccia della dimostrazione.* Sia $f_i(x) = \prod_{s \in G}(x - su_i) = x^n - p_{i1}x^{n-1} + p_{i2}x^{n-2} - \cdots$, dove x è un'indeterminata. Allora $I = F[p_{11}, \dots, p_{mn}] \subseteq \operatorname{Inv} G$ ed E è intero su I. Per l'esercizio 1, p. 411, E è dunque un I-modulo finitamente generato. Poiché I è noetheriano, $\operatorname{Inv} G$ è finitamente generato come I-modulo, diciamo da $v_1, \dots, v_r$. Allora $\operatorname{Inv} G = F[p_{11}, \dots, p_{mn}, v_1, \dots, v_r]$.)

7.11 Anelli artiniani commutativi

Lo studio degli anelli artiniani costituisce una parte importante della teoria della struttura degli anelli sviluppata nel capitolo 4. È interessante vedere quale forma assuma la teoria nel caso commutativo e considerare i rapporti fra la condizione artiniana e quella noetheriana. Il primo risultato in questa direzione vale per anelli anche non commutativi.

Teorema 7.13. *Se R è un anello artiniano a sinistra (a destra), allora R è noetheriano a sinistra (a destra). Inoltre R ha soltanto un numero finito di ideali massimali.*

Dimostrazione. Sia $J = \operatorname{rad} R$ il radicale di Jacobson di R. Per il teorema 4.3 (p. 202), J è nilpotente, sicché esiste un intero n tale che $J^n = 0$. Consideriamo la successione di ideali $R \supseteq J \supseteq J^2 \supseteq \cdots \supseteq J^n = 0$. Consideriamo R come R-modulo sinistro. Abbiamo la successione degli R-moduli $\bar{M}_i = J^i/J^{i+1}$, dove $J^0 = R$. Essi sono tutti annullati da J e

possono quindi considerarsi moduli sull'anello artiniano semiprimitivo $\bar{R} = R/J$. Poiché tutti i moduli su un anello artiniano semiprimitivo sono completamente riducibili (teorema 4.4, p. 208), tali sono i moduli $\bar{M}_i$. Inoltre ogni modulo completamente riducibile artiniano (noetheriano) è noetheriano (artiniano) e ammette dunque una serie di composizione. Per ogni $\bar{M}_i$ si ha quindi una successione di sottomoduli

$$\bar{M}_i = \bar{M}_{i1} \supset \bar{M}_{i2} \supset \cdots \supset \bar{M}_{in_i} \supset \bar{M}_{i,n_i+1} = 0$$

tale che ciascun $\bar{M}_{ij}/\bar{M}_{i,j+1}$ è irriducibile. Questi quozienti possono considerarsi R-moduli. Ad essi corrisponde una successione di ideali sinistri $M_{i1} = J^i \supset M_{i2} \supset \cdots \supset M_{i,n_i+1} = J^{i+1}$ tale che $M_{ij}/M_{i,j+1}$ è un R-modulo irriducibile. Riunendo queste successioni otteniamo una serie di composizione di R come R-modulo sinistro. L'esistenza di tale serie implica che R è tanto noetheriano a sinistra quanto artiniano a sinistra. Lo stesso ragionamento si applica agli anelli artiniani a destra. Ciò prova la prima parte.

Per la seconda osserviamo che ogni ideale massimale I di R contiene J e che $\bar{I} = I/J$ è un ideale massimale dell'anello artiniano semiprimitivo $\bar{R}$. Abbiamo $\bar{R} = \bar{R}_1 \oplus \cdots \oplus \bar{R}_s$, dove gli $\bar{R}_i$ sono ideali minimali. Ne segue che i soli ideali massimali di $\bar{R}$ sono gli ideali $\bar{M}_j = \bar{R}_1 + \cdots + \bar{R}_{j-1} + \bar{R}_{j+1} + \cdots + \bar{R}_s$, e che i soli ideali massimali di R sono le loro controimmagini M_j, cioè le somme $R_1 + \cdots + R_{j-1} + R_{j+1} + \cdots + R_s$ modulo il nucleo J, dove R_j è l'ideale di R tale che $\bar{R}_j = R_j/J$. □

Per gli anelli commutativi vale il seguente inverso parziale del teorema 7.13.

Teorema 7.14. *Se R è un anello commutativo noetheriano con un numero finito di ideali primi, tutti massimali, allora R è artiniano.*

Dimostrazione. Il radicale di Jacobson J è l'intersezione degli ideali massimali di R, e il nilradicale N è l'intersezione degli ideali primi di R. L'ipotesi che tutti gli ideali primi siano massimali implica dunque $J = N$. Pertanto J è un ideale nil e, poiché R è noetheriano, è finitamente generato. Come si vede facilmente, ciò implica che J è nilpotente. Poiché R contiene soltanto un numero finito di ideali massimali, $\bar{R} = R/J$ è un prodotto sottodiretto di un numero finito di campi. Allora $\bar{R}$ è somma diretta di un numero finito di campi (lemma a p. 202) ed è dunque artiniano. Come nella dimostrazione precedente, si ha la catena di ideali $R \supseteq J \supseteq \cdots \supseteq J^{n-1} \supseteq J^n = 0$, e ciascun J^i/J^{i+1} è un modulo noetheriano completamente riducibile sull'anello artiniano semiprimitivo $\bar{R}$. Allora J^i/J^{i+1} ha una serie di composizione e R ha una serie di composizione come R-modulo. Dunque R è artiniano. □

È facile determinare la struttura degli anelli artiniani commutativi. La descrive il teorema seguente.

Teorema 7.15. *Sia R un anello artiniano commutativo. Allora R si scrive in uno e un solo modo come somma diretta $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$, dove gli R_i sono anelli locali artiniani e noetheriani, e quindi l'ideale massimale di R_i è nilpotente. Viceversa, se $R = R_1 \oplus \cdots \oplus R_s$, dove gli R_i sono anelli locali noetheriani con ideali massimali nilpotenti, allora R è artiniano.*

Dimostrazione. Basiamo la prima parte sui risultati relativi ai moduli ottenuti a proposito del teorema di Krull–Schmidt (pp. 110–115) e sul fatto che per un anello commutativo R si ha l'isomorfismo $R \cong \operatorname{End}_R R$. Abbiamo visto che R ha una serie di composizione come R-modulo. Quindi $R = R_1 \oplus \cdots \oplus R_s$, dove gli R_i sono R-moduli indecomponibili con serie di composizione. Ne segue che $\operatorname{End}_R R_i$ è un anello locale. Ora $R_i \cong \operatorname{End}_{R_i} R_i = \operatorname{End}_R R_i$, sicché R_i è un anello locale. Un anello ammette una sola decomposizione in ideali indecomponibili (p. 204), dunque gli R_i sono unici. La proprietà artiniana di R si trasmette agli R_i. Per il teorema 7.13 ciascun R_i è quindi anche noetheriano. È chiaro inoltre che l'ideale massimale $\operatorname{rad} R_i$ di R_i è nilpotente.

Per il viceversa supponiamo dapprima che R sia un anello locale commutativo il cui ideale massimale J è nilpotente. Sia P un ideale primo di R. Allora $P \subseteq J$ e $J^n \subseteq P$ per qualche n. Poiché P è primo, ne segue $J = P$. Dunque P è il solo ideale primo di R. Essendo R noetheriano, per il teorema 7.14 è artiniano. Il caso generale $R = R_1 \oplus \cdots \oplus R_s$ segue immediatamente da questo caso particolare. □

Se R è un anello artiniano e M è un R-modulo finitamente generato, M ammette una serie di composizione, poiché R è anche noetheriano e quindi M è artiniano e noetheriano. Possiamo pertanto definire la *lunghezza* $l(M)$ di M come la lunghezza di una qualsiasi serie di composizione di M. La lunghezza è spesso uno strumento utile per dimostrare risultati sui moduli sopra anelli artiniani.

7.12 Varietà algebriche affini. Il Nullstellensatz di Hilbert

Sia F un campo algebricamente chiuso, sia $F^{(n)}$ lo spazio vettoriale di dimensione n delle n-uple $(a_1, a_2, \ldots, a_n)$, $a_i \in F$, e sia $F[x_1, x_2, \ldots, x_n]$ l'anello dei polinomi in n indeterminate x_i su F. Se S è un sottoinsieme di $F[x_1, \ldots, x_n]$, indichiamo con $V(S)$ l'insieme dei punti $(a_1, \ldots, a_n) \in F^{(n)}$ tali che $f(a_1, \ldots, a_n) = 0$ per ogni $f \in S$, e chiamiamo $V(S)$ la *varietà (algebrica affine)* definita da S. È chiaro che $V(S) = V(I)$, dove $I = (S)$ è l'ideale generato da S, e anche che $V(I) = V(\operatorname{nilrad} I)$. Pertanto, se I_1 e I_2 sono due ideali tali che $\operatorname{nilrad} I_1 = \operatorname{nilrad} I_2$, allora $V(I_1) = V(I_2)$. Un risultato fondamentale, dovuto a Hilbert, è che, viceversa, se $V(I_1) = V(I_2)$ per due ideali di $F[x_1, \ldots, x_n]$, con F algebricamente chiuso, allora $\operatorname{nilrad} I_1 = \operatorname{nilrad} I_2$. Vi sono diversi modi di dimostrare questo risultato. In questo paragrafo daremo una dimostrazione molto naturale, dovuta a Seidenberg, basata sul teorema di Krull secondo cui il nilradicale di un ideale è l'intersezione degli ideali primi che lo contengono, e su un teorema generale della teoria dell'eliminazione che abbiamo dimostrato in modo del tutto elementare in *BA I*, pp. 322–325. Per comodità riportiamo il teorema sull'eliminazione delle incognite.

Sia $K = \mathbb{Z}$ oppure $\mathbb{Z}/(p)$, con p primo, e siano $A = K[t_1, \ldots, t_r]$, $B = A[x_1, \ldots, x_n]$, dove le t e le x sono indeterminate. Siano $F_1, \ldots, F_m, G \in B$. Allora si può determinare, in un numero finito di passi, una famiglia finita $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_s\}$, dove ogni $\Gamma_j = \{f_{j1}, \ldots, f_{jm_j}; g_j\}$ è costituito da elementi di A, tale che, per ogni campo F che estenda K e per ogni $(c_1, \ldots, c_r)$, $c_i \in F$, il sistema di equazioni e di una disuguaglianza

$$\begin{gathered} F_1(c_1, \ldots, c_r; x_1, \ldots, x_n) = \cdots = F_m(c_1, \ldots, c_r; x_1, \ldots, x_n) = 0, \\ G(c_1, \ldots, c_r; x_1, \ldots, x_n) \neq 0 \end{gathered} \tag{27}$$

ammette una soluzione nelle x in qualche estensione E di F se e solo se i c_i soddisfano uno dei sistemi Γ_j:

$$f_{j1}(c_1, \ldots, c_r) = \cdots = f_{jm_j}(c_1, \ldots, c_r) = 0, \qquad g_j(c_1, \ldots, c_r) \neq 0. \tag{28}$$

Inoltre, se le condizioni sono soddisfatte, esiste una soluzione della (27) in una qualche estensione algebrica E di F.

Per i nostri scopi, la parte importante di questo risultato è l'ultima affermazione. Essa implica il seguente teorema, che esprime forse il vero significato della proprietà di un campo di essere algebricamente chiuso.

Teorema 7.16. *Siano F un campo algebricamente chiuso e $f_1, \ldots, f_m, g \in F[x_1, \ldots, x_n]$, dove le x_i sono indeterminate. Supponiamo che il sistema di equazioni e di una disuguaglianza*

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0, \quad g(x_1, \ldots, x_n) \neq 0 \tag{29}$$

abbia una soluzione in qualche estensione E di F. Allora la (29) ha una soluzione in F.

Dimostrazione. L'anello primo del campo F è uno degli anelli $K = \mathbb{Z}$ o $\mathbb{Z}/(p)$. Scegliendo un numero sufficiente di indeterminate ausiliarie $t_1, \ldots, t_r$, possiamo definire polinomi $F_1, \ldots, F_m, G \in B$, come nel teorema di eliminazione, tali che

$$F_i(c_1, \ldots, c_r; x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n),$$
$$G(c_1, \ldots, c_r; x_1, \ldots, x_n) = g(x_1, \ldots, x_n).$$

Dal risultato citato segue che, se la (29) ha una soluzione in qualche estensione E di F, esiste un j per il quale vale la (28). A sua volta ciò implica che la (29) ha una soluzione in un'estensione algebrica di F. Poiché F è algebricamente chiuso, l'unica estensione algebrica di F è F stesso (*BA I*, p. 216, oppure p. 460 di questo volume). Quindi la (29) è risolubile in F. □

Il teorema di Hilbert, detto *Nullstellensatz*, è una conseguenza immediata di questo risultato e della caratterizzazione del nilradicale come intersezione di ideali primi.

Nullstellensatz. *Sia I un ideale dell'anello dei polinomi $F[x_1, \ldots, x_n]$ in n indeterminate x_i su un campo algebricamente chiuso F, e sia $g \in F[x_1, \ldots, x_n]$. Supponiamo $g(a_1, \ldots, a_n) = 0$ per tutti i punti $(a_1, \ldots, a_n)$ della varietà $V(I)$ definita da I. Allora $g \in \operatorname{nilrad} I$.*

Dimostrazione. Supponiamo $g \notin \operatorname{nilrad} I$. Esiste allora un ideale primo $P \supseteq I$ tale che $g \notin P$. Consideriamo il dominio $D = F[x_1, \ldots, x_n]/P = F[\bar{x}_1, \ldots, \bar{x}_n]$, dove $\bar{x}_i = x_i + P$. Per $f = f(x_1, \ldots, x_n) \in I$, si ha $f \in P$ e quindi $f(\bar{x}_1, \ldots, \bar{x}_n) = 0$. D'altra parte $g \notin P$, perciò $g(\bar{x}_1, \ldots, \bar{x}_n) \neq 0$. Ora $F[x_1, \ldots, x_n]$ è noetheriano, sicché I ha un sistema finito di generatori $f_1, \ldots, f_m$. Sia E il campo delle frazioni di D. Allora E è un'estensione di F che contiene gli elementi $\bar{x}_1, \ldots, \bar{x}_n$ tali che $f_i(\bar{x}_1, \ldots, \bar{x}_n) = 0$, $1 \leq i \leq m$, e $g(\bar{x}_1, \ldots, \bar{x}_n) \neq 0$. Per il teorema 7.16 esistono pertanto $a_1, \ldots, a_n \in F$ tali che $f_i(a_1, \ldots, a_n) = 0$ e $g(a_1, \ldots, a_n) \neq 0$. Poiché gli f_i generano I, si ha $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$. Ciò contraddice l'ipotesi e prova che $g \in \operatorname{nilrad} I$. □

Evidentemente il Nullstellensatz implica che, se I_1 e I_2 sono ideali di $F[x_1, \ldots, x_n]$ tali che $V(I_1) = V(I_2)$, allora $I_1 \subseteq \operatorname{nilrad} I_2$, e quindi $\operatorname{nilrad} I_1 \subseteq \operatorname{nilrad}(\operatorname{nilrad} I_2) = \operatorname{nilrad} I_2$. Per simmetria, $\operatorname{nilrad} I_2 \subseteq \operatorname{nilrad} I_1$, sicché $\operatorname{nilrad} I_1 = \operatorname{nilrad} I_2$. Un importante caso particolare del Nullstellensatz è il

Teorema 7.17. *Se I è un ideale proprio di $F[x_1, \ldots, x_n]$, con F algebricamente chiuso, allora $V(I) \neq \varnothing$.*

Dimostrazione. Se $V(I) = \varnothing$, allora $g = 1$ soddisfa la condizione del Nullstellensatz, sicché $1 \in \operatorname{nilrad} I$, e quindi $1 \in I$, contro l'ipotesi che I sia proprio. □

Il Nullstellensatz ci permette anche di determinare gli ideali massimali di $F[x_1, \ldots, x_n]$. Se $(a_1, \ldots, a_n) \in F^{(n)}$, l'ideale $M_{a_1,\ldots,a_n} = (x_1 - a_1, \ldots, x_n - a_n)$ è massimale in $F[x_1, \ldots, x_n]$, poiché $F[x_1, \ldots, x_n]/M_{a_1,\ldots,a_n} \simeq F$. Evidentemente $V(M_{a_1,\ldots,a_n})$ consta del solo punto $(a_1, \ldots, a_n)$. Se I è un qualunque ideale proprio, il risultato precedente e il Nullstellensatz implicano che $I \subseteq \operatorname{nilrad} M_{a_1,\ldots,a_n}$ per qualche punto $(a_1, \ldots, a_n)$. Poiché $M_{a_1,\ldots,a_n}$ è massimale, esso coincide con il proprio nilradicale, e dunque $I \subseteq M_{a_1,\ldots,a_n}$. Vediamo quindi che gli unici ideali massimali di $F[x_1, \ldots, x_n]$ sono quelli della forma $M_{a_1,\ldots,a_n}$. Inoltre, poiché $V(M_{a_1,\ldots,a_n}) = \{(a_1, \ldots, a_n)\}$, si ottiene il seguente risultato.

Corollario. *Se F è un campo algebricamente chiuso, l'applicazione $(a_1, \ldots, a_n) \mapsto M_{a_1,\ldots,a_n} = (x_1 - a_1, \ldots, x_n - a_n)$ è una biiezione di $F^{(n)}$ sull'insieme degli ideali massimali di $F[x_1, \ldots, x_n]$.*

Supponiamo ora che F sia un qualsiasi campo infinito. Consideriamo di nuovo $F^{(n)}$ e $F[x_1, \ldots, x_n]$ e definiamo, per un sottoinsieme S di $F[x_1, \ldots, x_n]$, la varietà $V(S)$ come nel caso

algebricamente chiuso. Se inoltre V_1 è una varietà, indichiamo con $i(V_1)$ l'ideale dei polinomi $f \in F[x_1, \ldots, x_n]$ che si annullano in ogni $(a_1, \ldots, a_n) \in V_1$. Le seguenti proprietà risultano direttamente dalla definizione:

1. $V(F[x_1, \ldots, x_n]) = \varnothing$;
2. $V(\varnothing) = F^{(n)}$;
3. $V(\bigcup S_\alpha) = \bigcap V(S_\alpha)$;
4. $V(S) = V(I)$ se $I = (S)$ è l'ideale generato da S;
5. $V(I_1 I_2) = V(I_1) \cup V(I_2)$ per due ideali qualsiasi I_1, I_2;
6. $V(S_1) \supseteq V(S_2)$ se $S_1 \subseteq S_2$;
7. $i(\varnothing) = F[x_1, \ldots, x_n]$;
8. $i(V_1) \supseteq i(V_2)$ se $V_1 \subseteq V_2$;
9. $i(V(I_1)) \supseteq I_1$ per ogni ideale I_1;
10. $V(i(V_1)) \supseteq V_1$ per ogni varietà V_1.

Dalle relazioni (6), (8), (9) e (10) discendono immediatamente le seguenti:

11. $V(i(V(I_1))) = V(I_1)$;
12. $i(V(i(V_1))) = i(V_1)$.

Richiamiamo ora un importante teorema dimostrato in *BA I*, p. 136: se F è un campo infinito e $f(x_1, \ldots, x_n)$ è un polinomio non nullo a coefficienti in F, esistono $a_i \in F$ tali che $f(a_1, \ldots, a_n) \neq 0$. Evidentemente ciò implica

13. $i(F^{(n)}) = 0$.

Le relazioni (1)–(5) mostrano che le varietà soddisfano gli assiomi per i chiusi di uno spazio topologico. La topologia risultante si chiama *topologia di Zariski* dello spazio $F^{(n)}$. Gli aperti in questa topologia sono gli insiemi $F^{(n)} - V$, con V una varietà. Se $V = V(S)$, allora $F^{(n)} - V = \bigcup_{f \in S}(F^{(n)} - V(\{f\}))$. Pertanto gli aperti $O_f = F^{(n)} - V(\{f\})$ formano una base per gli aperti di $F^{(n)}$. Evidentemente O_f è l'insieme dei punti $(a_1, \ldots, a_n)$ tali che $f(a_1, \ldots, a_n) \neq 0$.

Osserviamo che, se F è algebricamente chiuso (quindi infinito), $F^{(n)}$ con la sua topologia di Zariski si identifica con lo spettro massimale dell'anello $F[x_1, \ldots, x_n]$. Più precisamente, fra questi due spazi vi è un omeomorfismo canonico. Si tratta dell'applicazione $(a_1, \ldots, a_n) \mapsto M_{a_1, \ldots, a_n}$ data nel corollario precedente. Poiché la condizione $f(a_1, \ldots, a_n) = 0$ per un polinomio $f(x_1, \ldots, x_n)$ equivale a $f \in M_{a_1, \ldots, a_n}$, l'applicazione definita induce una biiezione fra l'insieme dei chiusi di $F^{(n)}$ e l'insieme dei chiusi di Maxspec (si veda p. 403). Abbiamo dunque un omeomorfismo.

Quando $F = \mathbb{R}$ o $\mathbb{C}$, la topologia di Zariski su $F^{(n)}$ ha proprietà assai diverse da quelle della consueta topologia euclidea. Consideriamo alcune di queste proprietà per $F^{(n)}$, con F un qualsiasi campo infinito. Poiché ogni punto $(a_1, \ldots, a_n)$ è la varietà definita dall'ideale $M_{a_1, \ldots, a_n} = (x_1 - a_1, \ldots, x_n - a_n)$, è chiaro che $F^{(n)}$ è uno spazio T_1. Esso, tuttavia, non è uno spazio di Hausdorff. Al contrario, $F^{(n)}$ è *irriducibile*, nel senso che due aperti non vuoti qualsiasi

di $F^{(n)}$ si intersecano. In altre parole, ogni aperto non vuoto è denso in $F^{(n)}$. Poiché gli insiemi O_f costituiscono una base, basta vedere che, se $O_f \neq \varnothing$ e $O_g \neq \varnothing$, allora $O_f \cap O_g \neq \varnothing$. Il teorema sul non annullamento dei polinomi implica che $O_f \neq \varnothing$ se e solo se $f \neq 0$. È chiaro inoltre che $O_f \cap O_g = O_{fg}$. Poiché $F[x_1, \dots, x_n]$ è un dominio, da $O_f \neq \varnothing$, $O_g \neq \varnothing$ segue $O_f \cap O_g \neq \varnothing$.

Osserviamo poi che lo spazio $F^{(n)}$ con la topologia di Zariski è *noetheriano*, nel senso che vale la condizione della catena ascendente per gli aperti di $F^{(n)}$. Equivalentemente vale la condizione della catena discendente per le varietà. Sia $V_1 \supseteq V_2 \supseteq \cdots$ una catena discendente di varietà. Si ha allora la catena ascendente di ideali $i(V_1) \subseteq i(V_2) \subseteq \cdots$, perciò esiste m tale che $i(V_j) = i(V_{j+1})$ per ogni $j \geq m$. Poiché $V_j = V(i(V_j))$, si ha $V_j = V_{j+1}$ per $j \geq m$.

Consideriamo ora il caso più semplice, $n = 1$. La varietà $V(\{f\})$ definita da un solo polinomio f è un insieme finito se $f \neq 0$ ed è l'intero spazio F se $f = 0$. Inoltre, assegnato un qualsiasi insieme finito $\{a_i \mid 1 \leq i \leq r\}$, si ha $V(\{f\}) = \{a_i\}$ per $f = \prod_i (x - a_i)$. Ne segue che i chiusi nella topologia di Zariski sono i sottoinsiemi finiti (compreso l'insieme vuoto) e lo spazio intero. Gli aperti di F sono l'insieme vuoto e i complementari degli insiemi finiti. I complementari dei singoli punti costituiscono una sottobase per gli aperti, dato che ogni aperto non vuoto è un'intersezione finita di tali insiemi.

Si osservi che la topologia di Zariski fornisce più aperti della topologia prodotto ottenuta considerando $F^{(n)}$ come prodotto di n copie di F. Per esempio, l'aperto di $F^{(n)}$ definito da $x_1 + \cdots + x_n \neq 0$ non si può ottenere come unione di aperti della forma $O_1 \times O_2 \times \cdots \times O_n$, con O_i aperto in F.

Ogni polinomio $f(x_1, \dots, x_n)$ definisce una *funzione polinomiale*

$$(a_1, \dots, a_n) \longmapsto f(a_1, \dots, a_n) \tag{30}$$

da $F^{(n)}$ in F. Abbiamo considerato tali funzioni in *BA I*, pp. 134–138. Il teorema citato sul non annullamento dei polinomi mostra che l'applicazione che manda il polinomio $f(x_1, \dots, x_n)$ nella funzione definita dalla (30) è un isomorfismo di $F[x_1, \dots, x_n]$ sull'anello delle funzioni polinomiali. Più in generale, consideriamo un secondo spazio $F^{(m)}$. Una successione $(f_1, \dots, f_m)$, con $f_i = f_i(x_1, \dots, x_n)$, definisce allora un'*applicazione polinomiale*

$$(a_1, \dots, a_n) \longmapsto (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) \tag{31}$$

da $F^{(n)}$ in $F^{(m)}$. Tali applicazioni sono continue da $F^{(n)}$ in $F^{(m)}$, entrambi muniti della topologia di Zariski. Per vederlo prendiamo un intorno qualunque della forma O_g di $(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$. Abbiamo allora un polinomio $g(x_1, \dots, x_m)$ tale che $g(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) \neq 0$. Il polinomio

$$h(x_1, \dots, x_n) = g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

è dunque diverso da zero in $F[x_1, \dots, x_n]$, e la (31) manda O_h in O_g. Dunque la (31) è continua. Osserviamo che, poiché gli aperti non vuoti sono densi, per dimostrare che un'applicazione polinomiale è nulla (ossia manda ogni elemento in 0) basta mostrarlo su un aperto non vuoto.

Queste nozioni rudimentali di geometria algebrica sono spesso utili in situazioni «puramente algebriche». Negli esercizi seguenti daremo alcuni esempi dell'uso della topologia di Zariski.

Esercizi. In tutti gli esercizi supponiamo F algebricamente chiuso (e quindi infinito). Le topologie sono quelle di Zariski.

1. Sia $a \in M_n(F)$ e sia $f_a(\lambda) = \lambda^n - \operatorname{tr}(a)\lambda^{n-1} + \cdots + (-1)^n \det a$ il polinomio caratteristico di a. Mostrare che le applicazioni $a \mapsto \operatorname{tr} a, \dots, a \mapsto \det a$ sono funzioni polinomiali sullo

spazio vettoriale di dimensione n^2. Mostrare che l'insieme delle matrici invertibili è un aperto di $M_n(F)$.

2. Siano $\{\rho_1, \ldots, \rho_n\}$ le radici caratteristiche di a (in un certo ordine) e sia $g(x_1, \ldots, x_n)$ un polinomio simmetrico nelle x_i a coefficienti in F. Mostrare che l'applicazione $a \mapsto g(\rho_1, \ldots, \rho_n)$ è una funzione polinomiale su $M_n(F)$. Mostrare che l'insieme delle matrici simili a matrici diagonali con elementi diagonali distinti è un aperto di $M_n(F)$.

3. Siano $f, g \in F[x_1, \ldots, x_n]$, e supponiamo $g(a_1, \ldots, a_n) = 0$ per ogni $(a_1, \ldots, a_n)$ tale che $f(a_1, \ldots, a_n) = 0$. Mostrare che ogni fattore primo di f è un fattore di g.

4. Per $a \in M_n(F)$, sia U_a la trasformazione lineare $y \mapsto aya$ di $M_n(F)$ in sé. Sia $d(a) = \det U_a$. Usare il Nullstellensatz di Hilbert e il teorema 7.2 di *BA I*, p. 418, per dimostrare che $d(a) = (\det a)^{2n}$.

5. Dare un'altra dimostrazione del risultato dell'esercizio 4, osservando che basta provare la relazione per a nell'aperto delle matrici simili a matrici diagonali con elementi diagonali non nulli. Calcolare $d(a)$ e $\det a$ per una matrice diagonale.

6. Mostrare che il nilradicale di ogni ideale di $F[x_1, \ldots, x_n]$ è l'intersezione degli ideali massimali che lo contengono.

7. Sia V una varietà in $F^{(n)}$. Si definisce *funzione polinomiale* su V un'applicazione $p|_V$, dove p è una funzione polinomiale su $F^{(n)}$. Queste funzioni formano, rispetto alle consuete operazioni sulle funzioni, un'algebra $A(V)$ su F. Mostrare che $A(V) \simeq F[x_1, \ldots, x_n]/i(V) = F[\bar{x}_1, \ldots, \bar{x}_n]$, con $\bar{x}_i = x_i + i(V)$. Quest'ultima algebra su F si chiama *algebra delle coordinate* della varietà V. Si dice che V è *irriducibile* se $i(V)$ è primo. In tal caso gli elementi del campo delle frazioni dell'algebra delle coordinate si chiamano *funzioni razionali* su V. Se V' è una varietà in $F^{(m)}$, un'applicazione di V in V' si dice *regolare* se ha la forma $g|_V$, dove g è un'applicazione polinomiale da $F^{(n)}$ in $F^{(m)}$. Mostrare che, se p' è una funzione polinomiale su V', allora $p'g$ è una funzione polinomiale su V e che l'applicazione $\eta(g)\colon p' \mapsto p'g$ è un omomorfismo di algebre da $A(V')$ in $A(V)$. Mostrare che $g \mapsto \eta(g)$ è una biiezione fra l'insieme delle applicazioni regolari da V in V' e l'insieme degli omomorfismi di algebre da $A(V')$ in $A(V)$.

7.13 Decomposizioni primarie

In questo paragrafo consideriamo i classici teoremi di decomposizione di Lasker e Noether, che esprimono gli ideali degli anelli noetheriani come intersezioni finite di ideali primari. Usando la condizione della catena ascendente è facile vedere che ogni ideale proprio I di un anello noetheriano R si può scrivere come intersezione di ideali indecomponibili, nel senso che un ideale I è indecomponibile se $I \neq I_1 \cap I_2$ per ogni coppia di ideali $I_j \neq I$. Inoltre in ogni anello noetheriano gli ideali indecomponibili sono primari, in un senso che definiremo tra poco. Questo tipo di decomposizione è un debole analogo della decomposizione di un elemento in prodotto di potenze di primi. A ogni ideale primario è associato un ideale primo univocamente determinato. Tuttavia gli ideali primari non sono necessariamente potenze di primi e non ogni potenza di un primo è primaria. Benché la decomposizione in ideali primari non sia in generale unica, essa gode di importanti proprietà di unicità. Tali proprietà, insieme all'esistenza della decomposizione primaria, sono i risultati principali della teoria di Lasker e Noether. Cominceremo dalle questioni di unicità, poiché queste non coinvolgono la proprietà noetheriana. I risultati classici si possono generalizzare ai moduli e il passaggio ai moduli rende le argomentazioni un po' più trasparenti.

Nella nostra trattazione considereremo dapprima il caso generale dei moduli e lo specializzeremo poi per ottenere i risultati sugli ideali.

Se M è un modulo per R e $a \in R$, indichiamo con a_M, come nel ğ 3.1, l'applicazione $x \mapsto ax$, $x \in M$. Poiché R è commutativo, questo è un endomorfismo di M come R-modulo. Abbiamo l'omomorfismo $\rho_M \colon a \mapsto a_M$ da R nell'anello degli endomorfismi di M, e $\ker \rho_M$ è l'insieme degli $a \in R$ tali che $ax = 0$ per ogni x. Come di consueto, scriviamo $\operatorname{ann}_R x$ per l'ideale degli elementi $b \in R$ tali che $bx = 0$. Evidentemente $\ker \rho_M = \bigcap_{x \in M} \operatorname{ann}_R x = \operatorname{ann}_R M$. Se $ax = 0$ per qualche $x \neq 0$, chiameremo l'elemento a dell'anello R un *divisore dello zero del modulo* M. Gli elementi a che non sono divisori dello zero sono quelli per cui a_M è iniettivo. Consideriamo ora il nilradicale degli ideali $\ker \rho_M$ e $\operatorname{ann}_R x$ per un dato x. Per definizione, il primo è l'insieme degli $a \in R$ per i quali esiste un intero m tale che $a^m \in \ker \rho_M$, cioè $a^m x = 0$ per ogni x o, equivalentemente, $a_M^m = (a^m)_M = 0$. Analogamente $a \in \operatorname{nilrad}(\operatorname{ann}_R x)$ se e solo se esiste m tale che $a^m x = 0$ o, equivalentemente, se la restrizione di a_M al sottomodulo Rx è nilpotente.

Il caso di maggiore interesse è quello in cui $M = R/I$ con I ideale di R. Poiché dovremo considerare contemporaneamente tale modulo e i moduli R/I' per ideali I' di R contenenti I, e poiché $R/I' = (R/I)/(I'/I)$, dobbiamo formulare le definizioni e i risultati in termini di un modulo e di un suo sottomodulo. La definizione seguente mostra come procederemo.

Definizione 7.4. Un sottomodulo Q di un R-modulo M si dice *primario* se $Q \neq M$ e, per ogni $a \in R$, $a_{M/Q}$ è iniettivo oppure nilpotente.

Ciò significa evidentemente che, se a è un divisore dello zero di M/Q, esiste un intero m tale che $a^m x \in Q$ per ogni $x \in M$. L'insieme P degli elementi che soddisfano quest'ultima condizione è l'ideale $\operatorname{nilrad}(\operatorname{ann}_R(M/Q))$. Questo ideale è primo, poiché se $a \notin P$ e $b \notin P$, allora $a_{M/Q}$ e $b_{M/Q}$ sono iniettivi. Ne segue che $(ab)_{M/Q} = a_{M/Q} b_{M/Q}$ è iniettivo, e dunque $ab \notin P$. Chiameremo P l'*ideale primo associato* al sottomodulo primario Q. Se $M = R$, i sottomoduli sono gli ideali. Allora la condizione $a^m x \in Q$ per ogni $x \in R$ equivale a $a^m \in Q$. In questo caso, dunque, un ideale proprio Q è primario se e solo se da $ab \in Q$ e $b \notin Q$ segue che esiste m tale che $a^m \in Q$. Il primo associato a Q è il nilradicale di questo ideale.

Esempi.

1. Sia R un dominio a ideali principali e sia $Q = (p^e) = (p)^e$, con p primo. È facile vedere che se $a \in R$ e $a \notin P = (p)$, allora $a_{R/Q}$ è invertibile, dunque iniettivo. D'altra parte, se $a \in P$, allora $a_{R/Q}^e = 0$. Quindi Q è primario e P è l'ideale primo associato. È anche facile vedere che 0 e gli ideali (p^e) sono i soli ideali primari di R.

2. Sia $R = \mathbb{Z}$ e sia M un gruppo abeliano finito, scritto additivamente e considerato nel modo consueto come $\mathbb{Z}$-modulo. Supponiamo che ogni elemento di M abbia ordine una potenza di un primo p. Allora 0 è un sottomodulo p-primario di M, poiché, se $a \in \mathbb{Z}$ e $(a, p) = 1$, a_M è iniettivo, mentre, se a è divisibile per p, a_M è nilpotente. L'ideale primo associato a 0 è (p).

3. Sia $R = F[x, y, z]/(xy - z^2)$, dove F è un campo e x, y, z sono indeterminate. Per $a \in F[x, y, z]$, sia $\bar{a}$ la sua immagine in R mediante l'omomorfismo canonico. Sia $P = (\bar{x}, \bar{z})$ l'ideale di R generato da $\bar{x}, \bar{z}$. L'ideale corrispondente in $F[x, y, z]$ è (x, z), poiché esso contiene $xy - z^2$. Dato che $F[x, y, z]/(x, z) \simeq F[y]$, ne segue che P è primo in R. Poiché dal teorema di Krull risulta chiaro che il nilradicale di ogni potenza di un ideale primo è l'ideale primo stesso, l'ideale P^2 di R ha P come nilradicale. Esso tuttavia non è primario, poiché $\bar{x} \notin P^2$, $\bar{y} \notin P$, ma $\bar{x}\bar{y} = \bar{z}^2 \in P^2$.

Possiamo ottenere molti esempi di ideali primari utilizzando la seguente proposizione.

Proposizione 7.24. *Se P è un ideale massimale di R, ogni ideale Q compreso fra P e P^e, $e \geq 1$, è primario e ha P come ideale primo associato.*

Dimostrazione. Se $a \in P$, allora $a^e \in P^e \subseteq Q$. Se $a \notin P$, affermiamo che $a + Q$ è un'unità in R/Q. Infatti, poiché P è massimale, R/P è un campo. Abbiamo dunque un elemento $a' \in R$ e uno $z \in P$ tali che $aa' = 1 - z$. Poiché $z + Q$ è nilpotente in R/Q, $(1 - z) + Q$ è un'unità in R/Q, e quindi $a + Q$ è un'unità in R/Q. È ora chiaro che, se $ab \in Q$, allora $b \in Q$. Abbiamo mostrato che, se $a \in P$, $a_{R/Q}$ è nilpotente e, se $a \notin P$, $a_{R/Q}$ è iniettivo. È dunque chiaro che Q è primario e P è il primo associato. □

Questo risultato permette di costruire esempi di ideali primari che non sono potenze di primi. Per esempio, sia $P = (x, y)$ in $F[x, y]$. Esso è massimale, poiché $F[x, y]/P \simeq F$. Si ha $(x, y) \supsetneq (x^2, y) \supsetneq (x^2, xy, y^2) = P^2$. Dunque (x^2, y) è un ideale primario che non è una potenza di un primo.

È chiaro che, se Q è un sottomodulo proprio di M e P è un sottoinsieme di R tale che (1) per ogni $a \in P$ esiste un intero m con $a^m x \in Q$ per ogni $x \in M$, e (2) per $a \in R - P$ l'endomorfismo $a_{M/Q}$ è iniettivo, allora Q è primario con P come ideale associato. Usiamo questo fatto per dimostrare la

Proposizione 7.25. *L'intersezione di un numero finito di sottomoduli primari di M aventi il medesimo ideale primo associato P è primaria e ha P come ideale primo associato.*

Dimostrazione. Basta dimostrarlo per due sottomoduli Q_1 e Q_2. La loro intersezione $Q_1 \cap Q_2$ è un sottomodulo proprio perché i Q_i sono propri. Sia $a \in P$. Esiste un intero m_i tale che $a^{m_i} x \in Q_i$ per ogni $x \in M$. Ponendo $m = \max(m_1, m_2)$, si ha $a^m x \in Q = Q_1 \cap Q_2$. Siano poi $a \in R - P$ e $x \in M - Q$. Possiamo supporre $x \notin Q_1$. Allora $ax \notin Q_1$, e quindi $ax \notin Q$. Dunque $a_{M/Q}$ è iniettivo. Quindi Q è primario con P come ideale primo associato. □

Abbiamo osservato che, per ogni x, l'insieme degli $a \in R$ per i quali esiste un intero m tale che $a^m x = 0$ è l'ideale $\operatorname{nilrad}(\operatorname{ann}_R x)$. Pertanto, se Q è un sottomodulo e $\bar{x} = x + Q$ in M/Q, l'insieme degli a per cui esiste m tale che $a^m x \in Q$ è l'ideale $\operatorname{nilrad}(\operatorname{ann}_R \bar{x})$. Se Q è primario, si ha il seguente importante risultato.

Proposizione 7.26. *Siano Q un sottomodulo primario di M, P il primo associato e $x \in M$. Sia $I_x = \{a \mid a^m x \in Q \text{ per qualche } m\}$. Allora $I_x = P$ se $x \notin Q$, mentre $I_x = R$ se $x \in Q$.*

Dimostrazione. Sia $x \notin Q$. Evidentemente $I_x \supseteq P$, poiché $a_{M/Q}$ è nilpotente per ogni $a \in P$. D'altra parte, se $a \notin P$, $a_{M/Q}$ è iniettivo. Ciò esclude che $a^m x \in Q$ per qualche m. Quindi $I_x = P$. L'altra affermazione, che $I_x = R$ se $x \in Q$, è chiara. □

Sia ora N intersezione finita di sottomoduli primari Q_i di M, $N = \bigcap_i Q_i$. Può accadere che alcuni siano superflui, ossia che N sia l'intersezione di una sottofamiglia propria dei Q_i. In tal caso possiamo scartarne alcuni fino a ottenere una *decomposizione irridondante* $N = \bigcap_i Q_i$, il che significa che per ogni j si ha $N \neq \bigcap_{i \neq j} Q_i$. Ciò equivale a supporre che, per ogni j, $Q_j \not\supseteq \bigcap_{i \neq j} Q_i$.

Dimostreremo due teoremi di unicità per le decomposizioni di un sottomodulo come intersezione di sottomoduli primari di M. Prima di affrontare il caso generale, illustriamo i risultati nel caso particolare degli ideali di un anello con il seguente esempio.

Esempio. Consideriamo l'ideale $I = (x^2, xy)$ in $F[x, y]$. Siano $Q = (x)$ e $Q_a = (y - ax, x^2)$ per $a \in F$. L'ideale Q è primo, quindi primario con ideale associato $P = Q$. Poiché $P_2 = (x, y)$ è

massimale e $P_2 \supseteq Q_a \supseteq P_2^2 = (x^2, xy, y^2)$, Q_a è primario con primo associato P_2. Evidentemente $I \subseteq Q \cap Q_a$. Sia ora $h(x,y) \in Q_a$, sicché

$$h(x,y) = f(x,y)x^2 + g(x,y)(y - ax)$$

per $f(x,y), g(x,y) \in F[x,y]$. Se $h(x,y) \in (x)$, si ha $g(x,y) = xk(x,y)$ e allora $h(x,y) \in I$. Quindi $Q \cap Q_a \subseteq I$, e dunque $I = Q \cap Q_a$. Poiché $Q \not\supseteq Q_a$ e $Q_a \not\supseteq Q$, la decomposizione è irridondante. Poiché $Q_a \neq Q_b$ per $a \neq b$, abbiamo decomposizioni distinte di I in intersezioni irridondanti di ideali primari. Si osservi che i primi associati P e P_2 sono comuni a tutte le decomposizioni, e così pure l'ideale primario Q. Ciò illustra i due teoremi generali di unicità che ora dimostreremo.

Il primo è il seguente.

Teorema 7.18. *Sia N un sottomodulo di M e sia $N = \bigcap_{i=1}^{s} Q_i$, dove i Q_i sono sottomoduli primari e la famiglia è irridondante. Sia $\{P_i\}$ l'insieme degli ideali primi associati ai Q_i. Allora un ideale primo P appartiene a $\{P_i\}$ se e solo se esiste $x \in M$ tale che l'insieme $I_x(N)$ degli elementi $a \in R$ per i quali esiste m con $a^m x \in N$ è l'ideale P. Pertanto l'insieme degli ideali primi $\{P_i\}$ è indipendente dalla particolare decomposizione primaria irridondante di N.*

Dimostrazione. Poiché $N = \bigcap_{i=1}^{s} Q_i$ e s è finito, è chiaro che per ogni $x \in M$ si ha $I_x(N) = \bigcap_{i=1}^{s} I_x(Q_i)$. Per la proposizione 7.26, $I_x(Q_i) = P_i$ se $x \notin Q_i$ e $I_x(Q_i) = R$ se $x \in Q_i$. Quindi $I_x(N) = \bigcap_j P_{i_j}$, dove l'intersezione è estesa agli indici i_j per cui $x \notin Q_{i_j}$. Supponiamo ora $I_x(N) = P$, con P ideale primo. Allora $P = \bigcap_j P_{i_j} \supseteq \prod_j P_{i_j}$, sicché $P \supseteq P_{i_j}$ per qualche i_j. Poiché $P_{i_j} \supseteq P$, si ha $P = P_{i_j}$. Consideriamo poi uno qualsiasi dei primi associati P_i. Per l'irridondanza della famiglia dei Q, possiamo scegliere $x \notin Q_i$ con $x \in \bigcap_{j \neq i} Q_j$. La formula per $I_x(N)$ dà allora $I_x(N) = P_i$. Ciò completa la dimostrazione. □

Chiameremo l'insieme degli ideali primi $\{P_i\}$ l'*insieme degli ideali primi associati* a $N = \bigcap_{i=1}^{s} Q_i$. Essi forniscono informazioni importanti sul sottomodulo N. Per esempio, si ha il seguente teorema.

Teorema 7.19. *Sia N un sottomodulo di M che sia intersezione di un numero finito di sottomoduli primari, e sia $\{P_i\}$ l'insieme degli ideali primi associati a N. Allora $\bigcup_i P_i$ è l'insieme dei divisori dello zero di M/N e $\bigcap_i P_i$ è il nilradicale di* $\ker \rho_{M/N}$.

Dimostrazione. Possiamo supporre $N = \bigcap_i Q_i$ come nel teorema precedente e P_i associato a Q_i. (Può accadere che $P_i = P_j$ per $i \neq j$.) La dimostrazione precedente mostra che, se $a \in P_i$, esiste un $x \in M - N$ tale che $a^m x \in N$ per qualche intero positivo m. Se si prende m minimo, $a^{m-1}x \notin N$ e $a(a^{m-1}x) \in N$, quindi a è un divisore dello zero di M/N. Pertanto ogni elemento di $\bigcup_i P_i$ è un divisore dello zero di M/N. Viceversa, sia a un divisore dello zero di M/N. Esiste allora $x \in M$, $x \notin N$, tale che $ax \in N$. Poiché $x \notin N$, si ha $x \notin Q_i$ per qualche i e $ax \in Q_i$. Quindi a_{M/Q_i} non è iniettivo, sicché $a \in P_i$. Pertanto $\bigcup_i P_i$ è l'insieme dei divisori dello zero di M/N. Questa è la prima affermazione del teorema. Per dimostrare la seconda, ricordiamo che $\operatorname{nilrad}(\ker \rho_{M/N})$ è l'insieme degli $a \in R$ per cui esiste m tale che $a^m x \in N$ per ogni $x \in M$. Esso è l'intersezione, al variare di i, degli insiemi degli $a \in R$ per i quali esiste un m_i tale che $a^{m_i} x \in Q_i$ per ogni $x \in M$. Quest'ultimo insieme è P_i. Quindi $\operatorname{nilrad}(\ker \rho_{M/N}) = \bigcap_i P_i$. □

Dal teorema di unicità e dalla proposizione 7.25 risulta chiaro anche che un sottomodulo che sia intersezione finita di sottomoduli primari di M è primario se e solo se ha un solo ideale primo associato.

Supponiamo ora che la decomposizione irridondante $N = \bigcap_{i=1}^{s} Q_i$ in sottomoduli primari sia *normale*, nel senso che Q_i distinti hanno ideali primi associati distinti. Si può ottenere questa condizione sostituendo ogni famiglia di Q_i associati allo stesso primo con la loro intersezione,

che è primaria per la proposizione 7.25. Nel caso di una decomposizione normale, abbiamo una corrispondenza biunivoca fra i sottomoduli primari della decomposizione e i loro ideali primi associati. Diremo ora *isolato* un sottomodulo primario Q_i della decomposizione normale $N = \bigcap_{i=1}^{s} Q_i$ se l'ideale primo associato P_i è minimale nell'insieme degli ideali primi associati a N. Il secondo teorema di unicità afferma che le componenti isolate compaiono in ogni decomposizione normale di N come intersezione di sottomoduli primari.

Teorema 7.20. *Sia $N = \bigcap_{i=1}^{s} Q_i$ una decomposizione primaria normale di N e sia P_i un primo associato minimale nell'insieme dei primi associati. Allora si può scegliere $a \in \bigcap_{j\neq i} P_j$, $a \notin P_i$. Per ogni tale a, la componente isolata Q_i corrispondente a P_i è caratterizzata come l'insieme degli $x \in M$ tali che $a^m x \in N$ per qualche intero m. Pertanto la componente isolata Q_i è indipendente dalla particolare decomposizione primaria normale di N.*

Dimostrazione. Se non esistesse un tale a, si avrebbe $P_i \supseteq \bigcap_{j\neq i} P_j$, e quindi $P_i \supseteq P_j$ per qualche $j \neq i$, contro la minimalità di P_i. Sia ora $a \in \bigcap_{j\neq i} P_j$, $a \notin P_i$. Allora a_{M/Q_j} è nilpotente per $j \neq i$, mentre a_{M/Q_i} è iniettivo. Quindi, se $x \in M$, esiste un intero m tale che $a^m x \in Q_j$ per $j \neq i$, perciò $a^m x \in \bigcap_{j\neq i} Q_j$. D'altra parte a^m_{M/Q_i} è iniettivo per ogni m, sicché $a^m x \in Q_i$ se e solo se $x \in Q_i$. Poiché $N = \bigcap_{k=1}^{s} Q_k$, la caratterizzazione enunciata per Q_i è provata e la sua conseguenza è chiara. □

Nell'esempio dato a p. 436, i primi associati sono (x) e (x, y), quindi (x) è minimale. La componente isolata corrispondente è (x), che compare in tutte le decomposizioni di $I = (x^2, xy)$. Osserviamo inoltre che, in un anello R in cui tutti i primi non nulli sono massimali (per esempio, un dominio a ideali principali), la decomposizione primaria normale è unica se nessuno dei primi associati è 0.

Supponiamo ora M noetheriano e mostriamo che ogni sottomodulo N di M si può esprimere come intersezione finita di sottomoduli primari. Diremo che un sottomodulo N di M è *indecomponibile (rispetto all'intersezione)* se non possiamo scrivere $N = N_1 \cap N_2$ con $N_i \neq N$ per $i = 1, 2$. Dimostriamo dapprima il

Lemma 1. *Se M è noetheriano, ogni sottomodulo $N \neq M$ si può scrivere come intersezione finita di sottomoduli indecomponibili.*

Dimostrazione. Se il risultato è falso, la famiglia dei sottomoduli per i quali è falso ha un elemento massimale N. Allora N non è indecomponibile, dunque vi sono sottomoduli N_1, N_2 tali che $N_i \neq N$ e $N_1 \cap N_2 = N$. Si ha quindi $N_i \supsetneq N$ e, per la massimalità di N, N_i è intersezione finita di sottomoduli indecomponibili. Lo è allora anche $N = N_1 \cap N_2$, contro l'ipotesi. □

Il risultato che vogliamo dimostrare sulle decomposizioni primarie sarà una conseguenza immediata di questo lemma e del seguente.

Lemma 2. *Se M è noetheriano, ogni sottomodulo proprio indecomponibile N di M è primario.*

Dimostrazione. La dimostrazione è dovuta a Noether ed è simile alla dimostrazione del lemma di Fitting (p. 113), che essa ha preceduto. Se N non è primario, esiste $a \in R$ tale che $a_{M/N}$ non è né iniettivo né nilpotente. Consideriamo la successione di sottomoduli di M/N

$$0 \subseteq \ker a_{M/N} \subseteq \ker a^2_{M/N} \subseteq \cdots .$$

Poiché M/N è noetheriano, esiste m tale che $\ker a^m_{M/N} = \ker a^{m+1}_{M/N} = \cdots$. Poiché $a_{M/N}$ non è nilpotente, $\ker a^m_{M/N} \neq M/N$. Dunque $\ker a^m_{M/N} = N_1/N$ con N_1 un sottomodulo proprio di M contenente N. Inoltre, poiché $a_{M/N}$ non è iniettivo, $\ker a^m_{M/N} \neq 0$, sicché $N_1 \neq N$. Consideriamo ora il sottomodulo $N_2 = a^m M + N$ e sia $x \in N_1 \cap N_2$. Allora $x = a^m y + z$, con $y \in M$, $z \in N$, e $a^m x \in N$. Ne segue che $a^{2m} y \in N$ e la condizione $\ker a^m_{M/N} = \ker a^{2m}_{M/N}$ dà $a^m y \in N$. Allora

$x = a^m y + z \in N$. Pertanto $N_1 \cap N_2 = N$ e $N_2 \neq N$, poiché $N_1 \neq M$. Quindi $N = N_1 \cap N_2$ è decomponibile, contro l'ipotesi. □

I due lemmi hanno evidentemente la conseguenza seguente.

Teorema 7.21. *Ogni sottomodulo di un modulo noetheriano M ammette una decomposizione come intersezione finita di sottomoduli primari di M.*

Quanto abbiamo fatto si applica agli ideali degli anelli noetheriani. In questo caso otteniamo che, se I è un ideale proprio di un anello noetheriano, allora $I = \bigcap_i Q_i$ con i Q_i ideali primari. Possiamo anche supporre che questa rappresentazione di I sia irridondante e che gli ideali primi P_i associati ai Q_i siano distinti. L'insieme $\{P_i\}$ è univocamente determinato e i P_i si chiamano i *primi associati* di I. I Q_j i cui ideali primi associati P_j sono minimali nell'insieme $\{P_i\}$ sono univocamente determinati, ossia compaiono in ogni rappresentazione normale di I come intersezione di ideali primari.

Il teorema 7.19 si specializza come segue. Se $\{P_i\}$ è l'insieme dei primi associati di I, allora $\bigcup_i P_i$ è l'insieme dei divisori dello zero modulo I, ossia degli elementi $z \in R$ per i quali esiste $y \in R - I$ tale che $yz \in I$. Inoltre $\bigcap_i P_i$ è il nilradicale di I. Evidentemente $\bigcap_i P_i = \bigcap_j P_j$, dove $\{P_j\}$ è l'insieme dei primi associati minimali in $\{P_i\}$.

Se I è un ideale proprio di un anello R, un ideale primo P si dice *primo minimale sopra I* se $P \supseteq I$ e non esiste alcun ideale primo P' tale che $P \supsetneq P' \supseteq I$. Se R è noetheriano, vi è soltanto un numero finito di primi minimali sopra un dato I; sono precisamente i primi minimali fra gli ideali primi associati di I. Infatti, se P è un qualunque ideale primo contenente I, si ha $P \supseteq \operatorname{nilrad} I = \bigcap_j P_j$, con i P_j primi associati minimali di I. Allora $P \supseteq \prod_j P_j$ e $P \supseteq P_j$ per qualche j. Quindi P coincide con uno dei P_j se e solo se P è un primo minimale sopra I. Prendendo $I = 0$ (e $R \neq 0$), vediamo che un anello noetheriano R contiene soltanto un numero finito di ideali primi P minimali nel senso che non esiste un ideale primo P' tale che $P \supsetneq P'$. Questi ideali primi si chiamano gli *ideali primi minimali* di R. Evidentemente R è un dominio se e solo se 0 è il suo unico ideale primo minimale.

Per i nilradicali nel caso noetheriano si ha anche il seguente risultato.

Teorema 7.22. *Se I è un ideale di un anello noetheriano R e N è il suo nilradicale, esiste un intero m tale che $N^m \subseteq I$. In particolare, se Q è un ideale primario di R e P è il primo associato, allora $P^m \subseteq Q$ per qualche intero m.*

Dimostrazione. N ha un sistema finito di generatori $z_1, \ldots, z_r$, il che significa che N è costituito dagli elementi $\sum_{i=1}^r a_i z_i$, $a_i \in R$. Abbiamo interi $m_i \geq 1$ tali che $z_i^{m_i} \in I$. Poniamo $m = \sum_{i=1}^r m_i - (r-1)$. Allora ogni prodotto di m degli z_i contiene un fattore della forma $z_i^{m_i}$ e appartiene pertanto a I. Ne segue che ogni prodotto di m elementi di N appartiene a I. Dunque $N^m \subseteq I$. Se Q è primario, il primo associato P è $\operatorname{nilrad} Q$. La seconda affermazione segue quindi dalla prima. □

Esercizi.

1. Sia S un sottomonoide del monoide moltiplicativo di R, sia M un R-modulo e sia N un sottomodulo che sia intersezione di un numero finito di sottomoduli primari. Mostrare che $M_S = N_S$ se e solo se $(\bigcap_i P_i) \cap S \neq \varnothing$, dove $\{P_i\}$ è l'insieme degli ideali primi associati di N. Mostrare che, se Q è un sottomodulo primario e $Q_S \neq M_S$, allora Q_S è un R_S-sottomodulo primario di M_S. Mostrare che, se $N_S \neq M_S$ (N come prima), allora N_S ammette una decomposizione come intersezione finita di R_S-sottomoduli primari.

2. Sia N un sottomodulo di M e supponiamo che $N = \bigcap_{i=1}^s Q_i$ sia una decomposizione

primaria normale di N. Sia $\{P_i\}$ l'insieme dei primi associati. Diciamo *isolato* un sottoinsieme T di $\{P_i\}$ se, per ogni $P_j \in T$, ogni $P_i \subseteq P_j$ appartiene a T. Mostrare che, se T è isolato, l'intersezione $\bigcap_j Q_j$, estesa agli indici j tali che $P_j \in T$, è indipendente dalla decomposizione primaria normale assegnata di N. Questo sottomodulo si chiama *componente isolata* di N corrispondente a T.

3. Se I_1 e I_2 sono ideali di un anello R, si definisce il quoziente $(I_1 : I_2) = \{a \in R \mid aI_2 \subseteq I_1\}$. Osservare che $(I_1 : I_2) \supseteq I_1$. Mostrare che, se R è noetheriano, $(I_1 : I_2) = I_1$ se e solo se I_2 non è contenuto in alcuno dei primi associati di I_1.

7.14 Il lemma di Artin–Rees. Il teorema di intersezione di Krull

Nel resto del capitolo dimostreremo alcuni dei principali teoremi della teoria degli anelli commutativi noetheriani. Alcuni di questi risultati furono ottenuti dapprima mediante i teoremi sulla decomposizione primaria dei paragrafi precedenti. In seguito si trovarono dimostrazioni più semplici, fondate su un lemma scoperto indipendentemente e quasi contemporaneamente da E. Artin e D. Rees. Cominceremo da questo risultato. Nella dimostrazione ci serviremo di un particolare sottoanello di un anello di polinomi, definito da un ideale dell'anello dei coefficienti.

Sia R un anello, $R[x]$ l'anello dei polinomi in un'indeterminata x su R, e I un ideale di R. Introduciamo l'*anello di Rees* T definito da I come la R-sottoalgebra di $R[x]$ generata da Ix. Dunque

$$T = R + Ix + I^2x^2 + \cdots + I^nx^n + \cdots . \tag{32}$$

Supponiamo ora che R sia commutativo e noetheriano. Allora I ha un insieme finito di generatori come R-modulo. Se questi sono $b_1, b_2, \ldots, b_n$, allora Ix è generato come R-modulo da $b_1x, b_2x, \ldots, b_nx$. Dalla (32) segue che T è generato, come R-algebra, da $b_1x, \ldots, b_nx$. Quindi, per il corollario del teorema della base di Hilbert (p. 418), T è noetheriano.

Sia ora M un R-modulo. Otteniamo l'$R[x]$-modulo $R[x] \otimes_R M$, i cui elementi sono della forma $\sum x^i \otimes m_i$, $m_i \in M$. È comodo considerare questo $R[x]$-modulo come un insieme di polinomi in x a coefficienti nel modulo M. Introduciamo a tal fine l'insieme $M[x]$ dei polinomi formali in x a coefficienti in M. Questo insieme si può considerare nel modo ovvio come un $R[x]$-modulo. Per la proprietà universale di $R[x] \otimes_R M$ otteniamo un omomorfismo di gruppi di $R[x] \otimes_R M$ su $M[x]$ che manda $\sum x^i \otimes m_i$ in $\sum m_i x^i$. Poiché $\sum m_i x^i = 0$ implica $m_i = 0$ per ogni i, l'omomorfismo è un isomorfismo. È inoltre chiaro che si tratta di un $R[x]$-isomorfismo. Possiamo dunque identificare $R[x] \otimes_R M$ con $M[x]$, e preferiamo lavorare con quest'ultimo modello. È chiaro che ogni insieme di generatori di M come R-modulo genera $M[x]$ come $R[x]$-modulo.

Consideriamo il sottoinsieme TM di $M[x]$. È il T-sottomodulo di $M[x]$ generato da M e ha la forma

$$TM = M + (IM)x + (I^2M)x^2 + \cdots + (I^kM)x^k + \cdots . \tag{33}$$

Ogni insieme di generatori di M come R-modulo genera TM come T-modulo. Quindi, se M è un R-modulo finitamente generato, TM è un T-modulo finitamente generato. Se inoltre R è noetheriano, anche T è noetheriano e allora TM è un T-modulo noetheriano. Useremo questo fatto per dimostrare il seguente lemma.

Lemma di Artin–Rees. *Siano R un anello commutativo noetheriano, I un ideale di R, M un R-modulo finitamente generato e M_1, M_2 sottomoduli di M. Esiste un intero positivo k tale che, per ogni $n \geq k$,*

$$I^nM_1 \cap M_2 = I^{n-k}(I^kM_1 \cap M_2). \tag{34}$$

Dimostrazione. Per ogni k e ogni $n \geq k$ si ha $I^{n-k}(I^k M_1 \cap M_2) \subseteq I^n M_1 \cap M_2$. Dobbiamo dunque mostrare che esiste un k per il quale vale l'inclusione inversa per ogni $n \geq k$. Definiamo come sopra l'anello T e il T-sottomodulo TM di $M[x]$. Consideriamo in TM il sottogruppo

$$N = (M_1 \cap M_2) + (IM_1 \cap M_2)x + (I^2 M_1 \cap M_2)x^2 + \cdots .$$

Poiché $I^j M_1 \cap M_2$ è un R-sottomodulo di $I^j M$ e

$$(Ix)(I^j M_1 \cap M_2)x^j \subseteq (I^{j+1} M_1 \cap M_2)x^{j+1},$$

N è un T-sottomodulo di TM. Poiché TM è un T-modulo noetheriano, N ha un insieme finito di generatori, diciamo $u_1, \ldots, u_m$. Possiamo scrivere $u_i = \sum_{j=0}^{k} n_{ij} x^j$, dove $n_{ij} \in I^j M_1 \cap M_2$, scegliendo k abbastanza grande per tutti i generatori. Sia ora $n \geq k$ e sia $u \in I^n M_1 \cap M_2$, cosicché $ux^n \in N$. Esistono $f_i \in T$ tali che $ux^n = \sum_i f_i u_i$. Scrivendo $f_i = \sum_l f_{il} x^l$, $f_{il} \in I^l$, otteniamo $ux^n = \sum_{i,j,l} f_{il} n_{ij} x^{j+l}$. Poiché $j \leq k$, confrontando i coefficienti di x^n si esprime u come somma di termini fv con $v \in I^j M_1 \cap M_2$, $j \leq k$, e $f \in I^{n-j}$. Ora

$$I^{n-j}(I^j M_1 \cap M_2) = I^{n-k} I^{k-j}(I^j M_1 \cap M_2) \subseteq I^{n-k}(I^k M_1 \cap M_2).$$

Pertanto $u \in I^{n-k}(I^k M_1 \cap M_2)$, e quindi $I^n M_1 \cap M_2 \subseteq I^{n-k}(I^k M_1 \cap M_2)$. □

La prima applicazione del lemma di Artin–Rees è il seguente teorema.

Teorema di intersezione di Krull. *Siano R un anello commutativo noetheriano, I un ideale di R e M un R-modulo finitamente generato. Poniamo $I^\infty M = \bigcap_{n=1}^{\infty} I^n M$. Allora $I(I^\infty M) = I^\infty M$.*

Dimostrazione. Poniamo $M_1 = M$, $M_2 = I^\infty M$. Esiste allora un k per il quale $I^n M \cap I^\infty M = I^{n-k}(I^k M \cap I^\infty M)$ per ogni $n \geq k$. Prendendo $n = k+1$ otteniamo $I^{k+1} M \cap I^\infty M = I(I^k M \cap I^\infty M)$. Poiché $I^k M \cap I^\infty M = I^\infty M$ e $I^{k+1} M \cap I^\infty M = I^\infty M$, segue la relazione cercata $I(I^\infty M) = I^\infty M$. □

Nel ğ3.14 (p. 174) abbiamo ottenuto un criterio per l'uguaglianza $IM = M$, dove I è un ideale di un anello commutativo R e M è un R-modulo finitamente generato: $IM = M$ se e solo se $I + \operatorname{ann}_R M = R$. In termini di elementi, quest'ultima condizione equivale all'esistenza di $b \in I$ tale che $(1+b)M = 0$. Infatti, se b è un tale elemento, allora $1 = -b + (1+b)$ e $-b \in I$, $1+b \in \operatorname{ann}_R M$. Perciò $1 \in I + \operatorname{ann}_R M$ e, trattandosi di un ideale, $I + \operatorname{ann}_R M = R$. Il viceversa è chiaro.

Combinando questo risultato con il teorema di intersezione di Krull vediamo che, se I è un ideale di un anello noetheriano e M è un modulo finitamente generato, esiste $b \in I$ tale che $(1+b)I^\infty M = 0$. Se $I = \operatorname{rad} R$, il radicale di Jacobson di R, ogni $1+b$, $b \in I$, è invertibile. Possiamo quindi concludere che $(\operatorname{rad} R)^\infty M = 0$. Ciò segue anche dal lemma di Nakayama. In ogni caso abbiamo il seguente risultato.

Teorema 7.23. *Sia M un modulo finitamente generato su un anello noetheriano R e sia $J = \operatorname{rad} R$. Allora $\bigcap_{n=1}^{\infty} J^n M = 0$.*

Un'interessante specializzazione dei risultati precedenti si ottiene prendendo $M = R$ (che è generato da 1). I sottomoduli di R sono gli ideali. Il lemma di Artin–Rees afferma allora che, dati tre ideali I, I_1, I_2 di R, esiste un k tale che, per ogni $n \geq k$,

$$I^n I_1 \cap I_2 = I^{n-k}(I^k I_1 \cap I_2). \tag{35}$$

Prendendo $I_1 = R$ e cambiando leggermente la notazione, otteniamo che, se I_1 e I_2 sono ideali di un anello noetheriano R, esiste un k tale che, per $n \geq k$,

$$I_1^n \cap I_2 = I_1^{n-k}(I_1^k \cap I_2). \tag{36}$$

È questa la forma originaria del lemma data da Rees. Prendendo $M = R$ nel teorema 7.23,[26]

[26] L'originale rinvia qui al teorema 7.21. Il risultato appena applicato è il teorema 7.23. [N.d.T.]

otteniamo

$$\bigcap_{n=1}^{\infty} J^n = 0 \tag{37}$$

per il radicale di Jacobson J di un anello commutativo noetheriano.

Come vedremo nel ğ7.18, i risultati di questo paragrafo svolgono un ruolo importante nello studio dei completamenti degli anelli.

7.15 Il polinomio di Hilbert di un modulo graduato

Nello stesso lavoro in cui dimostrò il teorema della base e il teorema delle sizigie, Hilbert ottenne un altro risultato notevole sulla dimensione delle componenti omogenee di un modulo graduato sull'anello dei polinomi $R = F[x_1, \ldots, x_m]$ a coefficienti in un campo F (si veda il riferimento a p. 387). Egli mostrò che, se $M = \bigoplus M_n$ è graduato e M_n è la componente omogenea di grado n, esiste un polinomio $f(t)$ di grado $\leq m-1$ a coefficienti razionali tale che $f(n) = [M_n : F]$ per ogni n sufficientemente grande. In questo paragrafo dimostreremo il teorema in forma più generale e nei paragrafi successivi lo applicheremo per ricavare i risultati principali sulla dimensione negli anelli noetheriani.

Ricordiamo che un anello R è graduato da una famiglia indicizzata di sottogruppi R_i, $i = 0, 1, 2, \ldots$, del suo gruppo additivo se $R = \bigoplus R_i$ e $R_i R_j \subseteq R_{i+j}$ per ogni i, j. Allora $R_0^2 \subseteq R_0$ e si vede facilmente che $1 \in R_0$, sicché R_0 è un sottoanello di R. È chiaro che $R^+ = \sum_{j>0} R_j$ è un ideale di R. Se R è commutativo, lo possiamo considerare come algebra su R_0. Ricordiamo anche la definizione di un modulo graduato M sull'anello graduato R (p. 384). Si ha $M = \bigoplus_{i\geq 0} M_i$, dove gli M_i sono sottogruppi e $R_i M_j \subseteq M_{i+j}$ per ogni i, j. Gli elementi di M_i si dicono *omogenei di grado* i. Vale la seguente proposizione.

Proposizione 7.27. *Un anello commutativo graduato R è noetheriano se e solo se R_0 è noetheriano e R è finitamente generato come R_0-algebra. Se queste condizioni valgono e M è un R-modulo graduato finitamente generato, ogni M_i è un R_0-modulo finitamente generato.*

Dimostrazione. Se R_0 è noetheriano e R è una R_0-algebra finitamente generata, R è noetheriano per il corollario del teorema della base di Hilbert (p. 418). Supponiamo ora R noetheriano. Allora $R_0 \cong R/R^+$ è immagine omomorfa dell'anello noetheriano R, quindi è noetheriano. L'ideale R^+ di R è generato come R-modulo da un numero finito di elementi $x_1, \ldots, x_m$. Sostituendo a ciascun x_i le sue componenti omogenee, possiamo supporre che gli x_i siano elementi omogenei di R^+. Affermiamo che gli x_i generano R come R_0-algebra. Basta mostrare che ogni elemento omogeneo si scrive come polinomio negli x_i a coefficienti in R_0. Procediamo per induzione sul grado di omogeneità. Il risultato è chiaro in grado zero. Sia ora u omogeneo di grado $n > 0$. Possiamo scrivere $u = \sum_{i=1}^m u_i x_i$ con $u_i \in R$. Uguagliando le componenti omogenee, possiamo supporre che u_i sia omogeneo di grado $n - \deg x_i < n$, poiché $x_i \in R^+$. Allora u_i è un polinomio negli x_j a coefficienti in R_0, e lo stesso vale per $u = \sum u_i x_i$.

Supponiamo ora che R sia noetheriano e che M sia un R-modulo graduato finitamente generato. Possiamo scegliere un insieme di generatori omogenei $\{u_1, \ldots, u_r\}$ di M. Scelti gli x_i come sopra, si vede facilmente che ogni elemento di M_n è combinazione R_0-lineare di elementi $y_i u_i$, dove y_i è un monomio negli x_j e $\deg y_i + \deg u_i = n$. Poiché il numero di tali elementi è finito, M_n è finitamente generato come R_0-modulo. □

Supponiamo d'ora in poi che (1) R sia noetheriano, (2) R_0 sia artiniano (oltre che noetheriano) e (3) M sia un R-modulo graduato finitamente generato. Ciascun M_n è allora finitamente generato come R_0-modulo, dunque è artiniano e noetheriano. Perciò M_n ha una serie di composizione come R_0-modulo e resta univocamente determinato l'intero non negativo $l(M_n)$, la

lunghezza della sua serie di composizione. Per studiare queste lunghezze introduciamo la *funzione generatrice*, o *serie di Poincaré*, del modulo graduato M, definita come l'elemento

$$P(M,t) = \sum_{n=0}^{\infty} l(M_n)t^n \tag{38}$$

del campo $\mathbb{Q}((t))$ delle serie formali di Laurent (p. 425). Possiamo ora enunciare il seguente teorema.

Teorema 7.24 (Hilbert–Serre). *Se R è generato da elementi omogenei $x_1, \dots, x_m$, con $\deg x_i = e_i > 0$, allora $P(M,t)$ è un'espressione razionale della forma*

$$\frac{f(t)}{\prod_{i=1}^{m}(1-t^{e_i})}, \tag{39}$$

dove $f(t) \in \mathbb{Z}[t]$.

Per la dimostrazione ci occorre il seguente lemma.

Lemma. *Sia $0 \to M_0 \to M_1 \to \cdots \to M_s \to 0$ una successione esatta di moduli finitamente generati su un anello artiniano R_0 e sia $l(M_i)$ la lunghezza di M_i. Allora $\sum_{i=0}^{s}(-1)^i l(M_i) = 0$.*

Dimostrazione. Se $s = 0$ oppure $s = 1$, il risultato segue immediatamente dalla definizione di esattezza. Se $s = 2$, abbiamo la successione esatta corta $0 \to M_0 \to M_1 \to M_2 \to 0$. Allora $M_2 \cong M_1/M_0$ e $l(M_2) = l(M_1) - l(M_0)$, da cui $l(M_0) - l(M_1) + l(M_2) = 0$. Supponiamo ora $s > 2$. Possiamo inserire la successione data nella successione di omomorfismi

$$0 \to M_0 \to \operatorname{im} M_0 \to M_1 \to \operatorname{im} M_1 \to \cdots \to \operatorname{im} M_{s-1} \to M_s \to 0,$$

dove $M_i \to \operatorname{im} M_i$ si ottiene restringendo il codominio di $M_i \to M_{i+1}$ e $\operatorname{im} M_i \to M_{i+1}$ è un'iniezione. Abbiamo allora le successioni esatte

$$\begin{gathered} 0 \to M_0 \to \operatorname{im} M_0 \to 0, \\ 0 \to \operatorname{im} M_{k-1} \to M_k \to \operatorname{im} M_k \to 0 \quad (1 \le k \le s-1), \\ 0 \to \operatorname{im} M_{s-1} \to M_s \to 0, \end{gathered}$$

dalle quali ricaviamo

$$\begin{aligned} &l(M_0) = l(\operatorname{im} M_0), \\ &l(M_k) = l(\operatorname{im} M_{k-1}) + l(\operatorname{im} M_k) \qquad (1 \le k \le s-1), \\ &l(M_s) = l(\operatorname{im} M_{s-1}). \end{aligned}$$

Sommando queste uguaglianze a segni alterni otteniamo la relazione cercata $\sum_{i=0}^{s}(-1)^i l(M_i) = 0$. □

Dimostrazione del teorema 7.24. Procediamo per induzione sul numero m dei generatori omogenei. Se $m = 0$, allora $R = R_0$ e M è un R_0-modulo finitamente generato. Per n sufficientemente grande si ha quindi $M_n = 0$ e il risultato vale con $f(t) = P(M,t)$.

Supponiamo ora che il risultato valga per $m-1$ generatori omogenei di R. Facciamo agire x_m su M. Otteniamo un R-endomorfismo x_m^* che manda M_n in M_{n+e_m}, $n = 0, 1, 2, \dots$. Dunque $\ker x_m^*$ e $\operatorname{im} x_m^*$ sono sottomoduli omogenei e abbiamo i moduli graduati $K = \ker x_m^* = \bigoplus K_n$, $C = \operatorname{coker} x_m^* = \bigoplus C_n$. Abbiamo le successioni esatte

$$0 \to K_n \to M_n \to M_{n+e_m} \to C_{n+e_m} \to 0.$$

Per il lemma,

$$l(M_n) - l(M_{n+e_m}) = l(K_n) - l(C_{n+e_m}).$$

Moltiplicando per t^{n+e_m} e sommando su $n = 0, 1, 2, \ldots$, otteniamo

$$(t^{e_m} - 1)P(M,t) = P(K,t)t^{e_m} - P(C,t) + g(t), \tag{40}$$

dove $g(t)$ è un polinomio in t. Ora $x_m K = 0$ e $x_m C = 0$. Pertanto C e K sono a tutti gli effetti moduli su R/Rx_m. Poiché R/Rx_m è un anello graduato con $m-1$ generatori omogenei di gradi $e_1, \ldots, e_{m-1}$ e C, K sono moduli graduati su questo anello, abbiamo

$$P(K,t) = \frac{f_1(t)}{\prod_{i=1}^{m-1}(1-t^{e_i})}, \qquad P(C,t) = \frac{f_2(t)}{\prod_{i=1}^{m-1}(1-t^{e_i})}.$$

Sostituendo nella (40) si ottiene il teorema. □

Il caso più importante è quello in cui si possono scegliere i generatori in R_1, ossia $e_i = 1$ per ogni i. Ciò avviene se $R = R_0[x_1, \ldots, x_m]$, dove R_0 è artiniano, gli x_i sono indeterminate e la graduazione è quella usuale, in cui R_n è l'insieme dei polinomi omogenei di grado n. In effetti questo caso si può considerare il più generale, poiché ogni anello graduato con $e_i = 1$ è immagine di $R_0[x_1, \ldots, x_m]$ mediante un omomorfismo graduato, e ogni modulo sull'anello immagine si può considerare come modulo su $R_0[x_1, \ldots, x_m]$. Per le applicazioni è tuttavia comodo supporre che R sia un qualunque anello che soddisfi le condizioni precedenti e sia generato da elementi di R_1. In questo caso il teorema 7.24 afferma che $P(M,t) = f(t)/(1-t)^m$. Possiamo servircene per dimostrare il risultato principale sulle lunghezze $l(M_n)$.

Teorema 7.25 (Hilbert–Serre). *Supponiamo che R sia generato da m elementi omogenei di grado 1. Esiste allora un unico polinomio $\widetilde{l}(t)$ di grado $\leq m-1$ a coefficienti razionali tale che $l(M_n) = \widetilde{l}(n)$ per ogni n sufficientemente grande.*

Dimostrazione. Si ha $P(M,t) = \sum_{n=0}^{\infty} l(M_n)t^n = f(t)/(1-t)^m$. Scriviamo $f(t) = (1-t)^m q(t) + r(t)$, con $\deg r(t) < m$. Allora $r(t) = a_0 + a_1(1-t) + \cdots + a_{m-1}(1-t)^{m-1}$, $a_i \in \mathbb{Q}$, e quindi

$$\frac{f(t)}{(1-t)^m} = q(t) + \frac{a_0}{(1-t)^m} + \frac{a_1}{(1-t)^{m-1}} + \cdots + \frac{a_{m-1}}{1-t}. \tag{41}$$

Dalla formula di derivazione $\left((1-t)^{-k}\right)' = k(1-t)^{-(k+1)}$ si vede facilmente che

$$\frac{1}{(1-t)^k} = \frac{1}{(k-1)!}\sum_{n\geq 0}(n+k-1)\cdots(n+1)t^n.$$

Il coefficiente di t^n a destra è un polinomio in n di grado $k-1$ a coefficienti razionali. Pertanto il coefficiente di t^n in $a_0/(1-t)^m + a_1/(1-t)^{m-1} + \cdots + a_{m-1}/(1-t)$ è $\widetilde{l}(n)$, dove $\widetilde{l}$ è un polinomio di grado $\leq m-1$ a coefficienti razionali. Per la (41), $\widetilde{l}(n) = l(M_n)$ se $n > \deg q(t)$. L'unicità è chiara, poiché un polinomio a coefficienti razionali di grado $\leq m-1$ che si annulli in m interi consecutivi è nullo. □

Il polinomio $\widetilde{l} = \widetilde{l}(M)$ si chiama *polinomio (caratteristico) di Hilbert* del modulo graduato M. Il teorema 7.25 mostra che $\widetilde{l}$ assume valori interi negli interi non negativi. Da ciò non segue che $\widetilde{l} \in \mathbb{Z}[t]$. È però facile determinare i polinomi con questa proprietà. Per ogni $n = 1, 2, 3, \ldots$ definiamo il polinomio

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \tag{42}$$

e poniamo $\binom{x}{0} = 1$. Evidentemente $\binom{x}{n} \in \mathbb{Q}[x]$ e, poiché $\deg\binom{x}{n} = n$, questi polinomi formano una base dello spazio vettoriale $\mathbb{Q}[x]$ su $\mathbb{Q}$. Come per i coefficienti binomiali, si ha

$$\Delta\binom{x}{n} \equiv \binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}. \tag{43}$$

Se x è un intero, $\binom{x}{n}$ è il prodotto di n interi consecutivi diviso per $n!$, e si vede facilmente che è un intero. Perciò ogni combinazione lineare a coefficienti interi dei polinomi $1, \binom{x}{1}, \ldots, \binom{x}{n}$ assume valori interi per valori interi dell'argomento. Viceversa, vale la seguente proposizione.

Proposizione 7.28. *Sia $f(x)$ un polinomio di grado n a coefficienti razionali che assuma valori interi in un insieme di $n+1$ interi consecutivi.*[27] *Allora $f(x)$ è una combinazione lineare a coefficienti interi dei polinomi $\binom{x}{j}$, $0 \le j \le n$.*

Dimostrazione. Possiamo scrivere $f(x) = a_0 + a_1\binom{x}{1} + \cdots + a_n\binom{x}{n}$ con a_i razionali. Allora $\Delta f(x) \equiv f(x+1) - f(x) = a_1 + a_2\binom{x}{1} + \cdots + a_n\binom{x}{n-1}$. Per induzione sul grado concludiamo che ogni a_i con $i > 0$ è intero. Ne segue anche $a_0 \in \mathbb{Z}$. □

Esercizi.

1. Determinare le lunghezze $l(R_n)$, $n = 0, 1, 2, \ldots$, dove R_n è l'insieme dei polinomi omogenei di grado n in $R = F[x_1, \ldots, x_m]$ e F è un campo. Determinare $P(R, t)$ come espressione razionale in t.

2. Sia f una funzione a valori interi su $\mathbb{N} = \{0, 1, 2, \ldots\}$ tale che $f(n+1) - f(n) = \widetilde{g}(n)$, dove $\widetilde{g}(t) \in \mathbb{Q}[t]$ ha grado $m-1$. Mostrare che esiste un polinomio $\widetilde{f}(t) \in \mathbb{Q}[t]$ di grado m tale che $f(n) = \widetilde{f}(n)$ per $n \in \mathbb{N}$.

7.16 Il polinomio caratteristico di un anello locale noetheriano

Consideriamo anzitutto una costruzione generale che a un ideale I e a un modulo M sull'anello R associa un anello graduato $G_I(R)$ e un modulo graduato $G_I(M)$. Poniamo

$$G_I(R) = \bigoplus_{n\ge 0} I^n/I^{n+1}, \qquad G_I(M) = \bigoplus_{n\ge 0} I^n M/I^{n+1}M,$$

dove $I^0 = R$. Se $\overline{a}_i \in I^i/I^{i+1}$ e $\overline{x}_j \in I^j M/I^{j+1}M$, allora $\overline{a}_i = a_i + I^{i+1}$, $\overline{x}_j = x_j + I^{j+1}M$, $x_j \in I^j M$. La classe $a_i x_j + I^{i+j+1}M$ è indipendente dalla scelta dei rappresentanti a_i, x_j. Sono quindi ben definite le operazioni

$$\overline{a}_i\,\overline{x}_j = \overline{a_i x_j}, \qquad \left(\sum_i \overline{a}_i\right)\left(\sum_j \overline{x}_j\right) = \sum_{i,j} \overline{a_i x_j}.$$

Si verifica facilmente che, prendendo $M = R$, si ottiene su $G_I(R)$ una struttura di anello con unità $1 + I$. Inoltre $G_I(M)$ è un modulo graduato su $G_I(R)$ con componenti omogenee $I^n M/I^{n+1}M$. Chiameremo $G_I(R)$ e $G_I(M)$ rispettivamente *anello graduato* e *modulo graduato associati all'ideale I*.

C'è un altro modo di definire $G_I(R)$ e $G_I(M)$. Consideriamo gli anelli T e i moduli TM introdotti nel §7.14 per dimostrare il lemma di Artin–Rees. Avevamo definito

$$T = \sum_{n\ge 0} I^n x^n \subseteq R[x], \qquad TM = \sum_{n\ge 0} (I^n M)x^n \subseteq M[x] = R[x] \otimes_R M,$$

dove x è un'indeterminata. È chiaro che T è un anello graduato con componente omogenea n-esima $T_n = I^n x^n$ e che TM è un T-modulo graduato con componente omogenea n-esima

[27] Nell'originale si legge «n interi consecutivi». Per un polinomio di grado n ne occorrono $n+1$, come si vede anche dalla dimostrazione per differenze. Già $f(x) = x/2$ assume un valore intero in 0 senza essere a valori interi. [N.d.T.]

$(I^nM)x^n$. Abbiamo un omomorfismo di R-algebre graduate di T su $G_I(R)$ che manda bx^k, con $b \in I^k$, $k \geq 1$, in $b + I^{k+1}$ e in grado zero è la proiezione $R \to R/I$. Il nucleo è IT. Possiamo dunque identificare $G_I(R)$ con T/IT. Analogamente possiamo identificare $G_I(M)$ con TM/ITM, dove $ITM = \sum_n (I^{n+1}M)x^n$.

Nel ğ7.14 abbiamo mostrato che, se l'anello R è noetheriano, anche T è noetheriano e inoltre, se M è un R-modulo finitamente generato, TM è un T-modulo finitamente generato. Mediante gli isomorfismi precedenti otteniamo il risultato seguente.

Proposizione 7.29. *Se R è noetheriano, $G_I(R)$ è noetheriano per ogni ideale I. Se inoltre M è un R-modulo finitamente generato, $G_I(M)$ è un $G_I(R)$-modulo finitamente generato.*

Nel caso in cui R/I sia artiniano, potremmo applicare i risultati del paragrafo precedente per definire un polinomio di Hilbert del modulo graduato $G_I(M)$. È infatti chiaro che $G_I(R)$ è generato dalla sua componente omogenea di grado uno I/I^2. Non proseguiremo in questa direzione e ci limiteremo al caso di maggior interesse, quello in cui R è locale noetheriano con ideale massimale J e $I = Q$ è un ideale J-primario (ossia un ideale primario con primo associato J). Ricordiamo che, essendo J massimale, ogni ideale Q per il quale $J^e \subseteq Q \subseteq J$ per qualche $e \geq 1$ è J-primario (proposizione 7.24, p. 435). D'altra parte, se Q è J-primario, allora $Q \subseteq J$ e $Q \supseteq J^e$ per qualche e (teorema 7.22, p. 440). Dunque la condizione su Q equivale a $J^e \subseteq Q \subseteq J$ per qualche e. La condizione richiesta che R/Q sia artiniano è certamente soddisfatta, poiché R/Q è un anello locale il cui ideale massimale J/Q è nilpotente (teorema 7.15).

Possiamo applicare i risultati sul polinomio di Hilbert a $G_Q(R)$, sia come anello sia come modulo su se stesso. Siano $y_1, \ldots, y_m$ elementi di Q le cui classi $y_i + Q^2$ generano Q/Q^2 come R-modulo. Si vede facilmente che le classi $y_i + Q^2$ generano $Q/Q^2 + Q^2/Q^3 + \cdots$ come $G_Q(R)$-modulo. Pertanto, per la dimostrazione della proposizione 7.27, questi elementi generano $G_Q(R)$ come algebra su R/Q. Dal teorema di Hilbert–Serre segue che esiste un polinomio $\widetilde{l}(t) \in \mathbb{Q}[t]$ di grado $\leq m-1$ tale che $\widetilde{l}(n) = l(Q^n/Q^{n+1})$ per n sufficientemente grande, dove $l(Q^n/Q^{n+1})$ è la lunghezza di Q^n/Q^{n+1} come R/Q-modulo.

Passiamo a considerare R/Q^n come R-modulo. Abbiamo la catena di sottomoduli $R \supseteq Q \supseteq Q^2 \supseteq \cdots \supseteq Q^n$, con fattori $R/Q, Q/Q^2, \ldots, Q^{n-1}/Q^n$, che si possono considerare come R/Q-moduli. Come tali hanno serie di composizione e lunghezze. Lo stesso vale pertanto per R/Q^n, che ha lunghezza $l(R/Q^n)$. Poiché

$$l(R/Q^{n+1}) - l(R/Q^n) = l(Q^n/Q^{n+1}) = \widetilde{l}(n)$$

per n sufficientemente grande, segue che esiste un polinomio $\chi_Q^R \in \mathbb{Q}[t]$ di grado $\leq m$ tale che $\chi_Q^R(n) = l(R/Q^n)$ per n sufficientemente grande (esercizio 2, p. 448). Possiamo enunciare questo risultato senza far riferimento all'anello graduato $G_Q(R)$.

Teorema 7.26. *Sia R un anello locale noetheriano con ideale massimale J e sia Q un ideale J-primario. Si supponga che Q/Q^2 sia generato da m elementi come R-modulo. Allora, per ogni $n = 1, 2, 3, \ldots$, R/Q^n ha una serie di composizione come R-modulo. Se $l(R/Q^n)$ è la sua lunghezza, esiste un polinomio $\chi_Q^R \in \mathbb{Q}[t]$ di grado $\leq m$ tale che $l(R/Q^n) = \chi_Q^R(n)$ per ogni n sufficientemente grande.*

Il polinomio χ_Q^R si chiama *polinomio caratteristico di R rispetto a Q*. La sua proprietà più importante è il grado, poiché questo è indipendente dalla scelta di Q ed è quindi un invariante di R. Per vederlo, sia Q' un altro ideale J-primario. Esistono interi positivi s, s' tali che $(Q')^s \subseteq Q$ e $Q^{s'} \subseteq Q'$. Allora $R \supseteq Q^n \supseteq (Q')^{sn}$ e $l(R/Q^n) \leq l(R/(Q')^{sn})$. Dunque $\chi_Q^R(n) \leq \chi_{Q'}^R(sn)$ per n sufficientemente grande. Ne segue $\deg \chi_Q^R \leq \deg \chi_{Q'}^R$ e, per simmetria, $\deg \chi_Q^R = \deg \chi_{Q'}^R$. Indicheremo il grado comune delle χ_Q^R con $d = d(R)$.

7.17 Dimensione di Krull

Introduciamo ora una nozione di dimensione per gli anelli noetheriani che misura la grandezza di un tale anello mediante la lunghezza delle catene di ideali primi distinti contenute nell'anello. Per i nostri scopi conviene indicare una catena finita di ideali primi distinti con $P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$ e chiamare s la *lunghezza* della catena. Con questa convenzione diamo la definizione seguente.

Definizione 7.4. *Se R è un anello noetheriano, la dimensione di Krull di R, denotata con* $\dim R$*, è l'estremo superiore delle lunghezze delle catene di ideali primi distinti in R. Se le lunghezze di queste catene non sono limitate,* $\dim R = \infty$.

Osserviamo che la dimensione di Krull di un anello noetheriano può essere infinita. Esempi di tali anelli sono stati dati da M. Nagata. Osserviamo inoltre che, nel considerare una catena $P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$, possiamo passare alla localizzazione R_P, di ideale massimale P_P. La corrispondenza fra gli ideali primi di R_P e gli ideali primi di R contenuti in P dà una catena di ideali primi $P_P \supsetneq P_{1P} \supsetneq \cdots \supsetneq P_{sP}$ in R_P. Considereremo dunque dapprima la teoria della dimensione per gli anelli locali noetheriani. Se R è un tale anello e J è il suo ideale massimale, è chiaro che basta considerare le catene che iniziano con $P_0 = J$. Il teorema fondamentale sulla dimensione negli anelli locali noetheriani è il seguente.

Teorema 7.27. *Sia R un anello locale noetheriano. I tre interi seguenti, associati a R, sono uguali.*

1. *Il grado $d = d(R)$ del polinomio caratteristico χ_Q^R di un qualunque ideale J-primario Q di R.*
2. *Il numero minimo $m = m(R)$ di elementi di R che generano un ideale J-primario Q di R.*
3. $\dim R$.

(I primi due numeri sono evidentemente finiti. A priori il terzo potrebbe non esserlo. Il teorema afferma che anch'esso è finito ed è uguale a $d(R)$ e a $m(R)$. Ne segue dunque che ogni anello locale noetheriano ha dimensione finita.)

Dimostrazione. Dimostreremo il teorema stabilendo le disuguaglianze $d \leq m \leq \dim R \leq d$.

$d \leq m$. È parte del teorema 7.26.

$m \leq \dim R$. Se $\dim R = \infty$ non c'è nulla da dimostrare. Supponiamo pertanto $\dim R < \infty$ e procediamo per induzione su $\dim R$. Si ha $\dim R = 0$ se e solo se J è l'unico ideale primo di R. In tal caso R è artiniano per il teorema 7.14. Allora $J^e = 0$ per qualche e e 0 è J-primario. Dunque $m = 0$. La disuguaglianza $m \leq \dim R$ vale quindi per $\dim R = 0$. Supponiamo ora $0 < \dim R < \infty$. Siano $P_1, \ldots, P_r$ i primi minimali di R (si veda p. 433). Poiché ogni ideale primo di R contiene uno dei P_i ed è contenuto in J, si ha $J \not\subset P_i$ per $1 \leq i \leq r$. Per il lemma di evitamento dei primi (p. 390) esiste pertanto un elemento $x \in J$ che non appartiene a $\bigcup_i P_i$. Consideriamo l'anello $R' = R/Rx$. È un anello locale di ideale massimale J/Rx. Ogni catena di ideali primi distinti in R' ha la forma $P_0'/Rx \supsetneq \cdots \supsetneq P_s'/Rx$, dove i P_i' sono ideali primi di R contenenti Rx. Ora P_s' contiene uno dei primi minimali P_i e $P_s' \neq P_i$, poiché $x \notin P_i$. Per qualche i abbiamo dunque una catena di ideali primi $P_0' \supsetneq \cdots \supsetneq P_s' \supsetneq P_i$. Ciò mostra che $\dim R' \leq \dim R - 1$. D'altra parte, se $y_1 + Rx, \ldots, y_{m'} + Rx$ generano un ideale (J/Rx)-primario Q'/Rx in R', allora $y_1, \ldots, y_{m'}, x$ generano l'ideale J-primario Q' in R. Quindi $m(R) \leq m(R')+1$. Per l'ipotesi induttiva $m(R') \leq \dim R'$. Pertanto $m(R) \leq m(R') + 1 \leq \dim R' + 1 \leq \dim R$.

$\dim R \leq d$. Procediamo per induzione su d. Se $d = 0$, la lunghezza $l(R/J^n)$ è costante per n sufficientemente grande. Quindi $J^n = J^{n+1}$ per n sufficientemente grande, e $J^n = 0$ per il lemma di Nakayama. Pertanto R è artiniano e J è l'unico ideale primo di R (teoremi 7.14 e 7.15, pp. 426–427). Allora $\dim R = 0$ e $\dim R = 0 = d$.

Supponiamo ora $d > 0$. Dobbiamo dimostrare che, se $P_0 = J \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$ è una catena di ideali primi in R, allora $s \leq d$. Ci riduciamo al caso di un dominio considerando il dominio R/P_s, che è locale di ideale massimale J/P_s e ammette la catena di ideali primi $J/P_s \supsetneq P_1/P_s \supsetneq \cdots \supsetneq P_s/P_s = 0$. Si ha $(J/P_s)^n = (J^n + P_s)/P_s$, sicché

$$(R/P_s)/(J/P_s)^n = (R/P_s)/((J^n + P_s)/P_s) \cong R/(J^n + P_s).$$

Dunque $l((R/P_s)/(J/P_s)^n) = l(R/(J^n + P_s)) \leq l(R/J^n)$. Ne segue che $d(R/P_s) \leq d(R)$. Basta quindi dimostrare $s \leq d$ nel caso in cui R è un dominio e si ha la catena di ideali primi $J = P_0 \supsetneq \cdots \supsetneq P_{s-1} \supsetneq 0$. Sia $x \in P_{s-1}$, $x \neq 0$, e consideriamo R/Rx, che è locale di ideale massimale J/Rx e possiede la catena di ideali primi $J/Rx \supsetneq \cdots \supsetneq P_{s-1}/Rx$. Vogliamo mostrare che $d(R/Rx) \leq d(R) - 1$. Come sopra, $l((R/Rx)/(J/Rx)^n) = l(R/(J^n + Rx))$. Ora

$$l(R/(J^n + Rx)) = l(R/J^n) - l((J^n + Rx)/J^n), \qquad l((J^n + Rx)/J^n) = l(Rx/(J^n \cap Rx)).$$

Per il lemma di Artin–Rees esiste un intero positivo k tale che $J^n \cap Rx = J^{n-k}(J^k \cap Rx)$ per ogni $n \geq k$. Pertanto

$$l((J^n + Rx)/J^n) \geq l(Rx/J^{n-k}x).$$

Poiché $x \neq 0$ nel dominio R, la moltiplicazione per x è un isomorfismo di R-moduli di R su Rx e manda J^{n-k} su $J^{n-k}x$. Dunque $R/J^{n-k} \cong Rx/J^{n-k}x$ come R-moduli e quindi $l(Rx/J^{n-k}x) = l(R/J^{n-k})$. Ne segue che

$$\begin{aligned} l((R/Rx)/(J/Rx)^n) &= l(R/(J^n + Rx)) \\ &= l(R/J^n) - l(Rx/(J^n \cap Rx)) \\ &\leq l(R/J^n) - l(R/J^{n-k}). \end{aligned}$$

Ciò implica $d(R/Rx) \leq d(R) - 1$. Per induzione su d concludiamo che $s - 1 \leq d(R) - 1$ e quindi $s \leq d(R)$. □

Applichiamo ora il teorema 7.27 ad anelli noetheriani qualsiasi. Se R è un tale anello, definiamo l'*altezza* di un ideale primo P di R come l'estremo superiore delle lunghezze delle catene di ideali primi $P_0 = P \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$. È chiaro che l'altezza, $\operatorname{ht} P$, è la dimensione dell'anello locale noetheriano R_P. Essa è finita per il teorema 7.27. Ne segue evidentemente questa conseguenza piuttosto sorprendente.

Teorema 7.28. *Ogni anello noetheriano soddisfa la condizione delle catene discendenti per gli ideali primi.*

Un'altra conseguenza immediata del teorema principale è la seguente.

Teorema generalizzato dell'ideale principale (Krull). *Se I è un ideale proprio di un anello noetheriano e I è generato da m elementi, ogni primo minimale sopra I ha altezza $\leq m$.*

Dimostrazione. Sia P un primo minimale sopra I. L'asserto equivale a $\operatorname{ht} P_P \leq m$ in R_P. Ora P_P è un primo minimale sopra I_P in R_P e, poiché P_P è l'unico ideale massimale di R_P, esso è l'unico ideale primo di R_P contenente I_P. Pertanto I_P è P_P-primario. D'altra parte, se $y_1, \ldots, y_m$ generano I, allora $y_1/1, \ldots, y_m/1$ generano I_P. Quindi $\operatorname{ht} P_P = \dim R_P \leq m$. □

Un caso particolare del teorema precedente è il seguente.

Teorema dell'ideale principale. *Sia y un elemento non invertibile di un anello noetheriano R. Allora ogni ideale primo minimale sopra Ry ha altezza ≤ 1.*

Dalle definizioni è chiaro che la dimensione di Krull di un anello noetheriano è l'estremo superiore delle altezze dei suoi ideali massimali o, equivalentemente, l'estremo superiore delle dimensioni di Krull delle sue localizzazioni negli ideali massimali.

Consideriamo ora la dimensione di Krull dell'anello dei polinomi $F[x_1, \ldots, x_m]$ in m indeterminate su un campo algebricamente chiuso F. Ricordiamo che ogni ideale massimale M di $F[x_1, \ldots, x_m]$ è generato da m elementi $x_1 - a_1, x_2 - a_2, \ldots, x_m - a_m$, $a_i \in F$ (p. 426). Dunque $\operatorname{ht} M \leq m$. D'altra parte abbiamo la catena di ideali primi

$$\sum_{i=1}^{m} R(x_i - a_i) \supsetneq \sum_{i=1}^{m-1} R(x_i - a_i) \supsetneq \cdots \supsetneq R(x_1 - a_1) \supsetneq 0. \tag{44}$$

Ne segue che $\operatorname{ht} M = m$. Poiché ciò vale per ogni ideale massimale, si conclude che $\dim F[x_1, \ldots, x_m] = m$.

Ricaveremo ora un'importante applicazione del teorema generalizzato dell'ideale principale ai sistemi di equazioni polinomiali a coefficienti in un campo algebricamente chiuso.

Teorema 7.29. *Sia F un campo algebricamente chiuso e siano $x_1, \ldots, x_m$ indeterminate. Consideriamo in $R = F[x_1, \ldots, x_m]$ i polinomi $f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)$. Si supponga che il sistema di equazioni*

$$f_1(x_1, \ldots, x_m) = 0, \ \ldots, \ f_n(x_1, \ldots, x_m) = 0 \tag{45}$$

abbia una soluzione in $F^{(m)}$ e che $m > n$. Allora la (45) ha infinite soluzioni in $F^{(m)}$.

Dimostrazione. Supponiamo, per assurdo, che il sistema abbia soltanto un numero finito di soluzioni $(\alpha_1^{(1)}, \ldots, \alpha_m^{(1)}), \ldots, (\alpha_1^{(r)}, \ldots, \alpha_m^{(r)})$. Sia $I = \sum_{i=1}^{n} Rf_i$. La varietà $V(I)$ è dunque

$$S = \{(\alpha_1^{(1)}, \ldots, \alpha_m^{(1)}), \ldots, (\alpha_1^{(r)}, \ldots, \alpha_m^{(r)})\}.$$

Sia $I_j = \sum_{i=1}^{m} R(x_i - \alpha_i^{(j)})$, $1 \leq j \leq r$. Allora $V(I_j)$ consiste del solo punto $(\alpha_1^{(j)}, \ldots, \alpha_m^{(j)})$ e $S = \bigcup_{j=1}^{r} V(I_j) = V(\prod_{j=1}^{r} I_j)$ (p. 430). Quindi, posto $I' = \prod_{j=1}^{r} I_j$, si ha $V(I') = S = V(I)$, e per il teorema degli zeri di Hilbert $\operatorname{nilrad} I = \operatorname{nilrad} I'$. Sia P un ideale primo minimale sopra I. Allora $P \supset \operatorname{nilrad} I = \operatorname{nilrad} I'$. Pertanto $P \supset I' = \prod_j I_j$, sicché $P \supset I_j$ per qualche j e, poiché I_j è massimale, $P = I_j$. Abbiamo visto che ogni ideale massimale in R ha altezza m. Quindi ogni primo minimale sopra $I = \sum_{i=1}^{n} Rf_i$ ha altezza $m > n$, in contraddizione con il teorema generalizzato dell'ideale principale. □

Un utile caso particolare di questo teorema si ottiene prendendo come f_i polinomi con termine costante nullo (per esempio, polinomi omogenei di grado positivo). Questi ammettono la soluzione banale $(0, \ldots, 0)$. Il teorema mostra che, se vi sono più incognite che equazioni, il sistema (45) ha una soluzione non banale.

Se R è un anello locale noetheriano di ideale massimale J e $\dim R = m$, ogni insieme di m elementi $y_1, \ldots, y_m$ tale che $\sum_{i=1}^{m} Ry_i$ sia J-primario si chiama *sistema di parametri* per R. Di particolare interesse per la geometria sono gli anelli locali R per i quali lo stesso J può essere generato da $m = \dim R$ elementi. Tali anelli locali si dicono *regolari*. Gli esercizi seguenti ne indicano alcune proprietà.

Esercizi

1. Dimostrare che, se R è un anello locale noetheriano di ideale massimale J, allora $[J/J^2 : R/J] \geq \dim R$ e vale l'uguaglianza se e solo se R è regolare.[28]

2. Dimostrare che R è regolare di dimensione di Krull 0 se e solo se R è un campo.

[28] Nell'originale, a p. 454, il quoziente è stampato J^2/J, con numeratore e denominatore scambiati.

3. Sia R un anello locale regolare con $J \neq 0$. Dimostrare che $J \supsetneq J^2$. Dimostrare che, se $x \in J - J^2$, allora $R' = R/Rx$ è regolare e $\dim R' = \dim R - 1$.

4. Sia Rp un ideale primo principale di un anello commutativo R. Dimostrare che, se P è un ideale primo tale che $Rp \supsetneq P$, allora $P \subset \bigcap_{n=1}^{\infty}(Rp)^n$. Usare questo risultato per dimostrare che, se R è un anello locale che non è un dominio, ogni ideale primo principale di R è minimale.

5. Dimostrare che ogni anello locale regolare è un dominio. (Suggerimento. Procedere per induzione su $\dim R$. Il caso $\dim R = 0$ è risolto dall'esercizio 2. Supporre quindi $\dim R > 0$. Per l'esercizio 3 e l'ipotesi induttiva, R/Rx è un dominio per ogni $x \in J - J^2$. Dunque Rx è un ideale primo per ogni $x \in J - J^2$. Supporre che R non sia un dominio. Per l'esercizio 4, Rx è allora un ideale primo minimale per ogni $x \in J - J^2$. Siano $P_1, \ldots, P_s$ gli ideali primi minimali di R. Allora $J - J^2 \subset \bigcup_{i=1}^{s} P_i$ e $J \subset J^2 \cup \bigcup_{i=1}^{s} P_i$. Per il lemma di evitamento dei primi, $J \subset P_i$ per qualche i. Allora $J = P_i$ è un ideale primo minimale di R. Dunque $\dim R = 0$, contro l'ipotesi.)

6. Sia M un modulo su un anello commutativo R. Una successione di elementi $a_1, a_2, \ldots, a_n$ di R si dice una *R-successione su M* se (i) $(\sum_{i=1}^{n} Ra_i)M \neq M$ e (ii) per ogni i, $1 \leq i \leq n$, a_i non è un divisore dello zero sul modulo $M/\sum_{j=1}^{i-1} a_j M$. Se $M = R$, la chiameremo semplicemente una *R-successione*. Dimostrare che, se R è un anello locale regolare, $\dim R = m$ e $J = \operatorname{rad} R$, allora J può essere generato da una R-successione di m elementi contenuti in $J - J^2$.

7. Sia R un anello locale noetheriano di ideale massimale J. Dimostrare che, se J può essere generato da una R-successione, allora R è regolare.

7.18 Topologie I-adiche e completamenti

Sia I un ideale di un anello R, che per ora non supponiamo necessariamente commutativo, e sia M un R-modulo. Possiamo introdurre in M una topologia, la *topologia I-adica*, prescrivendo che l'insieme delle classi laterali $x + I^n M$, $x \in M$, $n = 1, 2, 3, \ldots$, sia una base per gli aperti di M. Se $z \in (x + I^n M) \cap (y + I^m M)$ e $q = \max(m, n)$, allora $z + I^q M \subset (x + I^n M) \cap (y + I^m M)$. Poiché, per definizione, gli aperti sono le unioni delle classi $x + I^n M$, ne segue che l'intersezione di due aperti è aperta. Gli altri assiomi per gli aperti, ossia che l'unione di una famiglia qualsiasi di aperti sia aperta e che M e $\varnothing$ siano aperti, sono evidentemente soddisfatti. Abbiamo quindi uno spazio topologico. In particolare, prendendo $M = R$ otteniamo la topologia I-adica di R, in cui una base per gli aperti è l'insieme delle classi laterali $x + I^n$, $x \in R$.

Ricordiamo che un gruppo G si dice *gruppo topologico* se è munito di una topologia e l'applicazione $(x, y) \mapsto xy^{-1}$ di $G \times G$ in G è continua. Un anello R è un *anello topologico* se è munito di una topologia tale che il suo gruppo additivo sia un gruppo topologico e la moltiplicazione sia continua. Un modulo M su un anello topologico R è un *modulo topologico* se è un gruppo topologico e l'applicazione $(a, x) \mapsto ax$ di $R \times M$ in M è continua.

Si verifica facilmente che R, munito della sua topologia I-adica, è un anello topologico e che, se M è un modulo munito della topologia I-adica, M è un modulo topologico su R.

La topologia I-adica in M è di Hausdorff se e solo se $I^\omega M = \bigcap_n I^n M = 0$. Infatti, se vale questa condizione, dati elementi distinti x, y di M esiste un n tale che $x - y \notin I^n M$, da cui segue che gli intorni aperti $x + I^n M$ e $y + I^n M$, rispettivamente di x e di y, sono disgiunti. Viceversa, se $\bigcap_n I^n M \neq 0$, sia $z \neq 0$ un elemento di $\bigcap_n I^n M$. Allora ogni aperto contenente 0 contiene z. Dunque z appartiene alla chiusura di $\{0\}$ e M non è uno spazio T_1, quindi neppure uno spazio di Hausdorff.

D'ora in poi supporremo $I^\omega = 0$ e $I^\omega M = 0$, sicché le topologie I-adiche di R e di M saranno di Hausdorff. Ricordiamo che queste condizioni sono soddisfatte se R è un anello commutativo noetheriano, $I = \operatorname{rad} R$ e M è un R-modulo finitamente generato (teorema 7.23, p. 443). Ricordiamo pure che, se R è un anello commutativo noetheriano e I è un suo ideale qualsiasi, allora $(1 + b)I^\omega = 0$ per qualche $b \in I$. Ne segue che, se I è un ideale proprio di un dominio noetheriano, allora $I^\omega = 0$. Un caso particolare importante si ottiene prendendo $R = F[x_1, \dots, x_n]$, dove F è un campo, e $I = \sum_i Rx_i$, l'ideale dei polinomi che si annullano in $(0, \dots, 0)$.

Come nel caso degli anelli di serie di potenze possiamo introdurre le nozioni di convergenza, successione di Cauchy, ecc. Conviene basare le definizioni sulla nozione di ordine di un elemento rispetto alla topologia I-adica. Sia x un elemento non nullo di M. Poiché $M \supset IM \supset I^2M \supset \cdots$ e $\bigcap_n I^n M = 0$, esiste un massimo intero n tale che $x \in I^n M$. Definiamo questo intero come l'*ordine* $o(x)$ e completiamo la definizione della funzione ordine ponendo $o(0) = \infty$. Usiamo queste definizioni anche in R. Esse implicano evidentemente che $o(x) = \infty$ se e solo se $x = 0$, che $o(-x) = o(x)$, che $o(x+y) \geq \min(o(x), o(y))$ e che, per $a \in R$, $o(ax) \geq o(a) + o(x)$. Ponendo dunque $|x| = 2^{-o(x)}$ e $|a| = 2^{-o(a)}$ (con la convenzione $2^{-\infty} = 0$), otteniamo

$$\begin{aligned}
&\text{(i)} && |x| \geq 0, \qquad |x| = 0 \iff x = 0,\\
&\text{(ii)} && |-x| = |x|,\\
&\text{(iii)} && |x + y| \leq \max(|x|, |y|),\\
&\text{(iv)} && |ax| \leq |a|\,|x|.
\end{aligned}$$

Queste relazioni valgono anche per R e i valori assoluti definiscono metriche in M e in R ponendo $d(x, y) = |x - y|$. Si hanno le consuete proprietà $d(x, y) = d(y, x)$, $d(x, y) \geq 0$ e $d(x, y) = 0$ se e solo se $x = y$. In luogo della disuguaglianza triangolare $d(x, y) \leq d(x, z) + d(z, y)$ vale la disuguaglianza più forte

$$d(x, y) \leq \max\big(d(x, z), d(z, y)\big). \tag{46}$$

Ne segue la curiosa conseguenza che tutti i triangoli sono isosceli, cioè, dati tre elementi x, y, z, due delle distanze $d(x, y)$, $d(x, z)$, $d(y, z)$ sono uguali. Infatti dalla (46) e dalla simmetria di d segue che nessuno dei numeri $d(x, y)$, $d(x, z)$, $d(y, z)$ può essere maggiore di entrambi gli altri, quindi due sono uguali.

La metrica $d(x, y) = |x - y|$ permette di introdurre nel modo consueto la convergenza delle successioni, le successioni di Cauchy, ecc. Diciamo che la successione $\{x_n\}$ *converge* a x e scriviamo $\lim x_n = x$ oppure $x_n \to x$ se per ogni reale $\varepsilon > 0$ esiste un intero $N = N(\varepsilon)$ tale che $|x - x_n| < \varepsilon$ per ogni $n \geq N$. Come al solito, da $x_n \to x$ e $y_n \to y$ segue $x_n + y_n \to x + y$, e da $x_n \to x$ e $a_n \to a$ segue $a_n x_n \to ax$.

La successione $\{x_n\}$ si dice *di Cauchy* se per ogni $\varepsilon > 0$ esiste un intero N tale che $|x_m - x_n| < \varepsilon$ per ogni $m, n \geq N$. Poiché, per $m > n$,

$$\begin{aligned}
|x_m - x_n| &= |(x_m - x_{m-1}) + (x_{m-1} - x_{m-2}) + \cdots + (x_{n+1} - x_n)|\\
&\leq \max(|x_m - x_{m-1}|, |x_{m-1} - x_{m-2}|, \dots, |x_{n+1} - x_n|),
\end{aligned}$$

$\{x_n\}$ è di Cauchy se e solo se per ogni $\varepsilon > 0$ esiste un N tale che $|x_{n+1} - x_n| < \varepsilon$ per ogni $n \geq N$. Diciamo che M è *completo* nella topologia I-adica se ogni successione di Cauchy di elementi di M converge.

Si hanno inoltre le consuete definizioni di convergenza delle serie. La serie $\sum_{n=1}^{\infty} x_n = x_1 + x_2 + \cdots$ converge se converge la successione delle somme parziali $s_n = x_1 + x_2 + \cdots + x_n$. Se $s_n \to s$, scriviamo $s = x_1 + x_2 + \cdots$. Osserviamo che, se M è completo, una serie $x_1 + x_2 + \cdots$ converge

se e solo se il suo termine n-esimo x_n converge a 0. Infatti, se vale tale condizione, la successione delle somme parziali è di Cauchy per l'osservazione precedente. Quindi $x_1 + x_2 + \cdots$ converge. Viceversa, se $x_1 + x_2 + \cdots$ converge, allora $s_n \to s$ e $s_{n-1} \to s$, quindi $x_n = s_n - s_{n-1} \to 0$.

Questo semplice criterio di convergenza delle serie in un modulo completo M permette di mostrare che, se R è completo rispetto alla topologia I-adica, ogni $b \in I$ è quasi-invertibile. Infatti, poiché $b^n \in I^n$, si ha $b^n \to 0$. Quindi la serie

$$1 + b + b^2 + \cdots$$

converge in R. Poiché

$$(1 + b + \cdots + b^{n-1})(1 - b) = 1 - b^n = (1 - b)(1 + b + \cdots + b^{n-1}),$$

passando al limite otteniamo $(1+b+b^2+\cdots)(1-b) = 1 = (1-b)(1+b+b^2+\cdots)$. Dunque b è quasi-invertibile con quasi-inverso $\sum_{n=1}^{\infty} b^n$. Ogni elemento dell'ideale I è quindi quasi-invertibile e pertanto $I \subset \operatorname{rad} R$, il radicale di Jacobson di R. Registriamo questo risultato nella forma seguente.

Proposizione 7.30. *Se R è completo rispetto alla topologia I-adica, allora $I \subset \operatorname{rad} R$.*

Se sappiamo inoltre che R/I è semiprimitivo, allora $I = \operatorname{rad} R$. Per esempio, ciò avviene se I è un ideale massimale di R.

Un'altra proprietà importante degli anelli completi rispetto a topologie I-adiche è la seguente proprietà di sollevamento degli idempotenti, strettamente legata alla proposizione 7.14. Ricordiamo che la proposizione 7.14 ha svolto un ruolo importante nello studio della topologia di $\operatorname{Spec} R$, lo spazio degli ideali primi di R.

Teorema 7.30. *Sia R un anello completo rispetto alla topologia I-adica definita dall'ideale I e sia $\bar{u} = u + I$ un idempotente di $\bar{R} = R/I$. Allora esiste un idempotente e in R tale che $\bar{e} = \bar{u}$.*

Dimostrazione. Supponiamo dapprima R commutativo. In tal caso possiamo applicare la proposizione 7.14, compresa la parte relativa all'unicità, all'anello R/I^n, $n = 1, 2, \ldots$. Abbiamo l'ideale I/I^n di R/I^n, che è nilpotente, e $(u + I^n)^2 \equiv u + I^n \pmod{I/I^n}$. Dalla proposizione 7.14 segue che esiste un unico elemento $e_n + I^n$ di R/I^n tale che $(e_n + I^n)^2 = e_n + I^n$ ed $e_n \equiv u \pmod{I}$. Allora $e_n^2 \equiv e_n \pmod{I^n}$, $e_n \equiv u \pmod{I}$ e, se e'_n è un secondo elemento che soddisfa queste condizioni, $e'_n \equiv e_n \pmod{I^n}$. Poiché $I^n \supset I^{n+k}$, $k = 1, 2, \ldots$, si ha $e_{n+k} \equiv e_n \pmod{I^n}$. Dunque $\{e_n\}$ è di Cauchy e converge a un elemento e. Abbiamo $e^2 = \lim e_n^2 = \lim e_n = e$ e $u \equiv e \pmod{I}$.

Sia ora R arbitrario. Sia R_1 la chiusura in R del sottoanello generato da u. Allora R_1 è commutativo e, posto $I_1 = I \cap R_1$, si ha un ideale I_1 di R_1 tale che $I_1^\omega = 0$. Inoltre, poiché R_1 è chiuso in R, esso è completo rispetto alla topologia I_1-adica. Si ha $(u + I_1)^2 = u + I_1$. Il risultato segue applicando la prima parte all'anello commutativo R_1. □

Una tecnica importante nella teoria degli anelli commutativi consiste nel passare da un anello R al suo completamento. Daremo ora le costruzioni dei completamenti di un anello R e di un modulo M rispetto alle loro topologie I-adiche (supponendo $I^\omega = 0$ e $I^\omega M = 0$). Indichiamo con $C(M)$ l'insieme delle successioni di Cauchy di elementi di M. Esso ha una struttura naturale di modulo, poiché la somma di due successioni di Cauchy è una successione di Cauchy e, se $\{x_n\}$ è di Cauchy e $a \in R$, anche $\{ax_n\}$ è di Cauchy. Il modulo $C(M)$ contiene il sottomodulo delle successioni costanti $\{x\}$ e il sottomodulo $Z(M)$ delle successioni infinitesime $\{z_n\}$, cioè di quelle per cui $z_n \to 0$. Possiamo formare i moduli $\widehat{M} = C(M)/Z(M)$ e $\widehat{R} = C(R)/Z(R)$. Se $\{a_n\} \in C(R)$ e $\{x_n\} \in C(M)$, allora $\{a_n x_n\} \in C(M)$, e quest'ultima successione appartiene a $Z(M)$ se $\{a_n\} \in Z(R)$ oppure $\{x_n\} \in Z(M)$. Questi fatti si verificano facilmente. Ne segue che $Z(R)$ è un ideale di $C(R)$ e dunque $\widehat{R}$ ha struttura di anello. Inoltre, dati $\hat{a} \in \widehat{R}$ e $\hat{x} \in \widehat{M}$, si

può definire $\hat{a}\hat{x}$ prendendo rappresentanti $\{a_n\}$ e $\{x_n\}$ di $\hat{a}$ e $\hat{x}$ e ponendo $\hat{a}\hat{x} = \{a_n x_n\} + Z(M)$. In questo modo $\widehat{M}$ diventa un $\widehat{R}$-modulo.

Poiché $Z(M)$ non contiene successioni costanti all'infuori di $\{0\}$, possiamo identificare M con l'insieme delle classi laterali, rispetto a $Z(M)$, delle successioni costanti. In particolare R si identifica con un sottoanello di $\widehat{R}$ e M è un R-sottomodulo di $\widehat{M}$.

Indichiamo ora con $\widehat{I}$ il sottoinsieme di $\widehat{R}$ formato dagli elementi $\{a_n\} + Z(R)$ tali che ogni $a_n \in I$. Allora $\widehat{I}$ è un ideale di $\widehat{R}$ e $\widehat{I}^k$ è l'insieme degli elementi $\{b_n\} + Z(R)$ tali che $b_n \in I^k$. Ne segue che $\widehat{I}^\omega = 0$. Analogamente $\widehat{I}^\omega \widehat{M} = 0$, sicché su $\widehat{R}$ e su $\widehat{M}$ si hanno le topologie di Hausdorff definite da $\widehat{I}$. È chiaro che le topologie indotte su M e su R sono quelle I-adiche. Inoltre, se $\{x_n\} + Z(M)$ è un elemento di $\widehat{M}$, allora $\{x_n\} + Z(M) = \lim x_n$ in $\widehat{M}$. Dunque M è denso in $\widehat{M}$. Inoltre $\widehat{M}$ è completo. Sia infatti $\{x_n^{(k)}\} + Z(M)$, $k = 1, 2, \ldots$, una successione di Cauchy in $\widehat{M}$. Per ogni $\{x_n^{(k)}\}$ possiamo scegliere $x^{(k)} \in M$ in modo che $|(\{x_n^{(k)}\} + Z(M)) - x^{(k)}| < 1/2^k$. Si vede facilmente che $\{x^{(k)}\}$ è una successione di Cauchy e che, denotata con $\hat{x}$ la sua classe, $\lim_k(\{x_n^{(k)}\} + Z(M)) = \hat{x}$. Dunque $\widehat{M}$ è completo e, analogamente, $\widehat{R}$ è completo rispetto alle topologie $\widehat{I}$-adiche. Chiamiamo $\widehat{M}$ e $\widehat{R}$ i *completamenti*, rispettivamente, di M e di R.

Specializziamo ora queste considerazioni al caso più interessante in cui R sia un anello commutativo noetheriano e M un R-modulo finitamente generato. Con le notazioni precedenti, dimostriamo dapprima quanto segue.

Proposizione 7.31. *$\widehat{M} = \widehat{R}M$.*

Dimostrazione. Sia $\{x_1, \ldots, x_r\}$ un sistema di generatori di M come R-modulo e sia $\hat{y}$ un elemento qualsiasi di $\widehat{M}$. Allora $\hat{y} = \lim y_n$ con $y_n \in M$. Evidentemente $y_{n+1} - y_n \to 0$, sicché, posto $o(y_{n+1} - y_n) = s_n$, si ha $s_n \to \infty$. Poiché $M = \sum_i Rx_i$, si ha $I^m M = \sum_i I^m x_i$, quindi possiamo scrivere $y_{n+1} - y_n = \sum_{j=1}^r a_{nj} x_j$ con $a_{nj} \in I^{s_n}$. Scriviamo ora $y_i = \sum_{j=1}^r b_{ij} x_j$ con $b_{ij} \in R$. Allora

$$y_n = y_1 + (y_2 - y_1) + \cdots + (y_n - y_{n-1}) = \sum_{j=1}^r b_{nj} x_j,$$

dove $b_{nj} = b_{1j} + a_{1j} + \cdots + a_{n-1,j}$. Le r successioni $\{b_{nj}\}$, $1 \le j \le r$, sono di Cauchy. Pertanto $\lim_{n\to\infty} b_{nj} = \hat{b}_j$ in $\widehat{R}$. Allora $\hat{y} = \lim y_n = \sum_j \hat{b}_j x_j$. Dunque $\widehat{M} = \widehat{R}M$. □

Abbiamo definito l'ideale $\widehat{I}$ di $\widehat{R}$ come l'insieme delle classi $\{a_n\} + Z(R)$ con $a_n \in I$. Evidentemente $I \subset \widehat{I}$, perciò $\widehat{R}I \subset \widehat{I}$. Poiché $\{a_n\} + Z(R) = \lim a_n$, è chiaro che I è denso in $\widehat{I}$. La dimostrazione della proposizione precedente mostra che $\widehat{R}I = \widehat{I}$. Consideriamo ora un sottomodulo N di M. Poiché R è noetheriano e M è finitamente generato, anche N è finitamente generato. Evidentemente $I^\omega N \subset I^\omega M = 0$. Si hanno la topologia I-adica di N e la topologia indotta su N come sottospazio di M. Dimostriamo ora la proposizione seguente.

Proposizione 7.32. *Se N è un sottomodulo del modulo M sull'anello noetheriano (commutativo) R e I è un ideale di R, la topologia I-adica di N coincide con la topologia indotta dalla topologia I-adica di M.*

Dimostrazione. Una base di intorni di 0 nella topologia I-adica di N è l'insieme $\{I^n N\}$ e una base di intorni di 0 nella topologia indotta è $\{I^n M \cap N\}$. Per mostrare che le due topologie sono identiche, cioè hanno gli stessi aperti, basta mostrare che, dato un $I^n N$ qualsiasi, esiste un $I^m M \cap N \subset I^n N$ e che, dato un $I^n M \cap N$ qualsiasi, esiste un $I^q N$ tale che $I^q N \subset I^n M \cap N$. Poiché $I^n N \subset I^n M \cap N$, la seconda asserzione è chiara. Per la prima usiamo il lemma di Artin–Rees. Secondo tale lemma esiste un intero k tale che per ogni $q \ge k$ si abbia $I^q M \cap N = I^{q-k}(I^k M \cap N)$. Prendendo $q = n + k$, otteniamo quindi $I^{n+k} M \cap N = I^n (I^k M \cap N) \subset I^n N$. □

Dimostreremo ora l'importante risultato che il completamento di un anello noetheriano rispetto a una topologia I-adica è noetheriano. La dimostrazione si basa sul metodo degli anelli e

dei moduli graduati introdotto nel ğ 7.16. Ricordiamo di aver mostrato che, se I è un ideale di un anello noetheriano R, l'anello graduato associato $G_I(R)$ è noetheriano e che, se R è noetheriano e M è un R-modulo finitamente generato, il modulo graduato $G_I(M)$ è un $G_I(R)$-modulo finitamente generato (proposizione 7.29, p. 449).

Ci occorre la proposizione seguente.

Proposizione 7.33. *Siano R un anello noetheriano, I un ideale di R tale che $I^\omega = 0$ e $\widehat{R}$ il completamento di R rispetto alla topologia I-adica. Siano $G_I(R)$ e $G_{\widehat{I}}(\widehat{R})$ gli anelli graduati di R e di $\widehat{R}$ associati rispettivamente agli ideali I e $\widehat{I}$. Allora $G_I(R) \cong G_{\widehat{I}}(\widehat{R})$.*

Dimostrazione. Si ha $R_i = I^i/I^{i+1}$, $\widehat{R}_i = \widehat{I}^i/\widehat{I}^{i+1}$. Dalla definizione di $\widehat{I}$ è chiaro che $I^i \cap \widehat{I}^{i+1} = I^{i+1}$. Per la densità di R in $\widehat{R}$, dato $\hat{b} \in \widehat{I}^i$ esiste un $b \in R$ tale che $\hat{b} - b \in \widehat{I}^{i+1}$. Allora $b \in I^i = \widehat{I}^i \cap R$. Dunque $\widehat{I}^i = I^i + \widehat{I}^{i+1}$. Ora abbiamo

$$\begin{aligned}\widehat{R}_i &= \widehat{I}^i/\widehat{I}^{i+1} = (I^i + \widehat{I}^{i+1})/\widehat{I}^{i+1} \\ &\cong I^i/(\widehat{I}^{i+1} \cap I^i) = I^i/I^{i+1} = R_i.\end{aligned}$$

Dalla definizione della moltiplicazione negli anelli graduati segue che $G_{\widehat{I}}(\widehat{R}) \cong G_I(R)$. □

Ci occorre anche la proposizione seguente.

Proposizione 7.34. *Sia R completo rispetto a una topologia I-adica e sia M un R-modulo tale che $I^\omega M = 0$. Si supponga che $G_I(M)$ sia finitamente generato come $G_I(R)$-modulo. Allora M è finitamente generato come R-modulo.*

Dimostrazione. Scegliamo un sistema di generatori $\{\bar{x}_1, \dots, \bar{x}_n\}$ di $G_I(M)$ come $G_I(R)$-modulo. Possiamo supporre $\bar{x}_i = x_i + I^{e_i+1}M$, con $x_i \in I^{e_i}M$, $x_i \notin I^{e_i+1}M$. Mostreremo che $\{x_1, \dots, x_n\}$ genera M come R-modulo. Osserviamo dapprima che, se $\bar{u}$ è un elemento omogeneo di grado m di $G_I(M)$, possiamo scrivere $\bar{u} = \sum_i \bar{a}_i \bar{x}_i$, dove $\bar{a}_i$ è un elemento omogeneo di grado $m - e_i$ di $G_I(R)$. Sia ora u_1 un elemento qualsiasi di M. Supponiamo che $o(u_1) = m_1 \geq 0$. Allora $\bar{u}_1 = u_1 + I^{m_1+1}M \in M^{(m_1)}$ e $\bar{u}_1 \neq 0$. Esistono quindi $a_{1i} \in I^{m_1-e_i}$ tali che $\bar{u}_1 = \sum_i \bar{a}_{1i}\bar{x}_i$. Allora $u_2 = u_1 - \sum_i a_{1i}x_i \in I^{m_1+1}M$ e pertanto $o(u_2) = m_2 > m_1$. Ripetiamo l'argomento con u_2 e otteniamo $a_{2i} \in I^{m_2-e_i}$ tali che $u_2 - \sum_i a_{2i}x_i \in I^{m_2+1}M$. Proseguendo così otteniamo una successione di interi $m_1 < m_2 < m_3 < \cdots$, una successione di elementi $u_1, u_2, \dots$ con $u_k \in I^{m_k}M$ e, per ogni i, una successione $a_{1i}, a_{2i}, \dots$ con $a_{ki} \in I^{m_k-e_i}$ tali che $u_k - \sum_i a_{ki}x_i = u_{k+1}$. Poiché R è completo, le serie infinite $\sum_k a_{ki}$ convergono. Sia $\sum_k a_{ki} = a_i$. Affermiamo che $u_1 = \sum_i a_i x_i$. Infatti scriviamo

$$\begin{aligned}u_1 - \sum_i a_i x_i &= u_1 - \sum_i \Big(\sum_k a_{ki}\Big)x_i \\ &= u_1 - \sum_i \Big(\sum_{k=1}^{q} a_{ki}\Big)x_i - \sum_i \Big(\sum_{l=q+1}^{\infty} a_{li}\Big)x_i \\ &= u_{q+1} - \sum_i \Big(\sum_{l=q+1}^{\infty} a_{li}\Big)x_i \in I^q M.\end{aligned}$$

Poiché $I^\omega M = 0$, otteniamo $u_1 - \sum_i a_i x_i = 0$ e $u_1 = \sum_i a_i x_i$. □

Se M è un ideale di R, allora $G_I(M)$ è un ideale di $G_I(R)$. Si ha dunque la seguente conseguenza dell'ultimo risultato.

Corollario. *Sia R completo rispetto a una topologia I-adica e si supponga che $G_I(R)$ sia noetheriano. Allora R è noetheriano.*

Possiamo ora dimostrare il risultato principale.

Teorema 7.31. *Se R è un anello commutativo noetheriano, I è un ideale di R tale che $I^\omega = 0$ e $\widehat{R}$ è il completamento di R rispetto alla topologia I-adica, allora $\widehat{R}$ è noetheriano.*

Dimostrazione. Per la proposizione 7.29, $G_I(R)$ è noetheriano. Per la proposizione 7.33 è dunque noetheriano $G_{\widehat{I}}(\widehat{R})$. Dal corollario segue allora che $\widehat{R}$ è noetheriano. □

La proprietà noetheriana degli anelli di serie di potenze su anelli noetheriani (teorema 7.12, p. 424) segue anche dal teorema 7.31. Sia R noetheriano e sia I l'ideale di $R[x_1, \dots, x_r]$ costituito dai polinomi $f(x_1, \dots, x_r)$ tali che $f(0, \dots, 0) = 0$. Allora $I^\omega = 0$ e possiamo formare il completamento di $R[x_1, \dots, x_r]$ rispetto alla topologia I-adica. Si tratta dell'anello $R[[x_1, \dots, x_r]]$. Poiché $R[x_1, \dots, x_r]$ è noetheriano per il teorema della base di Hilbert, anche l'anello $R[[x_1, \dots, x_r]]$ è noetheriano.

Esercizi

1. Sia R un anello e sia I un suo ideale tale che $I^\omega = 0$. Se $m < n$, si ha l'omomorfismo canonico $\theta_{mn} \colon R/I^n \to R/I^m$. Questi omomorfismi definiscono un limite inverso $\varprojlim R/I^n$ come a p. 73. Dimostrare che tale limite inverso è isomorfo a $\widehat{R}$.

2. Dimostrare che, se R è noetheriano, $\widehat{R}$ è un R-modulo piatto.

Riferimenti bibliografici

- E. Noether, «Idealtheorie in Ringbereichen», *Mathematische Annalen*, vol. 83 (1921), pp. 24–66.
- O. Zariski e Pierre Samuel, *Commutative Algebra*, voll. I e II, D. van Nostrand, 1958 e 1960. Nuova stampa, Springer-Verlag, New York, 1975.
- M. Atiyah e I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass., 1969.
- P. Samuel, *Algèbre commutative*, dispense ciclostilate dell'École Normale Supérieure, Parigi, 1969.
- I. Kaplansky, *Commutative Rings*, Allyn and Bacon, Boston, 1970.

8 Teoria dei campi

Nel primo volume (BAI) abbiamo sviluppato una parte considerevole della teoria dei campi. In particolare abbiamo trattato piuttosto ampiamente la teoria di Galois delle equazioni e la relativa teoria delle estensioni di grado finito. Fra gli argomenti affrontati vi erano i campi di spezzamento di un polinomio, la separabilità, i campi perfetti, le tracce e le norme, e i campi finiti.

Riprendiamo ora lo studio dei campi, cominciando con la costruzione della chiusura algebrica di un campo e con la dimostrazione della sua unicità a meno di isomorfismi. Daremo poi una deduzione alternativa dei risultati principali della teoria di Galois finita, fondata su una corrispondenza generale fra i sottocampi di un campo e certi anelli di endomorfismi del suo gruppo additivo. Estenderemo inoltre la teoria finita alla teoria di Galois di Krull per le estensioni algebriche di grado infinito. Un importante complemento della teoria di Galois finita è lo studio dei prodotti incrociati, strumento classico per studiare il gruppo di Brauer $\mathrm{Br}(F)$ associato a un campo. Ce ne occuperemo nei ğğ8.4, 8.5 e 8.8. Nei ğğ8.9 e 8.11 studieremo la struttura di due importanti tipi di estensioni abeliane di un campo: le estensioni di Kummer e le p-estensioni abeliane. Queste estensioni si possono descrivere mediante certi gruppi abeliani associati al campo di base. Per le p-estensioni i gruppi sono definiti mediante gli anelli dei vettori di Witt. Questi anelli sono di notevole interesse anche indipendentemente dall'applicazione alle p-estensioni. Il ğ8.10 è dedicato alla loro definizione e alla loro teoria elementare. Nel ğ8.7 consideriamo il concetto di chiusura normale e la struttura delle estensioni normali.

I primi due terzi del capitolo riguardano le estensioni algebriche. In seguito consideriamo la struttura delle estensioni arbitrarie. Mostreremo che si possono ottenere in due tappe: prima un'estensione puramente trascendente e poi una algebrica. A questo procedimento sono associati i concetti di base di trascendenza e di grado di trascendenza. Considereremo anche l'analisi più delicata che riguarda le basi di trascendenza separanti e una nozione generale di separabilità applicabile a estensioni anche non algebriche. Le derivazioni hanno un ruolo importante in queste considerazioni. Mostreremo altresì che esse permettono di sviluppare una teoria di Galois per le estensioni puramente inseparabili di esponente uno.

Nel ğ8.13 estendiamo ai domini il concetto di grado di trascendenza dei campi. Nel ğ8.18 consideriamo i prodotti tensoriali di campi anche non algebrici e nel ğ8.19 il concetto di composto libero di due estensioni dello stesso campo.

8.1 Chiusura algebrica di un campo

Ricordiamo che un campo F si dice *algebricamente chiuso* se ogni polinomio monico $f(x)$ di grado positivo a coefficienti in F ha una radice in F. Poiché r è una radice, cioè $f(r) = 0$, se e solo se $x - r$ è un fattore di $f(x)$ in $F[x]$, questa condizione equivale a dire che gli unici polinomi irriducibili di $F[x]$ sono quelli lineari, e dunque anche a dire che ogni polinomio di grado positivo in $F[x]$ è prodotto di fattori lineari. Un'altra condizione equivalente è che F non abbia estensioni algebriche proprie. Infatti, se E è un'estensione di F e $a \in E$ è algebrico su F, allora $[F(a) : F]$ è il grado del polinomio minimo $f(x)$ di a su F, monico e irriducibile. Dunque $a \in F$ se e solo se $\deg f(x) = 1$. Se perciò E è algebrico su F e $E \neq F$, esistono in $F[x]$ polinomi monici irriducibili di grado almeno due, e F non è algebricamente chiuso. Viceversa, se F non è algebricamente chiuso, esiste un polinomio monico irriducibile $f(x) \in F[x]$ di grado almeno due. Allora il campo $F[x]/(f(x))$ è un'estensione algebrica propria di F.

Ricordiamo che, se E è un'estensione del campo F, gli elementi di E algebrici su F costituiscono un sottocampo A di E/F (cioè un sottocampo di E contenente F). Evidentemente

$E = A$ se e solo se E è algebrico su F. All'estremo opposto, se $A = F$, si dice che F è *algebricamente chiuso in* E. In ogni caso A è algebricamente chiuso in E, perché ogni elemento di E algebrico su A è algebrico su F e dunque appartiene ad A. Questi risultati sono stati dimostrati in BAI, pp. 270–271, come casi particolari dei teoremi sulla dipendenza integrale. Diamo ora dimostrazioni alternative basate sulla formula delle dimensioni

$$[E : F] = [E : K][K : F] \tag{1}$$

per un'estensione E/F e un campo intermedio K. La formula, dimostrata in BAI, p. 215, per le estensioni di grado finito, si dimostra allo stesso modo nel caso generale. Infatti, come nel caso finito, si vede direttamente che, se (u_α) è una base di E/K e (v_β) è una base di K/F, allora $(u_\alpha v_\beta)$ è una base di E/F. Dalla formula delle dimensioni segue la proposizione seguente.

Proposizione 8.1. *Si ha $[E : F] < \infty$ se e solo se $E = F(a_1, \ldots, a_n)$, dove a_1 è algebrico su F e ogni a_{i+1} è algebrico su $F(a_1, \ldots, a_i)$.*

La dimostrazione è evidente. La proposizione dà subito i risultati enunciati sugli elementi algebrici. Se $a, b \in E$ sono algebrici su F, ovviamente b è algebrico su $F(a)$ e quindi $F(a, b)$ ha grado finito. Gli elementi $a \pm b$, ab e, per $a \neq 0$, a^{-1} sono dunque algebrici. Gli elementi algebrici formano perciò un sottocampo A contenente F. Se c è algebrico su A, evidentemente è algebrico su un sottocampo $F(a_1, \ldots, a_n)$ con $a_i \in A$. Allora $F(a_1, \ldots, a_n, c)$ ha grado finito su F e c è algebrico su F, dunque $c \in A$.

Osserviamo anche che, se gli a_i sono algebrici, si ha

$$F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n]. \tag{2}$$

Questo è ben noto per $n = 1$ (BAI, p. 214) e segue per induzione per ogni n. Dimostriamo ora la

Proposizione 8.2. *Se E è un'estensione algebricamente chiusa di F, il sottocampo A/F degli elementi di E algebrici su F è algebricamente chiuso.*

Dimostrazione. Sia $f(x)$ un polinomio monico di grado positivo a coefficienti in A. Allora $f(x)$ ha una radice r in E ed evidentemente r è algebrico su A. Quindi $r \in A$, e A è algebricamente chiuso. □

Il risultato mostra che, se un campo F ha un'estensione algebricamente chiusa, ne ha una algebrica su F. Chiameremo un'estensione E/F *chiusura algebrica* di F se (1) E è algebrico su F e (2) E è algebricamente chiuso. Passiamo a dimostrare l'esistenza e l'unicità a meno di isomorfismi di una chiusura algebrica di un qualunque campo F.

Se F è numerabile questi risultati si ottengono con un argomento diretto. Cominciamo enumerando i polinomi monici di grado positivo come $f_1(x), f_2(x), f_3(x), \ldots$, cosa evidentemente possibile. Definiamo per induzione una successione di estensioni ponendo $F_0 = F$ e prendendo per F_i un campo di spezzamento di $f_i(x)$ su F_{i-1}. La costruzione di tali campi è stata data in BAI, p. 225. È chiaro che ogni F_i è numerabile e che possiamo realizzare tutte queste costruzioni in un insieme S sufficientemente grande. Possiamo allora prendere in esso $E = \bigcup_i F_i$. In alternativa possiamo definire E come limite diretto dei campi F_i. Si verifica facilmente che E è una chiusura algebrica di F. In BAI, p. 227, abbiamo mostrato che, se K_1 e K_2 sono due campi di spezzamento su F di $f(x) \in F[x]$, esiste un isomorfismo di K_1/F su K_2/F. Un semplice argomento induttivo permette di dedurne il teorema di isomorfismo per le chiusure algebriche di un campo numerabile.

Lo schema di dimostrazione appena delineato si estende al caso generale mediante l'induzione transfinita. Così procedette E. Steinitz, che per primo dimostrò questi risultati. Vi sono parecchie dimostrazioni alternative basate sul lemma di Zorn. Ne daremo una che impiega il seguente risultato, interessante anche di per sé.

Proposizione 8.3. *Se A è un'estensione algebrica di un campo infinito F, allora $|A| = |F|$.*

Dimostrazione. A è unione disgiunta di insiemi finiti, ciascuno dei quali è l'insieme delle radici in A di un polinomio monico irriducibile di grado positivo. Allora $|A|$ coincide con la cardinalità di questa famiglia di insiemi finiti, quindi con quella dell'insieme dei polinomi corrispondenti. Poiché il prodotto di due cardinali infiniti è il maggiore dei due, l'insieme dei polinomi monici di grado fissato ha cardinalità $|F|$, e altrettanto vale per l'insieme di tutti i polinomi monici. Quindi $|A| = |F|$. □

Se F è finito, l'argomento precedente mostra che ogni sua estensione algebrica è finita o numerabile. Possiamo ora provare l'esistenza delle chiusure algebriche.

Teorema 8.1. *Ogni campo F ha una chiusura algebrica.*

Dimostrazione. Immergiamo dapprima F in un insieme S sufficientemente ampio. Precisamente, supponiamo $|S| > |F|$ se F è infinito, e S più che numerabile se F è finito. Definiamo ora un insieme $\mathcal{A}$ i cui elementi sono le terne $(E, +, \cdot)$, dove E è un sottoinsieme di S contenente F e $+, \cdot$ sono operazioni binarie in E per le quali $(E, +, \cdot)$ è un'estensione algebrica di F. Ordiniamo parzialmente $\mathcal{A}$ ponendo $(E, +, \cdot) \geq (E', +', \cdot')$ se E è un'estensione di E'. Per il lemma di Zorn esiste un elemento massimale $(E, +, \cdot)$. Allora E è un'estensione algebrica di F. Affermiamo che è algebricamente chiuso. In caso contrario avremmo un'estensione algebrica propria $E' = E(a)$ di E. Poiché $|E'| < |S|$, possiamo definire un'applicazione iniettiva di E' in S che sia l'identità su E e trasportare l'addizione e la moltiplicazione di E' sulla sua immagine. Si ottiene così un elemento di $\mathcal{A}$ strettamente maggiore di $(E, +, \cdot)$, contro la massimalità. La contraddizione mostra che E è una chiusura algebrica di F. □

Affrontiamo ora la questione dell'unicità delle chiusure algebriche. È utile estendere a insiemi di polinomi la nozione di campo di spezzamento di un polinomio. Se $\Gamma = \{f\}$ è un insieme di polinomi monici a coefficienti in F, un'estensione E/F si dice *campo di spezzamento* di Γ su F se (1) ogni $f \in \Gamma$ è prodotto di fattori lineari in $E[x]$ e (2) E è generato su F dalle radici degli $f \in \Gamma$. È chiaro che, se E è un campo di spezzamento di Γ su F, nessun sottocampo proprio di E/F è campo di spezzamento di Γ e che, per ogni campo intermedio K, E è campo di spezzamento di Γ su K. Poiché una chiusura algebrica E di F è algebrica, è chiaro che E è campo di spezzamento su F dell'intero insieme dei polinomi monici di grado positivo in $F[x]$. Il teorema di isomorfismo per le chiusure algebriche sarà quindi conseguenza di un risultato generale sull'isomorfismo dei campi di spezzamento che ora dimostreremo. Il punto di partenza è il risultato seguente, dimostrato in BAI, p. 227.

Sia $\eta : a \mapsto \bar{a}$ un isomorfismo di un campo F su un campo $\bar{F}$, sia $f(x) \in F[x]$ monico di grado positivo, sia $\bar{f}(x)$ il polinomio corrispondente in $\bar{F}[x]$ (mediante l'isomorfismo che coincide con η su F e manda x in x) e siano E e $\bar{E}$ campi di spezzamento rispettivamente di $f(x)$ su F e di $\bar{f}(x)$ su $\bar{F}$. Allora η si estende a un isomorfismo di E su $\bar{E}$. Estendiamo ora questo risultato a insiemi di polinomi.

Teorema 8.2. *Sia $\eta : a \mapsto \bar{a}$ un isomorfismo di un campo F su un campo $\bar{F}$, sia Γ un insieme di polinomi monici $f(x) \in F[x]$, sia $\bar{\Gamma}$ l'insieme corrispondente dei polinomi $\bar{f}(x) \in \bar{F}[x]$ e siano E e $\bar{E}$ campi di spezzamento rispettivamente di Γ su F e di $\bar{\Gamma}$ su $\bar{F}$. Allora η si estende a un isomorfismo di E su $\bar{E}$.*

Dimostrazione. La dimostrazione è un'applicazione diretta del lemma di Zorn. Consideriamo l'insieme delle estensioni di η a monomorfismi di sottocampi di E/F in $\bar{E}/\bar{F}$ e usiamo il lemma di Zorn per ottenerne uno massimale. Esso è necessariamente definito su tutto E, altrimenti ne otterremmo uno più grande applicando il risultato citato a uno dei polinomi $f(x) \in \Gamma$. Ora, se ζ è un monomorfismo di E in $\bar{E}$ tale che $\zeta|_F = \eta$, è chiaro che $\zeta(E)$ è un campo di spezzamento di $\bar{\Gamma}$ su $\bar{F}$. Pertanto $\zeta(E) = \bar{E}$ e ζ è un isomorfismo di E su $\bar{E}$. □

Come abbiamo osservato, il risultato vale in particolare per le chiusure algebriche. Ponendo $\bar{F} = F$ e $\eta = 1$, otteniamo il seguente teorema.

Teorema 8.3. *Due chiusure algebriche qualsiasi di un campo F sono isomorfe su F.*

D'ora in poi riserveremo la notazione $\bar{F}$ a una qualunque scelta di chiusura algebrica di F. Se A è una qualsiasi estensione algebrica di F, la sua chiusura algebrica $\bar{A}$ è un'estensione algebrica di A, dunque di F, e pertanto è una chiusura algebrica di F. Si ha quindi un isomorfismo di $\bar{A}/F$ su $\bar{F}/F$. Esso manda A/F in un sottocampo di $\bar{F}/F$. Vediamo così che ogni estensione algebrica A/F si può realizzare come sottocampo della chiusura algebrica $\bar{F}/F$.

Esercizio

1. Sia E un'estensione algebrica di un campo F e sia A una chiusura algebrica di F. Mostrare che E/F è isomorfo a un sottocampo di A/F. (Suggerimento: considerare la chiusura algebrica di E e osservare che essa è una chiusura algebrica di F.)

8.2 La corrispondenza di Jacobson–Bourbaki

Sia E un campo, F un suo sottocampo e $\mathrm{End}_F E$ l'anello delle trasformazioni lineari di E considerato come spazio vettoriale su F. Abbiamo l'applicazione

$$F \longmapsto \mathrm{End}_F E, \tag{3}$$

che è iniettiva poiché si può ricavare F da $\mathrm{End}_F E$ prendendo $\mathrm{End}_{\mathrm{End}_F E} E$. Quest'ultimo è l'insieme delle moltiplicazioni $x \mapsto ax$, $a \in F$ (pp. 205–206), e applicando i suoi elementi a 1 si ottiene F.

Per un campo E fissato cerchiamo ora una caratterizzazione degli anelli di endomorfismi $\mathrm{End}_F E$ che non faccia esplicito riferimento ai sottocampi F. Per ogni $b \in E$ abbiamo anzitutto la moltiplicazione $b_E \colon x \mapsto bx$, $x \in E$, che appartiene a $\mathrm{End}_F E$ qualunque sia il sottocampo F considerato. È questo uno degli elementi della caratterizzazione che daremo. Il secondo si basa su una topologia per gli insiemi di applicazioni, che ora definiremo.

Siano X e Y insiemi arbitrari. L'insieme Y^X delle applicazioni di X in Y si può munire della topologia prodotto (di copie di Y), dando a Y la topologia discreta. Una base di aperti di questa topologia è costituita dagli insiemi $O_{f,\{x_i\}}$, dove f è un'applicazione di X in Y, $\{x_i \mid 1 \leq i \leq n\}$ è un sottoinsieme finito di X e

$$O_{f,\{x_i\}} = \{g \in Y^X \mid g(x_i) = f(x_i),\ 1 \leq i \leq n\}.$$

Chiameremo questa topologia la *topologia finita* di Y^X e useremo lo stesso nome per la topologia indotta sui suoi sottoinsiemi. Se X e Y sono gruppi, l'insieme $\hom(X, Y)$ degli omomorfismi di X in Y è chiuso in Y^X. Infatti, se f appartiene alla chiusura di $\hom(X, Y)$ e x_1, x_2 sono elementi arbitrari di X, l'aperto $O_{f,\{x_1,x_2,x_1x_2\}}$ contiene un $g \in \hom(X, Y)$. Da $g(x_1x_2) = g(x_1)g(x_2)$ segue $f(x_1x_2) = f(x_1)f(x_2)$ e, poiché ciò vale per ogni x_1, x_2, risulta $f \in \hom(X, Y)$. Analogamente, se M, N sono moduli su un anello R (non necessariamente commutativo), $\hom_R(M, N)$ è chiuso in N^M. Il teorema di densità per i moduli completamente riducibili (p. 197) ammette una formulazione semplice in termini della topologia finita: se M è un R-modulo completamente riducibile, l'insieme R_M delle moltiplicazioni $a_M \colon x \mapsto ax$ è denso in $\mathrm{End}_{\mathrm{End}_R M} M$, ossia la chiusura di R_M è $\mathrm{End}_{\mathrm{End}_R M} M$. Questa formulazione è chiara dalla definizione della topologia. Dimostriamo ora un risultato che comprende una caratterizzazione degli anelli $\mathrm{End}_F E$ per un campo E e un suo sottocampo F.

Teorema 8.4. *Sia E un campo, Σ l'insieme dei suoi sottocampi e Γ l'insieme dei sottoanelli L dell'anello degli endomorfismi del gruppo additivo di E tali che (1) $L \supseteq E_E$, l'insieme delle moltiplicazioni a_E in E per gli elementi a di E, e (2) L sia chiuso nella topologia finita. Allora $F \mapsto \mathrm{End}_F E$ è una biiezione di Σ su Γ che inverte l'ordine, e anche la sua inversa inverte l'ordine.*

Dimostrazione. Abbiamo visto che l'applicazione indicata è iniettiva e che $F_1 \supseteq F_2$ se e solo se $\mathrm{End}_{F_1} E \subseteq \mathrm{End}_{F_2} E$. Resta da provarne la suriettività. Sia L un anello di endomorfismi del gruppo additivo di E con le proprietà indicate e consideriamo E come L-modulo nel modo naturale. Poiché E è un campo, non ha ideali diversi da $0, E$, e quindi è irriducibile come E-modulo. Poiché $L \supseteq E_E$, esso è irriducibile anche come L-modulo. L'inclusione $L \supseteq E_E$ implica $\mathrm{End}_L E \subseteq \mathrm{End}_E E$. Poiché E è commutativo, $\mathrm{End}_E E = E_E$. Dunque $\mathrm{End}_L E$ è un sottoanello di E_E e ha pertanto la forma F_E, l'insieme delle moltiplicazioni in E definite dagli elementi di un sottoanello F di E. Per il lemma di Schur, F_E è un anello con divisione, perciò F è un sottocampo di E. Per il teorema di densità L è denso in $\mathrm{End}_{\mathrm{End}_L E} E = \mathrm{End}_F E$. Poiché L è chiuso, si ha $L = \mathrm{End}_F E$ per il sottocampo F. Ciò dimostra la suriettività di $F \mapsto \mathrm{End}_F E$ su Γ. La nostra applicazione è quindi biiettiva. □

Abbiamo già individuato l'applicazione inversa di Γ in Σ. La dimostrazione precedente la fornisce di nuovo, in forma leggermente diversa e più comoda: dato $L \in \Gamma$, il sottocampo corrispondente F è l'insieme degli $a \in E$ tali che

$$a_E l = l a_E \tag{4}$$

per ogni $l \in L$.

L'anello di endomorfismi $L = \mathrm{End}_F E$ contiene E_E e pertanto si può considerare come E-E-bimodulo definendo $al = a_E l$, $la = l a_E$, per $l \in L$, $a \in E$. Poiché la si potrebbe anche interpretare come l'immagine di a mediante l, quando intendiamo quest'ultima scriveremo sempre $l(a)$. Per ora ci interessa solo l'azione sinistra di E su L, ossia L come spazio vettoriale (sinistro) su E.

Consideriamo dapprima la dimensione $[L : E]$ (come spazio vettoriale sinistro su E). Supponiamo che $x_1, \ldots, x_n$ siano elementi di E linearmente indipendenti su F. Esistono allora $l_i \in L = \mathrm{End}_F E$ tali che

$$l_i(x_j) = \delta_{ij}, \qquad 1 \leq i, j \leq n. \tag{5}$$

Per $a_i \in E$ si ha quindi $\sum_i a_i l_i(x_j) = a_j$, da cui segue che gli l_i sono elementi di L linearmente indipendenti su E. Questo implica evidentemente che, se $[E : F] = \infty$, anche $[L : E] = \infty$. Se invece $[E : F] < \infty$ e $(x_1, \ldots, x_n)$ è una base, gli l_i che soddisfano (5) sono univocamente determinati. Inoltre, se $l \in L$ e $l(x_j) = a_j$, allora $\sum_i a_i l_i(x_j) = l(x_j)$. Poiché gli x_j formano una base di E/F e $l, \sum_i a_i l_i$ sono trasformazioni lineari in E/F, si ha $l = \sum_i a_i l_i$. Dunque $(l_1, \ldots, l_n)$ è una base di L su E. Abbiamo dimostrato il seguente importante risultato.

Proposizione 8.4. *Se F è un sottocampo del campo E e $L = \mathrm{End}_F E$, allora $[E : F] < \infty$ se e solo se $[L : E] < \infty$, e in tal caso $[E : F] = [L : E]$. Inoltre, se $(x_1, \ldots, x_n)$ è una base di E/F, le trasformazioni lineari l_i tali che $l_i(x_j) = \delta_{ij}$, $1 \leq i, j \leq n$, formano una base di L su E.*

Nella corrispondenza del teorema 8.4 fra sottocampi di E e anelli di endomorfismi del suo gruppo additivo, ai sottocampi di codimensione finita in E ($[E : F] < \infty$) corrispondono dunque i sottoanelli L tali che $[L : E] < \infty$. Mostreremo ora che in questo caso la condizione (2), che L sia chiuso, è superflua. Ciò segue dalla proposizione seguente.

Proposizione 8.5. *Ogni sottospazio V di dimensione finita su E dell'anello degli endomorfismi del gruppo additivo di E è chiuso nella topologia finita.*

Dimostrazione. Sia $x \in E$ e consideriamo l'applicazione $x^*\colon l \mapsto l(x)$ di V in E. Essa è E-lineare, quindi $x^* \in V^*$, lo spazio duale di V/E. Sia W il sottospazio di V^* generato dagli x^*. Poiché $x^*(l) = l(x) = 0$ per ogni x implica $l = 0$, si ha $W = V^*$. Se $[V : E] = n$, possiamo quindi scegliere $x_i \in E$, $1 \le i \le n$, tali che $(x_1^*, \dots, x_n^*)$ sia una base di V^*. Esiste allora una base $(l_1, \dots, l_n)$ di V su E per la quale $l_i(x_j) = \delta_{ij}$. Sia ora l nella chiusura di V e sia x un elemento qualunque di E. Esistono $a_i \in E$ tali che $\sum_i a_i l_i(x_j) = l(x_j)$ per $1 \le j \le n$ e $\sum_i a_i l_i(x) = l(x)$. Le prime equazioni, insieme a $l_i(x_j) = \delta_{ij}$, danno $a_i = l(x_i)$, cosicché gli a_i sono indipendenti da x. L'ultima equazione mostra allora che $l = \sum_i a_i l_i \in V$. Dunque V è chiuso. □

Il teorema 8.4 e le proposizioni 8.4 e 8.5 implicano immediatamente la seguente corrispondenza.

Corrispondenza di Jacobson–Bourbaki. *Sia E un campo, Φ l'insieme dei sottocampi F di codimensione finita in E e Δ l'insieme dei sottoanelli L dell'anello degli endomorfismi del gruppo additivo di E tali che (1) $L \supseteq E_E$, l'insieme delle moltiplicazioni in E per gli elementi di E, e (2) L abbia dimensione finita come spazio vettoriale sinistro su E. Allora $F \mapsto \operatorname{End}_F E$ è una biiezione di Φ su Δ che inverte l'ordine e la cui inversa inverte l'ordine. In questa corrispondenza $[E : F] = [\operatorname{End}_F E : E]$. Dato $L \in \Delta$, il sottocampo corrispondente F è l'insieme degli $a \in E$ tali che $a_E l = l a_E$ (ossia $al = la$) per ogni $l \in L$.*

Esercizi.

1. Sia $E = (\mathbb{Z}/(p))(x)$, dove p è primo e x è un'indeterminata, e sia $F = (\mathbb{Z}/(p))(x^{p^e})$, con $e \ge 1$. Gli operatori $D_i \in \operatorname{End}_F E$ siano definiti da $D_i x^m = \binom{m}{i} x^{m-i}$, $1 \le i \le p^e - 1$. Verificare che, per $a \in E$,
$$D_j a_E = \sum_{i=0}^{j} (D_{j-i} a) D_i$$
(con $D_0 = 1$), e che $D_i D_j = \binom{i+j}{i} D_{i+j}$ se $i + j \le p^e - 1$, mentre $D_i D_j = 0$ se $i + j \ge p^e$. Dimostrare che $(1, D_1, \dots, D_{p^e-1})$ è una base di $\operatorname{End}_F E$ su E.

2. Sia $[E : F] = n < \infty$ e siano $(l_1, \dots, l_n)$ una base di $\operatorname{End}_F E$ su E e $(x_1, \dots, x_n)$ una base di E su F. Mostrare che la matrice $(l_i(x_j)) \in M_n(E)$ è invertibile.

3. Estendere i risultati di questo paragrafo agli anelli con divisione.

8.3 La teoria di Galois finita

Se K ed E sono campi, indichiamo con $\hom(K, E)$ il gruppo additivo degli omomorfismi del gruppo additivo $(K, +, 0)$ in $(E, +, 0)$. Se K ed E hanno un sottocampo comune F, indichiamo con $\hom_F(K, E)$ il sottoinsieme delle applicazioni F-lineari di K in E. Il gruppo additivo $\hom(K, E)$ ha una struttura di E-K-bimodulo: per $a \in E$, $f \in \hom(K, E)$ si definisce af ponendo $(af)(x) = af(x)$, $x \in K$, e per $b \in K$ si definisce fb mediante $(fb)(x) = f(bx)$. Il sottoinsieme $\hom_F(K, E)$ è un sottomodulo del bimodulo $\hom(K, E)$. Nel caso particolare $K = E$, esaminato nel paragrafo precedente, si ottengono $\operatorname{End} E$ e $\operatorname{End}_F E$. Questi sono E-E-bimoduli e le due operazioni di modulo sono le moltiplicazioni a sinistra e a destra per gli elementi di E_E. Il risultato dimostrato sulla dimensione di $\operatorname{End}_F E$ nel caso $[E : F] < \infty$ ammette la seguente estensione.

Proposizione 8.6. *Siano E, K estensioni del campo F e sia $[K : F] = n < \infty$. Allora la dimensione di $\hom_F(K, E)$ come spazio vettoriale sinistro su E è $[K : F] = n$.*

Dimostrazione. La dimostrazione è identica a quella del caso particolare. Se $(x_1, \dots, x_n)$ è una base di K/F, sia l_i l'applicazione lineare di K/F in E/F tale che $l_i(x_j) = \delta_{ij}$ per $1 \le i, j \le n$. Come nel caso particolare si vede che $(l_1, \dots, l_n)$ è una base di $\hom_F(K, E)$ su E. □

Sia s un omomorfismo di anelli di K in E. L'esistenza di un tale omomorfismo presuppone che i due campi abbiano la stessa caratteristica, e allora s è un monomorfismo di K in E. Evidentemente $s \in \hom(K, E)$. Inoltre, per $a, b \in K$, si ha $s(ab) = s(a)s(b)$. In termini di operatori ciò si scrive

$$sa = s(a)s \tag{6}$$

per ogni $a \in K$. Se K ed E hanno un sottocampo comune F, un omomorfismo di anelli di K/F in E/F è un omomorfismo di K in E che è l'identità su F. Allora $s \in \hom_F(K, E)$.

Ricordiamo il teorema di indipendenza di Dedekind per i caratteri: caratteri distinti di un gruppo a valori in un campo sono linearmente indipendenti su quel campo (BAI, p. 291). Ne segue che omomorfismi di anelli distinti di K in E sono linearmente indipendenti su E. Da questo fatto e dalla proposizione 8.6 ricaviamo il risultato seguente.

Proposizione 8.7. *Se K ed E sono estensioni del campo F e $[K : F] = n < \infty$, esistono al più n omomorfismi (di anelli) di K/F in E/F.*

Dimostrazione. Se $s_1, \ldots, s_m$ sono omomorfismi distinti di K/F in E/F, sono elementi di $\hom_F(K, E)$ linearmente indipendenti su E. Poiché la dimensione sinistra di $\hom_F(K, E)$ su E è n, segue $m \leq n$. □

Supponiamo che G sia un gruppo di automorfismi di E. Poniamo

$$EG = \left\{ \sum_i a_i s_i \;\middle|\; a_i \in E,\ s_i \in G \right\}. \tag{7}$$

Allora EG contiene $E_E = E1$ e la (6) mostra che EG è un sottoanello dell'anello $\operatorname{End} E$ degli endomorfismi del gruppo additivo di E, poiché implica $(as)(bt) = as(b)st$ per s, t automorfismi e $a, b \in E$. Se G è finito, diciamo $G = \{s_1 = 1, s_2, \ldots, s_n\}$, gli s_i formano una base di EG su E. Dunque $[EG : E] = n = |G|$. Allora EG soddisfa le condizioni richieste agli anelli di endomorfismi nella corrispondenza di Jacobson–Bourbaki. Il sottocampo corrispondente F è l'insieme degli $a \in E$ tali che $a_E l = l a_E$ per ogni $l \in EG$. Poiché $a_E b_E = b_E a_E$, queste condizioni si riducono alle condizioni, in numero finito, $a_E s_i = s_i a_E$, ossia $as_i = s_i a$ per ogni $s_i \in G$. Per la (6) ciò equivale a $s_i(a) = a$ per $1 \leq i \leq n$. Il campo associato a EG nella corrispondenza è quindi

$$F = \operatorname{Inv} G, \tag{8}$$

il sottocampo di E degli elementi fissati da ogni $s_i \in G$. Abbiamo

$$[E : F] = [EG : E] = |G| \tag{9}$$

e

$$EG = \operatorname{End}_F E. \tag{10}$$

Sia ora $\operatorname{Gal} E/F$ il gruppo di Galois di E/F, ossia il gruppo degli automorfismi di E che fissano ogni elemento di F. Evidentemente $\operatorname{Gal} E/F \supseteq G$. Sia $t \in \operatorname{Gal} E/F$. Allora $t \in \operatorname{End}_F E$ e, per la (10), $t = \sum_{i=1}^n a_i s_i$, $a_i \in E$, $s_i \in G$. Per il teorema di indipendenza di Dedekind, $t = s_i$ per qualche i. Dunque

$$\operatorname{Gal} E/F = G. \tag{11}$$

Ci servirà anche il seguente risultato sui sottoanelli di EG contenenti E_E.

Proposizione 8.8. *Sia G un gruppo finito di automorfismi del campo E. I sottoanelli di EG che contengono E_E sono gli anelli EH, con H sottogruppo di G.*

Dimostrazione. Ogni EH è chiaramente un sottoanello di EG che contiene $E_E = E1$. Viceversa, sia S un tale sottoanello e sia $H = S \cap G$. È chiaro che H è un sottomonoide di G e, poiché G è finito, H è un sottogruppo. È evidente che $EH \subseteq S$. Affermiamo che $EH = S$. Altrimenti avremmo un elemento $a_1 s_1 + a_2 s_2 + \cdots + a_r s_r \in S$ tale che nessun s_j appartenga a H e ogni a_j sia non nullo. Evidentemente $r > 1$. Supponendolo minimo, la dimostrazione del teorema di Dedekind dà un elemento con le stesse proprietà per un valore minore di r. La contraddizione dimostra che $S = EH$. □

Diremo che un sottocampo F di E è *galoisiano in* E, o anche che E *è galoisiano su* F, se esiste un gruppo di automorfismi G di E tale che $\operatorname{Inv} G = F$. Possiamo ora enunciare il risultato principale sui gruppi finiti di automorfismi di un campo.

Teorema 8.5. *Sia E un campo. Indichiamo con Λ l'insieme dei gruppi finiti di automorfismi di E e con Ψ l'insieme dei sottocampi di E che sono galoisiani in E e hanno codimensione finita in E. Abbiamo allora le applicazioni $G \mapsto \operatorname{Inv} G$ di Λ in Ψ e $F \mapsto \operatorname{Gal} E/F$ di Ψ in Λ. Esse sono inverse l'una dell'altra e invertono l'ordine. Si ha*

$$|G| = [E : \operatorname{Inv} G]. \tag{12}$$

Se $F \in \Psi$ e K è un sottocampo di E contenente F, anche $K \in \Psi$. Inoltre $\operatorname{Gal} E/K$ *è un sottogruppo di* $\operatorname{Gal} E/F$ *ed è normale in* $\operatorname{Gal} E/F$ *se e solo se K è galoisiano su F. In tal caso*

$$\operatorname{Gal} K/F \cong (\operatorname{Gal} E/F)/(\operatorname{Gal} E/K). \tag{13}$$

Dimostrazione. È chiaro che $G \mapsto \operatorname{Inv} G$ e $F \mapsto \operatorname{Gal} E/F$ invertono l'ordine. Per definizione di Ψ, $G \mapsto \operatorname{Inv} G$ è suriettiva e, poiché $\operatorname{Gal}(E/\operatorname{Inv} G) = G$, è biiettiva con inversa $F \mapsto \operatorname{Gal} E/F$. La (9) coincide con la (12). Sia ora $F \in \Psi$ e sia K un sottocampo di E contenente F. Allora $F = \operatorname{Inv} G$ per un gruppo finito G di automorfismi di E. Poiché $K \supseteq F$, l'anello corrispondente $\operatorname{End}_K E$ nella corrispondenza di Jacobson–Bourbaki è un sottoanello di $\operatorname{End}_F E = EG$ contenente E_E. Per la proposizione 8.8 esso è della forma EH con H sottogruppo di G. Allora $K = \operatorname{Inv} H \in \Psi$. Per $s \in G$, il gruppo sHs^{-1} è un sottogruppo di G e $\operatorname{Inv}(sHs^{-1}) = s(K)$. Dunque H è normale in G se e solo se $s(K) = K$ per ogni $s \in G$. In questo caso la restrizione $\bar{s} = s|_K$ è un automorfismo di K. Queste restrizioni formano un gruppo finito $\overline{G}$ di automorfismi di K ed è chiaro che $F = \operatorname{Inv} \overline{G}$. Dunque, se H è normale in G, K è galoisiano su F. Inoltre $\overline{G} = \operatorname{Gal} K/F$ e $s \mapsto \bar{s}$ è un epimorfismo di G su $\overline{G}$, il cui nucleo è evidentemente $\operatorname{Gal} E/K$. Otteniamo così l'isomorfismo (13). Resta da mostrare che, se K è galoisiano su F, H è normale in G o, equivalentemente, $s(K) = K$ per ogni $s \in G$. Se $s(K) \neq K$, la restrizione $s|_K$ è un omomorfismo di K/F in E/F che non è un automorfismo di K/F. D'altra parte, l'ordine di $\operatorname{Gal} K/F$ è $[K : F]$. Avremmo così $[K : F]+1$ omomorfismi distinti di K/F in E/F, in contrasto con la proposizione 8.7. Ciò conclude la dimostrazione. □

Resta da determinare la struttura delle estensioni galoisiane di dimensione finita. Usiamo a tale scopo un importante complemento al teorema di isomorfismo dei campi di spezzamento, dato in BAI, p. 227: se E è un campo di spezzamento su F di un polinomio $f(x)$ a radici distinte, allora $|\operatorname{Gal} E/F| = [E : F]$. Si vede facilmente che si può sostituire all'ipotesi delle radici distinte la condizione che $f(x)$ sia *separabile*, ossia che i suoi fattori irriducibili abbiano radici distinte. Se $F' = \operatorname{Inv}(\operatorname{Gal} E/F)$, allora $F' \supseteq F$ e $[E : F'] = |\operatorname{Gal} E/F| = [E : F]$, da cui segue che $F = F'$ è galoisiano in E. Viceversa, sia E galoisiano di dimensione finita su F. Sia $a \in E$ e sia $\{a_1 = a, \ldots, a_r\}$ l'orbita di a sotto $G = \operatorname{Gal} E/F$. Allora il polinomio minimo di a su F è $g(x) = \prod_i (x - a_i)$, prodotto di fattori lineari distinti in E. Poiché E ha dimensione finita su F, è generato da un numero finito di elementi $a, b, \ldots$. È chiaro allora che E è un campo di

spezzamento su F del prodotto dei polinomi minimi di $a, b, \ldots$, e questo polinomio è separabile. Abbiamo dunque il seguente teorema.

Teorema 8.6. *E è galoisiano di dimensione finita su F se e solo se è un campo di spezzamento su F di un polinomio separabile $f(x) \in F[x]$.* (Si confronti il teorema 4.7 a p. 238 di BAI.)

I teoremi 8.5 e 8.6 danno il cosiddetto teorema fondamentale della teoria di Galois, ossia la corrispondenza tra i sottocampi di E/F e i sottogruppi di $G = \operatorname{Gal} E/F$ (BAI, p. 239).

Esercizi.

1. Sia E galoisiano su F (non necessariamente di dimensione finita) e sia K un sottocampo di E/F di dimensione finita su F. Mostrare che ogni isomorfismo di K/F in E/F si può estendere a un automorfismo di E.

2. Sia s un omomorfismo di anelli di K in E, cosicché $s \in \hom(K, E)$. Mostrare che Es è un sottomodulo di $\hom(K, E)$ come E-K-bimodulo. Mostrare che omomorfismi di anelli distinti di K in E danno così luogo a bimoduli non isomorfi e che ogni E-K-bimodulo di dimensione uno su E è isomorfo a un Es.

3. Servirsi della teoria dei moduli completamente riducibili per dimostrare che, se $s_1, \ldots, s_r$ sono omomorfismi di anelli distinti di K in E, ogni E-K-sottobimodulo di $\sum_{i=1}^{r} Es_i$ ha la forma $\sum_j Es_{i_j}$, dove $\{s_{i_j}\}$ è un sottoinsieme di $\{s_i\}$.

4. Sia $\overline{F}$ la chiusura algebrica di F e siano E e F' sottocampi di $\overline{F}/F$ di dimensione finita, con E galoisiano su F. Sia E' il sottocampo di $\overline{F}/F$ generato da E e F'. Mostrare che E' è galoisiano su F' e che $g' \mapsto g'|_E$ è un isomorfismo di $G' = \operatorname{Gal}(E'/F')$ sul sottogruppo $\operatorname{Gal}(E/(E \cap F'))$ di $G = \operatorname{Gal} E/F$ (si veda il lemma 4 a p. 254 di BAI). Mostrare che $E'/F' \cong E \otimes_{E \cap F'} F'$.

8.4 Prodotti incrociati e gruppo di Brauer

Facciamo ora una digressione nell'algebra non commutativa per presentare un'importante applicazione della teoria di Galois allo studio del gruppo di Brauer delle classi di similitudine delle algebre centrali semplici di dimensione finita su un campo F. Studieremo una costruzione di algebre centrali semplici, dette *prodotti incrociati*, definite mediante un'estensione galoisiana E e un sistema di fattori del gruppo di Galois nel gruppo moltiplicativo E^* degli elementi non nulli di E. Nel caso delle estensioni cicliche questi prodotti incrociati si chiamano *algebre cicliche*. Furono introdotte da Dickson nel 1906, a quanto pare ispirandosi a una precedente costruzione di algebre con divisione di dimensione infinita data da Hilbert nei suoi *Grundlagen der Geometrie* (1899). I prodotti incrociati più generali furono studiati da Dickson e dai suoi allievi negli anni Venti. La forma della teoria che esporremo è dovuta essenzialmente a Emmy Noether.

Partiamo da un'estensione galoisiana E/F di dimensione finita con gruppo di Galois G. Formiamo uno spazio vettoriale A su E con una base $\{u_s \mid s \in G\}$ in corrispondenza biunivoca con G. Gli elementi di A si scrivono quindi in uno e un solo modo nella forma $\sum_{s \in G} \rho_s u_s$, $\rho_s \in E$. Introdurremo in A una moltiplicazione che ne farà un'algebra su F. Le relazioni che definiscono questa moltiplicazione sono

$$u_s \rho = (s\rho) u_s, \qquad u_s u_t = k_{s,t} u_{st}, \tag{14}$$

dove i $k_{s,t}$ sono elementi non nulli di E e u_s indica $1u_s$. Più precisamente, definiamo il prodotto

in A mediante

$$\left(\sum_{s\in G}\rho_s u_s\right)\left(\sum_{t\in G}\sigma_t u_t\right)=\sum_{s,t}k_{s,t}\rho_s(s\sigma_t)u_{st}, \tag{15}$$

dove $k_{s,t}\in E^*$. In particolare $u_su_t=k_{s,t}u_{st}$ e dunque per ogni $s,t,v\in G$ abbiamo $(u_su_t)u_v=k_{s,t}u_{st}u_v=k_{s,t}k_{st,v}u_{stv}$ e $u_s(u_tu_v)=u_s(k_{t,v}u_{tv})=(sk_{t,v})k_{s,tv}u_{stv}$. Perché il prodotto (15) sia associativo occorre perciò che

$$k_{s,t}k_{st,v}=(sk_{t,v})k_{s,tv},\qquad s,t,v\in G. \tag{16}$$

Queste sono precisamente le condizioni perché l'applicazione $(s,t)\mapsto k_{s,t}$ di $G\times G$ nel gruppo moltiplicativo E^* sia un 2-cociclo (p. 361). L'azione di G su E^* è qui quella naturale, in cui $s\rho$ è l'immagine di ρ mediante $s\in G$. Come nel caso delle estensioni di gruppi, chiamiamo il 2-cociclo $k\colon (s,t)\mapsto k_{s,t}$ un *sistema di fattori* di G in E^*. Supporremo d'ora in avanti che i $k_{s,t}$ soddisfino (16), cosicché k sia un sistema di fattori. È allora immediato verificare che il prodotto (15) è associativo. Vale inoltre la distributività rispetto all'addizione. Le condizioni (16) implicano

$$k_{1,s}=k_{1,1},\qquad k_{s,1}=sk_{1,1}. \tag{17}$$

Da queste segue che

$$1=k_{1,1}^{-1}u_1 \tag{18}$$

è l'unità moltiplicativa di A. Infine, rispetto alla struttura di spazio vettoriale di A sul sottocampo F di E, valgono le condizioni di algebra

$$\alpha(ab)=(\alpha a)b=a(\alpha b) \tag{19}$$

per $\alpha\in F$, $a,b\in A$, che seguono direttamente da (15). Pertanto A è un'algebra su F. La chiamiamo *prodotto incrociato di E e G rispetto al sistema di fattori k* e scriviamo $A=(E,G,k)$ quando vogliamo esplicitare i dati della definizione.

Studiamo la struttura dei prodotti incrociati, cominciando dal seguente teorema.

Teorema 8.7. *$A=(E,G,k)$ è centrale semplice su F e $[A:F]=n^2$, dove $n=[E:F]$. Inoltre E (identificato con $E1$) è un sottocampo di A tale che $C_A(E)=E$.*

Dimostrazione. Per le dimensioni abbiamo $[A:F]=[A:E][E:F]=n^2$. Osserviamo poi che $u_su_{s^{-1}}=k_{s,s^{-1}}k_{1,1}1$ è un elemento non nullo di E e lo stesso vale per $u_{s^{-1}}u_s$, quindi u_s è invertibile in A. Sia ora B un ideale di A e scriviamo $\bar a=a+B$ per $a\in A$. Supponiamo $B\neq A$, cosicché $\overline{A}=A/B\neq 0$. Allora $\rho\mapsto\bar\rho$ è un monomorfismo di E in $\overline{A}$ e gli elementi $\bar u_s$ sono invertibili in $\overline{A}$. Abbiamo le relazioni $\bar u_s\bar\rho=\overline{s\rho}\,\bar u_s$. L'argomento di indipendenza di Dedekind sulle relazioni di lunghezza minima (BAI, p. 291) mostra che gli $\bar u_s$ sono linearmente indipendenti a sinistra su $\overline{E}=\{\bar\rho\mid\rho\in E\}$. Perciò $[\overline{A}:\overline{E}]=n$ e $[\overline{A}:\overline{E}][\overline{E}:\overline{F}]=n^2=[A:F]$. Ne segue che $B=0$ e A è semplice. Sia $\rho\in E$ e supponiamo che $\sum\rho_su_s$ commuti con ρ. Allora $\sum(\rho-s\rho)\rho_su_s=0$, da cui $\rho=s\rho$ per ogni s tale che $\rho_s\neq 0$. Se dunque $\sum\rho_su_s$ commuta con ogni $\rho\in E$, si ha $\rho_s=0$ per ogni $s\neq 1$, e quindi $\sum\rho_su_s=\rho_1u_1\in E$. Abbiamo così $C_A(E)=E$. Supponiamo ora che c appartenga al centro di A. Allora $c\in E=C_A(E)$ e $cu_s=u_sc$, da cui $sc=c$ per ogni $s\in G$. Dunque $c\in F$. Quindi il centro è F e A è centrale semplice su F. □

Il fatto che E sia un sottocampo di $A=(E,G,k)$ con $C_A(E)=E$ implica che E è un campo di spezzamento di A: $A_E=E\otimes_F A\cong M_n(E)$ (teorema 4.8, p. 221). Ricordiamo che le classi di similitudine $[A]$ delle algebre centrali semplici di dimensione finita su F che hanno una data estensione E di F come campo di spezzamento costituiscono un sottogruppo $\mathrm{Br}(E/F)$ del

gruppo di Brauer $\mathrm{Br}(F)$ del campo F (p. 228). Il risultato appena dimostrato implica che ogni sistema di fattori k di G in E^* determina un elemento $[(E,G,k)]$ di $\mathrm{Br}(E/F)$. Consideriamo ora l'elemento $[k] = kB^2(G,E^*)$ di $H^2(G,E^*) = Z^2(G,E^*)/B^2(G,E^*)$ (p. 361). Affermiamo che tutti i sistemi di fattori appartenenti a $[k]$ determinano lo stesso elemento di $\mathrm{Br}(E/F)$. Se $k' \in [k]$, valgono le relazioni

$$k'_{s,t} = \mu_s(s\mu_t)\mu_{st}^{-1}k_{s,t}, \qquad s,t \in G, \tag{20}$$

dove $\mu_s \in E^*$. Sia $A' = (E,G,k')$ il prodotto incrociato definito da k' e sia (u'_s) una base di A' tale che $u'_s\rho = (s\rho)u'_s$ e $u'_su'_t = k'_{s,t}u'_{st}$. Riprendiamo il prodotto incrociato $A = (E,G,k)$ con la base (u_s) su E scelta come sopra. Poniamo $v_s = \mu_s u_s$. È chiaro che i v_s formano una base di A su E. Inoltre $v_s\rho = \mu_s u_s\rho = \mu_s(s\rho)u_s = (s\rho)v_s$ e

$$v_sv_t = \mu_s u_s\mu_t u_t = \mu_s(s\mu_t)u_su_t = \mu_s(s\mu_t)k_{s,t}u_{st} = \mu_s(s\mu_t)k_{s,t}\mu_{st}^{-1}v_{st} = k'_{s,t}v_{st}.$$

Da queste relazioni è chiaro che $\sum \rho_s v_s \mapsto \sum \rho_s u'_s$ è un isomorfismo di A su A'. Dunque $A \cong A'$ e quindi $A \sim A'$, cioè $[A] = [A']$ nel gruppo di Brauer.

Possiamo ora definire un'applicazione

$$[k] \longmapsto [(E,G,k)] \tag{21}$$

di $H^2(G,E^*)$ in $\mathrm{Br}(E/F)$. Mostreremo che si tratta di un isomorfismo. Dimostriamo anzitutto la suriettività della (21) mediante il seguente teorema.

Teorema 8.8. *Sia A un'algebra centrale semplice di dimensione finita su F, che abbia come campo di spezzamento un'estensione galoisiana E/F di dimensione finita. Esiste un sistema di fattori k tale che $A \sim (E,G,k)$.*

Dimostrazione. Per il teorema di Wedderburn $A \cong M_r(\Delta)$ con Δ algebra centrale con divisione. E è un campo di spezzamento di A se e solo se lo è di Δ, e la condizione perché ciò accada è che esista un r' tale che E sia un sottocampo di $A' = M_{r'}(\Delta)$ con $C_{A'}(E) = E$ (teorema 4.8, p. 221). Per il teorema 4.11, $[A' : F] = [E : F][C_{A'}(E) : F] = n^2$. Evidentemente $A' \sim A$. Ricordiamo che, per il teorema 4.9 (p. 222), ogni F-automorfismo di E si può estendere a un automorfismo interno di A'. Dunque per ogni $s \in G$ esiste $u_s \in A'$ invertibile tale che $s\rho = u_s\rho u_s^{-1}$, $\rho \in E$. Sia ora $t \in G$. L'elemento $u_su_tu_{st}^{-1}$ commuta evidentemente con ogni $\rho \in E$. Allora $u_su_tu_{st}^{-1} = k_{s,t} \in E^*$ e $u_su_t = k_{s,t}u_{st}$. Le condizioni di associatività $(u_su_t)u_v = u_s(u_tu_v)$ implicano, come sopra, che $k\colon (s,t) \mapsto k_{s,t}$ è un sistema di fattori. Possiamo quindi formare il prodotto incrociato (E,G,k). È chiaro che $A'' = \{\sum \rho_s u_s \mid \rho_s \in E\}$ è una sottoalgebra di A'. Abbiamo un omomorfismo di (E,G,k) su questa sottoalgebra, che è un isomorfismo poiché (E,G,k) è semplice. Dunque $A'' \cong (E,G,k)$ e $[A'' : F] = n^2 = [A' : F]$, da cui $A'' = A'$. Così $A \sim A' \cong (E,G,k)$. □

Dimostriamo ora la seguente formula fondamentale di moltiplicazione dei prodotti incrociati.

Teorema 8.9. $(E,G,k) \otimes_F (E,G,l) \sim (E,G,kl)$.

Dimostrazione. Poniamo $A = (E,G,k)$, $B = (E,G,l)$. Nel considerare il prodotto tensoriale $A \otimes_F B$, possiamo supporre che A e B siano sottoalgebre di un'algebra AB nella quale ogni elemento di A commuta con ogni elemento di B. Inoltre, se $x_1,\dots,x_r \in A$ (rispettivamente in B) sono linearmente indipendenti su F, sono linearmente indipendenti su B (rispettivamente su A), nel senso che $\sum x_iy_i = 0$, con $y_i \in B$ (rispettivamente in A), solo se tutti gli y_i sono nulli. Distinguiamo le due copie di E contenute in A e B denotandole rispettivamente con E_1 ed E_2. Abbiamo un isomorfismo $\rho \mapsto \rho_i$ di E su E_i e scriviamo $s\rho_i$ per $(s\rho)_i$. Abbiamo una base (u_s) di A su E_1 e una base (v_s) di B su E_2 tali che

$$u_s\rho_1 = (s\rho_1)u_s, \quad u_su_t = (k_{s,t})_1u_{st}, \quad v_s\rho_2 = (s\rho_2)v_s, \quad v_sv_t = (l_{s,t})_2v_{st}.$$

Poiché E/F è separabile, ha un elemento primitivo: $E = F(\theta)$. Sia $f(\lambda)$ il polinomio minimo di θ su F. In $E[\lambda]$ si ha $f(\lambda) = \prod_{s\in G}(\lambda - s\theta)$ e quindi $f(\lambda) = \prod_s(\lambda - s\theta_1)$ e $f(\lambda) = \prod_s(\lambda - s\theta_2)$ rispettivamente in $E_1[\lambda]$ e $E_2[\lambda]$. Consideriamo in $E_1[\lambda]$ il polinomio di interpolazione di Lagrange

$$f_s(\lambda) = \frac{f(\lambda)}{(\lambda - s\theta_1)f'(s\theta_1)} = \frac{\prod_{t\neq s}(\lambda - t\theta_1)}{\prod_{t\neq s}(s\theta_1 - t\theta_1)}. \tag{22}$$

Poiché $1 - \sum_{s\in G} f_s(\lambda)$ ha grado $\leq n-1$ e si annulla negli n valori distinti $s\theta_1$, è identicamente nullo e

$$\sum_{s\in G} f_s(\lambda) = 1. \tag{23}$$

Inoltre, se $s \neq t$,

$$f_s(\lambda)f_t(\lambda) \equiv 0 \pmod{f(\lambda)}. \tag{24}$$

Consideriamo ora la sottoalgebra commutativa E_1E_2 di AB e poniamo

$$e_s = f_s(\theta_2) \in E_1E_2. \tag{25}$$

Allora $e_s \neq 0$, poiché $1, \theta_2, \ldots, \theta_2^{n-1}$ sono linearmente indipendenti su E_1. Per la (23) si ha $\sum_{s\in G} e_s = 1$ e per la (24) si ha $e_se_t = 0$ se $s \neq t$. Moltiplicando $\sum e_s = 1$ per e_t si ottiene $e_t^2 = e_t$. Abbiamo dunque

$$e_s^2 = e_s, \qquad e_se_t = 0 \text{ se } s \neq t, \qquad \sum_s e_s = 1. \tag{26}$$

La definizione di e_s dà $(\theta_2 - s\theta_1)e_s = 0$, poiché $(\theta_2 - s\theta_1)\prod_{t\neq s}(\theta_2 - t\theta_1) = f(\theta_2) = 0$. Per $\rho_2 \in E_2$ ne segue

$$\rho_2 e_s = (s\rho_1)e_s. \tag{27}$$

Dunque $E_1E_2 = \bigoplus_s E_1E_2e_s = \bigoplus_s E_1e_s$ e $E_1e_s \cong E$. Come abbiamo visto (p. 204), questa decomposizione di E_1E_2 in somma diretta di algebre semplici è unica.

Consideriamo ora gli automorfismi interni $x \mapsto u_txu_t^{-1}$ e $x \mapsto v_txv_t^{-1}$ di AB. Essi stabilizzano E_1E_2, quindi permutano le componenti semplici di E_1E_2 e, con esse, gli idempotenti e_s. Applicando questi automorfismi alle relazioni (27) e tenendo presente che il primo è l'identità su B e il secondo è l'identità su A, si ottiene

$$\rho_2(u_te_su_t^{-1}) = (ts\rho_1)(u_te_su_t^{-1}),$$
$$(t\rho_2)(v_te_sv_t^{-1}) = (s\rho_1)(v_te_sv_t^{-1}).$$

Dal confronto con la (27) segue

$$u_te_s = e_{ts}u_t, \qquad v_te_s = e_{st^{-1}}v_t. \tag{28}$$

Poniamo ora

$$e_{s,t} = e_su_su_t^{-1}. \tag{29}$$

Allora $e_{s,s} = e_s$ e dalla (28) si vede che gli n^2 elementi $e_{s,t}$ formano un sistema di unità matriciali:

$$e_{s,t}e_{s',t'} = \delta_{t,s'}e_{s,t'}, \qquad \sum_s e_{s,s} = 1. \tag{30}$$

Pertanto, per il teorema 4.6, $AB \cong M_n(C)$, dove C è il centralizzante in AB degli $e_{s,t}$. Si ha altresì $C \cong e_{1,1}ABe_{1,1}$ e passiamo a calcolare quest'algebra. Anzitutto $[AB : F] = n^4$, da cui $[C : F] = n^2$ e $[e_{1,1}ABe_{1,1} : F] = n^2$. Ora $e_{1,1}ABe_{1,1}$ contiene $E_1e_{1,1} = E_1e_1$ e, ponendo

$$w_s = u_s v_s e_{1,1}, \tag{31}$$

per la (28) abbiamo $w_s = e_{1,1}u_s v_s$, cosicché $w_s \in e_{1,1}ABe_{1,1}$. Si ha

$$w_s(\rho_1 e_{1,1}) = u_s v_s \rho_1 e_1 = (s\rho_1)u_s v_s e_1 = (s\rho_1)e_{1,1}w_s$$

e

$$\begin{aligned} w_s w_t &= u_s v_s u_t v_t e_1 = u_s u_t v_s v_t e_1 = (k_{s,t})_1 u_{st}(l_{s,t})_2 v_{st} e_1 \\ &= (k_{s,t})_1 (l_{s,t})_2 e_1 w_{st} = (k_{s,t})_1 (l_{s,t})_1 e_1 w_{st} \\ &= (k_{s,t} l_{s,t})_1 w_{st}. \end{aligned}$$

Ne segue che $e_{1,1}ABe_{1,1}$ contiene una sottoalgebra isomorfa a (E, G, kl). Dal confronto delle dimensioni segue $e_{1,1}ABe_{1,1} \cong (E, G, kl)$, quindi $(E, G, k) \otimes_F (E, G, l) \sim (E, G, kl)$. □

L'applicazione $[k] \mapsto [(E, G, k)]$ del gruppo $H^2(G, E^*)$ sul gruppo $\mathrm{Br}(E/F)$ è dunque moltiplicativa. Ne segue che $[1] \mapsto [1]$, cioè $(E, G, 1) \sim 1$. Per concludere la dimostrazione che $[k] \mapsto [(E, G, k)]$ è un isomorfismo ci occorre l'implicazione «solo se» del seguente teorema.

Teorema 8.10. *$(E, G, k) \sim 1$ se e solo se $k \sim 1$.*

Dimostrazione. Abbiamo visto che $k \sim 1$ implica $(E, G, k) \sim 1$. Viceversa, supponiamo $(E, G, k) \sim 1$. Abbiamo allora un isomorfismo $a \mapsto a'$ di $(E, G, 1)$ su (E, G, k). L'immagine E' di $E \subseteq (E, G, 1)$ è un sottocampo di (E, G, k) e per ogni $s \in G = \mathrm{Gal}\, E/F$ abbiamo un elemento invertibile $v'_s \in (E, G, k)$ tale che $v'_s\rho' = (s\rho)'v'_s$, $\rho \in E$, e $v'_s v'_t = v'_{st}$. L'isomorfismo $\rho' \mapsto \rho$ di E' su $E \subseteq (E, G, k)$ si può estendere a un automorfismo η di (E, G, k). Esso manda v'_s in un elemento v_s e valgono $v_s\rho = (s\rho)v_s$, $v_s v_t = v_{st}$. D'altra parte per ogni $s \in G$ abbiamo un u_s tale che $u_s\rho = (s\rho)u_s$ e $u_s u_t = k_{s,t}u_{st}$. Allora $u_s v_s^{-1}$ commuta con ogni $\rho \in E$, perciò $u_s v_s^{-1} = \mu_s \in E$ e $u_s = \mu_s v_s$. Ne segue $k_{s,t} = \mu_s(s\mu_t)\mu_{st}^{-1}$ e dunque $k \sim 1$. □

Riformuliamo il risultato principale ottenuto.

Teorema 8.11. *L'applicazione $[k] \mapsto [(E, G, k)]$ è un isomorfismo di $H^2(G, E^*)$ su $\mathrm{Br}(E/F)$.*

Nel teorema 6.14 (p. 361) abbiamo dimostrato che, se G è un gruppo finito e A un G-modulo, si ha $[k]^{|G|} = \{1\}$ per ogni $[k] \in H^n(G, A)$, $n > 0$. In particolare ciò vale per ogni $[k] \in H^2(G, E^*)$. Dal teorema 8.11 segue allora $(E, G, k)^{|G|} \sim 1$ per ogni prodotto incrociato. Possiamo migliorare questo risultato in modo importante. Scriviamo $A = (E, G, k) = M_r(\Delta)$ con Δ algebra con divisione. Abbiamo $[\Delta : F] = d^2$, $[A : F] = n^2 = r^2d^2$, perciò $n = rd$. L'intero d si chiama *indice* di Δ. Poiché Δ è determinata da A a meno di isomorfismi, possiamo anche chiamare d l'*indice di A*. Vale allora il teorema seguente.

Teorema 8.12. *Se d è l'indice di $A = (E, G, k)$, allora $A^d \sim 1$.*

Baseremo la dimostrazione sulle matrici di trasformazioni semilineari. Sia S una trasformazione s-semilineare di uno spazio vettoriale V di dimensione finita su un campo E: S è additiva e $S(\alpha x) = (s\alpha)(Sx)$ per $\alpha \in E$, $x \in V$. Sia $(x_1, \ldots, x_n)$ una base di V/E e scriviamo $Sx_i = \sum_{j=1}^n \sigma_{ji}x_j$. La matrice $\sigma = (\sigma_{ji})$ si chiama *matrice di S rispetto a $(x_1, \ldots, x_n)$*. La trasformazione è determinata da σ e s: se $x = \sum_i \xi_i x_i$, allora $Sx = \sum_{i,j}(s\xi_i)\sigma_{ji}x_j$. Se T è una trasformazione t-semilineare di matrice τ, si verifica subito che ST è st-semilineare e ha matrice $\sigma(s\tau)$, dove $s\tau = (s\tau_{ij})$.

Dimostrazione del teorema 8.12. Poiché $A = M_r(\Delta)$, possiamo identificare A con $\mathrm{End}_{\Delta'} V$, l'algebra delle trasformazioni lineari di uno spazio vettoriale V di dimensione r su $\Delta' = \Delta^{\mathrm{op}}$. Poiché $A = (E, G, k)$ contiene il sottocampo E, possiamo considerare V come spazio vettoriale

sia su E sia su F. Abbiamo $[V:F]=[V:E][E:F]=[V:E]n$ e $[V:F]=[V:\Delta'][\Delta':F]=rd^2=nd$. Perciò $[V:E]=d$. Sia (u_s) una base di $A=(E,G,k)$ su E tale che $u_s\rho=(s\rho)u_s$ e $u_su_t=k_{s,t}u_{st}$. La prima relazione mostra che l'elemento $u_s\in\operatorname{End}_{\Delta'}V$ è una trasformazione s-semilineare di V/E. Sia $(x_1,\dots,x_d)$ una base di V/E e sia $M(s)$ la matrice di u_s rispetto a essa. La relazione $u_su_t=k_{s,t}u_{st}$ dà allora la relazione matriciale

$$M(s)\,sM(t)=k_{s,t}M(st). \tag{32}$$

Prendendo i determinanti otteniamo

$$k_{s,t}^d\mu_{st}=(s\mu_t)\mu_s, \tag{33}$$

dove $\mu_s=\det M(s)$. Poiché $u_su_{s^{-1}}$ è un elemento non nullo di E, $M(s)\,sM(s^{-1})$ è una matrice scalare non nulla. Dunque $M(s)$ è invertibile e $\mu_s\neq 0$. Dalla (33) segue allora $k_{s,t}^d=(s\mu_t)\mu_s\mu_{st}^{-1}$, perciò $k^d\sim 1$. Per il teorema 8.11, $A^d\sim 1$. □

Rimane un'ultima questione riguardante $\operatorname{Br}(E/F)$ e $H^2(G,E^*)$. Supponiamo $E\supseteq L\supseteq F$, con L galoisiano su F, e sia $H=\operatorname{Gal}E/L$. Allora $H\triangleleft G$ e $\overline{G}=\operatorname{Gal}L/F\cong G/H$. Più precisamente, abbiamo l'omomorfismo canonico $s\mapsto\bar{s}=s|_L$ di G su $\overline{G}$ con nucleo H. Dunque $G/H\cong\overline{G}$ mediante $sH\mapsto\bar{s}$. Sia A' un'algebra centrale semplice di dimensione finita su F, spezzata da L. Allora A' è spezzata anche da E. Mediante l'isomorfismo del teorema 8.11, possiamo associare ad A' un elemento $[k']$ di $H^2(\overline{G},L^*)$ e un elemento $[k]$ di $H^2(G,E^*)$. Daremo una relazione esplicita tra $[k']$ e $[k]$: mostreremo che, se k' è $(\bar{s},\bar{t})\mapsto k'_{\bar{s},\bar{t}}\in L^*\subseteq E^*$, allora k è

$$(s,t)\longmapsto k'_{\bar{s},\bar{t}},$$

dove $s\mapsto\bar{s}$, $t\mapsto\bar{t}$ nell'omomorfismo canonico di G su $\overline{G}$. Per la definizione dell'isomorfismo tra $H^2(G,E^*)$ e $\operatorname{Br}(E/F)$ ciò è conseguenza immediata del teorema seguente.

Teorema 8.13 (H. Hasse). *Sia E galoisiano su F con gruppo di Galois G, sia L un sottocampo di E/F galoisiano su F e siano $H=\operatorname{Gal}E/L$, $\overline{G}=\operatorname{Gal}L/F$. Sia $A'=(L,\overline{G},k')$ un prodotto incrociato di L e $\overline{G}$ con sistema di fattori k'. Allora $A'\sim A=(E,G,k)$, dove $k_{s,t}=k'_{\bar{s},\bar{t}}$ e $s\mapsto\bar{s}$, $t\mapsto\bar{t}$ nell'omomorfismo canonico di G su $\overline{G}$.*

Dimostrazione (Artin, Nesbitt e Thrall). Formiamo $A=A'\otimes_F M_m(F)$, dove $m=[E:L]$. Evidentemente $A\sim A'$. Poiché L è una sottoalgebra di A', abbiamo in A la sottoalgebra $L\otimes_F M_m(F)\cong M_m(L)$.

Consideriamo E come spazio vettoriale su L e definiamo alcune trasformazioni semilineari di E/L. Anzitutto abbiamo le trasformazioni lineari $\rho_E\colon x\mapsto\rho x$ per $\rho\in E$. Abbiamo poi gli automorfismi $s\in G$. Poiché $s(\xi x)=(s\xi)(sx)=(\bar{s}\xi)(sx)$ per $\xi\in L$, $x\in E$, l'operatore s è una trasformazione $\bar{s}$-semilineare di E/L. Inoltre $s\rho_E=(s\rho)_Es$ (cfr. (6)). Scegliamo una base $(x_1,\dots,x_m)$ di E/L e consideriamo le matrici in $M_m(L)$ delle varie trasformazioni semilineari rispetto a questa base. Sia $\mu(\rho)$ la matrice di ρ_E rispetto a $(x_1,\dots,x_m)$. Allora $\rho\mapsto\mu(\rho)$ è un monomorfismo di E. L'insieme di matrici $\mu(E)$ è quindi un sottocampo di $M_m(L)/L$ isomorfo a E/L. Sia τ_s la matrice della trasformazione $\bar{s}$-semilineare s rispetto a $(x_1,\dots,x_m)$. Abbiamo la relazione matriciale

$$\tau_{st}=\tau_s(\bar{s}\tau_t) \tag{34}$$

e dalla relazione $s\rho_E=(s\rho)_Es$ otteniamo

$$\tau_s\,\bar{s}\mu(\rho)=\mu(s\rho)\tau_s. \tag{35}$$

Sia ora $(v_{\bar{s}})_{\bar{s}\in\overline{G}}$ una base di A' su L tale che $v_{\bar{s}}\xi = (\bar{s}\xi)v_{\bar{s}}$, $\xi \in L$, e $v_{\bar{s}}v_{\bar{t}} = k'_{\bar{s},\bar{t}}v_{\overline{st}}$. Poniamo $u_s = \tau_s v_{\bar{s}} \in A$, poiché $\tau_s \in M_m(L) \subseteq A$ e $A' \subseteq A$. Allora $u_s\mu(\rho) = \tau_s v_{\bar{s}}\mu(\rho) = \tau_s\,\bar{s}\mu(\rho)v_{\bar{s}} = \mu(s\rho)\tau_s v_{\bar{s}}$ per la (35). Dunque

$$u_s\mu(\rho) = \mu(s\rho)u_s. \tag{36}$$

Inoltre, per la (34),

$$\begin{aligned} u_s u_t &= \tau_s v_{\bar{s}}\tau_t v_{\bar{t}} = \tau_s(\bar{s}\tau_t)v_{\bar{s}}v_{\bar{t}} = \tau_{st}k'_{\bar{s},\bar{t}}v_{\overline{st}} \\ &= k'_{\bar{s},\bar{t}}\tau_{st}v_{\overline{st}} = \mu(k'_{\bar{s},\bar{t}})u_{st}. \end{aligned}$$

Pertanto

$$u_s u_t = \mu(k'_{\bar{s},\bar{t}})u_{st}. \tag{37}$$

Le (36) e (37) danno un omomorfismo in A di (E, G, k), dove $k_{s,t} = k'_{\bar{s},\bar{t}}$. Poiché (E, G, k) è semplice, si tratta di un monomorfismo. D'altra parte $[(E, G, k) : F] = [E : F]^2$ e $[A : F] = [L : F]^2 m^2 = [L : F]^2[E : L]^2 = [E : F]^2$. Abbiamo quindi $A \cong (E, G, k)$. □

Esercizi.

1. Mostrare che, se L è un sottocampo dell'estensione galoisiana E/F, vale $(E, G, k)_L \sim (E, H, k')$ su L, dove $H = \operatorname{Gal} E/L$ e k' si ottiene restringendo k a $H \times H$.[29]

2. Sia $\overline{F}$ la chiusura algebrica di F e siano E, F' sottocampi di $\overline{F}/F$ di dimensione finita, con E/F galoisiana. Sia E' il sottocampo di $\overline{F}/F$ generato da E e F'. Poniamo $G = \operatorname{Gal} E/F$, $G' = \operatorname{Gal} E'/F'$. Abbiamo quindi l'isomorfismo canonico $g' \mapsto g'|_E$ di G' su un sottogruppo di G (esercizio 4, p. 475). Mostrare che $(E, G, k)_{F'} \sim (E', G', k')$, dove k' si ottiene restringendo k a G' (identificato con il sottogruppo di G). *Suggerimento.* Considerare il caso $F' \cap E = F$. Combinarlo con l'esercizio 1 per ottenere il caso generale.

8.5 Algebre cicliche

Il tipo più semplice di prodotto incrociato $A = (E, G, k)$ è quello in cui E è un'estensione ciclica di F, ossia E è di Galois su F con gruppo di Galois ciclico G. Sia s un generatore di G e sia $u = u_s$. Allora $(u_{s^i})^{-1}u^i$ centralizza E, cosicché $u^i = \mu_i u_{s^i}$, con $\mu_i \in E^*$. Possiamo sostituire u_{s^i} con u^i, $0 \le i < n = [G : 1]$. Con tale sostituzione al sistema di fattori k subentra il sistema k' dato da

$$k'_{s^i,s^j} = \begin{cases} 1 & \text{se } 0 \le i + j < n, \\ \gamma & \text{se } n \le i + j \le 2n - 2. \end{cases} \tag{38}$$

Il prodotto incrociato A è generato da E e da u e ogni elemento di A si scrive in uno e un solo modo nella forma

$$\rho_0 + \rho_1 u + \cdots + \rho_{n-1}u^{n-1}, \qquad \rho_i \in E. \tag{39}$$

La moltiplicazione in A è determinata dalle relazioni

$$u\rho = (s\rho)u, \qquad u^n = \gamma. \tag{40}$$

[29] L'originale reca il segno di isomorfismo. In generale le dimensioni su L sono $[E : F]^2$ e $[E : L]^2$, rispettivamente. La relazione è la similitudine nel gruppo di Brauer e, più precisamente, $(E, G, k)_L \cong M_{[L:F]}((E, H, k'))$. [N.d.T.]

Poiché u^n commuta con u e con ogni elemento di E^*, u^n appartiene al centro F di A. Pertanto $\gamma \in F^*$. Indicheremo ora $A = (E, G, k)$ con (E, s, γ) e la chiameremo *algebra ciclica* definita da E/F, dal generatore s di G e da $\gamma \in F^*$.

Specializziamo i risultati su $\mathrm{Br}(E/F)$ per E/F di Galois al caso in cui E/F è ciclica. In questo caso basta considerare i sistemi di fattori della forma (38). Chiamiamo un tale sistema *sistema di fattori normalizzato definito da* γ. Si vede facilmente che il sistema di fattori normalizzato definito da γ e quello definito da $\delta \in F^*$ sono coomologhi se e soltanto se $\delta = \gamma N_{E/F}(\mu)$, con $\mu \in E^*$. Siamo così condotti a considerare il gruppo $F^*/N(E^*)$, dove F^* è il gruppo moltiplicativo degli elementi non nulli di F e $N(E^*)$ è il sottogruppo degli elementi della forma $N_{E/F}(\mu)$, $\mu \in E^*$. È allora chiaro che abbiamo un isomorfismo di $F^*/N(E^*)$ su $H^2(G, E^*)$ che manda un elemento $\gamma N(E^*)$ del primo gruppo nella classe in $H^2(G, E^*)$ del sistema di fattori normalizzato definito da γ. Tenendo conto dell'isomorfismo dato nel teorema 8.11, si ottiene nel caso ciclico il risultato seguente.

Teorema 8.14. *L'applicazione* $\gamma N(E^*) \mapsto [(E, s, \gamma)]$ *è un isomorfismo di* $F^*/N(E^*)$ *su* $\mathrm{Br}(E/F)$.

Si vede inoltre facilmente che il teorema 8.13 implica il risultato seguente per E/F ciclica.

Teorema 8.15. *Sia* E *un'estensione ciclica di* F *e sia* L *un campo intermedio di* E/F. *Sia* $\bar{s} = s|_L$, *dove* s *è un generatore del gruppo di Galois di* E/F. *Allora* $(L, \bar{s}, \gamma) \sim (E, s, \gamma^m)$, *con* $m = [E : L]$.

Lasciamo la dimostrazione al lettore.

Esercizi

1. Dimostrare che $(E, s, \gamma) \sim 1$ se e soltanto se γ è una norma da E, ossia esiste $c \in E$ tale che $\gamma = N_{E/F}(c)$.

2. Dimostrare che $(E, s, \gamma) \otimes_F (E, s, \delta) \sim (E, s, \gamma\delta)$.

3. (Wedderburn.) Dimostrare che (E, s, γ) è un'algebra di divisione se $n = [E : F]$ è il più piccolo intero positivo m tale che $\gamma^m = N_{E/F}(c)$ per qualche $c \in E$.

4. Sia E_0 un'estensione ciclica di F_0 di dimensione n. Per esempio si può prendere F_0 finito con q elementi ed $E_0 \supseteq F_0$ tale che $[E_0 : F_0] = n$. Sia s_0 un generatore del gruppo di Galois di E_0/F_0. Sia $E = E_0(t)$ il campo delle espressioni razionali su E_0 in un'indeterminata t e sia s l'automorfismo di E che estende s_0 e fissa t. Dimostrare che, posto $F = F_0(t)$, E/F è ciclica con gruppo di Galois $\langle s \rangle$. Dimostrare che (E, s, t) è un'algebra di divisione.

5. Specializzare l'esercizio 2 di p. 484 per mostrare che, con le notazioni di quell'esercizio, se E/F è ciclica e $G = \langle s \rangle$, allora $(E, s, \gamma)_{F'} \sim (E', s^m, \gamma)$, dove $G' = \langle s^m \rangle$ e si identifica il generatore con il corrispondente automorfismo di E'/F'.

8.6 Teoria di Galois infinita

In questo paragrafo estenderemo la corrispondenza fra sottocampi e sottogruppi della teoria di Galois finita a certe estensioni algebriche infinite di un campo.

Osserviamo anzitutto che, se E è algebrico su F, ogni omomorfismo s di E in sé che fissi gli elementi di F è un automorfismo di E/F. Poiché ogni omomorfismo di un campo in un anello non nullo è iniettivo, basta mostrare che s è suriettivo. A questo scopo sia $a \in E$ e sia $f(x)$ il polinomio minimo di a. Sia $R = \{a = a_1, \ldots, a_l\}$ l'insieme delle radici di $f(x)$ in E. Allora s

stabilizza R e, poiché $s|_R$ è iniettivo, $s|_R$ è suriettivo. Dunque $a = sa_j$ per qualche j. Usiamo questo risultato per dimostrare la seguente proposizione.

Proposizione 8.9. *Se E è algebrico su F, allora $G = \operatorname{Gal} E/F$ è un insieme chiuso nella topologia finita di E^E.*

Dimostrazione. Sia $s \in \bar{G}$, la chiusura di G in E^E. Dalla definizione della topologia è chiaro che s è un omomorfismo di E in sé che fissa gli elementi di F. Allora s è un automorfismo, quindi $s \in G$. □

Da questo risultato risulta che, se vogliamo una corrispondenza biunivoca fra gruppi di automorfismi e campi intermedi di un'estensione algebrica, dobbiamo limitarci ai sottogruppi chiusi di automorfismi. Il seguente esempio mostra che si tratta di una restrizione effettiva.

Esempio Sia $F_p = \mathbb{Z}/(p)$ il campo di p elementi e sia $\bar{F}_p$ la sua chiusura algebrica. Poiché $\bar{F}_p$ è algebrico su F_p, l'applicazione $\pi\colon a \mapsto a^p$ in $\bar{F}_p$ è un automorfismo. Mostreremo che $\langle\pi\rangle$ non è chiuso in $\operatorname{Gal} \bar{F}_p/F_p$. Dobbiamo richiamare alcuni fatti della teoria dei campi finiti (BAI, pp. 287–290). In primo luogo ogni campo finito di caratteristica p ha cardinalità p^n e per ogni p^n esiste un campo F_{p^n} con $|F_{p^n}| = p^n$. Questo è un campo di spezzamento su F_p di $x^{p^n} - x$ ed è unico a meno di isomorfismo. Inoltre ogni elemento di F_{p^n} è radice di questo polinomio. I sottocampi di F_{p^n} sono gli F_{p^m} con $m \mid n$. Poiché $\bar{F}_p$ è la chiusura algebrica di F_p, esso contiene ogni F_{p^n}. Da $F_{p^m} \cup F_{p^n} \subseteq F_{p^{mn}}$ è chiaro che ogni sottoinsieme finito di $\bar{F}_p$ è contenuto in uno dei sottocampi F_{p^n}. È anche chiaro che ogni automorfismo di $\bar{F}_p/F_p$ stabilizza ogni sottocampo finito F_{p^n}. Il gruppo di Galois di F_{p^n}/F_p è costituito dalle potenze dell'applicazione $a \mapsto a^p$. Ne segue che, se s è un qualunque automorfismo di $\bar{F}_p/F_p$, la sua restrizione a ciascun F_{p^n} coincide con la restrizione a F_{p^n} di un'opportuna potenza di π. Ciò implica che la chiusura $\overline{\langle\pi\rangle}$ contiene ogni automorfismo di $\bar{F}_p/F_p$. Poiché il gruppo di questi automorfismi è chiuso, $\overline{\langle\pi\rangle} = \operatorname{Gal} \bar{F}_p/F_p$.

Mostriamo ora che $\overline{\langle\pi\rangle} \neq \langle\pi\rangle$, costruendo un automorfismo di $\bar{F}_p/F_p$ che non sia una potenza di π. Scegliamo a questo scopo un qualunque sottocampo proprio infinito K di $\bar{F}_p$. Per esempio possiamo prendere un primo q e come K l'unione dei sottocampi F_{p^m} per $m = q^r$, $r = 1, 2, \ldots$. Poiché questa famiglia di sottocampi è totalmente ordinata, la sua unione è un sottocampo, ed è chiaro che si tratta di un sottocampo infinito di $\bar{F}_p$. Esso è inoltre proprio, poiché non contiene alcun F_{p^n} per cui n non sia una potenza di q. Sia dunque K un qualsiasi sottocampo proprio infinito di $\bar{F}_p$ e sia $a \in \bar{F}_p$, $a \notin K$. Sia $f(x)$ il polinomio minimo di a su K. Allora $\deg f(x) > 1$ e $f(x)$ ha in $\bar{F}_p$ una radice $b \neq a$. Poiché $\bar{F}_p$ è un campo di spezzamento, sia su $K(a)$ sia su $K(b)$, della famiglia di polinomi $\{x^{p^n} - x \mid n = 1, 2, \ldots\}$, dal teorema 8.2 segue che esiste un automorfismo s di $\bar{F}_p/K$ che manda a in b. Dunque $s \neq 1$ e il sottocampo degli elementi fissati da s contiene K, perciò è infinito. D'altra parte, per $k \geq 1$, l'insieme dei punti fissi di π^k è l'insieme finito delle soluzioni di $x^{p^k} = x$. Ne segue che $s \neq \pi^k$ per ogni intero k, e quindi $s \notin \langle\pi\rangle$.

La teoria di Galois infinita degli automorfismi dei campi riguarda i campi di spezzamento di polinomi separabili. Sia F un campo, sia Γ un insieme di polinomi monici separabili con coefficienti in F e sia E un campo di spezzamento di Γ su F. Abbiamo il seguente risultato.

Proposizione 8.10. *Ogni sottoinsieme finito di E è contenuto in un campo intermedio L/F che è un'estensione di Galois di dimensione finita di F.*

Dimostrazione. Sia Γ' l'insieme dei prodotti dei polinomi di Γ. Se $f \in \Gamma'$, il sottocampo L_f generato su F dalle radici di f in E è un campo di spezzamento di f su F. Per il teorema 8.6 è un'estensione di Galois di dimensione finita di F. Evidentemente $L_{fg} \supseteq L_f \cup L_g$. Quindi $E' = \bigcup_{f\in\Gamma'} L_f$ è un sottocampo di E e, poiché ogni $f \in \Gamma$ è prodotto di fattori lineari in $E'[x]$, si ha $E' = E$. Pertanto E è unione di estensioni di Galois di dimensione finita di F. Il risultato

ne segue immediatamente. □

Dimostriamo ora la seguente proposizione.

Proposizione 8.11. *Sia K un campo intermedio di E/F che sia di Galois su F. Allora ogni automorfismo di E/F stabilizza K. Inoltre l'applicazione $s \mapsto s|_K$ da $\operatorname{Gal} E/F$ in $\operatorname{Gal} K/F$ è suriettiva.*

Dimostrazione. Sia $a \in K$ e sia $f(x)$ il polinomio minimo di a su F. Se $s \in \operatorname{Gal} K/F$, allora $f(s(a)) = 0$, cosicché $s(a)$ è una delle radici, in numero finito, di $f(x)$ in E. L'orbita di a sotto $\operatorname{Gal} K/F$ è dunque un insieme finito $\{a = a_1, \dots, a_r\}$. Ne segue che $f(x) = \prod_{i=1}^{r}(x - a_i)$ e che, se $t \in \operatorname{Gal} E/F$, $t(a)$ è uno degli a_i. Dunque $t(a) \in K$. Ciò prova la prima affermazione. Per la seconda, osserviamo che E è un campo di spezzamento di Γ su K. Per il teorema 8.2, ogni automorfismo di K/F si può quindi estendere a un automorfismo di E/F. Ciò prova la seconda affermazione. □

Possiamo ora dimostrare il teorema fondamentale della teoria di Galois infinita.

Teorema 8.16 (Krull). *Sia E un campo di spezzamento su F di un insieme Γ di polinomi monici separabili e sia $G = \operatorname{Gal} E/F$. Sia Λ l'insieme dei sottogruppi chiusi di G e sia Σ l'insieme dei campi intermedi di E/F. Abbiamo allora le applicazioni $H \mapsto \operatorname{Inv} H$ di Λ in Σ e $K \mapsto \operatorname{Gal} E/K$ di Σ in Λ. Esse sono inverse l'una dell'altra e invertono l'ordine. Un sottogruppo $H \in \Lambda$ è normale in G se e soltanto se $K = \operatorname{Inv} H$ è di Galois su F e, in tal caso,* $\operatorname{Gal} K/F \cong (\operatorname{Gal} E/F)/(\operatorname{Gal} E/K)$.

Dimostrazione. È chiaro che, se $H \in \Lambda$, allora $\operatorname{Inv} H \in \Sigma$ e che, se $K \in \Sigma$, $\operatorname{Gal} E/K$ è chiuso e quindi appartiene a Λ. È anche chiaro che le applicazioni indicate invertono l'ordine. Sia ora $a \in E$, $a \notin F$, e sia L un sottocampo che contiene a ed è di Galois di dimensione finita su F. Esiste allora un automorfismo di L/F che non fissa a. Per la proposizione 8.11 esiste dunque un automorfismo di E/F che non fissa a. Ciò mostra che $\operatorname{Inv} G = F$. Potendo sostituire F con un qualunque campo intermedio K di E/F e G con $\operatorname{Gal} E/K$, vediamo che $\operatorname{Inv}(\operatorname{Gal} E/K) = K$. Sia ora H un sottogruppo chiuso e sia $K = \operatorname{Inv} H$. Sia L/K un sottocampo di E/K che sia di Galois di dimensione finita su K. Per la proposizione 8.11 (con K al posto di F e L al posto di K), $\operatorname{Gal} E/K$ e $H \subseteq \operatorname{Gal} E/K$ stabilizzano L, e le restrizioni a L degli $s \in \operatorname{Gal} E/K$ costituiscono $\operatorname{Gal} L/K$. L'insieme $\bar{H}$ delle restrizioni a L degli $h \in H$ costituisce un sottogruppo di $\operatorname{Gal} L/K$. Se questo sottogruppo fosse proprio, per la teoria di Galois finita esisterebbe $\xi \in L$, $\xi \notin K$, tale che $\bar{h}(\xi) = \xi$ per ogni $\bar{h} \in \bar{H}$. Ciò contraddice la definizione $K = \operatorname{Inv} H$. Dunque $\bar{H} = \operatorname{Gal} L/K$. Pertanto per ogni $s \in \operatorname{Gal} E/K$ esiste $h \in H$ tale che $s|_L = h|_L$. Per la proposizione 8.10 ciò implica che s appartiene alla chiusura di H. Quindi $s \in H$. Abbiamo così $\operatorname{Gal} E/\operatorname{Inv} H = H$. Ciò prova che le due applicazioni sono inverse.

Ora, se $K = \operatorname{Inv} H$ e $s \in G$, si ha $s(K) = \operatorname{Inv}(sHs^{-1})$. Ne segue che $H \triangleleft G$ se e soltanto se $s(K) = K$ per ogni $s \in G$. In tal caso K è di Galois su F, poiché gli automorfismi $s|_K$ formano un gruppo di automorfismi di K il cui campo degli elementi fissi è F. Come nella teoria di Galois finita ne segue che $\operatorname{Gal} K/F \cong (\operatorname{Gal} E/F)/(\operatorname{Gal} E/K)$. Infine, se K è un qualunque campo intermedio di E/F di Galois su F, ogni automorfismo di E/F stabilizza K, perciò $s(K) = K$ per $s \in G$. Allora $H = \operatorname{Gal} E/K$ è normale in G. □

Nelle applicazioni della teoria di Galois infinita è utile considerare la topologia del gruppo di Galois da un punto di vista un po' diverso, precisamente come quella di un limite inverso di gruppi finiti. Se L/F è un campo intermedio di E/F di Galois di dimensione finita su F, allora $H = \operatorname{Gal} E/L$ è un sottogruppo normale di indice finito in $G = \operatorname{Gal} E/F$, poiché $G/H \cong \operatorname{Gal} L/F$, che è un gruppo finito. Viceversa, ogni sottogruppo normale chiuso di indice finito si ottiene così.[30] La proposizione 8.10 mostra che E è l'unione dei sottocampi L tali che

[30] L'aggettivo «chiuso», sottinteso nel contesto del teorema di Krull, è necessario nella reciproca.

L/F sia di Galois di dimensione finita. Ne segue che $\bigcap H = 1$, con H che percorre la famiglia di tali sottogruppi normali di indice finito in G. Si vede facilmente che G è il limite inverso dei gruppi finiti G/H e che la topologia di G è quella del limite inverso di insiemi finiti. Da questo fatto, oppure mediante il teorema di Tychonoff, si vede facilmente anche che G è compatto.

Esercizi

1. Dimostrare le ultime due affermazioni del testo.
2. Sia F di Galois in E e si supponga che $\operatorname{Gal} E/F$ sia compatto. Dimostrare che E/F è algebrica e che E è un campo di spezzamento su F di un insieme di polinomi separabili. (Dunque il teorema di Krull è applicabile a E/F.)
3. Dimostrare che $\operatorname{Gal} \bar{F}_p/F_p$ non ha elementi di ordine finito diverso da 1.
4. Sia $E = F(t_1, t_2, \ldots)$ il campo delle frazioni di $F[t_1, t_2, \ldots]$, l'anello dei polinomi in un'infinità di indeterminate. Dimostrare che $\operatorname{Gal} E/F$ non è chiuso nella topologia finita.
5. Dimostrare che $\operatorname{Gal} \bar{F}_p/F_p \cong \operatorname{Gal} \bar{F}_q/F_q$ per ogni coppia di primi p, q.
6. Un *numero di Steinitz* è un prodotto formale $N = \prod_i p_i^{k_i}$ esteso a tutti i primi $p_i \in \mathbb{Z}$, dove $k_i = 0, 1, 2, \ldots$ oppure $k_i = \infty$. Se $M = \prod_i p_i^{l_i}$, scriviamo $M \mid N$ se $l_i \leq k_i$ per ogni i. Osservare che l'insieme dei numeri di Steinitz è un reticolo completo rispetto all'ordine parziale dato dalla divisibilità. Chiamiamo l'estremo superiore nel reticolo il *minimo comune multiplo* dei numeri di Steinitz. Se E è un sottocampo di $\bar{F}_p$, definiamo $\deg E$ come il numero di Steinitz che è il minimo comune multiplo dei gradi dei polinomi minimi su F_p degli elementi di E. Dimostrare che si ottiene così una corrispondenza biunivoca fra i sottocampi di $\bar{F}_p$ e i numeri di Steinitz.
7. Dimostrare che $\operatorname{Gal} \bar{F}_p/F_p$ non è numerabile.

8.7 Separabilità e normalità

Studieremo ora la struttura delle estensioni algebriche di un campo dato F. Gran parte delle considerazioni che seguono diventa banale in caratteristica zero, ma è importante per i campi di caratteristica prima. Operiamo in una chiusura algebrica $\bar{F}$ di F e ne consideriamo i sottocampi. Ciò equivale a considerare tutte le estensioni algebriche E di F, poiché ciascuna è isomorfa a un campo intermedio di $\bar{F}/F$. Sarà chiaro che quanto faremo è indipendente dall'immersione di E in $\bar{F}$, e nel seguito non vi richiameremo l'attenzione. Osserviamo inoltre che $\bar{F}$ è una chiusura algebrica di ogni suo campo intermedio E/F.

Sia Γ un insieme di polinomi monici con coefficienti in F e sia E il sottocampo di $\bar{F}/F$ generato dalle radici in $\bar{F}$ di tutti gli $f(x) \in \Gamma$. È chiaro che E è un campo di spezzamento su F dell'insieme Γ. È chiaro anche che ogni omomorfismo di E/F in $\bar{F}/F$ stabilizza l'insieme delle radici di ciascun $f(x)$ e quindi stabilizza E. Di conseguenza esso è un automorfismo di E/F. Diremo ora che un'estensione algebrica E/F è *normale* se ogni polinomio irriducibile di $F[x]$ che abbia una radice in E è prodotto di fattori lineari in $E[x]$. Dalla definizione è evidente che un'estensione normale è un campo di spezzamento, precisamente il campo di spezzamento su F dell'insieme dei polinomi minimi dei suoi elementi. Il risultato seguente fornisce perciò una caratterizzazione astratta dei campi di spezzamento come estensioni normali.

Teorema 8.17. *Se E è un campo di spezzamento su F di un insieme Γ di polinomi monici con coefficienti in F, allora E è normale su F.*

Dimostrazione. Sia $f(x) \in F[x]$ irriducibile e abbia una radice r in E. Si ha $f(x) = \prod_i (x - r_i)$ in $\bar{F}[x]$, con $r_1 = r$, e dobbiamo mostrare che ogni r_i appartiene a E (si prende f monico). Consideriamo $E(r_i)$. Questo campo contiene $F(r_i)$ ed è un campo di spezzamento di Γ su $F(r_i)$. Poiché r_1 e r_i, per ogni i, sono radici dello stesso polinomio irriducibile in $F[x]$, esiste un isomorfismo di $F(r)/F$ su $F(r_i)/F$ che manda r in r_i. Poiché $E(r)$ ed $E(r_i)$ sono campi di spezzamento di Γ rispettivamente su $F(r)$ e su $F(r_i)$, il teorema 8.2 mostra che esiste un isomorfismo di $E(r)$ su $E(r_i)$ che estende l'isomorfismo di $F(r)$ su $F(r_i)$. Poiché E è un campo di spezzamento di Γ su F, questo isomorfismo stabilizza E. Essendo $r \in E$, si ha $E(r) = E$. Dunque $E(r_i) = E$ e $r_i \in E$ per ogni i. □

Se E è un qualunque campo intermedio di $\bar{F}/F$, possiamo formare in $\bar{F}$ il campo di spezzamento N dell'insieme dei polinomi minimi degli elementi di E. Evidentemente $N \supseteq E$ e N è normale su F. È chiaro inoltre che N è il più piccolo sottocampo di $\bar{F}$ normale su F e contenente E. Chiamiamo N la *chiusura normale* di E.

Ricordiamo che un elemento algebrico si dice separabile se il suo polinomio minimo su F è separabile, e un'estensione algebrica E/F si dice separabile se ogni elemento di E è separabile (BAI, p. 238). Osserviamo che, se $a \in E$ è separabile su F, è separabile su ogni campo intermedio K, poiché il suo polinomio minimo su K è un fattore del polinomio minimo su F. Se E è algebrico e di Galois su F, allora è separabile e normale su F. Infatti, per $a \in E$ l'orbita sotto $\operatorname{Gal} E/F$ è finita e, se essa è $\{a_1 = a, a_2, \ldots, a_r\}$, il polinomio minimo di a su F è $\prod_{i=1}^{r}(x - a_i)$. Poiché questo è prodotto di fattori lineari distinti in $E[x]$, a è separabile. Dunque E è separabile e normale su F.

Sia ora $S\bar{F}$ il sottoinsieme degli elementi di $\bar{F}$ separabili su F. È chiaro che $S\bar{F}$ è contenuto nel campo di spezzamento su F di tutti i polinomi monici separabili di $F[x]$. Per il teorema 8.16, quest'ultimo campo è di Galois su F e quindi è separabile e normale su F. Allora $S\bar{F}$ contiene questo campo e coincide pertanto con il campo di spezzamento su F di tutti i polinomi monici separabili di $F[x]$. Chiamiamo $S\bar{F}$ la *chiusura algebrica separabile* di F.

Sia ora $a \in \bar{F}$ separabile su $S\bar{F}$ e sia $f(x)$ il suo polinomio minimo su $S\bar{F}$. Allora $f(x)$ ha radici distinte in $\bar{F}$ e quindi $(f(x), f'(x)) = 1$, dove $f'(x)$ è la derivata di $f(x)$ (BAI, p. 230). Facciamo agire $G = \operatorname{Gal} S\bar{F}/F$ su $f(x)$ nel modo ovvio. Otteniamo un numero finito di polinomi irriducibili distinti $f_i(x)$, $1 \leq i \leq r$, $f_1(x) = f(x)$, in $(S\bar{F})[x]$. Si ha $(f_i(x), f_i'(x)) = 1$ e $(f_i(x), f_j(x)) = 1$ per $i \neq j$. Allora $g(x) = \prod_{i=1}^{r} f_i(x) \in F[x]$ e $(g(x), g'(x)) = 1$, perciò $g(x)$ è separabile. Poiché $g(a) = 0$, vediamo che a è separabile su F, e quindi $a \in S\bar{F}$.

Possiamo usare questi risultati per dimostrare il seguente teorema.

Teorema 8.18. *Se E è un'estensione algebrica di F, gli elementi di E separabili su F formano un campo intermedio SE di E/F. Ogni elemento di E separabile su SE appartiene a SE.*

Dimostrazione. La prima affermazione è chiara, poiché $SE = S\bar{F} \cap E$. Anche la seconda è immediata: se $a \in E$ è separabile su SE, lo è su $S\bar{F} \supseteq SE$. Quindi $a \in S\bar{F} \cap E = SE$. □

Un'estensione algebrica E/F è *puramente inseparabile* su F se $SE = F$, e un elemento $a \in E$ è *puramente inseparabile* su F se $S(F(a)) = F$. La seconda parte dell'ultimo teorema mostra che E è puramente inseparabile su SE. Se la caratteristica è zero, E/F è puramente inseparabile se e soltanto se $E = F$ e a è puramente inseparabile se e soltanto se $a \in F$. Il caso interessante per queste considerazioni è quello della caratteristica $p \neq 0$. Per il resto del paragrafo supporremo di trovarci in questa situazione. Dedurremo alcuni criteri utili per stabilire se un elemento a sia separabile o puramente inseparabile. Dimostriamo dapprima la seguente proposizione.

Proposizione 8.12. *Se $a \in E$, allora a è separabile se e soltanto se $F(a) = F(a^p) = F(a^{p^2}) = \cdots$.*

Dimostrazione. Se a non è separabile, il suo polinomio minimo ha la forma $f(x) = g(x^p)$ (BAI,

p. 231). Allora $g(x)$ è irriducibile ed è quindi il polinomio minimo di a^p. Poiché $[F(a) : F] = \deg f(x)$ e $[F(a^p) : F] = \deg g(x)$, si ha $[F(a) : F(a^p)] = p$ e $F(a) \neq F(a^p)$. Supponiamo ora a separabile. Il polinomio minimo $f(x)$ di a su F ha radici distinte e perciò le ha anche il polinomio minimo $h(x)$ di a su $F(a^p)$. Ma a è radice di $x^p - a^p \in F(a^p)[x]$ e $x^p - a^p = (x-a)^p$. Allora $h(x) \mid x^p - a^p$ e, poiché $h(x)$ ha radici distinte, ne segue $h(x) = x - a$. Si ha dunque $a \in F(a^p)$. Elevando alla p-esima potenza vediamo che $a^p \in F(a^{p^2})$, quindi $a \in F(a^{p^2})$. Iterando si ottengono le relazioni richieste $F(a) = F(a^p) = F(a^{p^2}) = \cdots$. □

Dimostriamo ora il seguente criterio per gli elementi puramente inseparabili.

Proposizione 8.13. *Se a è puramente inseparabile su F, il suo polinomio minimo su F ha la forma $x^{p^e} - b$. Viceversa, se a è una radice di un polinomio della forma $x^{p^e} - b \in F[x]$, allora a è puramente inseparabile su F.*

Dimostrazione. Sia $f(x)$ il polinomio minimo di a e sia $e \geq 0$ il massimo intero tale che $f(x)$ sia un polinomio in x^{p^e}. Scriviamo $f(x) = g(x^{p^e})$, con $g(x) \in F[x]$. Allora $g(x)$ è irriducibile in $F[x]$ e non è un polinomio in x^p. Pertanto $g(x)$ è il polinomio minimo di $b = a^{p^e}$ e b è separabile su F. Inoltre $x^{p^e} - b$ è il polinomio minimo di a su $F(b)$. Dunque, se a è puramente inseparabile su F, si ha $b = a^{p^e} \in F$, $F(b) = F$ e $x^{p^e} - b$ è il polinomio minimo di a su F. Supponiamo ora che a sia radice di $x^{p^e} - b$ con $b \in F$. La formula per la potenza p^e-esima di una somma implica che ogni $c \in F(a)$ è radice di un polinomio della forma $x^{p^e} - d = (x-c)^{p^e}$ con $d \in F$. Il polinomio minimo di c su F ha dunque radici multiple, a meno che sia lineare. Se $c \in F(a)$ è separabile, si ha quindi $c \in F$. Pertanto a è puramente inseparabile. □

Esaminiamo ora più da vicino la struttura di un'estensione algebrica normale in caratteristica p. Sia E/F normale e sia $a \in E$. Scriviamo il polinomio minimo $f(x)$ di a su F nella forma $g(x^{p^e})$, con $g'(x) \neq 0$. Poiché $g(x)$ è irriducibile in $F[x]$ e ha la radice $a^{p^e} \in E$, si ha $g(x) = \prod_{i=1}^{r}(x - b_i)$ in $E[x]$, con $b_1 = a^{p^e}$. I b_i sono distinti poiché $g'(x) \neq 0$. Ora $f(x) = g(x^{p^e}) = \prod_i (x^{p^e} - b_i)$ è irriducibile in $F[x]$ e ha la radice a in E. Pertanto $f(x) = \prod_{j=1}^{rp^e}(x - a_j)$ in $E[x]$, con $a_1 = a$. Ne segue che ogni $x^{p^e} - b_i$ ha una radice in E, che possiamo supporre sia a_i. Allora $x^{p^e} - b_i = (x - a_i)^{p^e}$ e $f(x) = \prod_{i=1}^{r}(x - a_i)^{p^e} = h(x)^{p^e}$, dove $h(x) = \prod_{i=1}^{r}(x - a_i) \in E[x]$. La relazione $f(x) = h(x)^{p^e}$ mostra che i coefficienti di $h(x)$ soddisfano equazioni della forma $x^{p^e} = c \in F$. Essi sono quindi elementi puramente inseparabili di E. È ora chiaro che l'insieme degli elementi puramente inseparabili è un campo intermedio P/F e che i coefficienti di $h(x)$ appartengono a P. Inoltre a è radice di $h(x)$ e $h(x) = \prod_{i=1}^{r}(x - a_i)$ con gli a_i distinti. Dunque a è separabile su P. Poiché a era un elemento arbitrario di E, abbiamo dimostrato la seguente proposizione.

Proposizione 8.14. *Se E è normale su F, allora E è un'estensione separabile del suo sottocampo P degli elementi puramente inseparabili.*

Questo risultato mostra un fatto notevole. Si può ottenere ogni estensione algebrica effettuando prima un'estensione separabile e poi una puramente inseparabile, e per le estensioni normali è possibile invertire l'ordine. Determiniamo ora la struttura di tutte le estensioni che si possono costruire nel secondo modo.

Teorema 8.19. *(1) Se E è un'estensione algebrica di F tale che E sia separabile sul suo sottocampo P degli elementi puramente inseparabili, allora $E \cong P \otimes_F S$, dove S è il massimo sottocampo separabile di E su F. Viceversa, se P è un'estensione puramente inseparabile di F e S è un'estensione algebrica separabile di F, allora $P \otimes_F S$ è un'estensione algebrica di F il cui sottocampo degli elementi separabili è S e il cui sottocampo degli elementi puramente inseparabili è P.*

(2) Se E è algebrico e normale su F, allora $E \cong P \otimes_F S$ come in (1), con S di Galois su F. Viceversa, se P è puramente inseparabile su F e S è algebrico e di Galois su F, allora $P \otimes_F S$ è un'estensione algebrica normale di F.

Dimostrazione. (1) Supponiamo anzitutto $[E : F] < \infty$. Se a è un elemento qualsiasi di E e $f(x)$ è il suo polinomio minimo, abbiamo visto che $f(x) = g(x^{p^e})$, dove $g(x)$ è separabile. Allora $a^{p^e} \in S$. Ne segue che per ogni sottoinsieme finito $\{a_1, \dots, a_r\}$ di E esiste un e tale che $a_i^{p^e} \in S$ per ogni i. Poiché gli elementi che hanno questa proprietà formano un sottocampo e E è finitamente generato, esiste un e tale che $a^{p^e} \in S$ per ogni $a \in E$. Sia ora $(x_1, \dots, x_n)$ una base di E/P e scriviamo $x_i x_j = \sum_{k=1}^n c_{ijk} x_k$, con $c_{ijk} \in P$. Allora $y_i y_j = \sum_k d_{ijk} y_k$, dove $y_i = x_i^{p^e}$, $d_{ijk} = c_{ijk}^{p^e}$. Si ha $y_i \in S$ e $d_{ijk} \in S \cap P = F$. La tavola di moltiplicazione degli y_i mostra che $\sum_{i=1}^n F y_i$ è una F-sottoalgebra di E e $\sum_{i=1}^n P y_i$ è una P-sottoalgebra di E. Sia $a \in E$ e scriviamo $a = \sum_{i=1}^n a_i x_i$, con $a_i \in P$. Allora $a^{p^e} = \sum_i a_i^{p^e} y_i$. Poiché a è separabile su P, si ha $a \in P(a^{p^e}) = P[a^{p^e}]$. Ciò, insieme con la formula per a^{p^e}, implica $a \in \sum_i P y_i$, quindi gli y_i generano E come spazio vettoriale su P. Poiché il numero degli y_i è $n = [E : P]$, essi formano una base di E/P. Il ragionamento precedente mostra inoltre che, se $a \in S$, allora $a \in \sum_i F y_i$. Ne segue che $(y_1, \dots, y_n)$ è una base di S/F. L'esistenza di una famiglia di elementi che è simultaneamente una base di E/P e di S/F implica $E \cong P \otimes_F S$. Ciò prova la prima affermazione quando $[E : F] < \infty$.

Sia ora $[E : F]$ arbitrario. Sia L un campo intermedio di E/F di dimensione finita. Allora $S \cap L$ è il sottocampo degli elementi separabili di L e $P \cap L$ è quello degli elementi puramente inseparabili di L. Mostriamo che L si può immergere in un campo intermedio L' di dimensione finita tale che L' sia separabile su $P \cap L'$. Sia $L = F(a_1, \dots, a_r)$ e sia $f_i(x)$ un polinomio separabile con coefficienti in P avente a_i come radice. Siano $p_1, \dots, p_s$ i coefficienti di tutti gli $f_i(x)$ e poniamo $L' = F(a_1, \dots, a_r, p_1, \dots, p_s)$. Allora $L' = (L' \cap P)(a_1, \dots, a_r)$ e gli a_i sono separabili su $L' \cap P$. Quindi ogni elemento di L' è separabile su $L' \cap P$, e L' soddisfa così la condizione iniziale. Per completare la dimostrazione dobbiamo mostrare che ogni elemento di E è combinazione lineare di elementi di S con coefficienti in P e che elementi di S linearmente indipendenti su F sono linearmente indipendenti su P. Poiché ogni insieme finito di elementi si può immergere in un campo intermedio L' di dimensione finita che soddisfa le condizioni, entrambi i fatti risultano dalla prima parte. È così dimostrata la prima affermazione di (1).

Viceversa, sia $E = P \otimes_F S$, dove P è puramente inseparabile e S è un'estensione algebrica separabile di F. Sia (x_α) una base di S/F. Affermiamo che, per ogni $e \geq 0$, anche $(x_\alpha^{p^e})$ è una base di S/F. Il ragionamento è simile a quello usato sopra. Sia $a \in S$ e scriviamo $a = \sum_\alpha a_\alpha x_\alpha$, con $a_\alpha \in F$. Allora $a^{p^e} = \sum_\alpha a_\alpha^{p^e} x_\alpha^{p^e} \in \sum_\alpha F x_\alpha^{p^e}$, che è un'algebra su F. Poiché $a \in F[a^{p^e}]$, si ha $a \in \sum_\alpha F x_\alpha^{p^e}$, perciò ogni a è combinazione lineare degli $x_\alpha^{p^e}$. Per dimostrarne l'indipendenza lineare basta prendere un sottoinsieme finito della base originaria, diciamo $\{x_1, \dots, x_n\}$. Il sottocampo $F(x_1, \dots, x_n)$ è separabile di dimensione finita su F e ha una base $(x_1, \dots, x_n, y_1, \dots, y_m)$. Gli elementi $x_1^{p^e}, \dots, x_n^{p^e}, y_1^{p^e}, \dots, y_m^{p^e}$ generano allora $F(x_1, \dots, x_n)$ come spazio vettoriale su F. Poiché il loro numero è la dimensione, sono linearmente indipendenti su F. Dunque $\{x_1^{p^e}, \dots, x_n^{p^e}\}$ è un insieme linearmente indipendente.

Poiché gli x_α formano una base di S/F, ogni elemento di $P \otimes_F S$ si scrive in uno e un solo modo nella forma $\sum_\alpha b_\alpha \otimes x_\alpha$, con $b_\alpha \in P$. Esiste $e \geq 0$ tale che tutti i $b_\alpha^{p^e}$ appartengano a F. Quindi

$$\Big(\sum_\alpha b_\alpha \otimes x_\alpha\Big)^{p^e} = \sum_\alpha b_\alpha^{p^e} \otimes x_\alpha^{p^e} = 1 \otimes \sum_\alpha b_\alpha^{p^e} x_\alpha^{p^e} \in S.$$

Se $\sum_\alpha b_\alpha \otimes x_\alpha \neq 0$, qualche b_α è diverso da zero. Allora $b_\alpha^{p^e} \neq 0$ e $\sum_\alpha b_\alpha^{p^e} x_\alpha^{p^e} \neq 0$. Poiché S è un campo, questo elemento ha inverso in S e quindi $\sum_\alpha b_\alpha \otimes x_\alpha$ è invertibile. Ciò prova che $P \otimes_F S$ è un campo. È chiaro che P è un sottocampo puramente inseparabile, S un sottocampo algebrico separabile di E, ed $E = P \otimes_F S = P(S)$. Dunque E è generato su P da elementi algebrici separabili, perciò è algebrico separabile su P. Allora, per il risultato dimostrato per primo, $E = P' \otimes_F S'$, dove P' è il sottocampo degli elementi puramente inseparabili e S' quello

degli elementi separabili. Si ha $P' \supseteq P$, $S' \supseteq S$ e, poiché $E = P \otimes_F S$, segue $P' = P$ e $S' = S$. Ciò conclude la dimostrazione di (1).

(2) Se E è normale su F, per la proposizione 8.14 è separabile sul proprio sottocampo degli elementi puramente inseparabili. Dunque $E = S \otimes_F P$ come in (1). Sia $a \in S$ con polinomio minimo $f(x)$. Allora $f(x)$ è separabile e $f(x) = \prod_{i=1}^{r}(x - a_i)$ in $E[x]$, con $a_1 = a$. Poiché S è l'insieme degli elementi separabili di E, ogni a_i appartiene a S. Ciò implica che S è un campo di spezzamento su F di un insieme di polinomi separabili, perciò S è di Galois su F per il teorema 8.16. Viceversa, supponiamo $E = S \otimes_F P$, dove S è algebrico e di Galois su F e P è puramente inseparabile. Abbiamo mostrato in (1) che E è un campo algebrico su F. È chiaro che ogni automorfismo di S/F ha un'unica estensione a un automorfismo di E/P, e ciò implica che E è di Galois su P. Sia $a \in E$ e siano $f(x) \in F[x]$, $h(x) \in P[x]$ i polinomi minimi di a su F e su P, rispettivamente. Allora $h(x)^{p^e} \in F[x]$ per un opportuno e, e per un'opportuna scelta di e si ha $f(x) = h(x)^{p^e}$. Poiché E è di Galois su P, $h(x)$ è prodotto di fattori lineari in $E[x]$. Lo stesso vale quindi per $f(x)$. Pertanto E è normale su F. □

Questi risultati si applicano in particolare alla chiusura algebrica $\bar{F}$ di F. Si ha $\bar{F} = S\bar{F} \otimes_F P\bar{F}$, dove $S\bar{F}$ è il sottocampo di $\bar{F}$ degli elementi separabili e $P\bar{F}$ è il sottocampo degli elementi puramente inseparabili. Il campo $S\bar{F}$ è di Galois su F e lo abbiamo chiamato chiusura algebrica separabile di F. Ricordiamo che un campo si dice *perfetto* se ogni polinomio irriducibile a coefficienti nel campo è separabile (BAI, p. 226). In caratteristica zero ciò avviene sempre e in caratteristica p avviene se e soltanto se ogni elemento del campo è una potenza p-esima. Si vede facilmente che $P\bar{F}$ è perfetto e che è contenuto in ogni estensione perfetta di F. Per questa ragione $P\bar{F}$ si chiama *chiusura perfetta* di F.

Esercizi

1. Sia E/F algebrica e sia $K = F(x_1, \ldots, x_r)$ il campo delle frazioni di $F[x_1, \ldots, x_r]$, con le x_i indeterminate. Dimostrare che $E \otimes_F K \cong E(x_1, \ldots, x_r)$ e che quindi $E \otimes_F K$ è un campo.

2. Dimostrare che $F(x) \otimes_F F(y)$ non è un campo se x e y sono trascendenti.

3. Dimostrare che, se E/F contiene un elemento puramente inseparabile che non appartiene a F, $E \otimes_F E$ ha un elemento nilpotente non nullo.

4. (J. D. Reid.) Supponiamo che F_0 non sia perfetto e che $\operatorname{char} F_0 = p$. Sia $a \in F_0$, $a \notin F_0^p$ (il sottocampo delle potenze p-esime). Sia $E = F_0(x)$, con x trascendente su F_0. Poniamo $y = x^{p^2}(x^p + a)^{-1}$ e $F = F_0(y)$. Dimostrare che E non è separabile su F e che $P(E/F)$, il sottocampo di E degli elementi puramente inseparabili su F, è F.

5. Siano E e F come nell'esercizio 4. Dimostrare che $E \otimes_F E$ contiene elementi nilpotenti non nulli.

6. Se E è un'estensione di dimensione finita di F e $S = SE$ è il sottocampo degli elementi separabili, poniamo $[E : F]_s = [S : F]$ e $[E : F]_i = [E : S]$. Questi si chiamano rispettivamente *grado di separabilità* e *grado di inseparabilità* di E/F. Evidentemente $[E : F] = [E : F]_s[E : F]_i$. Dimostrare che, se K è separabile di dimensione finita su E, allora $[K : F]_s = [K : E]_s[E : F]_s$. Dimostrare che ciò vale anche se K è puramente inseparabile su E. Dimostrare infine che, per estensioni arbitrarie di dimensione finita nella torre $F \subseteq E \subseteq K$, si ha $[K : F]_s = [K : E]_s[E : F]_s$ e $[K : F]_i = [K : E]_i[E : F]_i$.[31]

[31] Nella prima delle ultime due uguaglianze l'originale omette il fattore $[E : F]_s$ che figurava nella formula immediatamente precedente.

7. Dimostrare che un'estensione algebrica di un campo perfetto è perfetta.

8. Sia P puramente inseparabile su F. Diciamo che P/F ha *esponente* $e \geq 0$ se e è il minimo intero tale che $a^{p^e} \in F$ per ogni $a \in P$, ossia, se $e > 0$, esiste a tale che $a^{p^{e-1}} \notin F$. Dimostrare che P/F ha un esponente se $[P : F] < \infty$ e che, se P/F ha esponente e,

$$P = P^{(0)} \supsetneq P^{(1)} \supsetneq \cdots \supsetneq P^{(e)} = F,$$

dove $P^{(i)} = F(P^{p^i})$. Dimostrare che $P^{(i-1)}/P^{(i)}$ è puramente inseparabile di esponente uno.

9. Sia P/F un'estensione puramente inseparabile di dimensione finita, di caratteristica p. Dimostrare che, se $P \neq F$, esiste un campo intermedio Q/F tale che $[P : Q] = p$.

10. Sia $P = F(a)$, dove $\operatorname{char} F = p$ e a è algebrico con polinomio minimo $\lambda^{p^e} - \alpha$ su F. Determinare tutti i campi intermedi di P/F.

8.8 Campi di spezzamento separabili

Proveremo ora l'esistenza di un campo di spezzamento separabile per ogni algebra centrale semplice A/F di dimensione finita. Potremo così estendere i risultati sul gruppo di Brauer ottenuti nel ğ 8.4 e renderli applicabili a tutte le algebre centrali semplici di dimensione finita. Ne dedurremo che, per ogni campo F, il gruppo di Brauer $\operatorname{Br}(F)$ è un gruppo di torsione.

Il teorema che vogliamo dimostrare è il seguente.

Teorema 8.20. *Se A è centrale semplice di dimensione finita su F, esiste un'estensione separabile di dimensione finita S/F che è un campo di spezzamento per A.*

Basta dimostrarlo per $A = \Delta$ algebra di divisione. In tal caso il risultato seguirà dal corollario al teorema 4.7 se mostreremo che Δ contiene un sottocampo massimale separabile. A questo scopo ci occorrono alcune osservazioni sulle derivazioni di algebre.

Osserviamo che, se A è un'algebra qualsiasi e $d \in A$, l'applicazione $D_d \colon x \mapsto [d, x] = dx - xd$ è una derivazione. È chiaro che D_d è lineare e il calcolo

$$\begin{aligned}[d, x]y + x[d, y] &= dxy - xdy + xdy - xyd \\ &= dxy - xyd = [d, xy]\end{aligned}$$

mostra che $D_d(xy) = (D_d x)y + x(D_d y)$. Chiamiamo D_d la *derivazione interna* determinata da d. Evidentemente vale la relazione $D_d = d_L - d_R$, dove d_L e d_R sono le moltiplicazioni a sinistra e a destra determinate da d. Poiché d_L e d_R commutano, abbiamo

$$D_d^k = (d_L - d_R)^k = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} d_L^i d_R^{k-i}.$$

Se la caratteristica è p, ciò dà $D_d^p = (d^p)_L - (d^p)_R = D_{d^p}$. Possiamo scrivere questa relazione nella forma

$$\underbrace{[d, [d, \ldots, [d}_{p \text{ volte}}, x] \ldots]] = [d^p, x]. \tag{41}$$

Siamo ora in grado di dimostrare il seguente teorema.

Teorema 8.21. *Ogni algebra di divisione centrale Δ/F di dimensione finita contiene un sottocampo massimale S separabile su F.*

Dimostrazione. Se $\Delta = F$ non vi è nulla da provare, perciò supponiamo $\Delta \supsetneq F$. Mostreremo dapprima che Δ contiene un elemento $a \notin F$ separabile su F. Scegliamo un qualunque $a \in \Delta$, $a \notin F$. Se $F(a)$ non è puramente inseparabile, contiene un elemento separabile che non appartiene a F, come volevamo. Supponiamo allora $F(a)$ puramente inseparabile. La caratteristica è p e il polinomio minimo di a su F ha la forma $x^{p^e} - \alpha$. Poniamo $d = a^{p^{e-1}}$. Abbiamo $d \notin F$ ma $d^p \in F$. Allora la derivazione interna D_d è diversa da zero, ma $D_d^p = D_{d^p} = 0$. Possiamo dunque scegliere $a \in \Delta$ tale che $[d, a] = b \neq 0$ e $[d, b] = 0$. Poniamo $c = ab^{-1}d$. Allora

$$D_d c = (D_d a)b^{-1}d = d.$$

Quindi $[d, c] = dc - cd = d$ e $dcd^{-1} = c + 1$. Vediamo ora che il sottocampo $F(c)/F$ ammette un automorfismo non banale, precisamente la restrizione a $F(c)$ dell'automorfismo interno $x \mapsto dxd^{-1}$. Si vede facilmente che, se E/F è puramente inseparabile, il solo automorfismo di E/F è l'identità. Dunque $F(c)$ non è puramente inseparabile. Vi è quindi in $F(c)$ un elemento separabile che non appartiene a F. In ogni caso esiste dunque un $a \notin F$ separabile su F.

Completeremo la dimostrazione mostrando che ogni sottocampo separabile massimale S di Δ è un sottocampo massimale di Δ. In caso contrario $\Delta' = C_\Delta(S) \supsetneq S$. Per il teorema del doppio centralizzante (teorema 4.10, p. 224), S è il centro di Δ', perciò Δ' è un'algebra di divisione centrale su S con $[\Delta' : S] \neq 1$. Per la prima parte della dimostrazione, abbiamo un sottocampo $S(a) \neq S$ che è separabile su S. Questo contraddice la massimalità di S come sottocampo separabile di Δ, poiché $S(a)$ è separabile su F. □

Come abbiamo visto, il teorema 8.21 implica il teorema 8.20.

Sia ora S un campo di spezzamento separabile di dimensione finita per A e sia E la chiusura normale di S. Allora E/F è un'estensione di Galois di dimensione finita. Poiché ogni estensione di un campo di spezzamento è un campo di spezzamento, E/F è un campo di spezzamento per A. Sia Δ l'algebra di divisione associata ad A dal teorema di Wedderburn e sia d il suo indice. Allora, per il teorema 8.12, $A^d \sim 1$. Ne segue evidentemente il teorema seguente.

Teorema 8.22. *Per ogni campo F,* $\mathrm{Br}(F)$ *è un gruppo di torsione.*

L'ordine di $\{A\}$ in $\mathrm{Br}(F)$ è detto *esponente* dell'algebra centrale semplice A. Poiché $\{A\}^d = 1$ per l'indice d di A, vediamo che l'esponente e di A è un divisore del suo indice.

Esercizi

1. Sia p un divisore primo dell'indice d di un'algebra centrale semplice A. Dimostrare che p divide l'esponente e di A. *Suggerimento.* Sia E un campo di spezzamento di Galois di A e sia $[E : F] = m$. Allora $d \mid m$, quindi $p \mid m$. Per la teoria di Galois e il teorema di Sylow esiste un campo intermedio K di E/F tale che $[E : K] = p^l$, dove p^l è la massima potenza di p che divide m. Sia e' l'esponente di $A' = A_K$ in $\mathrm{Br}(K)$. Dimostrare che $e' \mid e$ e che e' è una potenza di p diversa da 1.

2. Dimostrare che, se Δ è un'algebra di divisione centrale di grado $d = p_1^{l_1} \cdots p_r^{l_r}$, con $l_i > 0$ e p_i primi distinti, allora $\Delta \cong \Delta_1 \otimes \cdots \otimes \Delta_r$, dove il grado di Δ_i è $p_i^{l_i}$. (Il grado è la radice quadrata della dimensione. Per la dimostrazione occorre l'esercizio 9 di p. 226.)

8.9 Estensioni di Kummer

Ricordiamo che un'estensione E/F di dimensione finita si dice *abeliana* se E è di Galois su F e il gruppo di Galois G di E/F è abeliano. La stessa terminologia si può usare per estensioni di dimensione infinita, ma ci limiteremo al caso di dimensione finita. In questo paragrafo e nel

ğ 8.11 studieremo due tipi di estensioni abeliane di particolare interesse perché ammettono una trattazione puramente algebrica e piuttosto elementare.

Se G è un gruppo abeliano finito, il minimo comune multiplo e degli ordini dei suoi elementi si chiama *esponente* di G. Evidentemente $e \mid |G|$. In questo paragrafo considereremo un campo base F che, dato un intero positivo m, contiene m radici m-esime distinte dell'unità. Descriveremo le estensioni abeliane i cui gruppi di Galois hanno esponente $m' \mid m$. Le chiameremo *m-estensioni di Kummer* di F.

L'ipotesi che F contenga m radici m-esime distinte di 1, o equivalentemente che $x^m - 1 = \prod_{i=1}^{m}(x - \zeta_i)$ in $F[x]$ con le ζ_i distinte, implica che la caratteristica di F non divide m. L'insieme $U(m) = \{\zeta_i \mid 1 \le i \le m\}$ è un sottogruppo del gruppo moltiplicativo F^* di F, e $U(m) \supseteq U(m')$ per ogni $m' \mid m$. Osserviamo inoltre che, se G è un gruppo abeliano finito di esponente $m' \mid m$, il gruppo dei caratteri $\widehat{G}$ di G può essere identificato con $\hom(G, U(m))$, il gruppo degli omomorfismi di G in $U(m)$. Infatti, per definizione $\widehat{G}$ è il gruppo degli omomorfismi di G nel gruppo moltiplicativo dei numeri complessi. Per $\chi \in \widehat{G}$ e $g \in G$ si ha quindi $\chi(g)^m = \chi(g^m) = \chi(1) = 1$. Dunque $\chi(g)$ appartiene al gruppo delle radici m-esime complesse di 1, che si può identificare con $U(m)$. Possiamo pertanto identificare $\widehat{G}$ con $\hom(G, U(m))$. Ricordiamo che $|\widehat{G}| = |G|$ (p. 281). Ci serviranno alcune importanti conseguenze di questo fatto, che raccogliamo nel lemma seguente.

Lemma. *Sia G un gruppo abeliano finito e sia $\widehat{G}$ il suo gruppo dei caratteri.*

1. *Per ogni $s \neq 1$ in G esiste $\chi \in \widehat{G}$ tale che $\chi(s) \neq 1$.*
2. *Per ogni $s \in G$, indichiamo con $\hat{s}$ l'applicazione $\chi \mapsto \chi(s)$ di $\widehat{G}$ in $\mathbb{C}^*$ (o in $U(m)$, con m esponente di G). Allora $\hat{s} \in \widehat{\widehat{G}}$ e $s \mapsto \hat{s}$ è un isomorfismo di G su $\widehat{\widehat{G}}$.*
3. *Un insieme $\{\chi_1, \chi_2, \ldots, \chi_r\}$ di caratteri genera $\widehat{G}$ se e solo se l'unico $s \in G$ tale che $\chi_i(s) = 1$ per $1 \le i \le r$ è $s = 1$.*

Dimostrazione. (1) Sia $H = \{s \mid \chi(s) = 1 \text{ per ogni } \chi \in \widehat{G}\}$. Allora H è un sottogruppo e (1) seguirà se mostriamo che $H = 1$. Sia $\bar{G} = G/H$. Ogni $\chi \in \widehat{G}$ definisce un carattere $\bar{\chi}$ su $\bar{G}$ mediante $\bar{\chi}(gH) = \chi(g)$, e $\chi \mapsto \bar{\chi}$ è un monomorfismo di $\widehat{G}$ in $\widehat{\bar{G}}$. Poiché $|\widehat{G}| = |G|$ e $|\widehat{\bar{G}}| = |\bar{G}|$, ne segue $|G| \le |\bar{G}|$. Dunque $|G| = |\bar{G}|$ e $H = 1$.

(2) È chiaro che $\hat{s} \in \widehat{\widehat{G}}$ e che $s \mapsto \hat{s}$ è un omomorfismo. Se $\hat{s} = 1$, si ha $\chi(s) = 1$ per ogni $\chi \in \widehat{G}$, onde $s = 1$ per (1). Quindi $s \mapsto \hat{s}$ è un monomorfismo. Poiché $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$, si tratta di un isomorfismo.

(3) Per (2) possiamo considerare G come il gruppo dei caratteri di $\widehat{G}$. L'asserzione (3) equivale dunque alla seguente. Gli elementi $\{s_1, \ldots, s_r\}$ generano G se e solo se l'unico $\chi \in \widehat{G}$ tale che $\chi(s_i) = 1$, $1 \le i \le r$, è $\chi = 1$. Se gli s_i generano G, da $\chi(s_i) = 1$ per ogni i segue $\chi(s) = 1$ per ogni s, onde $\chi = 1$. Se invece il sottogruppo $H = \langle s_1, \ldots, s_r \rangle$ è diverso da G, allora $\bar{G} = G/H \neq 1$ e su $\bar{G}$ vi è un carattere $\bar{\chi} \neq 1$. Esso definisce su G un carattere χ mediante $\chi(g) = \bar{\chi}(gH)$, con $\chi(s_i) = 1$ per $1 \le i \le r$ e $\chi \neq 1$. □

Sia ora E un'estensione abeliana di F il cui gruppo di Galois G ha esponente $m' \mid m$. Siano E^*, F^* i gruppi moltiplicativi di E, F rispettivamente. Indichiamo con $M(E^*)$ l'insieme degli elementi di E^* le cui potenze m-esime appartengono a F^*, e con $N(E^*)$ l'insieme delle potenze m-esime degli elementi di $M(E^*)$. Allora $M(E^*)$ e $N(E^*)$ sono sottogruppi rispettivamente di E^* e F^*, $M(E^*) \supseteq F^*$ e $N(E^*) \supseteq F^{*m} = \{\alpha^m \mid \alpha \in F^*\}$.

Sia $\rho \in M(E^*)$ e poniamo

$$\chi_\rho(s) = (s\rho)\rho^{-1}, \qquad s \in G. \tag{42}$$

Poiché $\rho^m \in F^*$, si ha $(s\rho)^m = \rho^m$ e $\chi_\rho(s)^m = 1$, sicché $\chi_\rho(s) \in U(m)$. Inoltre, poiché $U(m) \subseteq F^*$,

$$\begin{aligned}\chi_\rho(st) &= (st\rho)\rho^{-1} = s((t\rho)\rho^{-1})((s\rho)\rho^{-1}) \\ &= (t\rho)\rho^{-1}(s\rho)\rho^{-1} = \chi_\rho(s)\chi_\rho(t).\end{aligned}$$

Dunque $\chi_\rho\colon s \mapsto \chi_\rho(s)$ è un carattere di G. Se $\rho_1, \rho_2 \in M(E^*)$, allora $\chi_{\rho_1\rho_2}(s) = s(\rho_1\rho_2)(\rho_1\rho_2)^{-1} = (s\rho_1)\rho_1^{-1}(s\rho_2)\rho_2^{-1} = \chi_{\rho_1}(s)\chi_{\rho_2}(s)$. Quindi $\rho \mapsto \chi_\rho$ è un omomorfismo di $M(E^*)$ in $\widehat{G}$. Dimostriamo il seguente teorema.

Teorema 8.23. *Sia F un campo contenente m radici m-esime distinte di 1 e sia E un'estensione abeliana di F il cui gruppo di Galois G ha esponente $m' \mid m$. Sia $M(E^*)$ il sottogruppo di E^* degli elementi le cui potenze m-esime appartengono a F^*. Si ha la successione esatta*

$$1 \longrightarrow F^* \hookrightarrow M(E^*) \xrightarrow{\lambda} \widehat{G} \longrightarrow 1, \tag{43}$$

dove la freccia di inclusione è quella naturale e λ manda ρ in χ_ρ, con $\chi_\rho(s) = s(\rho)\rho^{-1}$, $s \in G$. Il gruppo quoziente $M(E^*)/F^*$ è isomorfo a G. Si ha $E = F(M(E^*))$ e, per $\rho_i \in M(E^*)$, vale $E = F(\rho_1, \dots, \rho_r)$ se e solo se le classi $\rho_i F^*$ generano $M(E^*)/F^*$.

Dimostrazione. Per la prima asserzione dobbiamo mostrare che λ è suriettiva e ha nucleo F^*. Sia $\chi \in \widehat{G}$. Allora $\chi(st) = \chi(s)\chi(t) = (t\chi(s))\chi(t)$, perciò esiste $\rho \in E^*$ tale che $\chi(s) = (s\rho)\rho^{-1}$ (p. 361). Poiché $(s\rho)\rho^{-1} \in U(m)$, si ha $s\rho^m = \rho^m$ per ogni $s \in G$. Allora $\rho^m \in F^*$ e $\rho \in M(E^*)$. Dunque $\chi = \chi_\rho$ per $\rho \in M(E^*)$, e λ è suriettiva. Se ora $\chi_\rho = 1$, allora $s\rho = \rho$ per ogni $s \in G$, sicché $\rho \in F^*$. Quindi $\ker\lambda = F^*$.

L'esattezza della (43) implica $M(E^*)/F^* \cong \widehat{G}$. Poiché $\widehat{G} \cong G$, si ha $M(E^*)/F^* \cong G$, e l'omomorfismo λ di $M(E^*)$ su $\widehat{G}$ induce l'isomorfismo $\bar{\lambda}\colon \rho F^* \mapsto \chi_\rho$ di $M(E^*)/F^*$ su $\widehat{G}$. Dunque i caratteri $\chi_{\rho_1}, \dots, \chi_{\rho_r}$ generano $\widehat{G}$ se e solo se le classi $\rho_i F^*$ generano $M(E^*)/F^*$. Supponiamo che ciò avvenga e consideriamo il campo $E' = F(\rho_1, \dots, \rho_r)$. Sia $H = \mathrm{Gal}(E/E')$. Per $t \in H$ si ha $t\rho_i = \rho_i$ per $1 \le i \le r$, sicché $\chi_{\rho_i}(t) = 1$. Ciò implica $\chi(t) = 1$ per ogni $\chi \in \widehat{G}$, onde $t = 1$ per (1) del lemma. Dunque $H = 1$ ed $E = E' = F(\rho_1, \dots, \rho_r)$. Evidentemente ciò implica $E = F(M(E^*))$. Viceversa, siano $\rho_1, \dots, \rho_r \in M(E^*)$ generatori di E/F e sia $s \in G$. Da $s\rho_i = \rho_i$ per $1 \le i \le r$ segue $s\rho = \rho$ per ogni $\rho \in E$, e quindi $s = 1$. Dunque $\chi_{\rho_i}(s) = 1$ per ogni i implica $s = 1$. Per (3) del lemma, i χ_{ρ_i} generano $\widehat{G}$ e le classi $\rho_i F^*$ generano $M(E^*)/F^*$. □

Consideriamo ora l'applicazione $\mu\colon \rho \mapsto \rho^m(F^{*m})$ di $M(E^*)$ in $N(E^*)/F^{*m}$. Si tratta di un epimorfismo il cui nucleo consiste dei $\rho \in M(E^*)$ tali che $\rho^m = \alpha^m$, $\alpha \in F^*$. Allora $\rho\alpha^{-1} \in U(m) \subseteq F^*$, onde $\ker\mu = F^*$. Abbiamo quindi l'isomorfismo $\bar{\mu}\colon \rho F^* \mapsto \rho^m(F^{*m})$ di $M(E^*)/F^*$ su $N(E^*)/F^{*m}$. Per il teorema 8.23, $N(E^*)/F^{*m} \cong G$, sicché questo è un sottogruppo finito di F^*/F^{*m}. Vediamo dunque che ogni estensione di Kummer con gruppo di Galois di esponente $m' \mid m$ dà luogo a un sottogruppo finito $N(E^*)/F^{*m}$ di F^*/F^{*m}. Osserviamo inoltre che, se $\beta_1, \dots, \beta_r$ sono elementi di $N(E^*)$ le cui classi $\beta_i F^{*m}$ generano $N(E^*)/F^{*m}$, allora $E = F(\sqrt[m]{\beta_1}, \dots, \sqrt[m]{\beta_r})$, dove $\sqrt[m]{\beta}$ indica una radice di $x^m = \beta$.

Mostreremo che ogni sottogruppo finito di F^*/F^{*m} si ottiene in questo modo da un'estensione di Kummer. Se il sottogruppo dato è N/F^{*m}, esiste cioè un'estensione di Kummer E/F tale che $N(E^*) = N$. Poiché $x^m = 1$ per ogni $x \in F^*/F^{*m}$, l'esponente di N/F^{*m} divide necessariamente m. Lavoriamo in una chiusura algebrica $\bar{F}$ di F. Per $\beta \in F$ scegliamo in $\bar{F}$ un elemento ρ tale che $\rho^m = \beta$ e scriviamo $\rho = \sqrt[m]{\beta}$. Abbiamo il seguente risultato.

Teorema 8.24. *Sia N/F^{*m} un sottogruppo finito di F^*/F^{*m} e siano $\beta_1, \dots, \beta_r$ elementi di N le cui classi $\beta_i F^{*m}$ generano N/F^{*m}. Allora $E = F(\sqrt[m]{\beta_1}, \dots, \sqrt[m]{\beta_r})$ è una m-estensione di Kummer tale che $N(E^*) = N$.*

Dimostrazione. Osserviamo anzitutto che E è un campo di spezzamento di

$$f(x) = (x^m - \beta_1) \cdots (x^m - \beta_r). \tag{44}$$

Ciò è chiaro poiché $x^m - \beta_i = \prod_j (x - \zeta_j \rho_i)$ con $U(m) = \{\zeta_1, \zeta_2, \dots, \zeta_m\}$ e $\rho_i = \sqrt[m]{\beta_i}$. Inoltre, poiché $x^m - \beta_i$ ha radici distinte, il polinomio $f(x)$ è separabile (scegliendo distinti i β_i). Quindi E è un campo di spezzamento su F di un polinomio separabile, ed E/F è di Galois di dimensione finita. Siano $s, t \in G = \mathrm{Gal}(E/F)$. Si ha $s\rho_i = \zeta_{s(i)}\rho_i$, $t\rho_i = \zeta_{t(i)}\rho_i$. Allora $st\rho_i = \zeta_{s(i)}\zeta_{t(i)}\rho_i = ts\rho_i$, quindi G è abeliano. Poiché $s^m\rho_i = \zeta_{s(i)}^m \rho_i = \rho_i$, si ha $s^m = 1$ e l'esponente di G è $m' \mid m$. Pertanto E è una m-estensione di Kummer di F.

Rimane da provare $N(E^*) = N$. Poiché $\rho_i^m = \beta_i \in F^*$, si ha $\rho_i \in M(E^*)$. Poiché $E = F(\rho_1, \dots, \rho_r)$, dal teorema 8.23 segue che le classi $\rho_i F^*$ generano $M(E^*)/F^*$. Dunque le classi $\rho_i^m F^{*m} = \beta_i F^{*m}$ generano $N(E^*)/F^{*m}$. D'altra parte le stesse classi generano N/F^{*m}. Quindi $N = N(E^*)$. □

I risultati ottenuti stabiliscono una corrispondenza biunivoca fra l'insieme dei sottogruppi finiti di F^*/F^{*m} e l'insieme delle m-estensioni di Kummer di F contenute in $\bar{F}$. Questa corrispondenza conserva l'ordine dato dall'inclusione. Poiché l'insieme dei sottogruppi finiti di F^*/F^{*m} è un reticolo, anche l'insieme delle m-estensioni di Kummer è un reticolo, e la corrispondenza è un isomorfismo di reticoli.

8.10 Anelli dei vettori di Witt

Un'estensione E di un campo F di caratteristica $p \neq 0$ si chiama *p-estensione abeliana* di F se E è un'estensione abeliana e $[E : F] = p^e$. Equivalentemente, si può definire una p-estensione abeliana come un'estensione di Galois di dimensione finita con gruppo di Galois G abeliano p-primario. In *BAI*, p. 300, abbiamo costruito tali estensioni per $[E : F] = p$. Furono ottenute per primi da Artin e Schreier, che costruirono anche p-estensioni abeliane di dimensione p^2 nel dimostrare una caratterizzazione algebrica dei campi reali chiusi (si veda p. 674). A. A. Albert estese il procedimento di Artin e Schreier ottenendo una costruzione induttiva delle p-estensioni cicliche di dimensione p^e. Poco dopo Witt diede una costruzione diretta di tutte le p-estensioni abeliane, analoga a quella delle estensioni di Kummer. Il metodo di Witt si fondava su un'ingegnosa definizione di anello, l'*anello dei vettori di Witt*, associato a ogni anello commutativo di caratteristica p. Questi anelli hanno altre importanti applicazioni e presentano un notevole interesse anche al di là dell'applicazione che ne faremo alle p-estensioni abeliane.

Partiamo dall'anello $X = \mathbb{Q}[x_i, y_j, z_k]$ in $3m$ indeterminate x_i, y_j, z_k, $0 \leq i, j, k \leq m-1$, su $\mathbb{Q}$. Consideriamo l'anello $X^{(m)}$ delle m-uple $(a_0, a_1, \dots, a_{m-1})$, $a_i \in X$, con addizione e moltiplicazione per componenti. Fissato un numero primo p, definiamo l'applicazione

$$a = (a_0, a_1, \dots, a_{m-1}) \longmapsto \varphi a = (a^{(0)}, a^{(1)}, \dots, a^{(m-1)}), \tag{45}$$

dove

$$a^{(\nu)} = a_0^{p^\nu} + p a_1^{p^{\nu-1}} + \cdots + p^\nu a_\nu, \qquad 0 \leq \nu \leq m-1. \tag{46}$$

Dunque $a^{(0)} = a_0$, $a^{(1)} = a_0^p + p a_1, \dots$. Introduciamo anche l'applicazione $P\colon a \mapsto Pa = (a_0^p, a_1^p, \dots, a_{m-1}^p)$. La (46) dà allora

$$a^{(0)} = a_0, \qquad a^{(\nu)} = (Pa)^{(\nu-1)} + p^\nu a_\nu, \qquad \nu \geq 1. \tag{47}$$

Sia ora $A = (a^{(0)}, a^{(1)}, \dots, a^{(m-1)})$ arbitrario e definiamo l'applicazione ψ ponendo $\psi A = (a_0, a_1, \dots, a_{m-1})$, dove

$$\begin{aligned} &a_0 = a^{(0)}, \\ &a_\nu = \frac{1}{p^\nu}\left(a^{(\nu)} - a_0^{p^\nu} - pa_1^{p^{\nu-1}} - \cdots - p^{\nu-1}a_{\nu-1}^p\right), \qquad \nu \geq 1. \end{aligned} \tag{48}$$

Si verifica direttamente che $\psi\varphi a = a$ e $\varphi\psi A = A$. Quindi φ è biiettiva con inversa ψ.

Con le applicazioni $\varphi, \psi = \varphi^{-1}$ definiamo ora una nuova struttura di anello su $X^{(m)}$. Converrà indicare l'addizione e la moltiplicazione usuali (per componenti) con $\oplus$ e $\odot$ rispettivamente, e scrivere $u = (1, 1, \dots, 1)$ per l'unità di $X^{(m)}$. Definiamo allora la nuova addizione e la nuova moltiplicazione mediante

$$a + b = \varphi^{-1}(\varphi a \oplus \varphi b), \qquad ab = \varphi^{-1}(\varphi a \odot \varphi b). \tag{49}$$

Si ha $\varphi(0, \dots, 0) = (0, \dots, 0)$ e $\varphi(1, 0, \dots, 0) = (1, 1, \dots, 1) = u$. Quindi $(X^{(m)}, +, \cdot, 0, 1)$, con $1 = (1, 0, \dots, 0)$, è un anello e φ è un isomorfismo di $(X^{(m)}, +, \cdot, 0, 1)$ su $(X^{(m)}, \oplus, \odot, 0, u)$ (esercizio 10, p. 97 di *BAI*). Indichiamo il nuovo anello con X_m e scriviamo $(a^{(0)}, a^{(1)}, \dots, a^{(m-1)})$ per $\varphi(a_0, a_1, \dots, a_{m-1})$, ecc.

Esaminiamo ora le formule per $x + y, xy, x - y$ relative ai vettori «generici» $x = (x_0, x_1, \dots, x_{m-1})$, $y = (y_0, y_1, \dots, y_{m-1})$. Per esempio, abbiamo

$$\begin{aligned} (x+y)_0 &= x_0 + y_0, \quad (x+y)_1 = x_1 + y_1 - \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}x_0^i y_0^{p-i}, \\ (xy)_0 &= x_0 y_0, \qquad\qquad (xy)_1 = x_0^p y_1 + x_1 y_0^p + p x_1 y_1. \end{aligned}$$

In generale, se $\circ$ indica una delle operazioni $+, \cdot, -$, dalla definizione risulta che $(x \circ y)_\nu$ è un polinomio in $x_0, y_0, x_1, y_1, \dots, x_\nu, y_\nu$ a coefficienti razionali e termine costante nullo. Si vede inoltre facilmente che

$$(x+y)_\nu = x_\nu + y_\nu + f_\nu(x_0, y_0, \dots, x_{\nu-1}, y_{\nu-1}), \tag{50}$$

dove f_ν è un polinomio nelle indeterminate indicate. Il risultato fondamentale che dimostreremo ora è che $(x \circ y)_\nu$ è un polinomio in $x_0, y_0, \dots, x_\nu, y_\nu$ a coefficienti *interi* e termine costante nullo.

Sia $\mathbb{Z}[x_i, y_j] = \mathbb{Z}[x_0, y_0, \dots, x_{m-1}, y_{m-1}]$ e scriviamo (p^μ) per $p^\mu\mathbb{Z}[x_i, y_j]$, $\mu \geq 0$.

Lemma 1. *Siano $\mu \geq 1$, $0 \leq k \leq m-1$, $a = (a_\nu)$, $b = (b_\nu)$, con $a_\nu, b_\nu \in \mathbb{Z}[x_i, y_j]$, $0 \leq \nu \leq m-1$, e siano $\varphi a = (a^{(\nu)})$, $\varphi b = (b^{(\nu)})$. Il sistema di congruenze*

$$a_\nu \equiv b_\nu \pmod{p^\mu}, \qquad 0 \leq \nu \leq k, \tag{51}$$

equivale a

$$a^{(\nu)} \equiv b^{(\nu)} \pmod{p^{\mu+\nu}}, \qquad 0 \leq \nu \leq k. \tag{52}$$

Dimostrazione. Poiché $a^{(0)} = a_0$ e $b^{(0)} = b_0$, il risultato è chiaro per $k = 0$. Per induzione su k possiamo supporre che (51) e (52) valgano per $\nu \leq k-1$ e mostrare che in tali condizioni $a_k \equiv b_k \pmod{p^\mu}$ se e solo se $a^{(k)} \equiv b^{(k)} \pmod{p^{\mu+k}}$. È chiaro che $a_k \equiv b_k \pmod{p^\mu}$ equivale a $p^k a_k \equiv p^k b_k \pmod{p^{\mu+k}}$. Dunque per la (47) basta mostrare che $(Pa)^{(k-1)} \equiv (Pb)^{(k-1)} \pmod{p^{\mu+k}}$ sotto l'ipotesi induttiva. Abbiamo $a_\nu \equiv b_\nu \pmod{p^\mu}$ per $0 \leq \nu \leq k-1$. Poiché $\binom{p}{i} \equiv 0 \pmod{p}$ per $1 \leq i \leq p-1$, ne segue $a_\nu^p \equiv b_\nu^p \pmod{p^{\mu+1}}$ per $0 \leq \nu \leq k-1$. L'ipotesi induttiva applicata ai vettori Pa, Pb dà $(Pa)^{(k-1)} \equiv (Pb)^{(k-1)} \pmod{p^{\mu+1+k-1}}$, come richiesto. □

Possiamo ora dimostrare il seguente teorema fondamentale.

Teorema 8.25. *Se $x \circ y$ indica $x+y, xy$ oppure $x-y$, allora $(x\circ y)_\nu$ è un polinomio in $x_0, y_0, \ldots, x_\nu, y_\nu$ a coefficienti interi e termine costante nullo.*

Dimostrazione. Poiché sappiamo già che i coefficienti sono razionali e il termine costante è nullo, basta mostrare che $(x\circ y)_\nu \in \mathbb{Z}[x_i, y_j]$. Ciò è chiaro per $(x\circ y)_0$, e lo supponiamo vero per $(x\circ y)_k,\ 0 \le k \le \nu-1$. Per la (47) abbiamo

$$p^\nu (x\circ y)_\nu = (x\circ y)^{(\nu)} - (P(x\circ y))^{(\nu-1)}. \tag{53}$$

Inoltre $(x\circ y)^{(\nu)} = x^{(\nu)} \circ y^{(\nu)} \in \mathbb{Z}[x_i, y_j]$, dove nel secondo membro si usa l'operazione ordinaria corrispondente. L'ipotesi induttiva implica $(P(x\circ y))^{(\nu-1)} \in \mathbb{Z}[x_i, y_j]$. Per la (53) basta dunque mostrare che $(x\circ y)^{(\nu)} \equiv (P(x\circ y))^{(\nu-1)} \pmod{p^\nu}$. Per la (47), $x^{(\nu)} \equiv (Px)^{(\nu-1)} \pmod{p^\nu}$ e $y^{(\nu)} \equiv (Py)^{(\nu-1)} \pmod{p^\nu}$. Quindi

$$\begin{aligned} (x\circ y)^{(\nu)} &= x^{(\nu)} \circ y^{(\nu)} \equiv (Px)^{(\nu-1)} \circ (Py)^{(\nu-1)} \\ &\equiv (Px \circ Py)^{(\nu-1)} \pmod{p^\nu}. \end{aligned} \tag{54}$$

Per ipotesi $(x\circ y)_k \in \mathbb{Z}[x_i, y_j]$ per $0 \le k \le \nu-1$. Per ogni polinomio a coefficienti interi vale $f(x_0, y_0, \ldots)^p \equiv f(x_0^p, y_0^p, \ldots) \pmod{p}$. Ne segue $(P(x\circ y))_k \equiv ((Px)\circ(Py))_k \pmod{p}$ per $0 \le k \le \nu-1$. Per il lemma 1 otteniamo

$$(P(x\circ y))^{(\nu-1)} \equiv (Px \circ Py)^{(\nu-1)} \pmod{p^\nu}. \tag{55}$$

Le formule (54) e (55) danno $(x\circ y)^{(\nu)} \equiv (P(x\circ y))^{(\nu-1)} \pmod{p^\nu}$, come si voleva. □

Conviene scrivere il risultato appena dimostrato nella forma

$$\begin{aligned} (x+y)_\nu &= s_\nu(x_0, y_0, \ldots, x_\nu, y_\nu) \in \mathbb{Z}[x_i, y_j], \\ (xy)_\nu &= m_\nu(x_0, y_0, \ldots, x_\nu, y_\nu) \in \mathbb{Z}[x_i, y_j], \\ (x-y)_\nu &= d_\nu(x_0, y_0, \ldots, x_\nu, y_\nu) \in \mathbb{Z}[x_i, y_j]. \end{aligned} \tag{56}$$

Sia η un endomorfismo dell'algebra $X/\mathbb{Q}$ e supponiamo che $\eta x_\nu = a_\nu$, $\eta y_\nu = b_\nu$, $0 \le \nu \le m-1$. Allora $\eta x^{(\nu)} = a^{(\nu)}$, $\eta y^{(\nu)} = b^{(\nu)}$, $\eta((x+y)^{(\nu)}) = \eta x^{(\nu)} + \eta y^{(\nu)} = a^{(\nu)} + b^{(\nu)}$ e $\eta((x+y)_\nu) = (a+b)_\nu$. Dunque per la (56)

$$(a+b)_\nu = s_\nu(a_0, b_0, \ldots, a_\nu, b_\nu). \tag{57}$$

Analogamente,

$$(ab)_\nu = m_\nu(a_0, b_0, \ldots, a_\nu, b_\nu), \tag{58}$$

$$(a-b)_\nu = d_\nu(a_0, b_0, \ldots, a_\nu, b_\nu). \tag{59}$$

Poiché esiste un endomorfismo di $X/\mathbb{Q}$ che manda le x_ν, y_ν in elementi arbitrari di X, le formule valgono per vettori arbitrari $a = (a_0, a_1, \ldots, a_{m-1})$, $b = (b_0, b_1, \ldots, b_{m-1})$ di X_m.

Possiamo ora definire l'anello $W_m(A)$ dei vettori di Witt su un qualunque anello commutativo A di caratteristica p. L'insieme $W_m(A)$ è quello delle m-uple $(a_0, a_1, \ldots, a_{m-1})$, $a_i \in A$, con l'usuale nozione di uguaglianza. Definiamo l'addizione e la moltiplicazione in $W_m(A)$ mediante

$$\begin{aligned} (a+b)_\nu &= s_\nu(a_0, b_0, \ldots, a_\nu, b_\nu), \\ (ab)_\nu &= m_\nu(a_0, b_0, \ldots, a_\nu, b_\nu), \end{aligned} \tag{60}$$

dove i secondi membri sono le immagini in A di $s_\nu(x_0, y_0, \ldots, x_\nu, y_\nu)$ e $m_\nu(x_0, y_0, \ldots, x_\nu, y_\nu)$ sotto l'omomorfismo di $\mathbb{Z}[x_i, y_j]$ in A tale che $x_i \mapsto a_i,\ y_i \mapsto b_i,\ 0 \le i \le m-1$. Poniamo inoltre $0 = (0, \ldots, 0)$, $1 = (1, 0, \ldots, 0)$ in $W_m(A)$. Abbiamo così la struttura $(W_m(A), +, \cdot, 0, 1)$.

Teorema 8.26. $(W_m(A), +, \cdot, 0, 1)$ *è un anello commutativo.*

Dimostrazione. Per dimostrare una qualsiasi delle identità che definiscono un anello commutativo, ossia le leggi associative, commutative e distributive, siano a, b, c tre elementi qualunque di $W_m(A)$. Vi è un omomorfismo η di $\mathbb{Z}[x_i, y_j, z_k]$ in A tale che $x_\nu \mapsto a_\nu,\ y_\nu \mapsto b_\nu,\ z_\nu \mapsto c_\nu,\ 0 \leq \nu \leq m-1$. Indichiamo con I_m il sottoinsieme di X_m costituito dai vettori con componenti in $\mathbb{Z}[x_i, y_j, z_k]$. Per le (57)–(59) esso è un sottoanello di X_m. Il confronto di quelle formule con la (60) mostra inoltre che $(u_0, u_1, \ldots, u_{m-1}) \mapsto (\eta u_0, \eta u_1, \ldots, \eta u_{m-1})$ è un omomorfismo di $(I_m, +, \cdot)$ in $(W_m(A), +, \cdot)$. Questo omomorfismo manda $x = (x_0, x_1, \ldots, x_{m-1})$, $y = (y_0, y_1, \ldots, y_{m-1})$, $z = (z_0, z_1, \ldots, z_{m-1})$ rispettivamente in a, b, c. Poiché $(xy)z = x(yz)$ in I_m, si ha $(ab)c = a(bc)$. La moltiplicazione in $W_m(A)$ è dunque associativa. Analogamente si dimostrano le altre identità per la moltiplicazione e l'addizione. Lo stesso ragionamento mostra che 0 è lo zero per l'addizione e $1 = (1, 0, \ldots, 0)$ è l'unità per la moltiplicazione. Per provare l'esistenza degli opposti applichiamo l'omomorfismo a $-x$, la cui immagine è l'opposto di a. Ne segue che $(W_m(A), +, \cdot, 0, 1)$ è un anello commutativo. □

Chiamiamo $W_m(A)$ l'*anello dei vettori di Witt di lunghezza m su A*. È chiaro che $W_1(A)$ si identifica con A, poiché $a \mapsto (a)$ è un isomorfismo. È chiaro inoltre che, se η è un omomorfismo di A in un altro anello commutativo A' di caratteristica p, allora $(a_0, a_1, \ldots, a_{m-1}) \mapsto (\eta a_0, \eta a_1, \ldots, \eta a_{m-1})$ è un omomorfismo di $W_m(A)$ in $W_m(A')$. Otteniamo così un funtore W_m dalla categoria degli anelli commutativi di caratteristica p alla categoria degli anelli commutativi. In particolare, se A è un sottoanello di A', $W_m(A)$ è un sottoanello di $W_m(A')$.

Esaminiamo ora alcune proprietà fondamentali di $W_m(A)$. Introduciamo a tale scopo tre applicazioni importanti, P, R, V. Poiché A è un anello commutativo di caratteristica p, in A si ha l'endomorfismo di anelli $r \mapsto r^p$. Esso induce l'*endomorfismo di Frobenius* P di $W_m(A)$, dato da $Pa = (a_0^p, a_1^p, \ldots, a_{m-1}^p)$ per $a = (a_0, a_1, \ldots, a_{m-1})$. Definiamo poi l'*applicazione di restrizione* R di $W_m(A)$ in $W_{m-1}(A)$ mediante

$$R(a_0, a_1, \ldots, a_{m-1}) = (a_0, a_1, \ldots, a_{m-2}) \tag{61}$$

e l'*applicazione di traslazione* V di $W_{m-1}(A)$ in $W_m(A)$ mediante

$$V(a_0, a_1, \ldots, a_{m-2}) = (0, a_0, \ldots, a_{m-2}). \tag{62}$$

È immediato che R è un omomorfismo di anelli, e vedremo che V è un omomorfismo dei gruppi additivi. Abbiamo

$$RV(a_0, a_1, \ldots, a_{m-1}) = (0, a_0, \ldots, a_{m-2}) = VR(a_0, a_1, \ldots, a_{m-1}),$$

sicché $VR = RV$ come applicazioni di $W_m(A)$ in sé. Dalla formula è chiaro anche che $(VR)^m = 0$. Inoltre $PV = VP$ come applicazioni di $W_{m-1}(A)$ in $W_m(A)$, e $PR = RP$ come applicazioni di $W_m(A)$ in $W_{m-1}(A)$.

Lemma 2. *Negli anelli di Witt valgono le relazioni*

$$p1 = \underbrace{1 + 1 + \cdots + 1}_{p} = RV1, \tag{63}$$

$$V(a + b) = Va + Vb, \tag{64}$$

$$(Va)b = V(aPRb), \qquad a \in W_m(A),\ b \in W_{m+1}(A), \tag{65}$$

$$pa = RVPa. \tag{66}$$

Dimostrazione. Consideriamo i sottoanelli I_{m-1}, I_m, I_{m+1} di X_{m-1}, X_m e X_{m+1}, rispettivamente, costituiti dai vettori con componenti in $\mathbb{Z}[x_i, y_j]$. Definiamo R, V per questi anelli come

per gli anelli di Witt e definiamo P come prima. Consideriamo l'unità $1 = (1, 0, \dots, 0)$ di I_m. Si ha $\varphi 1 = (1, 1, \dots, 1)$, onde $(p1)^{(\nu)} = p$ per $0 \le \nu \le m-1$. D'altro canto $RV1 = (0, 1, \dots, 0)$, perciò la definizione di φ dà $(RV1)^{(0)} = 0$, $(RV1)^{(\nu)} = p$ per $1 \le \nu \le m-1$. Dunque $(RV1)^{(\nu)} \equiv (p1)^{(\nu)} \pmod{p^{\nu+1}}$ per $0 \le \nu \le m-1$. Per il lemma 1 ne segue $(RV1)_\nu \equiv (p1)_\nu \pmod p$. Abbiamo un omomorfismo di I_m in $W_m(A)$ che manda $x = (x_0, x_1, \dots, x_{m-1})$ in $(a_0, a_1, \dots, a_{m-1})$ e $y = (y_0, y_1, \dots, y_{m-1})$ in $(b_0, \dots, b_{m-1})$. Applicandolo a $RV1$ e $p1$, le relazioni precedenti e il fatto che A ha caratteristica p danno la (63).

Ora $Vx = (0, x_0, \dots, x_{m-1})$, $Vy = (0, y_0, \dots, y_{m-1})$. Quindi

$$(Vx)^{(\nu)} = px_0^{p^{\nu-1}} + p^2 x_1^{p^{\nu-2}} + \cdots + p^\nu x_{\nu-1} = px^{(\nu-1)}, \qquad 1 \le \nu \le m. \tag{67}$$

Poiché $(x+y)^{(\nu)} = x^{(\nu)} + y^{(\nu)}$, la (67) e le uguaglianze $(Vx)^{(0)} = (Vy)^{(0)} = (V(x+y))^{(0)} = 0$ danno $(V(x+y))^{(\nu)} = (Vx)^{(\nu)} + (Vy)^{(\nu)}$ per $0 \le \nu \le m$. Queste relazioni, applicando l'omomorfismo di $\mathbb{Z}[x_i, y_j]$ in A tale che $x_\nu \mapsto a_\nu$, $y_\nu \mapsto b_\nu$, $0 \le \nu \le m-1$, danno $(V(a+b))^{(\nu)} = (Va)^{(\nu)} + (Vb)^{(\nu)}$ per $0 \le \nu \le m$. L'identità ottenuta sui vettori universali si specializza così nella (64).

Per la (65) mostreremo che

$$((Vx)y)_\nu \equiv (V(xRPy))_\nu \pmod p, \qquad 0 \le \nu \le m, \tag{68}$$

per $x = (x_0, \dots, x_{m-1})$ e $y = (y_0, y_1, \dots, y_m)$. Poniamo $(Vx)y = (w_0, w_1, \dots, w_m)$, $V(xRPy) = (t_0, t_1, \dots, t_m)$. Occorre mostrare $w_\nu \equiv t_\nu \pmod p$ per $0 \le \nu \le m$. Per il lemma 1 ciò equivale a $w^{(\nu)} \equiv t^{(\nu)} \pmod{p^{\nu+1}}$. Ciò vale per $\nu = 0$, poiché $w^{(0)} = 0 = t^{(0)}$. Per $\nu \ge 1$, dalla (67) si hanno $w^{(\nu)} = px^{(\nu-1)}y^{(\nu)}$ e $t^{(\nu)} = px^{(\nu-1)}(PRy)^{(\nu-1)}$. Poiché $y^{(\nu)} = (Py)^{(\nu-1)} + p^\nu y_\nu$, seguono le congruenze

$$\begin{aligned} w^{(\nu)} = px^{(\nu-1)}y^{(\nu)} &\equiv px^{(\nu-1)}(Py)^{(\nu-1)} \\ &\equiv px^{(\nu-1)}(PRy)^{(\nu-1)} = t^{(\nu)} \pmod{p^{\nu+1}}. \end{aligned}$$

Vale dunque la (68). Applicandovi l'omomorfismo di $\mathbb{Z}[x_0, \dots, x_{m-1}, y_0, \dots, y_m]$ in A tale che $x_\nu \mapsto a_\nu$, $y_\nu \mapsto b_\nu$, otteniamo la (65).

Applicando R ai due membri della (65) si ottiene $(RVa)Rb = RV(aPRb)$. Ponendo $a = 1$, abbiamo $(RV1)(Rb) = RVPRb$. Poiché $RV1 = p1$ per la (63) e Rb può essere un qualsiasi elemento di $W_m(A)$, ne segue la (66). □

Possiamo ora ricavare le proprietà fondamentali di $W_m(A)$ che ci serviranno. Dimostriamo anzitutto il teorema seguente.

Teorema 8.27. *Il sottoanello fondamentale di $W_m(A)$ è isomorfo a $\mathbb{Z}/(p^m)$. È costituito dai vettori di Witt le cui componenti appartengono al sottoanello fondamentale di A, identificato con $\mathbb{Z}/(p)$.*

Dimostrazione. Per la (63), $p1 = RV1$. Per la (66) si ha allora $p^2 1 = (RV)^2 1$. Iterando otteniamo $p^k 1 = (RV)^k 1$. Quindi $p^{m-1}1 = (0, 0, \dots, 1) \ne 0$ e $p^m 1 = 0$. Il sottoanello fondamentale è dunque isomorfo a $\mathbb{Z}/(p^m)$. Il sottoanello fondamentale di A si identifica con $\mathbb{Z}/(p)$, e l'insieme dei vettori di Witt con componenti in $\mathbb{Z}/(p)$ è un sottoanello di cardinalità p^m. Esso coincide pertanto con il sottoanello fondamentale di $W_m(A)$. □

Teorema 8.28. *L'applicazione $(a_0, a_1, \dots, a_{m-1}) \mapsto a_0$ è un omomorfismo di $W_m(A)$ su A il cui nucleo N è un ideale nilpotente.*

Dimostrazione. Abbiamo visto che R è un omomorfismo di $W_m(A)$ in $W_{m-1}(A)$. Iterando si ottiene l'omomorfismo $R^{m-1}\colon (a_0,\dots,a_{m-1}) \mapsto (a_0)$ di $W_m(A)$ in $W_1(A)$. Poiché (a_0) si identifica con $a_0 \in A$, abbiamo l'omomorfismo $(a_0,a_1,\dots,a_{m-1}) \mapsto a_0$, chiaramente suriettivo. Il nucleo N è formato dagli elementi $(0,a_1,\dots,a_{m-1})$, sicché $N = RVW_m(A)$. Mostreremo che $N^m = 0$. Applicando R alla (65) si ottiene $(RVa)Rb = RV(aPRb)$ per $a \in W_m(A), b \in W_{m+1}(A)$. Poiché Rb può essere un elemento qualsiasi c di $W_m(A)$, abbiamo $(RVa)c = RV(aPc)$ per ogni $a, c \in W_m(A)$. Quindi

$$\begin{aligned}(RVa)(RVc) &= RV(aPRVc) = RV(aRVPc) = RV((RVPc)a)\\ &= (RV)^2(PcPa) \in (RV)^2W_m(A).\end{aligned}$$

Dunque $N^2 \subseteq (RV)^2W_m(A) = (RV)N$. Supponiamo che per un certo $k \geq 2$ si abbia $N^k \subseteq N(RV)^{k-2}N \subseteq (RV)^{k-1}N$. Per $d = RVa \in N$ e $b \in N^k$ possiamo scrivere $b = (RV)^k c$, $c \in W_m(A)$, poiché $N^k \subseteq (RV)^{k-1}N = (RV)^k W_m(A)$. Quindi $db = (RVa)((RV)^k c) \in N(RV)^{k-1}N$, onde $N^{k+1} \subseteq N(RV)^{k-1}N$. Inoltre, per $a, c \in W_m(A)$,

$$(RVa)((RV)^k c) = RV\big((RVPa)((RV)^{k-1}c)\big) \in RV\big(N(RV)^{k-2}N\big) \subseteq (RV)^k N.$$

Per ogni k si ha quindi $N^k \subseteq (RV)^{k-1}N = (RV)^k W_m(A)$. Poiché $(RV)^m = 0$, ne segue $N^m = 0$. □

Una conseguenza immediata del teorema 8.28 è la seguente.

Corollario. *Un elemento $a = (a_0,a_1,\dots,a_{m-1})$ di $W_m(A)$ è un'unità di $W_m(A)$ se e solo se a_0 è un'unità di A.*

Dimostrazione. Se a è un'unità, tale è a_0, poiché abbiamo un omomorfismo di $W_m(A)$ in A che manda a in a_0. Viceversa, se a_0 è un'unità, allora $a = a' + z$, dove $z \in N$ e $a' + N$ è un'unità di $W_m(A)/N$. Dalla nilpotenza di N segue che a è un'unità. □

Esercizi.

1. Ricavare le formule per s_ν, m_ν della (56) per $\nu = 0,1,2$.

2. Sia $W_1(A), W_2(A), \dots$ la successione degli anelli di Witt definiti dall'anello commutativo A di caratteristica p. Se $n > m$, abbiamo l'omomorfismo R^{n-m} di $W_n(A)$ in $W_m(A)$. Mostrare che questi anelli e omomorfismi definiscono un limite inverso $W(A) = \varprojlim W_m(A)$. Mostrare che $W(A)$ è isomorfo all'anello dei vettori di Witt di rango infinito, definito come l'insieme delle successioni infinite $a = (a_0,a_1,a_2,\dots)$, $a_\nu \in A$, con addizione e moltiplicazione date dalla (49), $0 = (0,0,\dots)$ e $1 = (1,0,0,\dots)$. Mostrare che $N = \{(0,a_1,a_2,\dots)\}$ è un ideale di $W(A)$ contenuto nel radicale di Jacobson.

3. Sia A un campo perfetto di caratteristica p (*BAI*, p. 233). Mostrare che $p^k W(A) = V^k W(A)$, dove $V(a_0,a_1,a_2,\dots) = (0,a_0,a_1,a_2,\dots)$. Mostrare che ogni elemento non nullo di $W(A)$ è della forma $p^k a$, con a unità, e dedurne che $W(A)$ è un dominio.

8.11 p-estensioni abeliane

Ricordiamo anzitutto la costruzione di Artin–Schreier delle estensioni cicliche di dimensione p di un campo F di caratteristica p. Sia β un elemento di F che non sia della forma $\alpha^p - \alpha$, $\alpha \in F$, e sia ρ un elemento della chiusura algebrica $\bar{F}$ di F tale che $\rho^p - \rho = \beta$. Allora $F(\rho)$ è un'estensione ciclica di F di dimensione p e ogni tale estensione si ottiene in questo modo. La

dimostrazione fa uso dell'analogo additivo del *Satz* 90 di Hilbert, che si può considerare come un risultato di coomologia. Estenderemo ora questi risultati alle p-estensioni abeliane, cominciando dal teorema di coomologia.

Supponiamo dapprima che E sia un'estensione di Galois di dimensione finita di un campo F di caratteristica p e formiamo l'anello $W_m(E)$ dei vettori di Witt su E di lunghezza $m \geq 1$. Esso contiene il sottoanello $W_m(F)$ e su di esso agisce il gruppo di Galois G di E/F mediante

$$s(\rho_0, \rho_1, \ldots, \rho_{m-1}) = (s\rho_0, s\rho_1, \ldots, s\rho_{m-1}). \tag{69}$$

Questa è un'azione per automorfismi e il sottoanello degli elementi fissi per ogni $s \in G = \mathrm{Gal}(E/F)$ è $W_m(F)$.

Per $\rho = (\rho_0, \rho_1, \ldots, \rho_{m-1}) \in W_m(E)$ definiamo la traccia $T(\rho) = \sum_{s\in G} s\rho$. Evidentemente $T(\rho) \in W_m(F)$. Poiché $(\rho + \sigma)_0 = \rho_0 + \sigma_0$ per $\rho = (\rho_0, \ldots, \rho_{m-1})$ e $\sigma = (\sigma_0, \ldots, \sigma_{m-1})$, otteniamo $T(\rho) = (T_{E/F}(\rho_0), \ldots)$. Ci servirà il seguente lemma.

Lemma 1. *Esiste $\rho \in W_m(E)$ tale che $T(\rho)$ è un'unità di $W_m(F)$.*

Dimostrazione. Per la proprietà di indipendenza di Dedekind degli automorfismi distinti di un campo esiste $\rho_0 \in E$ tale che $T_{E/F}(\rho_0) \neq 0$. Sia $\rho = (\rho_0, \ldots)$. Allora $T(\rho) = (T_{E/F}(\rho_0), \ldots)$. Poiché $T_{E/F}(\rho_0) \neq 0$, è un'unità di F. Per il corollario del teorema 8.28, $T(\rho)$ è quindi un'unità di $W_m(F)$. □

Useremo questo risultato per provare che, considerando il gruppo additivo $(W_m(E), +)$ come G-modulo per l'azione appena definita, si ha $H^1(G, W_m(E)) = 0$. In forma esplicita il risultato è il seguente.

Teorema 8.29. *Sia $s \mapsto \mu_s$ un'applicazione di G in $W_m(E)$ tale che $\mu_{st} = s\mu_t + \mu_s$. Allora esiste $\sigma \in W_m(E)$ tale che $\mu_s = s\sigma - \sigma$ per $s \in G$.*

Dimostrazione. È identica a quella del caso particolare $m = 1$, trattato nel teorema 4.33 di *BAI* (p. 298). Scegliamo $\rho \in W_m(E)$ in modo che $T(\rho)$ sia un'unità di $W_m(F)$ e poniamo $\tau = T(\rho)^{-1} \sum_{t\in G} \mu_t(t\rho)$. Allora

$$\begin{aligned} \tau - s\tau &= T(\rho)^{-1} \sum_t (\mu_{st}(st\rho) - (s\mu_t)(st\rho)) \\ &= T(\rho)^{-1} \left(\mu_s \sum_t t\rho \right) = \mu_s. \end{aligned}$$

Ponendo dunque $\sigma = -\tau$, si ha $\mu_s = s\sigma - \sigma$. □

Ricordiamo che l'applicazione di Frobenius $\rho = (\rho_0, \ldots, \rho_{m-1}) \mapsto P\rho = (\rho_0^p, \ldots, \rho_{m-1}^p)$ è un endomorfismo dell'anello $W_m(E)$. Introduciamo ora l'applicazione $\mathcal{P}$ definita da

$$\mathcal{P}(\rho) = P\rho - \rho. \tag{70}$$

È chiaro che si tratta di un endomorfismo del gruppo additivo di $W_m(E)$ (ma non dell'anello $W_m(E)$). Il nucleo di $\mathcal{P}$ è l'insieme dei vettori ρ tali che $\rho_\nu^p = \rho_\nu$ per $0 \leq \nu \leq m-1$, cioè dei vettori con componenti nel sottocampo fondamentale di E. Abbiamo visto (teorema 8.27) che questo insieme di vettori è il sottoanello fondamentale di $W_m(E)$ e si può identificare con $\mathbb{Z}/(p^m)$, il cui gruppo additivo è ciclico di ordine p^m. Se G è un qualunque gruppo abeliano finito di esponente $p^e \leq p^m$, il ragionamento di p. 494 mostra che il gruppo dei caratteri $\widehat{G}$ si può identificare con il gruppo degli omomorfismi di G nel gruppo additivo ciclico del sottoanello fondamentale di $W_m(E)$. D'ora in poi faremo questa identificazione.

Supponiamo ora che il gruppo di Galois G dell'estensione E/F sia abeliano di ordine p^f e scegliamo m tale che $p^m \geq p^e$, dove p^e è l'esponente di G. Introduciamo il sottoinsieme

$$SW_m(E) = \{\rho \in W_m(E) \mid \mathcal{P}\rho \in W_m(F)\}. \tag{71}$$

È un sottogruppo del gruppo additivo di $W_m(E)$ e contiene $W_m(F)$. Per $\rho \in SW_m(E)$ definiamo l'applicazione χ_ρ su G mediante $\chi_\rho(s) = s\rho - \rho$. Allora

$$\begin{aligned} P\chi_\rho(s) &= Ps\rho - P\rho = sP\rho - P\rho \\ &= sP\rho - s\rho + s\rho - P\rho = P\rho - \rho + s\rho - P\rho \\ &= s\rho - \rho = \chi_\rho(s), \end{aligned}$$

ossia $\mathcal{P}\chi_\rho(s) = 0$. Quindi $\chi_\rho(s)$ è nel sottoanello fondamentale di $W_m(E)$. Inoltre $\chi_\rho(st) = st\rho - \rho = st\rho - t\rho + t\rho - \rho = s\rho - \rho + t\rho - \rho = \chi_\rho(s) + \chi_\rho(t)$. Dunque χ_ρ è un omomorfismo di G nel gruppo additivo del sottoanello fondamentale di $W_m(E)$, e possiamo considerarlo un elemento del gruppo dei caratteri $\widehat{G}$. Siano ora $\rho, \sigma \in SW_m(E)$. Allora $\rho + \sigma \in SW_m(E)$ e $\chi_{\rho+\sigma}(s) = s(\rho + \sigma) - (\rho + \sigma) = s\rho - \rho + s\sigma - \sigma = \chi_\rho(s) + \chi_\sigma(s)$. Dunque $\rho \mapsto \chi_\rho$ è un omomorfismo del gruppo additivo $SW_m(E)$ in $\widehat{G}$. Se $\chi_\rho(s) = 0$ per ogni s, si ha $s\rho = \rho$ per ogni s, onde $\rho = \alpha \in W_m(F)$. Ne segue che $W_m(F)$ è il nucleo di $\rho \mapsto \chi_\rho$.

Osserviamo infine che questo omomorfismo è suriettivo. Infatti, sia $\chi \in \widehat{G}$. Allora $\chi(s)$ appartiene al sottoanello fondamentale e $\chi(st) = \chi(s) + \chi(t) = s\chi(t) + \chi(s)$. Per il teorema 8.29 esiste $\rho \in W_m(E)$ tale che $\chi(s) = s\rho - \rho$. Poiché $P\chi(s) = \chi(s)$, si ha $s(P\rho - \rho) = P\rho - \rho$ per $s \in G$. Quindi $\mathcal{P}\rho \in W_m(F)$, ossia $\rho \in SW_m(E)$ e $\chi_\rho = \chi$. Ciò prova la suriettività. Abbiamo ora $SW_m(E)/W_m(F) \cong \widehat{G} \cong G$. Abbiamo così dimostrato le prime due asserzioni del teorema seguente, esattamente analogo al teorema 8.23 della teoria di Kummer.

Teorema 8.30. *Sia F un campo di caratteristica $p \neq 0$, sia E una p-estensione abeliana di F il cui gruppo di Galois G ha esponente p^e, e sia $W_m(E)$ l'anello dei vettori di Witt su E di lunghezza $m \geq e$. Sia $SW_m(E)$ il sottogruppo additivo di $W_m(E)$ dei ρ tali che $\mathcal{P}\rho = P\rho - \rho \in W_m(F)$. Si ha la successione esatta*

$$0 \longrightarrow W_m(F) \hookrightarrow SW_m(E) \xrightarrow{\zeta} \widehat{G} \longrightarrow 0, \tag{72}$$

dove la freccia di inclusione è quella naturale e ζ manda ρ in χ_ρ, con $\chi_\rho(s) = s\rho - \rho$. Il gruppo quoziente $SW_m(E)/W_m(F)$ è isomorfo a G. Il campo E/F è generato dalle componenti dei vettori $\rho \in SW_m(E)$ e

$$E = F(\rho_0^{(1)}, \ldots, \rho_{m-1}^{(1)}, \rho_0^{(2)}, \ldots, \rho_{m-1}^{(2)}, \ldots, \rho_0^{(r)}, \ldots, \rho_{m-1}^{(r)})$$

se e solo se le classi $\rho^{(i)} + W_m(F)$, con $\rho^{(i)} = (\rho_0^{(i)}, \ldots, \rho_{m-1}^{(i)})$, generano $SW_m(E)/W_m(F)$.

La dimostrazione dell'ultima asserzione è identica a quella dell'asserzione corrispondente del teorema 8.23. Lasciamo al lettore la verifica dei dettagli.

Seguendo lo schema della trattazione della teoria di Kummer introduciamo ora l'insieme

$$QW_m(E) = \{\mathcal{P}(\rho) \mid \rho \in SW_m(E)\}. \tag{73}$$

È un sottogruppo del gruppo additivo di $W_m(F)$ che contiene $\mathcal{P}W_m(F)$, il sottogruppo dei vettori $\mathcal{P}\alpha$, $\alpha \in W_m(F)$. Abbiamo l'omomorfismo

$$\rho \longmapsto \mathcal{P}\rho + \mathcal{P}W_m(F) \tag{74}$$

di $SW_m(E)$ su $QW_m(E)/\mathcal{P}W_m(F)$. Un elemento ρ appartiene al nucleo di tale omomorfismo se e solo se $\mathcal{P}\rho = \mathcal{P}\alpha$, $\alpha \in W_m(F)$. Ciò equivale a $\mathcal{P}(\rho - \alpha) = 0$, ossia a dire che $\rho - \alpha$ appartiene al sottoanello fondamentale. Quindi il nucleo della (74) è $W_m(F)$ e si ha l'isomorfismo

$$QW_m(E)/\mathcal{P}W_m(F) \cong SW_m(E)/W_m(F). \tag{75}$$

Poiché il secondo gruppo è isomorfo a G, anche il primo lo è. Mostreremo ora che, se Q è un qualsiasi sottogruppo del gruppo additivo dell'anello $W_m(F)$ che contiene $\mathcal{P}W_m(F)$ e $Q/\mathcal{P}W_m(F)$ è finito, allora $Q = QW_m(E)$ per una p-estensione abeliana E/F. Ci occorre a tal fine il seguente lemma.

Lemma 2. *Sia $\beta = (\beta_0, \beta_1, \dots, \beta_{m-1}) \in W_m(F)$. Esistono in $\bar{F}$ elementi ρ_ν, $0 \le \nu \le m-1$, tali che $E = F(\rho_0, \rho_1, \dots, \rho_{m-1})$ è separabile di dimensione finita su F, e il vettore $\rho = (\rho_0, \rho_1, \dots, \rho_{m-1})$ di $W_m(E)$ soddisfa $\mathcal{P}\rho = \beta$.*

Dimostrazione. Se $m = 1$, scegliamo $\rho \in \bar{F}$ tale che $\rho^p - \rho = \beta$. Allora $F(\rho)$ è separabile, poiché $(x^p - x - \beta)' = -1$, onde $x^p - x - \beta$ ha radici distinte. Supponiamo di avere $\rho_0, \dots, \rho_{m-2} \in \bar{F}$ tali che $E' = F(\rho_0, \rho_1, \dots, \rho_{m-2})$ è separabile su F e $\mathcal{P}(\rho_0, \dots, \rho_{m-2}) = (\beta_0, \dots, \beta_{m-2})$ in $W_{m-1}(E')$. Consideriamo l'anello dei polinomi $E'[x]$ e l'anello di Witt $W_m(E'[x])$. In quest'ultimo sia $y = (\rho_0, \dots, \rho_{m-2}, x)$ e formiamo

$$\mathcal{P}y = (\rho_0^p, \dots, \rho_{m-2}^p, x^p) - (\rho_0, \dots, \rho_{m-2}, x).$$

Si ha $\mathcal{P}y = (\beta_0, \dots, \beta_{m-2}, f(x))$, $f(x) \in E'[x]$. Poiché

$$(\beta_0, \dots, \beta_{m-2}, f(x)) + (\rho_0, \dots, \rho_{m-2}, x) = (\rho_0^p, \dots, \rho_{m-2}^p, x^p),$$

la (50) dà $x^p = f(x) + x + \gamma$ con $\gamma \in E'$. Dunque $f(x) = x^p - x - \gamma$. Scegliendo $\rho_{m-1} \in \bar{F}$ tale che $f(\rho_{m-1}) = \beta_{m-1}$, il ragionamento con la derivata mostra che $E'(\rho_{m-1})$ è separabile su E'. Pertanto $E = F(\rho_0, \rho_1, \dots, \rho_{m-1})$ è separabile su F. Le formule mostrano che per $\rho = (\rho_0, \dots, \rho_{m-1})$ si ha $\mathcal{P}\rho = (\beta_0, \dots, \beta_{m-1})$. □

Teorema 8.31. *Sia Q un sottogruppo di $(W_m(F), +)$ contenente $\mathcal{P}W_m(F)$ e tale che $Q/\mathcal{P}W_m(F)$ sia finito. Allora esiste una p-estensione abeliana E di F tale che il gruppo di Galois di E/F ha esponente p^e, con $e \le m$, e $QW_m(E) = Q$.*

Dimostrazione. Siano $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(r)}$ elementi di Q le cui classi $\beta^{(i)} + \mathcal{P}W_m(F)$ generano $Q/\mathcal{P}W_m(F)$. Per il lemma 2, $\bar{F}$ contiene un campo E separabile di dimensione finita su F, generato da elementi $\rho_\nu^{(i)}$, $1 \le i \le r$, $0 \le \nu \le m-1$, tali che $\mathcal{P}(\rho_0^{(i)}, \dots, \rho_{m-1}^{(i)}) = (\beta_0^{(i)}, \dots, \beta_{m-1}^{(i)})$ in $W_m(E)$. Sia E' la chiusura normale di E in $\bar{F}$, cosicché E' è un'estensione di Galois di dimensione finita di F che contiene E. Formiamo $W_m(E')$ e facciamo agire su di esso, come prima, il gruppo di Galois G di E'/F. Per $s \in G$ e $\rho^{(i)} = (\rho_0^{(i)}, \dots, \rho_{m-1}^{(i)})$, da $\mathcal{P}\rho^{(i)} = \beta^{(i)}$ segue $\mathcal{P}(s\rho^{(i)}) = \beta^{(i)}$. Quindi $\mathcal{P}(s\rho^{(i)} - \rho^{(i)}) = 0$ e $s\rho^{(i)} - \rho^{(i)}$ appartiene al sottoanello fondamentale di $W_m(E')$. Ne segue $sE \subseteq E$ per $s \in G$, onde E è di Galois su F ed $E' = E$.

Per $s, t \in G$ si ha $s\rho^{(i)} = \rho^{(i)} + \gamma^{(i)}$, $t\rho^{(i)} = \rho^{(i)} + \delta^{(i)}$, con $\gamma^{(i)}, \delta^{(i)} \in W_m(F)$. Quindi $ts\rho^{(i)} = \rho^{(i)} + \gamma^{(i)} + \delta^{(i)} = st\rho^{(i)}$ e G è abeliano. Inoltre $s^k\rho^{(i)} = \rho^{(i)} + k\gamma^{(i)}$. Poiché $W_m(E)$ ha caratteristica p^m, ciò implica $s^{p^m} = 1$, e dunque G ha ordine p^g ed esponente p^e con $e \le m$. Sia χ_i il carattere di G definito da $\rho^{(i)}$, cioè $\chi_i(s) = s\rho^{(i)} - \rho^{(i)}$. È chiaro che $\chi_i(s) = 0$ per $1 \le i \le r$ implica $s = 1$. Ne segue che i χ_i generano $\widehat{G}$. Dunque, se ρ è un elemento di $W_m(E)$ tale che $\mathcal{P}\rho \in W_m(F)$, χ_ρ è una combinazione intera dei χ_i. Pertanto $\rho = \sum_i m_i\rho^{(i)} + \beta$, con $\beta \in W_m(F)$ e m_i interi. Allora $\mathcal{P}(\rho) = \sum_i m_i\beta^{(i)} + \mathcal{P}(\beta) \in Q$. Poiché ρ è un elemento arbitrario di $SW_m(E)$, ciò prova $QW_m(E) \subseteq Q$. L'inclusione opposta è chiara. □

I risultati ottenuti sono analoghi ai principali risultati sulle estensioni di Kummer. Essi stabiliscono una corrispondenza biunivoca fra le p-estensioni abeliane i cui gruppi di Galois hanno esponente p^e con $e \leq m$, e i sottogruppi Q di $(W_m(F), +)$ che contengono $\mathcal{P}W_m(F)$ come sottogruppo di indice finito.

Consideriamo ora il caso particolare delle p-estensioni cicliche. Anzitutto il teorema originario di Artin–Schreier è una conseguenza immediata della teoria generale. Ogni estensione ciclica di F di dimensione p è della forma $F(\rho)$, dove $\mathcal{P}\rho = \rho^p - \rho = \beta \in F$ e β è tale che non esiste $\alpha \in F$ con $\mathcal{P}\alpha = \beta$. Mostreremo ora che, se esiste una tale estensione, esistono estensioni cicliche di F di ogni dimensione p^m, $m \geq 1$. Ci occorre il lemma seguente.

Lemma 3. *Se $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1}) \in W_m(F)$, allora $p^{m-1}\beta \in \mathcal{P}W_m(F)$ se e solo se $\beta_0 \in \mathcal{P}F$.*

Dimostrazione. Iterando la (66) otteniamo $p^{m-1}\beta = (0, \ldots, 0, \beta_0^{p^{m-1}})$. Scriviamo poi

$$\begin{aligned}(0,\ldots,0,\beta_0) &- (0,\ldots,0,\beta_0^{p^{m-1}}) \\ &= [(0,\ldots,0,\beta_0) - (0,\ldots,0,\beta_0^p)] \\ &\quad + [(0,\ldots,0,\beta_0^p) - (0,\ldots,0,\beta_0^{p^2})] + \cdots \\ &\quad + [(0,\ldots,0,\beta_0^{p^{m-2}}) - (0,\ldots,0,\beta_0^{p^{m-1}})].\end{aligned}$$

Il secondo membro appartiene evidentemente a $\mathcal{P}W_m(F)$. Quindi $p^{m-1}\beta = (0, \ldots, 0, \beta_0^{p^{m-1}}) \in \mathcal{P}W_m(F)$ se e solo se $(0, \ldots, 0, \beta_0) \in \mathcal{P}W_m(F)$. Supponiamo che ciò avvenga e scriviamo $(0, \ldots, 0, \beta_0) = P\alpha - \alpha$ con $\alpha = (\alpha_0, \ldots, \alpha_{m-1}) \in W_m(F)$. Applicando R otteniamo $PR\alpha - R\alpha = 0$, dove $R\alpha = (\alpha_0, \ldots, \alpha_{m-2})$. Dunque per $\gamma = (\alpha_0, \alpha_1, \ldots, \alpha_{m-2}, 0)$ si ha $P\gamma = \gamma$ e, se $\delta = \alpha - \gamma$, allora $P\delta - \delta = (0, \ldots, 0, \beta_0)$. Inoltre $R\delta = R\alpha - R\gamma = 0$, onde $\delta = (0, \ldots, 0, \delta_{m-1})$. La (50) applicata a $P\delta = \delta + (0, \ldots, 0, \beta_0)$ implica $\mathcal{P}\delta_{m-1} = \beta_0$, cioè $\beta_0 \in \mathcal{P}F$. Viceversa, se questa condizione vale, si ha $\mathcal{P}\delta = (0, \ldots, 0, \beta_0)$ per $\delta = (0, \ldots, 0, \delta_{m-1})$, onde $p^{m-1}\beta \in \mathcal{P}W_m(F)$. □

Teorema 8.32. *Sia F un campo di caratteristica $p \neq 0$. Esistono estensioni cicliche di F di dimensione p^m, per ogni $m \geq 1$, se e solo se esistono tali estensioni di dimensione p. La condizione è $\mathcal{P}F \neq F$.*

Dimostrazione. Abbiamo visto che esiste un'estensione ciclica di dimensione p su F se e solo se $F \neq \mathcal{P}F$. Supponiamo che la condizione valga e scegliamo $\beta_0 \in F$, $\beta_0 \notin \mathcal{P}F$. Sia $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1})$, con β_i arbitrari in F per $i > 0$. Per il lemma 3, $p^{m-1}\beta \notin \mathcal{P}W_m(F)$. Ne segue che il sottogruppo Q di $(W_m(F), +)$ generato da β e $\mathcal{P}W_m(F)$ è tale che $Q/\mathcal{P}W_m(F)$ è ciclico di ordine p^m. Per il teorema 8.31, $Q = QW_m(E)$ per una p-estensione abeliana E/F. Abbiamo inoltre visto che il gruppo di Galois G di E/F è isomorfo a $Q/\mathcal{P}W_m(F)$. Esso è quindi ciclico di ordine p^m ed E/F è ciclica di dimensione p^m. □

Esercizio.

1. Mostrare che, se $\beta \in W_m(F)$ soddisfa $p^{m-1}\beta \in \mathcal{P}W_m(F)$, esiste $\gamma \in W_m(F)$ tale che $p\gamma \equiv \beta \pmod{\mathcal{P}W_m(F)}$. Servirsene per provare che ogni estensione ciclica di dimensione p^{m-1} su F si può immergere in un'estensione ciclica di dimensione p^m su F.

8.12 Basi di trascendenza

Un sottoinsieme finito $\{a_1, \ldots, a_n\}$, $n \geq 1$, di un'estensione E/F si dice *algebricamente dipendente* su F se l'omomorfismo

$$f(x_1, \ldots, x_n) \longmapsto f(a_1, \ldots, a_n) \tag{76}$$

dall'algebra dei polinomi $F[x_1, \ldots, x_n]$, con le x_i indeterminate, in E ha nucleo non nullo. In altre parole, esiste un polinomio non nullo $f(x_1, \ldots, x_n)$ tale che $f(a_1, \ldots, a_n) = 0$. Evidentemente se $\{a_1, \ldots, a_m\}$, $1 \leq m \leq n$, è algebricamente dipendente, lo è anche $\{a_1, \ldots, a_n\}$. Diremo ora che un qualsiasi sottoinsieme non vuoto di E è algebricamente dipendente su F se qualche suo sottoinsieme finito possiede questa proprietà. Vale il seguente criterio.

Teorema 8.33. *Un sottoinsieme non vuoto S di un'estensione E/F è algebricamente dipendente su F se e solo se esiste $a \in S$ che è algebrico su $F(S - \{a\})$.*

Dimostrazione. Se T è un sottoinsieme di E e a è algebrico su $F(T)$, allora a è algebrico su $F(U)$ per qualche sottoinsieme finito U di T. Basta pertanto dimostrare il teorema per S finito, diciamo $S = \{a_1, \ldots, a_n\}$. Supponiamo dapprima che S sia algebricamente dipendente. Dimostreremo per induzione su n che esiste un a_i algebrico su $F(S_i)$, dove $S_i = S - \{a_i\}$. Per $n = 1$ ciò è chiaro dalle definizioni; supponiamo dunque $n > 1$. Possiamo anche supporre che $\{a_1, \ldots, a_{n-1}\}$ sia *algebricamente indipendente* (ossia non algebricamente dipendente). Abbiamo allora un polinomio $f(x_1, \ldots, x_n) \neq 0$ tale che $f(a_1, \ldots, a_n) = 0$. Scriviamo

$$f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1})x_n^m + f_1(x_1, \ldots, x_{n-1})x_n^{m-1} + \cdots + f_m(x_1, \ldots, x_{n-1})$$

con $f_0(x_1, \ldots, x_{n-1}) \neq 0$. Allora $f_0(a_1, \ldots, a_{n-1}) \neq 0$, sicché

$$g(x) = f_0(a_1, \ldots, a_{n-1})x^m + f_1(a_1, \ldots, a_{n-1})x^{m-1} + \cdots + f_m(a_1, \ldots, a_{n-1})$$

è un polinomio non nullo in $F(a_1, \ldots, a_{n-1})[x]$ tale che $g(a_n) = 0$. Quindi a_n è algebrico su $F(a_1, \ldots, a_{n-1})$.

Viceversa, supponiamo che uno degli a_i sia algebrico su $F(S_i)$, con $S_i = S - \{a_i\}$. Possiamo supporre $i = n$. Esistono allora $b_1, \ldots, b_m \in F(a_1, \ldots, a_{n-1})$ tali che $g(a_n) = 0$ per $g(x) = x^m + b_1x^{m-1} + \cdots + b_m \in F(a_1, \ldots, a_{n-1})[x]$. Esistono polinomi $f_0, \ldots, f_m \in F[x_1, \ldots, x_{n-1}]$, con $f_0(a_1, \ldots, a_{n-1}) \neq 0$, tali che $b_i = f_i(a_1, \ldots, a_{n-1})f_0(a_1, \ldots, a_{n-1})^{-1}$. Ponendo

$$\begin{aligned} f(x_1, \ldots, x_n) = {} & f_0(x_1, \ldots, x_{n-1})x_n^m + f_1(x_1, \ldots, x_{n-1})x_n^{m-1} \\ & + \cdots + f_m(x_1, \ldots, x_{n-1}) \end{aligned}$$

si avrà $f(x_1, \ldots, x_n) \neq 0$ e $f(a_1, \ldots, a_n) = 0$. Dunque S è algebricamente dipendente su F. □

Introduciamo ora una corrispondenza dall'insieme E all'insieme $\mathcal{P}(E)$ dei suoi sottoinsiemi, che risulterà essere una relazione di dipendenza su E nel senso definito alle pp. 122–123.

Definizione 8.1. Un elemento a di E si dice *algebricamente dipendente su F dal sottoinsieme S* (che può essere vuoto) se a è algebrico su $F(S)$. In tal caso scriviamo $a \prec S$.

Con questa definizione, il teorema 8.33 afferma che un sottoinsieme non vuoto S è algebricamente dipendente su F se e solo se esiste $a \in S$ algebricamente dipendente su F da $S - \{a\}$. Mostreremo ora che la corrispondenza $\prec$ fra gli elementi e i sottoinsiemi di E soddisfa gli assiomi di una relazione di dipendenza, ossia si ha il

Teorema 8.34. *La corrispondenza $\prec$ da E a $\mathcal{P}(E)$ della definizione 8.1 è una relazione di dipendenza.*

Dimostrazione. Gli assiomi da verificare sono i seguenti. (i) Se $a \in S$, allora $a \prec S$. (ii) Se $a \prec S$, allora $a \prec U$ per qualche sottoinsieme finito U di S. (iii) Se $a \prec S$ e ogni $b \in S$ soddisfa $b \prec T$, allora $a \prec T$. (iv) Se $a \prec S$ e $a \not\prec S - \{b\}$ per qualche $b \in S$, allora $b \prec (S - \{b\}) \cup \{a\}$. L'assioma (i) è chiaro e la (ii) è stata osservata nella dimostrazione del teorema 8.33. Per provare la (iii), sia A il sottocampo di E degli elementi algebrici su $F(T)$. Allora $S \subseteq A$ e, se $a \prec S$, a è algebrico su A. Quindi $a \in A$, ossia $a \prec T$. Per provare la (iv), siano $a \prec S$ e $a \not\prec S - \{b\}$, con $b \in S$. Poniamo $K = F(T)$, dove $T = S - \{b\}$. Allora a è trascendente su K e algebrico su $K(b)$. Per il teorema 8.33, $\{a, b\}$ è quindi algebricamente dipendente su K e perciò esiste un polinomio $f(x, y) \neq 0$ nelle indeterminate x, y, a coefficienti in K, tale che $f(a, b) = 0$. Possiamo scrivere $f(x, y) = a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_m(x)$, con $a_i(x) \in K[x]$ e $a_0(x) \neq 0$. Allora $a_0(a) \neq 0$, sicché $f(a, y) \neq 0$ in $K(a)[y]$, e da $f(a, b) = 0$ risulta che b è algebrico su $K(a) = F(T \cup \{a\})$. Dunque $b \prec T \cup \{a\}$, come richiesto. □

Possiamo ora applicare alla dipendenza algebrica i risultati ottenuti sulle relazioni di dipendenza. Il concetto di base diventa quello di base di trascendenza, formulato nella

Definizione 8.2. Se E è un'estensione di F, un sottoinsieme B di E si dice *base di trascendenza* di E su F se (1) B è algebricamente indipendente e (2) ogni $a \in E$ è algebricamente dipendente da B.

I due risultati dimostrati nel caso generale danno ora il

Teorema 8.35. *E/F possiede una base di trascendenza e due basi di questo tipo hanno la stessa cardinalità.*

Si osservi che B può essere vuoto. Ciò accade se e solo se E è algebrico su F. La cardinalità $|B|$ si chiama il *grado di trascendenza* (tr deg) di E/F. Un campo E si dice *puramente trascendente* su F se possiede una base di trascendenza B per cui $E = F(B)$.

Esercizi.

1. Sia $E \supseteq K \supseteq F$. Mostrare che $\operatorname{tr\,deg} E/F = \operatorname{tr\,deg} E/K + \operatorname{tr\,deg} K/F$.
2. Mostrare che, se $\operatorname{char} F \neq 3$ ed $E = F(a, b)$ con a trascendente su F e $a^3 + b^3 = 1$, allora E non è puramente trascendente su F.
3. Sia $\mathbb{C}$ il campo dei numeri complessi e $\mathbb{Q}$ quello dei razionali. Mostrare che $\operatorname{tr\,deg} \mathbb{C}/\mathbb{Q} = |\mathbb{C}|$. Mostrare che, se B è una base di trascendenza di $\mathbb{C}/\mathbb{Q}$, ogni biiezione di B su sé stesso si estende a un automorfismo di $\mathbb{C}/\mathbb{Q}$. Concluderne che vi sono tanti automorfismi di $\mathbb{C}/\mathbb{Q}$ quante biiezioni di $\mathbb{C}$ su $\mathbb{C}$.
4. Mostrare che ogni campo intermedio di un'estensione finitamente generata E/F è finitamente generato su F.
5. Sia $E = F(x_1, \ldots, x_m)$, dove le x_i sono algebricamente indipendenti. Si dica *omogenea di grado* k ($k \in \mathbb{Z}$) un'espressione razionale $f = gh^{-1}$ se g è un polinomio omogeneo di grado r, h è un polinomio omogeneo di grado s e $r - s = k$. Mostrare che l'insieme E_0 delle espressioni razionali omogenee di grado 0 è un sottocampo di E puramente trascendente di grado di trascendenza $m - 1$ su F. Mostrare che E è un'estensione trascendente semplice di E_0.

8.13 Basi di trascendenza dei domini. Algebre affini

Sia D un dominio commutativo che sia un'algebra su un campo F e sia E il campo delle frazioni di D, cosicché $F \subseteq D \subseteq E$. Evidentemente, poiché $F(D)$ è un sottocampo di E contenente D, si

ha $F(D) = E$ e dunque D contiene una base di trascendenza di E/F (si veda l'osservazione (ii) sulle basi a p. 124). Chiamiamo $\operatorname{tr\,deg} E/F$ il *grado di trascendenza* di D/F. Questo concetto è importante nello studio degli omomorfismi fra domini che siano algebre sullo stesso campo F. Vale infatti il seguente teorema.

Teorema 8.36. *(i) Siano D/F e D'/F domini e supponiamo che esista un omomorfismo suriettivo η di D/F su D'/F. Allora $\operatorname{tr\,deg} D/F \geq \operatorname{tr\,deg} D'/F$. (ii) Inoltre, se $\operatorname{tr\,deg} D/F = \operatorname{tr\,deg} D'/F = m < \infty$, allora η è un isomorfismo.*

Dimostrazione. (i) Sia B' una base di trascendenza di D'/F. Per ogni $x' \in B'$ scegliamo $x \in D$ tale che $\eta x = x'$. Allora $C = \{x\}$ è un sottoinsieme algebricamente indipendente di D. Dunque C si può completare a una base B di E/F, dove E è il campo delle frazioni di D (si veda l'osservazione (i) a p. 124). Quindi

$$\operatorname{tr\,deg} D/F = |B| \geq |C| = |B'| = \operatorname{tr\,deg} D'/F.$$

(ii) Siano ora $B' = \{x'_1, \ldots, x'_m\}$, $C = \{x_1, \ldots, x_m\}$ con $\eta x_i = x'_i$. Poiché C è un insieme algebricamente indipendente di cardinalità $\operatorname{tr\,deg} E/F$, $B = C$ è una base di trascendenza di D/F. Sia a un elemento non nullo di D. Allora a è algebrico su $F(x_1, \ldots, x_m)$. Sia $m(\lambda) = \lambda^n + \alpha_1\lambda^{n-1} + \cdots + \alpha_n$, con $\alpha_i \in F(x_1, \ldots, x_m)$, il suo polinomio minimo su questo campo. Poiché $a \neq 0$, $\alpha_n \neq 0$. Possiamo scrivere $\alpha_i = g_i(x_1, \ldots, x_m)g_0(x_1, \ldots, x_m)^{-1}$ con $g_i, g_0 \in F[x_1, \ldots, x_m]$. Allora

$$g_0(x_1, \ldots, x_m)a^n + g_1(x_1, \ldots, x_m)a^{n-1} + \cdots + g_n(x_1, \ldots, x_m) = 0,$$

e quindi

$$g_0(x'_1, \ldots, x'_m)(\eta a)^n + \cdots + g_n(x'_1, \ldots, x'_m) = 0. \tag{77}$$

Poiché $\alpha_n \neq 0$, si ha $g_n(x_1, \ldots, x_m) \neq 0$ e, per l'indipendenza algebrica degli x'_i, $g_n(x'_1, \ldots, x'_m) \neq 0$. Allora, per la (77), $\eta a \neq 0$. Dunque $a \neq 0$ implica $\eta a \neq 0$ e η è un isomorfismo. □

Dimostriamo ora l'importante

Teorema di normalizzazione di Noether. *Sia D un dominio finitamente generato su un campo F, diciamo $D = F[u_1, \ldots, u_m]$. Sia $\operatorname{tr\,deg} D = r \leq m$. Allora esiste una base di trascendenza $\{v_1, \ldots, v_r\}$ tale che D è intero su $F[v_1, \ldots, v_r]$.*

Dimostrazione. Il risultato è ovvio se $m = r$, quindi supponiamo $m > r$. Gli u_i sono allora algebricamente dipendenti. Esiste pertanto un polinomio non nullo

$$f(x_1, \ldots, x_m) = \sum a_{j_1 \ldots j_m} x_1^{j_1} \cdots x_m^{j_m}$$

nelle indeterminate x_i, a coefficienti in F, tale che $f(u_1, \ldots, u_m) = 0$. Sia X l'insieme dei monomi $x_1^{j_1} \cdots x_m^{j_m}$ che compaiono in f con coefficienti non nulli. A ciascun monomio $x_1^{j_1} \cdots x_m^{j_m}$ associamo il polinomio $j_1 + j_2 t + \cdots + j_m t^{m-1} \in \mathbb{Z}[t]$, con t indeterminata. I polinomi ottenuti in questo modo dai monomi di X sono distinti. Poiché un polinomio di grado n in una indeterminata a coefficienti in un campo ha al più n zeri nel campo, esiste un intero $d \geq 0$ per il quale gli interi $j_1 + j_2 d + \cdots + j_m d^{m-1}$ ottenuti dai monomi di X sono distinti. Consideriamo ora il polinomio $f(x_1, x_1^d + y_2, \ldots, x_1^{d^{m-1}} + y_m)$, dove le y_i sono indeterminate. Abbiamo

$$\begin{aligned} &f(x_1, x_1^d + y_2, \ldots, x_1^{d^{m-1}} + y_m) \\ &\quad = \sum a_{j_1 \ldots j_m} x_1^{j_1} (x_1^d + y_2)^{j_2} \cdots (x_1^{d^{m-1}} + y_m)^{j_m} \\ &\quad = \sum a_{j_1 \ldots j_m} x_1^{j_1 + j_2 d + \cdots + j_m d^{m-1}} + g(x_1, y_2, \ldots, y_m), \end{aligned}$$

dove il grado in x_1 di g è inferiore al grado della somma $\sum a_{j_1\dots j_m} x_1^{j_1+j_2 d+\cdots+j_m d^{m-1}}$. Pertanto, per un opportuno $\beta \in F^*$, il polinomio $\beta f(x_1, x_1^d+y_2, \dots, x_1^{d^{m-1}}+y_m)$ è monico in x_1 a coefficienti in $F[y_2, \dots, y_m]$. Ponendo $w_i = u_i - u_1^{d^{i-1}}$, $2 \le i \le m$, abbiamo $\beta f(u_1, u_1^d+w_2, \dots, u_1^{d^{m-1}}+w_m) = 0$, da cui segue che u_1 è intero su $D' = F[w_2, \dots, w_m]$. Per induzione sul numero dei generatori, D' ha una base di trascendenza $\{v_i\}$ tale che D' è intero su $F[v_1, \dots, v_r]$. Allora D è intero su $F[v_1, \dots, v_r]$ per la transitività della dipendenza intera. □

Un'algebra commutativa finitamente generata su un campo si chiama *algebra affine*. Una tale algebra è noetheriana (corollario al teorema della base di Hilbert, p. 421). Ricordiamo che la dimensione di Krull di un anello noetheriano è definita come l'estremo superiore degli s per le catene di ideali primi $P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$ in R. Possiamo ora dimostrare il seguente teorema sulla dimensione di un dominio affine.

Teorema 8.37. *Sia D un dominio affine di grado di trascendenza r su F. Allora la dimensione di Krull soddisfa* $\dim D \ge r$, *e* $\dim D = r$ *se F è algebricamente chiuso.*

Dimostrazione. Per il teorema di normalizzazione di Noether possiamo scrivere $D = F[u_1, \dots, u_r, u_{r+1}, \dots, u_m]$, dove gli u_i, $1 \le i \le r$, costituiscono una base di trascendenza e i restanti u_j sono interi su $F[u_1, \dots, u_r]$. Allora $F[u_1, \dots, u_r]$ è fattoriale e quindi è integralmente chiuso nel suo campo delle frazioni. In queste condizioni possiamo applicare il teorema di discesa per mostrare che $\dim D = \dim F[u_1, \dots, u_r]$. Sia anzitutto $p_0 \supsetneq p_1 \supsetneq \cdots \supsetneq p_s$ una catena strettamente discendente di ideali primi di $F[u_1, \dots, u_r]$. Per il teorema 7.5 di esistenza di un primo sovrastante, esiste un ideale primo P_0 di D tale che $P_0^c = P_0 \cap F[u_1, \dots, u_r] = p_0$. Per il teorema 7.6 esiste un ideale primo P_1 di D tale che $P_1^c = p_1$ e $P_0 \supseteq P_1$. Allora $P_0 \supsetneq P_1$. Otteniamo quindi per induzione una catena di ideali primi $P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$ tali che $P_i \cap F[u_1, \dots, u_r] = p_i$, $0 \le i \le s$. Ciò implica $\dim D \ge \dim F[u_1, \dots, u_r]$. Sia ora $P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_s$ una catena di ideali primi P_i di D. Per il corollario 2 alla proposizione 7.17 (p. 410), $p_0 \supsetneq p_1 \supsetneq \cdots \supsetneq p_s$, $p_i = P_i^c$, è una catena strettamente discendente di ideali primi di $F[u_1, \dots, u_r]$. Ne segue che $\dim F[u_1, \dots, u_r] \ge \dim D$. Dunque $\dim D = \dim F[u_1, \dots, u_r]$. Ora in $F[u_1, \dots, u_r]$ si ha la catena di ideali primi

$$(u_1, \dots, u_r) \supsetneq (u_1, \dots, u_{r-1}) \supsetneq \cdots \supsetneq (u_1) \supsetneq (0).$$

Quindi $\dim D = \dim F[u_1, \dots, u_r] \ge r = \operatorname{tr\,deg} D/F$. D'altra parte abbiamo mostrato in precedenza (p. 453) che, se F è algebricamente chiuso, $\dim F[u_1, \dots, u_r] = r$ per u_i algebricamente indipendenti. La dimostrazione è completa. □

Esercizio.

1. Usare il teorema di normalizzazione di Noether per dimostrare il corollario che identifica gli ideali massimali di $F[x_1, \dots, x_n]$ (p. 430). *Traccia.* Sia M un ideale massimale di $F[x_1, \dots, x_n]$, dove le x_i sono indeterminate e F è algebricamente chiuso. Allora $F[x_1, \dots, x_n]/M$ è un campo che è anche un'algebra affine $F[\bar{x}_1, \dots, \bar{x}_n]$, con $\bar{x}_i = x_i + M$. Per il teorema di normalizzazione di Noether e la proposizione 7.17, $\operatorname{tr\,deg} F[x_1, \dots, x_n]/M = 0$. Poiché F è algebricamente chiuso, $F[x_1, \dots, x_n]/M = F$. Dunque $\bar{x}_i = a_i \in F$, $1 \le i \le n$, e $M = (x_1 - a_1, \dots, x_n - a_n)$.

8.14 Il teorema di Lüroth

Le estensioni puramente trascendenti E/F, specialmente quelle di grado di trascendenza finito, sembrano essere il tipo più semplice di estensioni. È chiaro che un tale campo è isomorfo

al campo delle frazioni $F(x_1, \ldots, x_n)$ dell'anello dei polinomi $F[x_1, \ldots, x_n]$ nelle indeterminate $x_1, \ldots, x_n$. Benché questi campi sembrino del tutto innocui, come si è osservato in *BA I* (p. 270), vi sono problemi difficili e irrisolti, in particolare sulla natura dei sottocampi di $F(x_1, \ldots, x_n)/F$. Un problema del tipo menzionato in *BA I* che, per quanto ne sappiamo, resta irrisolto (benché fosse enunciato come esercizio nella prima edizione delle *Lectures in Abstract Algebra* dell'autore, vol. III, 1964, p. 160) è il seguente. Si faccia agire il gruppo alterno A_n su $F(x_1, \ldots, x_n)$ mediante automorfismi di questo campo su F, in modo che $\pi x_i = x_{\pi i}$, $1 \leq i \leq n$, per $\pi \in A_n$, e sia $\operatorname{Inv} A_n$ il sottocampo dei punti fissi di questa azione. Il campo $\operatorname{Inv} A_n$ è puramente trascendente su F?

Il caso in cui la situazione è assai semplice è quello in cui E ha grado di trascendenza uno. Consideriamo questo caso. Sia $E = F(t)$, con t trascendente, e sia $u \in E$, $u \notin F$. Possiamo scrivere $u = f(t)g(t)^{-1}$ con $f(t), g(t) \in F[t]$ e $(f(t), g(t)) = 1$. Se n è il maggiore dei gradi di $f(t)$ e $g(t)$, possiamo scrivere

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n,$$
$$g(t) = b_0 + b_1 t + \cdots + b_n t^n,$$

con $a_i, b_i \in F$ e almeno uno fra a_n, b_n non nullo. Si ha $f(t) - ug(t) = 0$, ossia

$$(a_n - ub_n)t^n + (a_{n-1} - ub_{n-1})t^{n-1} + \cdots + (a_0 - ub_0) = 0, \tag{78}$$

e $a_n - ub_n \neq 0$ poiché almeno uno tra a_n, b_n è non nullo e $u \notin F$. La (78) mostra dunque che t è algebrico su $F(u)$ e $[F(t) : F(u)] \leq n$. Dimostriamo ora il risultato più preciso che segue.

Teorema 8.38. *Sia $E = F(t)$, con t trascendente su F, e sia $u \in F(t)$, $u \notin F$. Scriviamo $u = f(t)g(t)^{-1}$ con $(f(t), g(t)) = 1$ e sia $n = \max(\deg f(t), \deg g(t))$. Allora u è trascendente su F, t è algebrico su $F(u)$ e $[F(t) : F(u)] = n$. Inoltre il polinomio minimo di t su $F(u)$ è un multiplo scalare, per uno scalare di $F(u)$, di $f(x, u) = f(x) - ug(x)$.*

Dimostrazione. Poniamo $f(x, y) = f(x) - yg(x) \in F[x, y]$, con x, y indeterminate. Questo polinomio in x, y è di primo grado in y e non ha fattori $h(x)$ di grado positivo, poiché $(f(x), g(x)) = 1$. Esso è dunque irriducibile in $F[x, y]$. Ora t è algebrico su $F(u)$, sicché, se u fosse algebrico su F, t sarebbe algebrico su F, contrariamente all'ipotesi. Quindi u è trascendente su F. Allora $F[x, u] \simeq F[x, y]$ mediante l'isomorfismo su F che fissa x e manda u in y, e quindi $f(x, u)$ è irriducibile in $F[x, u]$. Ne segue che $f(x, u)$ è irriducibile in $F(u)[x]$ (*BA I*, p. 153). Poiché $f(t, u) = f(t) - ug(t) = 0$, ne segue che $f(x, u)$ è un multiplo scalare in $F(u)$ del polinomio minimo di t su $F(u)$. Dunque $[F(t) : F(u)]$ è il grado in x di $f(x, u)$. Questo grado è n, e la dimostrazione è completa. □

Una prima conseguenza del teorema è che possiamo determinare gli elementi u che generano $F(t)$. Essi hanno la forma $u = f(t)g(t)^{-1}$, dove $f(t)$ e $g(t)$ hanno grado 1 o 0, $(f(t), g(t)) = 1$ e almeno uno fra $f(t)$ e $g(t)$ non appartiene a F. Allora

$$u = \frac{at + b}{ct + d}, \tag{79}$$

dove $a, b, c, d \in F$, almeno uno fra a, c è non nullo e $at + b$, $ct + d$ non hanno fattori comuni di grado positivo. Si vede facilmente che questo insieme di condizioni equivale all'unica condizione

$$ad - bc \neq 0. \tag{80}$$

Ora, se $F(u) = F(t)$, esiste un unico automorfismo di $F(t)/F$ che manda t in u, e ogni automorfismo si ottiene in questo modo. La condizione (80) vale per la matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{81}$$

se e solo se A è invertibile. Consideriamo ora il gruppo lineare $\mathrm{GL}_2(F)$ di queste matrici (*BA I*, p. 375). Ogni matrice $A \in \mathrm{GL}_2(F)$ della forma (81) determina un generatore $u = (at+b)/(ct+d)$ di $F(t)$ e quindi l'automorfismo $\eta(A)$ di $F(t)/F$ tale che

$$\eta(A)t = \frac{at+b}{ct+d}. \tag{82}$$

Se $A' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \mathrm{GL}_2(F)$, allora

$$\eta(A)\eta(A')t = \frac{(a'a+b'c)t+(a'b+b'd)}{(c'a+d'c)t+(c'b+d'd)} = \eta(A'A)t. \tag{83}$$

Poiché ogni automorfismo di $F(t)/F$ manda t in un generatore, η è suriettivo. Per la (83), η è quindi un antiomomorfismo di $\mathrm{GL}_2(F)$ su $\mathrm{Gal}(F(t)/F)$. Il nucleo consta delle matrici A della forma (81) tali che $(at+b)(ct+d)^{-1} = t$, ossia $at+b = ct^2+dt$. Ciò dà $c = b = 0$ e $a = d$. Quindi il nucleo è l'insieme delle matrici scalari $a1$, $a \neq 0$. Il gruppo quoziente $\mathrm{GL}_2(F)/F^*1$ si chiama *gruppo lineare proiettivo* e si indica con $\mathrm{PGL}_2(F)$. Dunque $\mathrm{Gal}(F(t)/F)$ è antiisomorfo a $\mathrm{PGL}_2(F)$ e, poiché ogni gruppo è antiisomorfo a sé stesso (mediante $g \mapsto g^{-1}$), si ha anche $\mathrm{Gal}(F(t)/F) \simeq \mathrm{PGL}_2(F)$.

Per $E = F(t)$, con t trascendente, si possono determinare tutti i sottocampi di E/F: essi hanno la forma $F(u)$ per qualche u. Questo importante risultato è noto come

Teorema di Lüroth. *Se $E = F(t)$ con t trascendente su F, ogni campo intermedio K di E/F diverso da F ha la forma $F(u)$, con u trascendente su F.*

Dimostrazione. Sia $v \in K$, $v \notin F$. Abbiamo visto che t è algebrico su $F(v)$, e quindi t è algebrico su K. Sia $f(x) = x^n + k_1x^{n-1} + \cdots + k_n$ il polinomio minimo di t su K, sicché $k_i \in K$ e $n = [F(t) : K]$. Poiché t non è algebrico su F, qualche k_j non appartiene a F. Mostreremo che $K = F(u)$ per $u = k_j$. Possiamo scrivere $u = g(t)h(t)^{-1}$ con $g(t), h(t) \in F[t]$, $(g(t), h(t)) = 1$ e $m = \max(\deg h, \deg g) > 0$. Come abbiamo dimostrato nel teorema 8.38, $[E : F(u)] = m$. Poiché $K \supseteq F(u)$ e $[E : K] = n$, si ha evidentemente $m \geq n$, e vale l'uguaglianza se e solo se $K = F(u)$. Ora t è uno zero del polinomio $g(x) - uh(x) \in K[x]$. Esiste quindi $q(x) \in K[x]$ tale che

$$g(x) - uh(x) = q(x)f(x). \tag{84}$$

I coefficienti k_i di $f(x)$ appartengono a $F(t)$, cosicché esiste un polinomio non nullo $c_0(t)$ di grado minimo tale che $c_0(t)k_i = c_i(t) \in F[t]$ per $1 \leq i \leq n$. Allora $c_0(t)f(x) = f(x,t) = c_0(t)x^n + c_1(t)x^{n-1} + \cdots + c_n(t) \in F[x,t]$, e $f(x,t)$ è primitivo come polinomio in x, ossia i $c_i(t)$ sono primi fra loro nel loro insieme. Il grado in x di $f(x,t)$ è n e, poiché $k_j = g(t)h(t)^{-1}$ con $(g(t), h(t)) = 1$, il grado in t di $f(x,t)$ è almeno m. Nella (84) sostituiamo ora u con $g(t)h(t)^{-1}$ e i coefficienti di $q(x)$ con le loro espressioni in t. La (84) mostra che $f(x,t)$ divide $g(x)h(t) - g(t)h(x)$ in $F(t)[x]$. Poiché $f(x,t)$ e $g(x)h(t) - g(t)h(x)$ appartengono a $F[x,t]$ e $f(x,t)$ è primitivo come polinomio in x, esiste un polinomio $q(x,t) \in F[x,t]$ tale che

$$g(x)h(t) - g(t)h(x) = f(x,t)q(x,t). \tag{85}$$

Poiché il grado in t del primo membro è al più m e quello di $f(x,t)$ è almeno m, ne segue che tale grado è m e $q(x,t) = q(x) \in F[x]$. Il secondo membro è allora primitivo come polinomio in x e lo è quindi anche il primo. Per simmetria il primo membro è primitivo anche come polinomio in t. Dunque $q(x) = q \in F$. Allora $f(x,t)$ ha lo stesso grado in x e in t, sicché $m = n$, da cui $K = F(u)$. □

Indichiamo ora alcuni risultati noti sui sottocampi di estensioni puramente trascendenti di grado di trascendenza maggiore di uno. Usiamo la terminologia della geometria algebrica, nella quale un'estensione puramente trascendente E/F è detta *razionale* e un sottocampo di una tale E/F è detto *unirazionale*. In *BA I* (p. 270) abbiamo menzionato alcuni risultati e dato alcuni riferimenti sui campi unirazionali della forma $\operatorname{Inv} G$, dove G è un gruppo finito di automorfismi di un campo $F(x_1, \ldots, x_n)/F$ e le x_i sono indeterminate permutate da G. Altri risultati sulla razionalità e la non razionalità dei campi della forma $\operatorname{Inv} G$ sono raccolti nell'articolo di rassegna di D. J. Saltman, «Groups acting on fields: Noether's problem», *Contemporary Mathematics*, vol. 43 (1985), pp. 267–277.

Un risultato classico sui sottocampi delle estensioni razionali di grado di trascendenza due è il teorema di Castelnuovo–Zariski: se F è algebricamente chiuso di caratteristica 0, ogni sottocampo L di un'estensione razionale $F(x_1, x_2)$ tale che $F(x_1, x_2)$ sia affine su L è razionale. Il risultato non vale sempre in caratteristica $p \neq 0$ (si veda R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, p. 422).

Esempi di sottocampi non razionali di estensioni razionali di grado di trascendenza 3 su $\mathbb{C}$ sono dati nei lavori seguenti.

1. M. Artin e D. Mumford, «Some elementary examples of unirational varieties that are not rational», *Proc. London Math. Soc.*, vol. 25, 3ł serie (1972), pp. 75–95.

2. G. H. Clemens e P. A. Griffiths, «The intermediate Jacobian of the cubic threefold», *Annals of Math.* (2), vol. 95 (1972), pp. 281–356.

3. V. A. Iskovskikh e J. Manin, «Three dimensional quartics and counterexamples to the Lüroth problem», *Math. Sbornik*, vol. 86 (1971), pp. 140–166.

A. Beauville, J.-L. Colliot-Thélène, J.-J. Sansuc e Sir P. Swinnerton-Dyer, in «Variétés stablement rationnelles non rationnelles», *Annals of Math.* (2), vol. 121, pp. 283–318, hanno fornito un esempio di estensione $K/\mathbb{C}$ di grado di trascendenza tre tale che un'estensione puramente trascendente di grado di trascendenza tre su K è puramente trascendente di grado sei su $\mathbb{C}$, ma K non è razionale su $\mathbb{C}$.

Esercizi.

1. Sia F_q un campo di q elementi e sia K il sottocampo degli elementi di $F_q(t)$, t trascendente, fissati da $\operatorname{Gal}(F_q(t)/F_q)$. Determinare un elemento u tale che $K = F_q(u)$.

2. Sia $E = F(t, v)$, con t trascendente su F e $v^2 + t^2 = 1$. Mostrare che E è puramente trascendente su F.

I due esercizi seguenti delineano dimostrazioni dovute a Mowaffaq Hajja (in corso di pubblicazione in *Algebras, Groups, and Geometries*) del fatto che $\operatorname{Inv} A_3$ e $\operatorname{Inv} A_4$ sono razionali. Si tratta di un miglioramento di risultati di Burnside apparsi nel *Messenger of Mathematics*, vol. 37 (1908), p. 165. Ricordiamo inoltre che Takashi Maeda ha recentemente dimostrato (lavoro in corso di pubblicazione sul *J. of Algebra*) che $\operatorname{Inv} A_5$, per il campo base $\mathbb{Q}$, è razionale. La questione per $\operatorname{Inv} A_n$, con $n > 5$, è ancora aperta.

3. Mostrare che $\operatorname{Inv} A_3$ in $K = F(x_1, x_2, x_3)$ è razionale.

   Traccia. Distinguiamo tre casi: (i) F contiene una radice cubica primitiva dell'unità, il che implica $\operatorname{char} F \neq 3$; (ii) $\operatorname{char} F \neq 3$, ma F non contiene alcuna radice cubica primitiva dell'unità; (iii) $\operatorname{char} F = 3$.

In tutti i casi A_3 è il gruppo di automorfismi di K/F generato dall'automorfismo σ tale che $x_1 \mapsto x_2$, $x_2 \mapsto x_3$, $x_3 \mapsto x_1$. Inoltre $\mathrm{Gal}(K/\operatorname{Inv} A_3) = A_3$ e $[K : \operatorname{Inv} A_3] = |A_3| = 3$. Nel caso (i) poniamo $X_j = x_1 + w^j x_2 + w^{2j} x_3$ con $w^3 = 1$, $w \neq 1$. Allora $\sigma X_j = w^{-j} X_j$ e $K = F(X_1, X_2, X_3)$. Poniamo $Y_1 = X_1^2/X_2$, $Y_2 = X_2^2/X_1$, $Y_3 = X_3$. Allora $\sigma Y_j = Y_j$, sicché $F(Y_1, Y_2, Y_3) \subseteq \operatorname{Inv} A_3$. D'altra parte $X_1^3 = Y_1^2 Y_2$ e $K = F(X_1, X_2, X_3) = F(Y_1, Y_2, Y_3, X_1)$. Quindi $[K : F(Y_1, Y_2, Y_3)] \leq 3$. Ne segue che $\operatorname{Inv} A_3 = F(Y_1, Y_2, Y_3)$.

Nel caso (ii) aggiungiamo a K una radice cubica primitiva dell'unità w, ottenendo $K' = K(w) = F'(x_1, x_2, x_3)$ per $F' = F(w)$. Abbiamo $w^2 + w + 1 = 0$, (w, w^2) è una base di K'/K e di F'/F, ed esiste un automorfismo τ di K'/K tale che $w \mapsto w^2$. Come nel caso (i), definiamo $X_j = x_1 + w^j x_2 + w^{2j} x_3$, $j = 1, 2, 3$, $Y_1 = X_1^2/X_2$, $Y_2 = X_2^2/X_1$, $Y_3 = X_3 = x_1 + x_2 + x_3$. Allora in K' si ha $\operatorname{Inv} A_3 = F'(Y_1, Y_2, Y_3)$. Si ha $\tau Y_1 = Y_2$, $\tau Y_2 = Y_1$, $\tau Y_3 = Y_3 \in K$. Quindi, se $Y_1 = wZ_1 + w^2 Z_2$ con $Z_i \in K$, allora $Y_2 = w^2 Z_1 + wZ_2$ e $\sigma Y_2 = Y_2$ implica $\sigma Z_i = Z_i$. Pertanto in K si ha $\operatorname{Inv} A_3 = F(Z_1, Z_2, X_3)$.

Nel caso (iii) poniamo $\Delta = \sigma - 1$ e $U_j = \Delta^j x_1$, $j = 0, 1, 2$. Allora $K = F(U_0, U_1, U_2)$, $\sigma U_0 = U_0 + U_1$, $\sigma U_1 = U_1 + U_2$, $\sigma U_2 = U_2$. Poniamo $U = U_0 U_2 + U_1^2 - U_1 U_2$. Allora $K = F(U, U_1, U_2)$, $\sigma U = U$, $\sigma U_1 = U_1 + U_2$ e $\sigma U_2 = U_2$. Quindi $\sigma(U_1^3 - U_1 U_2^2) = U_1^3 - U_1 U_2^2$ e $\operatorname{Inv} A_3 \supseteq F(U, U_2, U_1^3 - U_1 U_2^2)$. Poiché $[K : F(U, U_2, U_1^3 - U_1 U_2^2)] \leq 3$, ne segue $\operatorname{Inv} A_3 = F(U, U_2, U_1^3 - U_1 U_2^2)$. (Cfr. l'esercizio 1, p. 271 di *BA I.*)

4. Mostrare che $\operatorname{Inv} A_4$ in $K = F(x_1, x_2, x_3, x_4)$ è razionale.

   Traccia. È chiaro che A_4 è generato dagli automorfismi α, β, σ di K/F tali che

	x_1	x_2	x_3	x_4
α	x_2	x_1	x_4	x_3
β	x_3	x_4	x_1	x_2
σ	x_2	x_3	x_1	x_4

   Se $\operatorname{char} F \neq 2$ definiamo

$$s = x_1 + x_2 + x_3 + x_4, \quad z_1 = x_1 + x_2 - x_3 - x_4,$$
$$z_2 = x_1 - x_2 + x_3 - x_4, \quad z_3 = x_1 - x_2 - x_3 + x_4.$$

   Allora $K = F(s, z_1, z_2, z_3)$. L'azione di α, β, σ su (s, z_1, z_2, z_3) è data dalla tavola

	s	z_1	z_2	z_3
α	s	z_1	$-z_2$	$-z_3$
β	s	$-z_1$	z_2	$-z_3$
σ	s	$-z_3$	z_1	$-z_2$

   Poniamo $Y_1 = z_1 z_3/z_2$, $Y_2 = \sigma Y_1 = z_2 z_3/z_1$, $Y_3 = \sigma^2 Y_1 = z_1 z_2/z_3$. Allora $F(s, Y_1, Y_2, Y_3) \subseteq \operatorname{Inv} H$, dove $H = \langle \alpha, \beta \rangle$. Poiché $z_1^2 = Y_1 Y_3$, $z_2^2 = Y_2 Y_3$, $F(s, Y_1, Y_2, Y_3, z_1, z_2) = K$ e $|H| = 4$, segue come prima che $\operatorname{Inv} H = F(s, Y_1, Y_2, Y_3)$. Poiché $\sigma s = s$ e $\sigma Y_1 = Y_2$, $\sigma Y_2 = Y_3$, $\sigma Y_3 = Y_1$, l'esercizio 3 mostra che $\operatorname{Inv}\langle \sigma \rangle$ in $F(s, Y_1, Y_2, Y_3)$ è razionale su $F(s)$. Ne segue che $\operatorname{Inv} A_4$ in K è razionale su F.

   Supponiamo ora $\operatorname{char} F = 2$. Poniamo $x = x_1$, $y = x_1 + x_3$, $z = x_1 + x_2$, $s = x_1 + x_2 + x_3 + x_4$, $X = xs + yz = x_1 x_4 + x_2 x_3$. Allora $K = F(x, y, z, s) = F(X, y, z, s)$ e

$$\alpha X = X, \quad \alpha y = y + s, \quad \alpha z = z, \qquad \alpha s = s,$$
$$\beta X = X, \quad \beta y = y, \qquad \beta z = z + s, \quad \beta s = s.$$

   Ne segue che il campo $\operatorname{Inv} H$ in K è $F(X, s, y(y + s), z(z + s))$. Abbiamo dunque $\operatorname{Inv} H = F(X, s, y(y + s), z(z + s))$. Se poniamo $X_1 = X = x_1 x_4 + x_2 x_3$, $X_2 = \sigma X = x_2 x_4 + x_3 x_1$,

$X_3 = \sigma^2 X = x_3x_4 + x_1x_2$, allora $y(y+s) = (x_1+x_3)(x_2+x_4) = X_1 + X_3$ e $z(z+s) = (x_1+x_2)(x_3+x_4) = X_2 + X_1$. Pertanto $\operatorname{Inv} H = F(X_1, X_2, X_3, s)$. La razionalità di $\operatorname{Inv} A_4$ segue ora dall'esercizio 3, poiché $\sigma s = s$, $\sigma X_1 = X_2$, $\sigma X_2 = X_3$, $\sigma X_3 = X_1$.

8.15 Separabilità delle estensioni arbitrarie

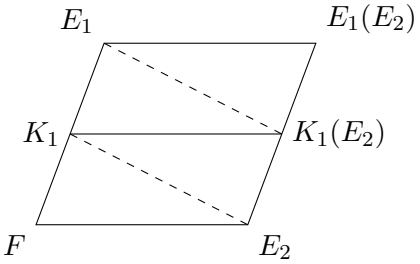
In questo paragrafo introdurremo, per estensioni arbitrarie, un concetto di separabilità che generalizza la nozione già nota per le estensioni algebriche. Esso si basa sul concetto di disgiunzione lineare, che definiamo ora.

Definizione 8.3. Sia E un'estensione di F e siano A, B sottoalgebre di E/F. Si dice che A e B sono *linearmente disgiunte su* F se l'omomorfismo canonico di $A \otimes_F B$ in E che manda $a \otimes b$ in ab, $a \in A$, $b \in B$, è un monomorfismo.

È chiaro che, se A e B soddisfano questa condizione e A' e B' sono sottoalgebre rispettivamente di A e B, allora A' e B' soddisfano la condizione. Siano K e L i sottocampi di E/F generati rispettivamente da A e B. Allora A e B sono linearmente disgiunte su F se e solo se K e L sono linearmente disgiunti su F. Per dimostrarlo basta mostrare che, se $k_1, \dots, k_m$ sono elementi di K linearmente indipendenti su F e $l_1, \dots, l_n$ sono elementi di L linearmente indipendenti su F, allora gli elementi $k_i l_j$, $1 \le i \le m$, $1 \le j \le n$, sono linearmente indipendenti su F. Ciò segue dalla disgiunzione lineare di A e B su F scrivendo $k_i = a_i a^{-1}$, $a_i, a \in A$, $1 \le i \le m$, e $l_j = b_j b^{-1}$, $b_j, b \in B$, $1 \le j \le n$. Viceversa, la disgiunzione lineare di K e L su F implica quella di A e B.

Il risultato seguente permette di stabilire la disgiunzione lineare per stadi.

Lemma 1. *Siano E_1, E_2 sottocampi di E/F e K_1 un sottocampo di E_1/F. Allora E_1 ed E_2 sono linearmente disgiunti su F se e solo se valgono le due condizioni: (1) K_1 ed E_2 sono linearmente disgiunti su F; (2) $K_1(E_2)$ ed E_1 sono linearmente disgiunti su K_1.*



Dimostrazione. Supponiamo che valgano le due condizioni. Sia (u_α) una base di E_2/F. Per la (1), questi elementi sono linearmente indipendenti su K_1 e, poiché appartengono a $K_1(E_2)$, per la (2) sono linearmente indipendenti su E_1. Quindi E_1 ed E_2 sono linearmente disgiunti su F. Viceversa, supponiamo che E_1 ed E_2 siano linearmente disgiunti su F. Allora la (1) è chiara, poiché $K_1 \subseteq E_1$. Siano (u_α) una base di E_1/K_1, (v_β) una base di K_1/F, (w_γ) una base di E_2/F. Allora $(u_\alpha v_\beta)$ è una base di E_1/F e, poiché E_1 ed E_2 sono linearmente disgiunti su F, l'insieme degli elementi $u_\alpha v_\beta w_\gamma$ è linearmente indipendente. Ciò implica che le sole relazioni della forma $\sum_i d_i u_{\alpha_i} = 0$, con i d_i nella sottoalgebra K_1E_2 generata da K_1 ed E_2, sono quelle banali, in cui tutti i d_i sono nulli. Poiché $K_1(E_2)$ è l'insieme degli elementi cd^{-1}, $c, d \in K_1E_2$, $d \neq 0$, ne segue che gli u_α sono linearmente indipendenti su $K_1(E_2)$. Vale dunque la (2). □

Supponiamo ora che la caratteristica sia $p \neq 0$ e immergiamo E nella sua chiusura algebrica $\bar{E}$. Per $e > 0$ indichiamo con $F^{p^{-e}}$ il sottoinsieme di $\bar{E}$ degli elementi a tali che $a^{p^e} \in F$. Si tratta di un sottocampo e si ha $F \subseteq F^{p^{-1}} \subseteq F^{p^{-2}} \subseteq \cdots$. Quindi $F^{p^{-\infty}} = \bigcup_{e \ge 1} F^{p^{-e}}$ è un sottocampo. Poiché la disgiunzione lineare è una proprietà dei sottoinsiemi finiti, è chiaro che

$F^{p^{-\infty}}$ ed E sono linearmente disgiunti su F se e solo se $F^{p^{-e}}$ ed E sono linearmente disgiunti su F per ogni e. Un risultato sulle estensioni algebriche separabili già dimostrato si può ora riformulare nel seguente modo.

Lemma 2. *Se E/F è algebrica separabile, allora E e $F^{p^{-\infty}}$ sono linearmente disgiunti su F.*

Dimostrazione. Basta mostrare che, se $a_1, \ldots, a_m$ sono elementi di E linearmente indipendenti su F, essi sono linearmente indipendenti su $F^{p^{-e}}$ per ogni e. Ciò equivale ad affermare che $a_1^{p^e}, \ldots, a_m^{p^e}$ sono linearmente indipendenti su F, proprietà delle estensioni algebriche separabili dimostrata a p. 489. Quindi E e $F^{p^{-\infty}}$ sono linearmente disgiunti su F. □

Dimostriamo ora il

Lemma 3. *Se E è puramente trascendente su F, allora E e $F^{p^{-\infty}}$ sono linearmente disgiunti su F.*

Dimostrazione. Basta provare il risultato per $E = F(x_1, \ldots, x_n)$, dove gli x_i sono algebricamente indipendenti. Inoltre, in questo caso, sarà sufficiente mostrare che $F[x_1, \ldots, x_n]$ e $F^{p^{-e}}$ sono linearmente disgiunti su F per ogni $e > 0$. Una base di $F[x_1, \ldots, x_n]/F$ è costituita da tutti i monomi $x_1^{k_1} \cdots x_n^{k_n}$, $k_i \geq 0$. L'applicazione $m \mapsto m^{p^e}$ dell'insieme dei monomi su un suo sottoinsieme è iniettiva. Pertanto, se (m_α) è la base dei monomi, l'insieme $\{m_\alpha^{p^e}\}$ è linearmente indipendente su F. Ne segue che $\{m_\alpha\}$ è linearmente indipendente su $F^{p^{-e}}$, e quindi $F[x_1, \ldots, x_n]$ e $F^{p^{-e}}$ sono linearmente disgiunti su F. □

Diciamo che un'estensione E/F è *separabilmente generata* su F se E ha una base di trascendenza B tale che E sia algebrico separabile su $F(B)$. In questo caso B si chiama *base di trascendenza separante* di E/F. L'esempio di un'estensione algebrica inseparabile E/F mostra che E/F può non essere separabilmente generata. L'esempio di $B = \{x^p\}$ in $F(x)$, con x trascendente, mostra che, anche se E è separabilmente generato su F, non ogni base di trascendenza ha la proprietà che E sia algebrico separabile su $F(B)$.

Possiamo ora dimostrare il nostro risultato principale.

Teorema 8.39. *Sia E un'estensione di un campo F di caratteristica $p > 0$. Sono equivalenti le seguenti proprietà di E/F:*

1. *Ogni sottocampo finitamente generato di E/F è separabilmente generato.*
2. *E e $F^{p^{-\infty}}$ sono linearmente disgiunti su F.*
3. *E e $F^{p^{-1}}$ sono linearmente disgiunti su F.*

Dimostrazione. (1) ⇒ (2). Per dimostrarlo, supponiamo che E sia algebrico separabile su $F(B)$, dove B è una base di trascendenza di E/F. Per il lemma 3, $F^{p^{-\infty}}$ e $F(B)$ sono linearmente disgiunti su F. Per il lemma 2, E e $F(B)^{p^{-\infty}}$ sono linearmente disgiunti su $F(B)$. Poiché $F(B)^{p^{-\infty}} \supseteq F^{p^{-\infty}}(B)$, ne segue che $F^{p^{-\infty}}(B)$ ed E sono linearmente disgiunti su $F(B)$. Per il lemma 1, E e $F^{p^{-\infty}}$ sono allora linearmente disgiunti su F. Poiché si tratta di una proprietà dei sottoinsiemi finiti, il risultato appena dimostrato prova che (1) ⇒ (2).

L'implicazione (2) ⇒ (3) è evidente.

(3) ⇒ (1). Supponiamo che E e $F^{p^{-1}}$ siano linearmente disgiunti su F e sia $K = F(a_1, \ldots, a_n)$ un sottocampo finitamente generato di E/F. Dimostriamo per induzione su n che dal sistema dato di generatori si può estrarre una base di trascendenza $a_{i_1}, \ldots, a_{i_r}$ (con $r = 0$ se tutti gli a_i sono algebrici su F) tale che K sia algebrico separabile su $F(a_{i_1}, \ldots, a_{i_r})$. Il risultato è chiaro per $n = 0$, perciò supponiamo $n > 0$. Il risultato è chiaro anche se $a_1, \ldots, a_n$ sono algebricamente

indipendenti. Supponiamo dunque che $a_1, \ldots, a_r$, $0 \leq r < n$, sia una base di trascendenza di K/F. Allora $a_1, \ldots, a_{r+1}$ sono algebricamente dipendenti su F, e possiamo scegliere un polinomio non nullo $f(x_1, \ldots, x_{r+1}) \in F[x_1, \ldots, x_{r+1}]$ di grado minimo tale che $f(a_1, \ldots, a_{r+1}) = 0$. Il polinomio f è allora irriducibile. Affermiamo che f non ha la forma $g(x_1^p, \ldots, x_{r+1}^p)$, con $g \in F[x_1, \ldots, x_{r+1}]$. Infatti $g(x_1^p, \ldots, x_{r+1}^p) = h(x_1, \ldots, x_{r+1})^p$ in $F^{p^{-1}}[x_1, \ldots, x_{r+1}]$ e, se $f(x_1, \ldots, x_{r+1}) = g(x_1^p, \ldots, x_{r+1}^p)$, allora $h(a_1, \ldots, a_{r+1}) = 0$. Siano $m_i(x_1, \ldots, x_{r+1})$, $1 \leq i \leq u$, i monomi che compaiono in h. Gli elementi $m_i(a_1, \ldots, a_{r+1})$ sono allora linearmente dipendenti su $F^{p^{-1}}$ e dunque, per la nostra ipotesi, sono linearmente dipendenti su F. Ciò dà fra $a_1, \ldots, a_{r+1}$ una relazione polinomiale non banale, a coefficienti in F e di grado inferiore al grado di f, contrariamente alla scelta di f.

Abbiamo così dimostrato che, per qualche i, $1 \leq i \leq r+1$, $f(x_1, \ldots, x_{r+1})$ non è un polinomio in x_i^p e nelle altre x. Allora a_i è algebrico su $F(a_1, \ldots, \widehat{a}_i, \ldots, a_{r+1})$, dove il cappello indica l'omissione di a_i. Ne segue che $\{a_1, \ldots, \widehat{a}_i, \ldots, a_{r+1}\}$ è una base di trascendenza di $F(a_1, \ldots, a_n)$ su F. Si ha dunque

$$F[a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1}] \simeq F[x_1, \ldots, x_{r+1}]$$

nel modo ovvio. Quindi il polinomio

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1})$$

è irriducibile in questo anello. Questo polinomio è allora irriducibile in $F(a_1, \ldots, \widehat{a}_i, \ldots, a_{r+1})[x]$. Poiché a_i è uno zero di $f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1})$ e questo non è un polinomio in x^p, vediamo che a_i è algebrico separabile su $F(a_1, \ldots, \widehat{a}_i, \ldots, a_{r+1})$ e quindi su $L = F(a_1, \ldots, \widehat{a}_i, \ldots, a_n)$. L'ipotesi induttiva si applica a L e ci fornisce un sottoinsieme $\{a_{i_1}, \ldots, a_{i_r}\}$ di $\{a_1, \ldots, \widehat{a}_i, \ldots, a_n\}$ che è una base di trascendenza separante di L su F. Poiché a_i è algebrico separabile su L, esso è algebrico separabile su $F(a_{i_1}, \ldots, a_{i_r})$. Dunque $\{a_{i_1}, \ldots, a_{i_r}\}$ è una base di trascendenza separante di $F(a_1, \ldots, a_n)$. □

Osserviamo che il risultato si applica in particolare a un'estensione algebrica E/F. In tal caso esso afferma che, se E e $F^{p^{-1}}$ sono linearmente disgiunti su F, allora E è separabile, e se E è separabile, allora E e $F^{p^{-\infty}}$ sono linearmente disgiunti su F (era il lemma 2). È quindi naturale estendere il concetto di separabilità a estensioni arbitrarie nel modo seguente.

Definizione 8.4. Un'estensione E/F si dice *separabile* se la caratteristica è 0, oppure se la caratteristica è $p \neq 0$ e valgono le condizioni equivalenti del teorema 8.39.[32]

L'implicazione (3) ⇒ (1) del teorema 8.39 è dovuta a MacLane. Da essa segue un risultato anteriore di F. K. Schmidt, che enunciamo come

Corollario. *Se F è perfetto, ogni estensione E/F è separabile.*

Dimostrazione. Ciò è chiaro, poiché F è perfetto se e solo se la caratteristica è 0 oppure è p e $F^{p^{-1}} = F$. □

Il seguente teorema raccoglie alcune proprietà delle estensioni separabili e indica anche proprietà che possono venire meno.

Teorema 8.40. *Siano E un'estensione di F e K un campo intermedio. (1) Se E è separabile su F, anche K è separabile su F. (2) Se E è separabile su K e K è separabile su F, allora E è separabile su F. (3) Se E è separabile su F, non è detto che sia separabile su K. (4) Se E è separabile su F, non è detto che abbia una base di trascendenza separante su F.*

[32] Qui e nel primo periodo successivo l'originale rinvia al teorema 8.37. Le tre condizioni equivalenti sulla separabilità figurano nel teorema 8.39.

Dimostrazione. Possiamo supporre che la caratteristica sia $p \neq 0$. (1) Ciò è chiaro, perché dalla disgiunzione lineare di E e $F^{p^{-1}}$ su F segue quella di K e $F^{p^{-1}}$ su F. (2) L'ipotesi è che E e $K^{p^{-1}}$ siano linearmente disgiunti su K e che K e $F^{p^{-1}}$ siano linearmente disgiunti su F. Allora E e $K(F^{p^{-1}})$ sono linearmente disgiunti su K, poiché $K(F^{p^{-1}}) \subseteq K^{p^{-1}}$. Quindi, per il lemma 1, E e $F^{p^{-1}}$ sono linearmente disgiunti su F e perciò E è separabile su F. (3) Si prenda $E = F(x)$ con x trascendente e $K = F(x^p)$. (4) Si prenda $E = F(x, x^{p^{-1}}, x^{p^{-2}}, \ldots)$ con x trascendente su F. Allora E ha grado di trascendenza uno su F e non è separabilmente generato su F. □

Esercizi.

1. Siano E_1/F e E_2/F sottocampi di E/F tali che E_1/F sia algebrica ed E_2/F sia puramente trascendente. Mostrare che E_1 ed E_2 sono linearmente disgiunti su F.
2. Sia F di caratteristica $p \neq 0$. Sia $E = F(a, b, c, d)$, dove a, b, c sono algebricamente indipendenti su F e $d^p = ab^p + c$. Mostrare che E non è separabilmente generato su $F(a, c)$.
3. (MacLane.) Sia F un campo perfetto di caratteristica p ed E un'estensione imperfetta di grado di trascendenza uno su F. Mostrare che E/F è separabilmente generata.

8.16 Derivazioni

Il concetto di derivazione è importante nella teoria dei campi e in altre parti dell'algebra. Lo abbiamo già incontrato in varie occasioni, la prima in BAI, p. 434. Considereremo ora questa nozione dapprima in tutta la sua generalità e poi nel caso particolare delle derivazioni di algebre commutative e di campi. Nel prossimo paragrafo vedremo alcune applicazioni delle derivazioni ai campi di caratteristica p.

Definizione 8.5. *Sia B un'algebra su un anello commutativo K e sia A una sottoalgebra. Una* derivazione *di A in B è un K-omomorfismo D di A in B tale che*

$$D(ab) = aD(b) + D(a)b \tag{86}$$

per $a, b \in A$. Se $A = B$, parliamo di una derivazione in A *(su K).*

Denotiamo con $\mathrm{Der}_K(A, B)$ l'insieme delle derivazioni di A in B. Allora $\mathrm{Der}_K(A, B) \subseteq \hom_K(A, B)$. Se $D_1, D_2 \in \mathrm{Der}_K(A, B)$, dalla condizione di derivazione (86) per le D_i segue

$$(D_1 + D_2)(ab) = a(D_1 + D_2)(b) + (D_1 + D_2)(a)b.$$

Pertanto $D_1 + D_2 \in \mathrm{Der}_K(A, B)$. Siano ora $k \in K$, $D \in \mathrm{Der}_K(A, B)$. Si ha

$$(kD)(ab) = k(D(ab)) = k(D(a)b + aD(b)) = (kD)(a)b + a(kD)(b).$$

Dunque $kD \in \mathrm{Der}_K(A, B)$ e $\mathrm{Der}_K(A, B)$ è un K-sottomodulo di $\hom_K(A, B)$.

Poniamo ora $B = A$ e scriviamo $\mathrm{Der}_K A$ per $\mathrm{Der}_K(A, A)$. Come mostreremo, questo insieme possiede una struttura assai più ricca di quella di un K-modulo (cfr. BAI, pp. 434–435). Siano $D_1, D_2 \in \mathrm{Der}_K A$, $a, b \in A$. Allora

$$\begin{aligned} D_1D_2(ab) &= D_1(aD_2(b) + D_2(a)b) \\ &= aD_1D_2(b) + D_1(a)D_2(b) + D_2(a)D_1(b) + D_1D_2(a)b. \end{aligned}$$

Scambiando D_1 e D_2 in questa relazione e sottraendo, otteniamo

$$[D_1D_2](ab) = a[D_1D_2](b) + [D_1D_2](a)b, \tag{87}$$

dove abbiamo scritto $[D_1D_2]$ per $D_1D_2 - D_2D_1$. Questo risultato, insieme con il fatto che $\mathrm{Der}_K A$ è un K-sottomodulo di $\mathrm{End}_K A$, equivale a dire che $\mathrm{Der}_K A$ è un'algebra di Lie di K-endomorfismi di A (BAI, p. 434).

Si può dire di più nel caso in cui K è un campo di caratteristica $p \neq 0$. Osserviamo anzitutto che, per K qualsiasi, se $D \in \mathrm{Der}_K A$ vale la *formula di Leibniz* per D^n,

$$D^n(ab) = \sum_{i=0}^{n} \binom{n}{i} D^i(a) D^{n-i}(b), \tag{88}$$

che si dimostra per induzione su n. Se K è un campo di caratteristica p, per $n = p$ la (88) diventa

$$D^p(ab) = D^p(a)b + aD^p(b). \tag{89}$$

Ciò mostra che $D^p \in \mathrm{Der}_K A$. Se V è uno spazio vettoriale su un campo K di caratteristica p, un sottospazio di $\mathrm{End}_K V$ chiuso rispetto all'operazione di parentesi $[D_1D_2]$ e alle potenze p-esime si chiama *p-algebra di Lie* (o *algebra di Lie ristretta*) di trasformazioni lineari di V. Abbiamo dunque mostrato che, se A è un'algebra su un campo di caratteristica p, $\mathrm{Der}_K A$ è una p-algebra di Lie di trasformazioni K-lineari di A.

Vi è un legame importante fra derivazioni e omomorfismi. Per ottenerlo si introduce l'algebra Δ dei *numeri duali* su K. Essa ha base $(1, \delta)$ su K, dove 1 è l'unità e δ è un elemento tale che $\delta^2 = 0$. Se B è un'algebra qualsiasi su K, possiamo formare l'algebra $B \otimes_K \Delta$ e considerare l'applicazione $b \mapsto b \otimes 1$ di B in $B \otimes_K \Delta$. Poiché Δ è libera su K, tale applicazione è un isomorfismo di algebre sulla sua immagine e possiamo identificare B con $B \otimes 1$. Possiamo anche identificare $\delta \in \Delta$ con $1 \otimes \delta$ in $B \otimes_K \Delta$. Fatte queste identificazioni, $B \otimes_K \Delta$ si presenta come l'insieme degli elementi

$$b_1 + b_2\delta, \qquad b_i \in B. \tag{90}$$

Questa rappresentazione di un elemento è unica e le operazioni di K-modulo sono quelle ovvie. Inoltre, se $b_i' \in B$,

$$(b_1 + b_2\delta)(b_1' + b_2'\delta) = b_1b_1' + (b_1b_2' + b_2b_1')\delta. \tag{91}$$

Sia ora D un K-omomorfismo di A in B. Definiamo una corrispondente applicazione $\alpha(D)$ di A in $B \otimes_K \Delta$ mediante

$$\alpha(D)\colon a \longmapsto a + D(a)\delta, \tag{92}$$

che è evidentemente un K-omomorfismo. Affermiamo che $\alpha(D)$ è un omomorfismo di algebre se e soltanto se D è una derivazione. Anzitutto, per ogni derivazione si ha $D(1) = 0$, poiché $D(1) = D(1^2) = 2D(1)$. Inoltre

$$\begin{aligned}(\alpha(D)(a))(\alpha(D)(b)) &= (a + D(a)\delta)(b + D(b)\delta) \\ &= ab + (aD(b) + D(a)b)\delta\end{aligned}$$

e $\alpha(D)(ab) = ab + D(ab)\delta$. Dunque $\alpha(D)(ab) = (\alpha(D)(a))(\alpha(D)(b))$ per ogni a, b se e soltanto se D è una derivazione, e $\alpha(D)$ è un omomorfismo di algebre se e soltanto se D è una derivazione.

Gli omomorfismi $\alpha(D)$ hanno una semplice caratterizzazione in termini dell'applicazione

$$\pi\colon b_1 + b_2\delta \longmapsto b_1, \qquad b_i \in B, \tag{93}$$

di $B \otimes_K \Delta$ in B, che è un omomorfismo suriettivo di K-algebre. Se $a \in A$, allora $\alpha(D)a = a + D(a)\delta$, cosicché $\pi\alpha(D)a = a$. Pertanto $\pi\alpha(D) = 1_A$. Viceversa, sia H un omomorfismo di A in $B \otimes_K \Delta$. Per ogni a scriviamo $H(a) = a_1 + a_2\delta$. Si definiscono così due applicazioni $a \mapsto a_1$ e $a \mapsto a_2$ di A in B, che sono K-omomorfismi. La condizione $\pi H = 1_A$ equivale ad avere $a_1 = a$ per ogni a. Indicando con D l'applicazione $a \mapsto a_2$, abbiamo $H(a) = a + D(a)\delta$. La condizione $H(ab) = H(a)H(b)$ equivale allora al fatto che D sia una derivazione.

Riassumiamo i risultati ottenuti nella seguente proposizione.

Proposizione 8.15. *Sia A una sottoalgebra di un'algebra B e sia D una derivazione di A in B. Allora $\alpha(D)\colon a \mapsto a + D(a)\delta$ è un omomorfismo di algebre di A in $B \otimes_K \Delta$ tale che $\pi\alpha(D) = 1_A$. Viceversa, ogni omomorfismo H di A in $B \otimes_K \Delta$ tale che $\pi H = 1_A$ ha la forma $\alpha(D)$, dove D è una derivazione di A in B.*

Il legame fra derivazioni e omomorfismi è importante perché consente di trasferire alle derivazioni risultati sugli omomorfismi di algebre. Si evitano così i calcoli laboriosi che sarebbero necessari per dimostrare direttamente tali risultati per le derivazioni. Come esempio dimostriamo la seguente proposizione.

Proposizione 8.16. *Sia A una sottoalgebra di un'algebra B, siano D, D_1, D_2 derivazioni di A in B e sia X un insieme di generatori di A. Diciamo che $a \in A$ è una D-*costante *se $Da = 0$. Allora (1) $D_1 = D_2$ se $D_1|X = D_2|X$. (2) L'insieme delle D-costanti è una sottoalgebra di A. Inoltre, se A è un'algebra con divisione, esso è una sottoalgebra con divisione.*

Dimostrazione. (1) La condizione $D_1|X = D_2|X$ implica $\alpha(D_1)|X = \alpha(D_2)|X$ per i corrispondenti omomorfismi di algebre di A in $B \otimes_K \Delta$. Poiché X genera A, si ha $\alpha(D_1) = \alpha(D_2)$. Quindi $D_1 = D_2$.

(2) La condizione che a sia una D-costante equivale al fatto che a sia fissato dall'omomorfismo $\alpha(D)$ di $A \subseteq B \otimes_K \Delta$ in $B \otimes_K \Delta$. L'insieme dei punti fissi di un omomorfismo di una sottoalgebra A di un'algebra C in C è una sottoalgebra, ed è una sottoalgebra con divisione se A è un'algebra con divisione. Il risultato per le derivazioni è dunque chiaro. □

Ricaviamo ora una formula per $D(a^{-1})$, dove a è un elemento invertibile di A e D una derivazione di A in B. Poiché 1 è una D-costante, applicando D ad $aa^{-1} = 1$ otteniamo

$$D(a)a^{-1} + aD(a^{-1}) = 0.$$

Si ha pertanto la formula

$$D(a^{-1}) = -a^{-1}D(a)a^{-1}, \tag{94}$$

che generalizza la ben nota formula del calcolo differenziale.

D'ora in poi considereremo derivazioni di algebre commutative in algebre commutative, ossia supporremo B commutativa. Siano $D \in \mathrm{Der}_K(A, B)$, $b \in B$. Moltiplicando per b la relazione $D(xy) = D(x)y + xD(y)$, $x, y \in A$, otteniamo

$$bD(xy) = bD(x)y + xbD(y).$$

Ciò mostra che bD, definita da $(bD)(x) = b(D(x))$, è ancora una derivazione. È chiaro che questa azione di B su $\mathrm{Der}_K(A, B)$ conferisce a $\mathrm{Der}_K(A, B)$ la struttura di un B-modulo.

Consideriamo ora il problema di prolungare una derivazione data D di una sottoalgebra A in B a una derivazione di una sottoalgebra più grande A'. Sia $\alpha(D)$ il corrispondente omomorfismo di A in $B \otimes_K \Delta$ tale che $\pi\alpha(D) = 1_A$. Il problema di prolungare D a una derivazione di A' equivale a prolungare $H = \alpha(D)$ a un omomorfismo H' di A' in $B \otimes_K \Delta$ tale che $\pi H' = 1_{A'}$. Se H' è un omomorfismo di A' in $B \otimes_K \Delta$ che prolunga H, si ha $\pi H' = 1_{A'}$ se e soltanto se

$\pi H'(x) = x$ per ogni x di un insieme di generatori di A' su A. Useremo queste osservazioni per trattare il problema del prolungamento.

Supponiamo ora $A' = A[u_1, \ldots, u_n]$, la sottoalgebra generata da A e da un sottoinsieme finito $\{u_1, \ldots, u_n\}$ di B. Sia $A[x_1, \ldots, x_n]$ l'algebra dei polinomi su A nelle indeterminate x_i e sia I il nucleo dell'omomorfismo di $A[x_1, \ldots, x_n]$ su A' che è l'identità su A e manda x_i in u_i, $1 \leq i \leq n$. Supponiamo dati un omomorfismo s di A in un'algebra commutativa C ed elementi v_i di C, $1 \leq i \leq n$. Si ha allora l'omomorfismo

$$f(x_1, \ldots, x_n) \longmapsto (sf)(v_1, \ldots, v_n) \tag{95}$$

di $A[x_1, \ldots, x_n]$ in C (BAI, p. 124). Qui sf denota il polinomio ottenuto da f applicando s ai suoi coefficienti. L'omomorfismo (95) induce un omomorfismo

$$f(x_1, \ldots, x_n) + I \longmapsto (sf)(v_1, \ldots, v_n) \tag{96}$$

di $A[x_1, \ldots, x_n]/I$ in C se e soltanto se $(sf)(v_1, \ldots, v_n) = 0$ per ogni $f \in I$. Poiché abbiamo l'isomorfismo $f(x_1, \ldots, x_n) + I \mapsto f(u_1, \ldots, u_n)$, vediamo che esiste un omomorfismo di A' in C che prolunga s e manda u_i in v_i, $1 \leq i \leq n$, se e soltanto se

$$(sf)(v_1, \ldots, v_n) = 0 \tag{97}$$

per ogni $f \in I$. È chiaro inoltre che basta che questa relazione valga per ogni f in un insieme qualsiasi di generatori X dell'ideale I.

Se $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$, scriviamo $\partial f/\partial x_i$ per il polinomio ottenuto da f mediante derivazione parziale formale rispetto a x_i. Ad esempio,

$$\frac{\partial}{\partial x_1}(x_1^3 x_2 x_3 + 3x_1 x_3^2) = 3x_1^2 x_2 x_3 + 3x_3^2.$$

Se D è una derivazione di A in B, indicheremo con $(Df)(x_1, \ldots, x_n)$ il polinomio di $B[x_1, \ldots, x_n]$ ottenuto applicando D ai coefficienti di f. Possiamo ora dimostrare il seguente teorema.

Teorema 8.41. *Sia B un'algebra commutativa, A una sottoalgebra, $A' = A[u_1, \ldots, u_n]$ con $u_i \in B$, e sia X un insieme di generatori del nucleo dell'omomorfismo di $A[x_1, \ldots, x_n]$ su A' tale che $a \mapsto a$ per $a \in A$ e $x_i \mapsto u_i$, $1 \leq i \leq n$. Sia D una derivazione di A in B. Allora D si può prolungare a una derivazione di A' in B che mandi u_i in v_i, $1 \leq i \leq n$, se e soltanto se*

$$(Df)(u_1, \ldots, u_n) + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(u_1, \ldots, u_n) v_i = 0 \tag{98}$$

per ogni $f \in X$.

Dimostrazione. La condizione perché D ammetta il prolungamento richiesto è che $\alpha(D)$ si possa prolungare a un omomorfismo di A' in $B \otimes_K \Delta$ che mandi u_i in $u_i + v_i\delta$, $1 \leq i \leq n$. Ciò accade se e soltanto se, per ogni $f \in X$,

$$(\alpha(D)f)(u_1 + v_1\delta, u_2 + v_2\delta, \ldots, u_n + v_n\delta) = 0. \tag{99}$$

Sia ora $a \in A$ e consideriamo il monomio $a x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, $k_i \geq 0$. Abbiamo

$$\begin{aligned}
&(a + D(a)\delta)(u_1 + v_1\delta)^{k_1} \cdots (u_n + v_n\delta)^{k_n} \\
&\quad = a u_1^{k_1} \cdots u_n^{k_n} + \big((Da) u_1^{k_1} \cdots u_n^{k_n} \\
&\qquad + k_1 a u_1^{k_1 - 1} u_2^{k_2} \cdots u_n^{k_n} v_1 + k_2 a u_1^{k_1} u_2^{k_2 - 1} u_3^{k_3} \cdots u_n^{k_n} v_2 \\
&\qquad + \cdots + k_n a u_1^{k_1} \cdots u_{n-1}^{k_{n-1}} u_n^{k_n - 1} v_n)\delta.
\end{aligned}$$

Dunque per ogni $f \in A[x_1, \ldots, x_n]$ si ha

$$(\alpha(D)f)(u_1 + v_1\delta, \ldots, u_n + v_n\delta) = f(u_1, \ldots, u_n) + \left((Df)(u_1, \ldots, u_n) + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(u_1, \ldots, u_n) v_i \right) \delta.$$

La condizione che la (99) valga per ogni $f \in X$ equivale quindi alla (98). □

Supponiamo poi che S sia un sottomonoide del monoide moltiplicativo di A e consideriamo le localizzazioni A_S e B_S. Possiamo dimostrare il seguente teorema.

Teorema 8.42. *Sia D una derivazione di A in B (commutativa) e sia S un sottomonoide del monoide moltiplicativo di A. Esiste allora un'unica derivazione D_S di A_S in B_S tale che il diagramma*

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle D_S} \\ B & \longrightarrow & B_S \end{array} \tag{100}$$

sia commutativo. Qui le applicazioni orizzontali sono gli omomorfismi canonici $a \mapsto a/1$ e $b \mapsto b/1$, rispettivamente.

Dimostrazione. Abbiamo l'omomorfismo $\alpha(D)$ di A in $B \otimes_K \Delta$ che manda a in $a + D(a)\delta$ e l'omomorfismo di $B \otimes_K \Delta$ in $B_S \otimes_K \Delta$ che manda $b \otimes u$ in $(b/1) \otimes u$. Abbiamo quindi l'omomorfismo di A in $B_S \otimes_K \Delta$ che manda a in $a/1 + (D(a)/1)\delta$. Se $s \in S$, allora $s/1 + (D(s)/1)\delta$ è invertibile e ha per inverso $1/s - (D(s)/s^2)\delta$. Per la proprietà universale di A_S esiste dunque un unico omomorfismo $H\colon A_S \to B_S \otimes_K \Delta$ che rende commutativo il diagramma

$$\begin{array}{ccc} A & \longrightarrow & A_S \\ {\scriptstyle \alpha(D)}\downarrow & & \downarrow{\scriptstyle H} \\ B \otimes_K \Delta & \longrightarrow & B_S \otimes_K \Delta \end{array} \tag{101}$$

Se π_S denota l'omomorfismo canonico di $B_S \otimes_K \Delta$ su B_S, la commutatività della (101) implica $\pi_S H = 1_{A_S}$. Dunque H ha la forma $\alpha(D_S)$, dove D_S è una derivazione di A_S in B_S. Questa D_S soddisfa la condizione del teorema. □

Specializziamo ora al caso dei campi. Consideriamo un'estensione di campi E/F come algebra su F. Sia K un sottocampo di E/F, sia D una derivazione di K/F in E/F e sia $a \in E$. Se a è trascendente su K, per il teorema 8.41 a ogni $b \in E$ corrisponde una derivazione di $K[a]$ in E che prolunga D e manda a in b. Il teorema 8.42 mostra poi che questa ha un unico prolungamento a una derivazione di $K(a)$ in E. Quindi, se a è trascendente su K, esiste un prolungamento di D a una derivazione di $K(a)$ che manda a in b. Per la proposizione 8.16 e il teorema 8.42 esso è unico. Sia ora a algebrico su K con polinomio minimo $f(x)$ su K. Allora $K(a) = K[a]$ e il teorema 8.41 mostra che D si può prolungare a una derivazione di $K(a)$ in E che manda a in b se e soltanto se

$$(Df)(a) + f'(a)b = 0. \tag{102}$$

Se a è separabile, $(f(x), f'(x)) = 1$ e $f'(a) \neq 0$. Per b vi è allora una sola scelta possibile,

$$b = -f'(a)^{-1}(Df)(a). \tag{103}$$

Dunque, in questo caso, D si può prolungare in uno e un solo modo a una derivazione di $K(a)$ in E. Se a è inseparabile, allora $f'(a) = 0$. La (102) mostra allora che D si può prolungare a una derivazione di $K(a)$ se e soltanto se i coefficienti di $f(x)$ sono D-costanti, e che in tal caso si può fare in modo che il prolungamento mandi a in un $b \in E$ qualsiasi.[33] Riassumiamo i risultati.

Proposizione 8.17. *Sia E un campo di estensione di F, sia K un campo intermedio, D una derivazione di K/F in E/F e a un elemento di E.*

(1) *Se a è trascendente su K, D si può prolungare a una derivazione di $K(a)$ in E che manda a in un $b \in E$ qualsiasi.*

(2) *Se a è algebrico separabile su K, D ha un unico prolungamento a una derivazione di $K(a)$ in E.*

(3) *Se a è algebrico inseparabile su K, D si può prolungare a una derivazione di $K(a)$ in E se e soltanto se i coefficienti del polinomio minimo di a su K sono D-costanti. Inoltre, se questa condizione è soddisfatta, esiste un prolungamento che manda a in un $b \in E$ qualsiasi.*

Supponiamo ora che E sia finitamente generato su F, ossia $E = F(a_1, \dots, a_n)$. Sia X un insieme di generatori dell'ideale I di $F[x_1, \dots, x_n]$, con x_i indeterminate, costituito dai polinomi f tali che $f(a_1, \dots, a_n) = 0$. Dai teoremi 8.41 e 8.42 segue che esiste una derivazione D di E/F in sé tale che $Da_i = b_i$, $1 \leq i \leq n$, se e soltanto se

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a_1, \dots, a_n) b_i = 0 \tag{104}$$

per ogni $f \in X$. Ricordiamo che $\mathrm{Der}_F E$ diventa uno spazio vettoriale su E definendo bD, per $b \in E$, $D \in \mathrm{Der}_F E$, mediante $(bD)(x) = b(D(x))$ (cfr. p. 533). Vogliamo calcolare la dimensione $[\mathrm{Der}_F E : E]$ quando $E = F(a_1, \dots, a_n)$. A questo scopo introduciamo lo spazio vettoriale $E^{(n)}$, di dimensione n, delle n-uple di elementi di E. Se $D \in \mathrm{Der}_F E$, D determina l'elemento $(Da_1, \dots, Da_n)$ di $E^{(n)}$, e abbiamo l'applicazione

$$\lambda_{a_1,\dots,a_n} \colon D \longmapsto (Da_1, \dots, Da_n) \tag{105}$$

di $\mathrm{Der}_F E$ in $E^{(n)}$. Si tratta evidentemente di un'applicazione lineare di spazi vettoriali su E e, poiché una derivazione è determinata dalla sua azione su un insieme di generatori, $\lambda = \lambda_{a_1,\dots,a_n}$ è iniettiva. Dunque $[\mathrm{Der}_F E : E]$ è la dimensione del sottospazio $\lambda(\mathrm{Der}_F E)$ di $E^{(n)}$. Sia ora $g \in F[x_1, \dots, x_n]$. Esso definisce un'applicazione dg di $E^{(n)}$ in E mediante

$$dg \colon (b_1, \dots, b_n) \longmapsto \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}(a_1, \dots, a_n) b_i. \tag{106}$$

Questa è evidentemente lineare. Il risultato dimostrato sopra afferma ora che $(b_1, \dots, b_n) \in \lambda(\mathrm{Der}_F E)$ se e soltanto se

$$df(b_1, \dots, b_n) = 0 \tag{107}$$

per ogni $f \in X$. Questo è un sistema di equazioni lineari che caratterizza $\lambda(\mathrm{Der}_F E)$. Ne risulta la formula per $[\mathrm{Der}_F E : E]$ enunciata nel teorema seguente.

[33] Nella generalità $D \colon K \to E$ dell'enunciato, il criterio esatto dato dalla (102) è $(Df)(a) = 0$. Che tutti i coefficienti di f siano D-costanti è sufficiente, ed è anche necessario se $D(K) \subseteq K$. In quest'ultimo caso, infatti, $Df \in K[x]$ ha grado minore del polinomio minimo monico f. Questa precisazione si applica anche al punto (3) della proposizione seguente. [N.d.T.]

Teorema 8.43. *Sia $E = F(a_1, \dots, a_n)$ e sia X un insieme di generatori dell'ideale dei polinomi f di $F[x_1, \dots, x_n]$ tali che $f(a_1, \dots, a_n) = 0$. Sia dX il sottospazio di $(E^{(n)})^*$ generato dalle funzioni lineari df, $f \in X$. Allora*

$$[\mathrm{Der}_F E : E] = n - [dX : E]. \tag{108}$$

Dimostrazione. Abbiamo $[\mathrm{Der}_F E : E] = [\lambda(\mathrm{Der}_F E) : E]$, e $\lambda(\mathrm{Der}_F E)$ è il sottospazio di $E^{(n)}$ costituito dagli elementi tali che $df(b_1, \dots, b_n) = 0$ per ogni $f \in X$. La (108) segue quindi dall'algebra lineare. □

Per il teorema della base di Hilbert possiamo prendere $X = \{f_1, \dots, f_m\}$. Dall'algebra lineare risulta allora che $[dX : E]$ è il rango della matrice jacobiana

$$J(f_1, \dots, f_m) = \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1}(a_1, \dots, a_n) & \cdots & \dfrac{\partial f_1}{\partial x_n}(a_1, \dots, a_n) \\ \vdots & & \vdots \\ \dfrac{\partial f_m}{\partial x_1}(a_1, \dots, a_n) & \cdots & \dfrac{\partial f_m}{\partial x_n}(a_1, \dots, a_n) \end{pmatrix}. \tag{109}$$

Combinando questo fatto con il teorema 8.43 otteniamo il corollario seguente.

Corollario. *Sia $E = F(a_1, \dots, a_n)$ e sia $X = \{f_1, \dots, f_m\}$ un insieme finito di generatori dell'ideale dei polinomi f di $F[x_1, \dots, x_n]$ tali che $f(a_1, \dots, a_n) = 0$. Allora*

$$[\mathrm{Der}_F E : E] = n - \text{rango}\, J(f_1, \dots, f_m), \tag{110}$$

dove $J(f_1, \dots, f_m)$ è la matrice jacobiana (109).

Stabiliamo ora un legame fra $[\mathrm{Der}_F E : E]$ e la struttura di E/F. Dimostriamo anzitutto la seguente proposizione.

Proposizione 8.18. *Se $E = F(a_1, \dots, a_n)$, allora $\mathrm{Der}_F E = 0$ se e soltanto se E è algebrico separabile su F.*

Dimostrazione. Se $a \in E$ è algebrico separabile su F, la proposizione 8.17(2), applicata alla derivazione nulla su F, mostra che $D(a) = 0$ per ogni derivazione di E/F. Se dunque E è algebrico separabile su F, allora $\mathrm{Der}_F E = 0$. Supponiamo ora che E non sia algebrico separabile su F. Possiamo supporre che $\{a_1, \dots, a_r\}$, $r \geq 0$, sia una base di trascendenza di E/F. Sia S il sottocampo degli elementi di E algebrici separabili su $F(a_1, \dots, a_r)$. Se $S = E$, allora $r > 0$ e abbiamo una derivazione di $F(a_1, \dots, a_r)$ in E che manda ciascun a_i, $1 \leq i \leq r$, in un elemento di E a piacere. Applicando successivamente la proposizione 8.17(2) ad $a_{r+1}, \dots, a_n$ otteniamo un prolungamento della derivazione di $F(a_1, \dots, a_r)$ in E a una derivazione di E/F. Possiamo quindi ottenere una derivazione non nulla di E/F.

Sia ora $E \neq S$. La caratteristica è allora $p \neq 0$ ed E è puramente inseparabile su S. Abbiamo $0 \neq [E : S] < \infty$ e possiamo scegliere un sottocampo proprio massimale K di E che contenga S. Se $a \in E$, $a \notin K$, allora $K(a) = E$ per la massimalità di K. Inoltre il polinomio minimo di a su K ha la forma $x^{p^e} - b$, poiché E è puramente inseparabile su S, e quindi su K. Se fosse $e > 1$, $K(a^{p^{e-1}})$ sarebbe un sottocampo proprio di E contenente propriamente K. Dunque $E = K(a)$, dove $x^p - b$ è il polinomio minimo di a su K. Per la proposizione 8.17(3) abbiamo una derivazione non nulla di E/K. Essendo questa una derivazione di E/F, abbiamo $\mathrm{Der}_F E \neq 0$ anche nel caso $E \neq S$. □

Possiamo ora dimostrare il teorema seguente, che lega $[\mathrm{Der}_F E : E]$ alla struttura di E/F.

Teorema 8.44. *Sia $E = F(a_1, \dots, a_n)$. Allora $[\mathrm{Der}_F E : E]$ è il minimo intero s per il quale esiste un sottoinsieme $\{a_{i_1}, \dots, a_{i_s}\}$ di $\{a_1, \dots, a_n\}$ tale che E sia algebrico separabile su*

$F(a_{i_1}, \ldots, a_{i_s})$. *Inoltre* $[\mathrm{Der}_F E : E]$ *è il grado di trascendenza di* E *su* F *se e soltanto se* E *è separabile su* F.

Dimostrazione. Consideriamo ancora l'applicazione $\lambda = \lambda_{a_1,\ldots,a_n}$ di $\mathrm{Der}_F E$ in $E^{(n)}$ definita dalla (105). Poniamo $s = [\mathrm{Der}_F E : E] = [\lambda(\mathrm{Der}_F E) : E]$ e sia $(D_1, D_2, \ldots, D_s)$ una base di $\mathrm{Der}_F E$ su E. Allora $s \leq n$ e $\lambda(\mathrm{Der}_F E)$ ha base $(D_1 a_1, \ldots, D_1 a_n), \ldots, (D_s a_1, \ldots, D_s a_n)$. La matrice $s \times n$ data da $(D_i a_j)$ ha dunque rango s. Possiamo quindi supporre che gli a_i siano ordinati in modo che

$$\det(D_i a_j)_{1 \leq i,j \leq s} \neq 0. \tag{111}$$

Poniamo $K = F(a_1, \ldots, a_s)$ e sia $D \in \mathrm{Der}_K E \subseteq \mathrm{Der}_F E$. Allora $D = \sum_i b_i D_i$, $b_i \in E$, e $D(a_j) = 0$ per $1 \leq j \leq s$ dà $\sum_i b_i D_i(a_j) = 0$ per $1 \leq j \leq s$. Per la (111) ciò implica $b_i = 0$ per ogni i, e quindi $D = 0$. Dunque $\mathrm{Der}_K E = 0$ e, per la proposizione 8.18, E è algebrico separabile su K. Viceversa, sia $\{a_{i_1}, \ldots, a_{i_t}\}$ un sottoinsieme di $\{a_1, \ldots, a_n\}$ tale che E sia algebrico separabile su $F(a_{i_1}, \ldots, a_{i_t})$. Riordinando gli a possiamo supporre che il sottoinsieme sia $\{a_1, \ldots, a_t\}$. Consideriamo l'applicazione di $\mathrm{Der}_F E$ in $E^{(t)}$ data da $D \mapsto (Da_1, \ldots, Da_t)$. Il nucleo di questa applicazione lineare è l'insieme delle D tali che $D(a_k) = 0$, $1 \leq k \leq t$, e quindi l'insieme delle D tali che $D(K) = 0$ per $K = F(a_1, \ldots, a_t)$. Ora $D(K) = 0$ significa $D \in \mathrm{Der}_K E$ e, poiché E è algebrico separabile su K, ne segue $D = 0$. L'applicazione $D \mapsto (Da_1, \ldots, Da_t)$ è quindi iniettiva e $t \geq s = [\mathrm{Der}_F E : E]$. Ciò conclude la dimostrazione della prima affermazione.

Per provare la seconda, osserviamo anzitutto che, se $[\mathrm{Der}_F E : E] = s$, possiamo supporre che E sia algebrico separabile su $F(a_1, \ldots, a_s)$. Allora $\{a_1, \ldots, a_s\}$ contiene una base di trascendenza di E/F e quindi $s \geq r = \mathrm{trdeg}(E/F)$. Se inoltre $r = s$, allora $\{a_1, \ldots, a_s\}$ è una base di trascendenza. Essa è quindi una base di trascendenza separante ed E è separabile su F. Viceversa, supponiamo che E sia separabile su F. La dimostrazione del teorema 8.39 mostra che possiamo scegliere fra gli a_i una base di trascendenza separante, e possiamo supporre che sia $\{a_1, \ldots, a_r\}$. Allora E è algebrico separabile su $F(a_1, \ldots, a_r)$ e quindi, come abbiamo mostrato nella prima parte, $r \geq [\mathrm{Der}_F E : E]$. Poiché avevamo $[\mathrm{Der}_F E : E] \geq r$, ciò dimostra che $[\mathrm{Der}_F E : E] = r$. □

Esercizi

1. Sia $E = F(a_1, \ldots, a_n)$. Mostrare che E è algebrico separabile su F se e soltanto se esistono n polinomi $f_1, \ldots, f_n \in F[x_1, \ldots, x_n]$ tali che $f_i(a_1, \ldots, a_n) = 0$ e
$$\det\left(\frac{\partial f_i}{\partial x_j}(a_1, \ldots, a_n)\right) \neq 0.$$

2. Sia D una derivazione in E/F e sia K il sottocampo delle D-costanti. Mostrare che $a_1, \ldots, a_m \in E$ sono linearmente dipendenti su K se e soltanto se il determinante wronskiano è nullo, ossia
$$\begin{vmatrix} a_1 & a_2 & \cdots & a_m \\ Da_1 & Da_2 & \cdots & Da_m \\ \vdots & \vdots & & \vdots \\ D^{m-1}a_1 & D^{m-1}a_2 & \cdots & D^{m-1}a_m \end{vmatrix} = 0.$$

3. (C. Faith.) Sia $E = F(a_1, \ldots, a_n)$ e sia K un sottocampo di E/F. Mostrare che $[\mathrm{Der}_F K : K] \leq [\mathrm{Der}_F E : E]$.

4. Sia A una sottoalgebra di un'algebra B su un anello commutativo K. Definiamo una *derivazione superiore di rango* m di A in B come una successione di K-omomorfismi

$$D = (D_0 = 1_A, D_1, \dots, D_m) \tag{112}$$

di A in B tali che

$$D_i(ab) = \sum_{j=0}^{i} D_j(a) D_{i-j}(b) \tag{113}$$

per $a, b \in A$. Sia $\Delta^{(m)}$ l'algebra $K[x]/(x^{m+1})$. Essa ha base $(1, \delta, \dots, \delta^m)$, con $\delta = x + (x^{m+1})$ e $\delta^{m+1} = 0$. Osservare che $B \otimes_K \Delta^{(m)}$ è l'insieme degli elementi

$$b_0 + b_1\delta + \cdots + b_m\delta^m, \tag{114}$$

dove si identifica b_i con $b_i \otimes 1$ e δ con $1 \otimes \delta$, e che un elemento (114) è zero se e soltanto se tutti i b_i sono nulli. Sia π l'omomorfismo di $B \otimes_K \Delta^{(m)}$ in B che manda $b_0 + b_1\delta + \cdots + b_m\delta^m$ in b_0. Mostrare che una successione di applicazioni $D = (D_0, D_1, \dots, D_m)$ di A in B è una derivazione superiore di rango m di A in B se e soltanto se

$$\alpha(D)\colon a \longmapsto D_0(a) + D_1(a)\delta + \cdots + D_m(a)\delta^m$$

è un omomorfismo di K-algebre di A in $B \otimes_K \Delta^{(m)}$ tale che $\pi\alpha(D) = 1_A$.

5. Siano A e B come nell'esercizio 4. Definiamo una *derivazione superiore di rango infinito* di A in B come una successione infinita di omomorfismi $D = (D_0 = 1, D_1, D_2, \dots)$ di A in B per i quali valga la (113). Stabilire un legame fra le derivazioni superiori di A in B e gli omomorfismi di A in $B[[x]]$, l'algebra delle serie formali di potenze in x a coefficienti in B.

8.17 Teoria di Galois per le estensioni puramente inseparabili di esponente uno

Sia E/F di caratteristica $p \neq 0$ e sia D una derivazione di E/F. Se $a \in E$, allora $D(a^p) = pa^{p-1}D(a) = 0$. Dunque ogni elemento di $F(E^p)$ è una costante rispetto a ogni derivazione di E/F. Se $c \in F(E^p)$ e $a \in E$, per $D \in \mathrm{Der}_F E$ si ha $D(ca) = cD(a)$. Nello studio delle derivazioni di E/F è quindi naturale sostituire F con $F(E^p)$. È quanto faremo ora. Cambiando notazione, possiamo così supporre $E^p \subseteq F$, il che significa che $E = F$ oppure che E è puramente inseparabile di esponente uno su F (si veda l'esercizio 8, p. 495). Limitiamo inoltre l'attenzione alle estensioni finitamente generate $E = F(a_1, \dots, a_n)$.

Sia $\{a_1, \dots, a_m\}$ un insieme minimale di generatori di E/F, sicché $m = 0$ se e soltanto se $E = F$. Supponiamo $m > 0$. Allora $a_1 \notin F$ e $a_i \notin F(a_1, \dots, a_{i-1})$ per $1 < i \leq m$. Poiché $a_i^p \in F$ per ogni i, il polinomio minimo di a_1 su F e quello di a_i su $F(a_1, \dots, a_{i-1})$ per $i > 1$ hanno la forma $x^p - b$. Quindi $[F(a_1) : F] = p$ e $[F(a_1, \dots, a_i) : F(a_1, \dots, a_{i-1})] = p$, da cui $[E : F] = p^m$. È chiaro che $E = F[a_1, \dots, a_m]$ e, poiché $a_i^p \in F$ per ogni i e $[E : F] = p^m$, l'insieme dei monomi

$$a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}, \qquad 0 \leq k_i < p, \tag{115}$$

costituisce una base di E/F. È pure chiaro che E/F è un prodotto tensoriale delle estensioni semplici $F(a_i)/F$.

Poniamo $F_i = F(a_1, \dots, \widehat{a_i}, \dots, a_m)$, dove si omette a_i. Allora $E = F_i(a_i)$ e il polinomio minimo di a_i su F_i ha la forma $x^p - b_i$, con $b_i \in F$. Per la proposizione 8.17(3) esiste una

derivazione D_i di E/F_i tale che $D_i(a_i) = 1$. Abbiamo dunque $D_i(a_j) = \delta_{ij}$. Ne segue immediatamente che le D_i, $1 \le i \le m$, formano una base di $\mathrm{Der}_F E$ come spazio vettoriale su E, e quindi $[\mathrm{Der}_F E : E] = m$. Poiché $[E : F] = p^m$, se ne deduce che $[\mathrm{Der}_F E : F] = mp^m$.

Consideriamo ora un campo qualsiasi E di caratteristica p e le derivazioni di E in sé stesso, senza fare riferimento a un particolare sottocampo di E. Esse sono gli endomorfismi D del gruppo $(E, +, 0)$ che soddisfano la condizione $D(ab) = D(a)b + aD(b)$. Si deduce da ciò che $D(ca) = cD(a)$ se c appartiene al campo primo P, e quindi D si può considerare come una derivazione di E/P. Diremo tuttavia semplicemente che D è una derivazione di E in sé stesso. Sia $\mathrm{Der}\, E$ l'insieme di queste applicazioni. Allora $\mathrm{Der}\, E$ è un insieme di endomorfismi del gruppo additivo $(E, +, 0)$ con le seguenti proprietà di chiusura.

(1) $\mathrm{Der}\, E$ è un sottospazio di $\mathrm{End}(E, +, 0)$, considerato come spazio vettoriale su E definendo bL, per $b \in E$, $L \in \mathrm{End}(E, +, 0)$, mediante $(bL)(a) = b(L(a))$.

(2) Se $D_1, D_2 \in \mathrm{Der}\, E$, allora $[D_1 D_2] \in \mathrm{Der}\, E$.

(3) Se $D \in \mathrm{Der}\, E$, allora $D^p \in \mathrm{Der}\, E$.

Chiameremo *p-E-algebra di Lie di endomorfismi di* $(E, +, 0)$ ogni sottoinsieme di $\mathrm{End}(E, +, 0)$ che possieda queste proprietà di chiusura. Usiamo questa terminologia in mancanza di una migliore, ma richiamiamo l'attenzione sul fatto che una p-E-algebra di Lie può non essere un'algebra di Lie su E nel senso usuale, poiché l'operazione $[D_1, D_2]$ non è E-bilineare.

Se F è un sottocampo di E tale che $[E : F] < \infty$ ed E è puramente inseparabile di esponente ≤ 1 su F, allora $\mathrm{Der}_F E$ è una p-E-algebra di Lie di endomorfismi di $(E, +, 0)$. Abbiamo inoltre visto che $[\mathrm{Der}_F E : E] < \infty$. Mostreremo ora che ogni p-E-algebra di Lie di derivazioni di E di dimensione finita su E si ottiene in questo modo. Si ha infatti il teorema seguente.

Teorema 8.45 (Jacobson). *Sia E un campo di caratteristica $p \neq 0$ e sia F un sottocampo tale che (1) $[E : F] < \infty$ e (2) E sia puramente inseparabile di esponente ≤ 1 su F. Allora $\mathrm{Der}_F E$ è una p-E-algebra di Lie di endomorfismi di $(E, +, 0)$ tale che $p^{[\mathrm{Der}_F E : E]} = [E : F]$. Viceversa, sia $\mathcal{D}$ una p-E-algebra di Lie di derivazioni di E tale che $[\mathcal{D} : E] < \infty$ e sia F l'insieme delle $\mathcal{D}$-costanti di E, ossia degli elementi che sono D-costanti per ogni $D \in \mathcal{D}$. Allora $[E : F] < \infty$ ed E è puramente inseparabile di esponente ≤ 1 su F. Inoltre $\mathcal{D} = \mathrm{Der}_F E$ e, se $(D_1, \dots, D_m)$ è una base di $\mathcal{D}$ su E, i monomi*

$$D_1^{k_1} D_2^{k_2} \cdots D_m^{k_m}, \qquad 0 \le k_i < p, \qquad (D_i^0 = 1), \tag{116}$$

formano una base di $\mathrm{End}_F E$ considerato come spazio vettoriale su E.

Dimostrazione. La prima affermazione è già stata dimostrata. Per provare la seconda usiamo la stessa idea impiegata per stabilire i risultati sui gruppi finiti di automorfismi di campi. Partendo dall'insieme dato di endomorfismi, definiamo un insieme L di endomorfismi che soddisfi le condizioni della corrispondenza di Jacobson–Bourbaki. Nel caso presente prendiamo come L l'insieme delle combinazioni E-lineari degli endomorfismi dati nella (116). Evidentemente L contiene $1 = D_1^0 \cdots D_m^0$, sicché contiene $E_E = E1$, e $[L : E] \le p^m$. Resta da mostrare che L è chiuso rispetto alla moltiplicazione per le D_i. Osserviamo anzitutto che, se D è una derivazione in E, la condizione $D(ab) = D(a)b + aD(b)$ dà la relazione fra operatori

$$Da_E = a_E D + D(a)_E, \tag{117}$$

dove a_E e $D(a)_E$ denotano rispettivamente le moltiplicazioni per a e per $D(a)$. Usando questa relazione si vede che

$$D_i(aD_1^{k_1} \cdots D_m^{k_m}) = aD_iD_1^{k_1} \cdots D_m^{k_m} + D_i(a)D_1^{k_1} \cdots D_m^{k_m}.$$

Per provare che $D_iL \subseteq L$ basta dunque mostrare che $D_iD_1^{k_1}\cdots D_m^{k_m} \in L$ per ogni i e per tutti i k_j con $0 \leq k_j < p$. Lo proveremo mostrando che $D_iD_1^{k_1}\cdots D_m^{k_m}$ è una combinazione lineare a coefficienti in E dei monomi $D_1^{k'_1}\cdots D_m^{k'_m}$ con $0 \leq k'_j < p$ e $\sum k'_j \leq \sum k_j + 1$. L'argomento è molto simile a quello usato nello studio delle algebre di Clifford (p. 230). Procediamo per induzione su $\sum k_j$ e, per gli esponenti k_j fissati, per induzione su i. Disponiamo delle formule

$$D_j^p = \sum_k b_{jk}D_k, \qquad b_{jk} \in E, \tag{118}$$

e

$$D_iD_j = D_jD_i + \sum_k d_{ijk}D_k, \qquad d_{ijk} \in E, \tag{119}$$

che seguono dal fatto che $\mathcal{D}$ è chiusa rispetto alle potenze p-esime e ai commutatori. Il risultato che vogliamo dimostrare è chiaro se $\sum k_j = 0$ e possiamo quindi supporre $\sum k_j > 0$. Qualche k è allora diverso da zero e supponiamo che k_j sia il primo degli esponenti positivo. Si ha quindi $D_1^{k_1}\cdots D_m^{k_m} = D_j^{k_j}\cdots D_m^{k_m}$. Se $i < j$, $D_iD_j^{k_j}\cdots D_m^{k_m}$ è uno dei monomi (116) per i quali la somma degli esponenti è $\sum_l k_l + 1$. La tesi vale dunque in questo caso. Lo stesso accade se $i = j$ e $k_j < p-1$. Siano ora $i = j$ e $k_j = p-1$. Allora $D_iD_j^{k_j}\cdots D_m^{k_m} = D_j^pD_{j+1}^{k_{j+1}}\cdots D_m^{k_m}$ e il risultato segue per induzione sostituendo a D_j^p l'espressione $\sum_k b_{jk}D_k$. Supponiamo ora $i > j$. Per la (119),

$$D_iD_j^{k_j}\cdots D_m^{k_m} = D_jD_iD_j^{k_j-1}\cdots D_m^{k_m} + \sum_k d_{ijk}D_kD_j^{k_j-1}\cdots D_m^{k_m}.$$

Anche in questo caso il risultato segue applicando al secondo membro entrambe le ipotesi induttive. È così stabilito il fatto essenziale che L è chiuso rispetto alla moltiplicazione. Si può dunque applicare a L la corrispondenza di Jacobson–Bourbaki, dalla quale risulta che, se $F = \{a \mid a_EB = Ba_E \text{ per ogni } B \in L\}$, allora F è un sottocampo tale che $[E : F] = [L : E]$ e $L = \mathrm{End}_F E$. Per definizione di L si ha $[L : E] \leq p^m$, e qui vale l'uguaglianza se e soltanto se i monomi (116) formano una base di L su E. Poiché $\mathcal{D}$ genera L, le condizioni che definiscono F si possono sostituire con $a_ED = Da_E$ per ogni $D \in \mathcal{D}$. Per la (117) ciò equivale a dire che a è una D-costante per ogni $D \in \mathcal{D}$. Dunque F è l'insieme delle $\mathcal{D}$-costanti e $\mathcal{D} \subseteq \mathrm{Der}_F E$. Allora E è puramente inseparabile di esponente ≤ 1 su F. Abbiamo $[E : F] = [L : E] \leq p^m$ e quindi $[E : F] = p^{m'}$ con $m' \leq m$. D'altra parte $\mathcal{D}$ contiene m derivazioni linearmente indipendenti su E, cosicché $[\mathrm{Der}_F E : E] \geq m$ e dunque $[E : F] \geq p^m$. Ne segue che $\mathcal{D} = \mathrm{Der}_F E$, $[\mathrm{Der}_F E : E] = m$ e $[L : E] = [E : F] = p^m$. Ciò conclude la dimostrazione. □

Esercizi

In questi esercizi supponiamo che E sia puramente inseparabile di esponente ≤ 1 su F di caratteristica p e che E sia finitamente generato su F.

1. (Baer.) Mostrare che esiste una derivazione D di E/F tale che F sia il sottocampo delle D-costanti di E.

2. Sia D una derivazione di E/F tale che F sia il sottocampo delle D-costanti. Mostrare che il polinomio minimo di D come trasformazione lineare di E/F ha la forma

$$x^{p^m} + c_1x^{p^{m-1}} + \cdots + c_m, \qquad c_i \in F,$$

dove $p^m = [E : F]$.[34] Mostrare che $(1, D, \ldots, D^{p^m-1})$ è una base di $\mathrm{End}_F E$ come spazio vettoriale su E.

[34] L'originale stampa l'ultimo termine come c_m. Il polinomio additivo inteso nell'esercizio termina con c_mx. Il termine costante del polinomio minimo deve essere nullo perché $D(1) = 0$. [N.d.T.]

3. (J. Barsotti, P. Cartier.) Mostrare che, se D è una derivazione in un campo F di caratteristica $p \neq 0$, allora $D^{p-1}(a^{-1}Da) = a^{-1}D^p a - (a^{-1}Da)^p$.

4. (M. Gerstenhaber, M. Ojanguren e M. R. Sridharan.) Sia E un campo di caratteristica $p \neq 0$ e sia V un E-sottospazio di $\operatorname{Der} E$ chiuso rispetto alle potenze p-esime. Mostrare che V è un sottoanello di Lie. Osservare che ciò mostra come la chiusura rispetto ai prodotti di Lie sia superflua nell'enunciato del teorema 8.45.

5. (Gerstenhaber, Ojanguren e Sridharan.) Estendere il teorema 8.45 per ottenere una corrispondenza biunivoca fra l'insieme dei sottocampi F di E tali che E/F sia puramente inseparabile di esponente uno e l'insieme delle p-E-algebre di Lie di derivazioni di E chiuse nella topologia finita.

8.18 Prodotti tensoriali di campi

Se E/F e K/F sono campi su F, che cosa si può dire dell'F-algebra $E \otimes_F K$? In particolare, è un campo o un dominio? È facile dare esempi in cui $E \otimes_F K$ non è un campo. Anzi, se $E \neq F$, allora $E \otimes_F E$ non è mai un campo. Per vederlo osserviamo che, per la proprietà fondamentale dei prodotti tensoriali, esiste un omomorfismo di gruppi additivi η di $E \otimes_F E$ in E tale che $a \otimes b \mapsto ab$, $a, b \in E$. Dalle definizioni è inoltre chiaro che questo è un omomorfismo di F-algebre. Sia ora $a \in E$, $a \notin F$. Allora $1, a$ sono F-indipendenti in E e quindi $1 \otimes 1$, $1 \otimes a$, $a \otimes 1$ e $a \otimes a$ sono F-indipendenti in $E \otimes_F E$. Dunque $1 \otimes a - a \otimes 1 \neq 0$, ma $\eta(1 \otimes a - a \otimes 1) = a - a = 0$. Pertanto $\ker \eta$ è un ideale non nullo di $E \otimes_F E$. L'esistenza di un tale ideale implica che $E \otimes_F E$ non è un campo.

Si vede facilmente anche che, se x e y sono indeterminate, $F(x) \otimes_F F(y)$ è un dominio ma non un campo (si veda più avanti).

Merita inoltre osservare che, se E è algebrico su F e $E \otimes_F K$ è un dominio, questa algebra è un campo. Ciò è chiaro se E ha dimensione finita su F. Infatti $E \otimes_F K$ si può allora considerare come un'algebra di dimensione finita su K, con $[E \otimes_F K : K] = [E : F]$, e un dominio di dimensione finita è necessariamente un campo. Il caso generale segue da questo, poiché ogni $a \in E \otimes_F K$ è contenuto in una sottoalgebra isomorfa a un'algebra $E_0 \otimes_F K$, dove E_0/F è finitamente generata e quindi di dimensione finita su F. Se $a \neq 0$, l'elemento corrispondente di $E_0 \otimes_F K$ è invertibile. Pertanto a è invertibile in $E \otimes_F K$.

Passiamo ora a uno studio sistematico dei prodotti tensoriali di campi. Nella nostra trattazione, per separabilità intenderemo la separabilità nel senso generale della definizione 8.4. La pura inseparabilità di E/F significherà che E è algebrico su F e che il sottocampo di E/F formato dagli elementi separabili su F coincide con F. Diremo che F è *algebricamente chiuso* (rispettivamente, *separabilmente algebricamente chiuso*) in E se ogni elemento di E algebrico (rispettivamente, algebrico separabile) su F appartiene a F. Dimostriamo dapprima il teorema seguente.

Teorema 8.46. *Siano E/F e K/F estensioni del campo F.*

1. *Se E/F è separabile e K/F è puramente inseparabile, $E \otimes_F K$ è un campo. Se invece E/F non è separabile, esiste un'estensione puramente inseparabile K/F di esponente 1 tale che $E \otimes_F K$ contenga un elemento nilpotente non nullo.*

2. *Se E/F è algebrica separabile, $E \otimes_F K$ non ha elementi nilpotenti non nulli per nessuna K/F, ed è un campo se F è separabilmente algebricamente chiuso in K.*

3. *Gli elementi di $E \otimes_F K$ sono invertibili oppure nilpotenti se E/F è puramente inseparabile e K/F è arbitraria, oppure se E/F è algebrica e F è separabilmente algebricamente chiuso in K.*

Dimostrazione. In (1) e nella prima parte di (3) possiamo supporre che la caratteristica sia $p \neq 0$.

(1) Supponiamo E/F separabile e K/F puramente inseparabile. Dalla separabilità segue che, se $a_1, \dots, a_m$ sono elementi F-indipendenti di E, essi sono linearmente indipendenti su F^{1/p^e} (contenuto nella chiusura algebrica di E) per ogni $e = 0, 1, 2, \dots$. Ciò implica che gli elementi $a_1^{p^e}, \dots, a_m^{p^e}$ sono F-indipendenti per ogni e. Sia ora K puramente inseparabile su F e sia $z = \sum_i a_i \otimes c_i \neq 0$ in $E \otimes_F K$, con $a_i \in E$, $c_i \in K$. Possiamo supporre gli a_i F-indipendenti ed esiste un e tale che $c_i^{p^e} \in F$, $1 \leq i \leq m$. Allora

$$z^{p^e} = \sum_i a_i^{p^e} \otimes c_i^{p^e} = \Big(\sum_i c_i^{p^e} a_i^{p^e}\Big) \otimes 1 \neq 0.$$

Dunque $\sum_i c_i^{p^e} a_i^{p^e} \neq 0$ e questo elemento di E è invertibile. Pertanto z^{p^e} è invertibile, quindi anche z è invertibile in $E \otimes_F K$. Ne segue che $E \otimes_F K$ è un campo.

Supponiamo ora che E/F non sia separabile. Esistono allora elementi F-indipendenti $a_1, \dots, a_m \in E$ che non sono $F^{1/p}$-indipendenti. Esistono perciò $c_i^{1/p}$, con $c_i \in F$ non tutti nulli, tali che $\sum_i c_i^{1/p} a_i = 0$. Allora $\sum_i c_i a_i^p = 0$, mentre $\sum_i c_i a_i \neq 0$ poiché non tutti i c_i sono nulli. Consideriamo il campo $K = F(c_1^{1/p}, \dots, c_m^{1/p})$. Si ha $K \supsetneq F$, poiché $K = F$ implicherebbe che gli a_i fossero F-dipendenti. Consideriamo l'elemento $z = \sum_i a_i \otimes c_i^{1/p} \in E \otimes_F K$. Esso è non nullo, poiché gli a_i sono F-indipendenti e non tutti i $c_i^{1/p}$ sono nulli in K. D'altra parte $z^p = \sum_i a_i^p \otimes c_i = (\sum_i c_i a_i^p) \otimes 1 = 0$. Dunque z è un elemento nilpotente non nullo di $E \otimes_F K$.

(2) Supponiamo E/F algebrica separabile e K/F arbitraria. Dobbiamo mostrare che $E \otimes_F K$ non ha nilpotenti non nulli ed è un campo se F è separabilmente algebricamente chiuso in K. Con l'argomento usato all'inizio del paragrafo ci riduciamo al caso in cui E è finitamente generato, dunque $[E : F] < \infty$. In questo caso, poiché E è algebrico separabile, $E = F[a] = F(a)$, dove il polinomio minimo $m(X)$ di a su F è irriducibile e separabile (cioè, per esempio, $(m(X), m'(X)) = 1$). Allora $E \otimes_F K \cong K[\bar{a}]$, dove il polinomio minimo di $\bar{a}$ su K è $m(X)$. Quindi $E \otimes_F K \cong K[X]/(m(X))$. Poiché $m(X)$ è separabile, la sua fattorizzazione in $K[X]$ è $m(X) = m_1(X) \cdots m_r(X)$, dove gli $m_i(X)$ sono polinomi monici irriducibili distinti. Allora

$$E \otimes_F K \cong K[X]/(m(X)) \cong \bigoplus_{i=1}^{r} K[X]/(m_i(X))$$

(esercizio 4, p. 410 di BAI). Poiché $K[X]/(m_i(X))$ è un campo, $E \otimes_F K$ è somma diretta di campi. È chiaro che un'algebra di questa forma non ha elementi nilpotenti non nulli. Ciò dimostra la prima affermazione di (2).

I coefficienti degli $m_i(X)$ sono algebrici separabili su F, poiché sono polinomi simmetrici elementari in alcune radici di $m(X)$, che sono algebriche separabili su F. Quindi, se F è separabilmente algebricamente chiuso in K, si ha $m_i(X) \in F[X]$. Allora $r = 1$ e $E \otimes_F K \cong K[X]/(m(X))$ è un campo.

(3) Sia E/F puramente inseparabile e K/F arbitraria. Sia $z = \sum_{i=1}^m a_i \otimes c_i$, con $a_i \in E$, $c_i \in K$. Possiamo scegliere e in modo che $a_i^{p^e} \in F$ per $1 \leq i \leq m$. Allora $z^{p^e} = \sum_i a_i^{p^e} \otimes c_i^{p^e} = 1 \otimes \sum_i a_i^{p^e} c_i^{p^e} \in 1 \otimes K$. Se $z^{p^e} \neq 0$, esso è invertibile, e quindi lo è z. In caso contrario z è nilpotente.

Sia ora E/F algebrica e sia F separabilmente algebricamente chiuso in K. Sia S il sottocampo degli elementi separabili di E/F. Allora E/S è puramente inseparabile. Ora $E \otimes_F K \cong E \otimes_S (S \otimes_F K)$ (esercizio 13(iv), p. 148). Poiché S/F è algebrica separabile e F è separabilmente algebricamente chiuso in K, per (2) $S \otimes_F K$ è un campo. Poiché E/S è puramente inseparabile, dalla prima parte di questa dimostrazione segue che gli elementi di $E \otimes_S (S \otimes_F K)$ sono nilpotenti oppure invertibili. Altrettanto vale quindi per $E \otimes_F K$. □

Consideriamo ora i prodotti tensoriali di campi in cui uno dei fattori è puramente trascendente.

Teorema 8.47. *Sia E/F puramente trascendente, diciamo $E = F(B)$ con B una base di trascendenza, e sia K/F arbitraria. Allora $E \otimes_F K$ è un dominio e il suo campo delle frazioni Q è puramente trascendente su $K = 1 \otimes_F K$, con base di trascendenza $B = B \otimes 1$. Inoltre, se F è algebricamente chiuso (rispettivamente, separabilmente algebricamente chiuso) in K, allora $E = F(B)$ è algebricamente chiuso (rispettivamente, separabilmente algebricamente chiuso) in $Q = K(B)$.*

Dimostrazione. Per semplicità identifichiamo E e K con i corrispondenti sottocampi $E \otimes 1$ e $1 \otimes K$ di $E \otimes_F K$. Essi sono linearmente disgiunti su F in $A = E \otimes_F K$. Ne segue che, se un sottoinsieme S di E è algebricamente indipendente su F, esso è algebricamente indipendente in A su K. Basta osservarlo per $S = \{s_1, \dots, s_m\}$. In questo caso l'indipendenza algebrica su F equivale alla condizione che i monomi $s_1^{k_1} \cdots s_m^{k_m}$, $k_i \geq 0$, siano distinti e linearmente indipendenti su F. Poiché ciò rimane vero sostituendo F con K, segue che S è algebricamente indipendente su K. In particolare questo vale per la base di trascendenza B di E. Consideriamo la sottoalgebra $K[B]$. Se C è un sottoinsieme finito di B, allora $K[C]$ è un dominio (teorema 2.13 di BAI, p. 128). Ne segue che $K[B]$ è un dominio ed è una sottoalgebra di $A = F(B) \otimes_F K$. Sia $z \in A$. Allora $z = \sum_i a_i c_i$ con $a_i \in F(B)$ e $c_i \in K$. Possiamo scrivere $a_i = p_i q^{-1}$ con $p_i, q \in F[B]$. Allora $z = pq^{-1}$, dove $p = \sum_i p_i c_i \in K[B]$. Viceversa, se $p \in K[B]$ e $q \in F[B]$, $q \neq 0$, allora $p, q^{-1} \in A$ e quindi $pq^{-1} \in A$. Ne segue che A è la localizzazione $K[B]_{F[B]^*}$ di $K[B]$ rispetto al monoide moltiplicativo $F[B]^*$ degli elementi non nulli di $F[B]$. Poiché $K[B]$ è un dominio, anche la sua localizzazione $K[B]_{F[B]^*}$ è un dominio. Inoltre essa è una sottoalgebra della localizzazione $K[B]_{K[B]^*}$, che è il campo delle frazioni Q di $K[B]$ e di A. Evidentemente $Q = K(B)$, il sottocampo di Q/K generato da B. Essendo B algebricamente indipendente su K, vediamo che Q è puramente trascendente su K con base di trascendenza B. Ciò dimostra la prima affermazione.

Per la seconda affermazione mostreremo che, se $K(B)$ contiene un elemento algebrico (algebrico separabile) su $F(B)$ che non appartiene a $F(B)$, allora K contiene un elemento algebrico (algebrico separabile) su F che non appartiene a F. Se esiste un tale elemento, è chiaro che esso si trova in $K(C)$ per qualche sottoinsieme finito C di B. Basta dunque dimostrare il risultato per B finito e poi, per induzione, basta dimostrarlo per $K(x)$ con x indeterminata. Supponiamo pertanto che $z \in K(x)$ sia algebrico su $F(x)$ e che $z \notin F(x)$. Sia $X^n + b_1 X^{n-1} + \cdots + b_n$ il polinomio minimo di z su $F(x)$, sicché $n > 1$. Scriviamo $b_i = p_i q^{-1}$, $p_i, q \in F[x]$. Allora $w = qz$ ha polinomio minimo $X^n + p_1 X^{n-1} + qp_2 X^{n-2} + \cdots + q^{n-1} p_n$. Sostituendo z con qz possiamo supporre $b_i \in F[x]$. Scriviamo ora $z = rs^{-1}$, dove $r, s \in K[x]$ sono primi fra loro. Abbiamo

$$-r^n = b_1 r^{n-1} s + b_2 r^{n-2} s^2 + \cdots + b_n s^n. \tag{120}$$

Se $\deg s > 0$, allora s ha un fattore primo in $K[x]$. Per la (120), questo è anche un fattore di r^n, quindi di r, contro l'ipotesi che r e s siano primi fra loro. Pertanto s è invertibile e possiamo supporre $z \in K[x]$, sicché $z = z(x) = c_0 + c_1 x + \cdots + c_m x^m$, con $c_i \in K$. Affermiamo che i c_i sono algebrici su F. Si ha la relazione $z(x)^n + b_1 z(x)^{n-1} + \cdots + b_n = 0$, dove $b_i = b_i(x) \in F[x]$. Quindi, per ogni $a \in F$, abbiamo

$$z(a)^n + b_1(a) z(a)^{n-1} + \cdots + b_n(a) = 0. \tag{121}$$

Poiché $b_i(a) \in F$, questo mostra che l'elemento $z(a)$ di K è algebrico su F. Se F è infinito, scegliamo $m+1$ elementi distinti $a_1, a_2, \ldots, a_{m+1}$ di F e scriviamo

$$\begin{aligned} z(a_1) &= c_0 + c_1 a_1 + \cdots + c_m a_1^m, \\ z(a_2) &= c_0 + c_1 a_2 + \cdots + c_m a_2^m, \\ &\vdots \\ z(a_{m+1}) &= c_0 + c_1 a_{m+1} + \cdots + c_m a_{m+1}^m. \end{aligned} \tag{122}$$

Poiché gli a_j sono distinti, il determinante di Vandermonde $\det(a_j^i)$ è non nullo. Possiamo dunque risolvere la (122) rispetto ai c_k mediante la regola di Cramer e vedere che ogni c_k è un'espressione razionale a coefficienti interi negli a_i e negli $z(a_j)$. Essendo gli a_i e gli $z(a_j)$ algebrici su F, ne segue che ogni c_k è algebrico su F. Se F è finito, lo sostituiamo con la sua chiusura algebrica $\bar{F}$, che è infinita. L'argomento mostra che ogni c_k è algebrico su $\bar{F}$ e, poiché $\bar{F}$ è algebrica su F, si conclude ancora che i c_k sono algebrici su F. Poiché $z \notin F(x)$, qualche c_k non appartiene a F. Abbiamo quindi un elemento di K algebrico su F che non appartiene a F.

Supponiamo infine che z sia algebrico separabile su $F(x)$. Allora $F(c_0, \ldots, c_m)$ contiene un elemento che non appartiene a F ed è algebrico separabile su F. Altrimenti questo campo sarebbe puramente inseparabile su F e quindi esisterebbe una potenza p^f, dove p è la caratteristica, tale che $c_k^{p^f} \in F$ per $0 \leq k \leq m$. Allora $z^{p^f} = c_0^{p^f} + c_1^{p^f} x^{p^f} + \cdots + c_m^{p^f} x^{mp^f} \in F(x)$, contro la separabilità di z su $F(x)$. Dunque, se $K(x)$ contiene un elemento algebrico separabile su $F(x)$ che non appartiene a $F(x)$, allora K contiene un elemento algebrico separabile su F che non appartiene a F. □

Nel risultato seguente indeboliamo l'ipotesi che E/F sia puramente trascendente, richiedendo soltanto la separabilità.

Teorema 8.48. *Sia E/F separabile e sia K/F arbitraria. Allora $E \otimes_F K$ non ha elementi nilpotenti non nulli.*

Dimostrazione. È chiaro che basta dimostrare il teorema quando E/F è finitamente generata. In tal caso E ha una base di trascendenza B su F tale che E sia algebrico separabile su $F(B)$ (teorema 8.39). Allora $E \otimes_F K \cong E \otimes_{F(B)} (F(B) \otimes_F K)$. Per il risultato precedente $F(B) \otimes_F K$ è un dominio. Se Q è il suo campo delle frazioni, $E \otimes_{F(B)} (F(B) \otimes_F K)$ è una sottoalgebra di $E \otimes_{F(B)} Q$. Poiché E è algebrico separabile su $F(B)$, per il teorema 8.46(2) $E \otimes_{F(B)} Q$ non ha elementi nilpotenti diversi da 0. Quindi $E \otimes_{F(B)} (F(B) \otimes_F K)$ non ha elementi nilpotenti non nulli e lo stesso vale per $E \otimes_F K$. □

Consideriamo ora il caso in cui F sia separabilmente algebricamente chiuso in uno dei fattori.

Teorema 8.49. *Sia F separabilmente algebricamente chiuso in E e sia K/F arbitraria. Allora ogni divisore dello zero di $E \otimes_F K$ è nilpotente.*

Dimostrazione. Sia B una base di trascendenza di K/F. Allora $E \otimes_F K \cong (E \otimes_F F(B)) \otimes_{F(B)} K$. Per il risultato precedente $E \otimes_F F(B)$ è un dominio e $F(B)$ è separabilmente algebricamente chiuso nel campo delle frazioni Q di $E \otimes_F F(B)$. Poiché $F(B)$ è separabilmente algebricamente chiuso in Q e K è algebrico su $F(B)$, dal teorema 8.46(3) segue che gli elementi di $Q \otimes_{F(B)} K$ sono invertibili oppure nilpotenti. Sia ora $z \in (E \otimes_F F(B)) \otimes_{F(B)} K$ un divisore dello zero in questa algebra. Allora z è un divisore dello zero nell'algebra più grande $Q \otimes_{F(B)} K$. Quindi z non vi è invertibile e pertanto è nilpotente. Poiché $E \otimes_F K \cong (E \otimes_F F(B)) \otimes_{F(B)} K$, ne segue che ogni divisore dello zero di $E \otimes_F K$ è nilpotente. □

Possiamo ora dimostrare il nostro risultato principale sulla questione di quando il prodotto tensoriale di due campi sia un dominio.

Teorema 8.50. *Siano E/F e K/F estensioni del campo F. Supponiamo (1) che almeno una*

delle estensioni E/F, K/F sia separabile e (2) che F sia separabilmente algebricamente chiuso in almeno uno dei campi E, K. Allora $E \otimes_F K$ è un dominio.

Dimostrazione. Per il risultato precedente, se F è separabilmente algebricamente chiuso in uno dei fattori, i divisori dello zero di $E \otimes_F K$ sono nilpotenti. D'altra parte, per il teorema 8.48, se uno dei fattori è separabile, $E \otimes_F K$ non ha elementi nilpotenti non nulli. Quindi $E \otimes_F K$ non ha divisori dello zero diversi da 0. □

Una classe di estensioni importante per la geometria algebrica (si vedano le *Foundations of Algebraic Geometry* di Weil, American Mathematical Society Colloquium Publications, vol. XXIX, 1946 e 1960) è descritta nella definizione seguente.

Definizione 8.6. *Un'estensione E/F si dice regolare se (1) E è separabile su F e (2) F è algebricamente chiuso in E.*

Osserviamo che un'estensione separabile E/F non contiene sottocampi propriamente estendenti F e puramente inseparabili su F. Pertanto nella definizione di regolarità possiamo sostituire la condizione (2) con la seguente: ($2'$) F è separabilmente algebricamente chiuso in E. La sufficienza nel prossimo teorema è un caso particolare del teorema 8.50.

Teorema 8.51. *Un'estensione E/F è regolare se e solo se $E \otimes_F K$ è un dominio per ogni campo K/F.*

Dimostrazione. Resta da dimostrare la necessità delle due condizioni. La necessità della separabilità segue dal teorema 8.46(1). Supponiamo ora che F non sia algebricamente chiuso in E. Allora E contiene un sottocampo $K \supsetneq F$ di dimensione finita su F. In tal caso $E \otimes_F K$ contiene $K \otimes_F K$, che non è un campo. Essendo di dimensione finita, $K \otimes_F K$ non è un dominio. Abbiamo dunque la necessità della condizione (2). □

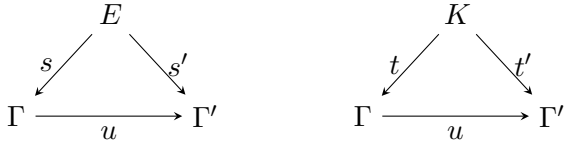
Si vede subito che, se F è algebricamente chiuso, ogni estensione E/F è regolare. Allora $E \otimes_F K$ è un dominio per ogni K/F. Quando $E \otimes_F K$ è un dominio per le estensioni E/F, K/F, denoteremo il campo delle frazioni di $E \otimes_F K$ con $E \cdot K$ (oppure $E \cdot_F K$).

Esercizi

1. Dimostrare che, se E/F è puramente trascendente, E/F è regolare.
2. Dimostrare che, se E_1/F ed E_2/F sono regolari, allora $E_1 \cdot E_2$ è regolare.

8.19 Compositi liberi di campi

Date due estensioni E/F e K/F, è naturale chiedersi quali siano i campi su F che possono essere generati da sottocampi rispettivamente isomorfi a E/F e K/F. Per precisare la domanda, definiamo un *composito* di E/F e K/F come una terna (Γ, s, t) in cui Γ è un campo su F e s, t sono monomorfismi rispettivamente di E/F e di K/F in Γ/F, tali che Γ/F sia generato dai sottocampi $s(E)$ e $t(K)$, cioè $\Gamma = F(s(E), t(K))$. I compositi (Γ, s, t) e (Γ', s', t') di E/F e K/F si dicono *equivalenti* se esiste un isomorfismo $u\colon \Gamma \to \Gamma'$ tale che i due diagrammi seguenti siano commutativi.



Di particolare interesse per la geometria algebrica sono i compositi liberi nel senso della definizione seguente.

Definizione 8.7. *Un composito di campi* (Γ, s, t) *di* E/F *e* K/F *si dice libero se, per ogni coppia di sottoinsiemi algebricamente indipendenti* C *e* D*, rispettivamente di* E/F *e di* K/F*, si ha* $s(C) \cap t(D) = \varnothing$ *e* $s(C) \cup t(D)$ *è algebricamente indipendente in* Γ/F*.*

Poiché ogni sottoinsieme algebricamente indipendente può essere incluso in una base di trascendenza, è chiaro che la condizione che (Γ, s, t) sia libero equivale alla seguente: per ogni coppia di basi di trascendenza B, B' rispettivamente di E/F e di K/F, si ha $s(B) \cap t(B') = \varnothing$ e $s(B) \cup t(B')$ è algebricamente indipendente. Osserviamo ora che in questa condizione si può sostituire «per ogni» con «per qualche». Vale infatti il seguente lemma.

Lemma 1. *Un composito* (Γ, s, t) *di* E/F *e* K/F *è libero se e solo se esistono basi di trascendenza* B *e* B' *rispettivamente di* E/F *e di* K/F *tali che* $s(B) \cap t(B') = \varnothing$ *e* $s(B) \cup t(B')$ *sia algebricamente indipendente in* Γ/F*.*

Dimostrazione. La necessità è chiara. Per provare la sufficienza, supponiamo di avere basi di trascendenza B e B' di E/F e K/F tali che $s(B) \cap t(B') = \varnothing$ e $s(B) \cup t(B')$ sia algebricamente indipendente su F. Per dimostrare che (Γ, s, t) è libero, basta evidentemente mostrare che, se B_1 è un'altra base di trascendenza di E/F, allora $s(B_1) \cap t(B') = \varnothing$ e $s(B_1) \cup t(B')$ è algebricamente indipendente su F. Basta perciò mostrare che, se C è un sottoinsieme finito algebricamente indipendente di E/F e D è un sottoinsieme finito di B', allora $s(C) \cap t(D) = \varnothing$ e $s(C) \cup t(D)$ è algebricamente indipendente su F. Esiste un sottoinsieme finito G di B tale che C dipenda algebricamente da G su F. Evidentemente $s(G) \cap t(D) = \varnothing$ e $s(G) \cup t(D)$ è una base di trascendenza di $F(s(G), s(C), t(D))/F$, sicché

$$\operatorname{tr\,deg} F(s(G), s(C), t(D))/F = |G| + |D|.$$

Inoltre $\operatorname{tr\,deg} F(s(G), s(C))/F = \operatorname{tr\,deg} F(s(G))/F = |G|$ e $\operatorname{tr\,deg} F(s(C))/F = |C|$. Ne segue che

$$\operatorname{tr\,deg} F(s(G), s(C), t(D))/F(s(C), t(D)) \leq |G| - |C|$$

(si veda l'esercizio 1, p. 517). Da questo e dalla formula precedente per il grado di trascendenza di $F(s(G), s(C), t(D))/F$ otteniamo

$$\operatorname{tr\,deg} F(s(C), t(D))/F \geq (|G| + |D|) - (|G| - |C|) = |D| + |C|.$$

Pertanto $s(C) \cap t(D) = \varnothing$ e $s(C) \cup t(D)$ è algebricamente indipendente su F. Dunque (Γ, s, t) è libero. □

Osserviamo pure che, se B e B' sono basi di trascendenza di E/F e di K/F che soddisfano le condizioni del lemma, $s(B) \cup t(B')$ è una base di trascendenza di Γ/F. Infatti gli elementi di $s(E)$ e di $t(K)$ sono algebrici su $F(s(B), t(B'))$ e, poiché Γ è generato da $s(E)$ e $t(K)$, ne segue che Γ è algebrico su $F(s(B), t(B'))$. Dunque $s(B) \cup t(B')$ è una base di trascendenza di Γ/F.

Possiamo usare questi risultati per costruire un composito libero di due campi dati qualsiasi E/F, K/F. Siano B e B' basi di trascendenza di E/F e K/F. Supponiamo dapprima che B e B' siano finite, diciamo $B = \{\xi_1, \ldots, \xi_m\}$, $B' = \{\zeta_1, \ldots, \zeta_n\}$. Sia Ω la chiusura algebrica del campo $F(x_1, \ldots, x_{m+n})$, dove le x_i sono indeterminate. Abbiamo monomorfismi s' e t' rispettivamente di $F(\xi_1, \ldots, \xi_m)/F$ e di $F(\zeta_1, \ldots, \zeta_n)/F$ in Ω, tali che $s'\xi_i = x_i$, $1 \leq i \leq m$, e $t'\zeta_j = x_{m+j}$, $1 \leq j \leq n$. Poiché E è algebrico su $F(B)$ e Ω è algebricamente chiuso, s' si può prolungare a un monomorfismo s di E/F in Ω/F (esercizio 1, p. 475). Analogamente t' si può prolungare a un monomorfismo t di K/F in Ω. Si vede allora subito che, per $\Gamma = F(sE, tK)$, la terna (Γ, s, t) è un composito libero di E e K.

Se almeno uno fra B e B' è infinito, modifichiamo come segue il procedimento usato per B e B' finiti. Possiamo supporre $|B'| \geq |B|$. Sia X un insieme disgiunto da B e da B' tale che $|X| = |B'|$. Possiamo decomporre X come unione disgiunta di due insiemi Y e Z tali che

$|Y| = |B|$, $|Z| = |X| = |B'|$. Sia $F(X)$ il campo delle frazioni dell'algebra dei polinomi $F[X]$. Sia Ω la chiusura algebrica di $F(X)$. Come prima possiamo definire un monomorfismo s di E/F in Ω/F la cui restrizione a B sia una biiezione di B su Y, e un monomorfismo t di K/F in Ω/F la cui restrizione a B' sia una biiezione di B' su Z. Allora (Γ, s, t), per $\Gamma = F(sE, tK)$, è un composito libero di E e K.

Vogliamo descrivere le classi di isomorfismo dei compositi liberi di due campi dati E/F e K/F. Consideriamo dapprima compositi di E e K che non siano necessariamente liberi. Formiamo $E \otimes_F K$ e sia P un ideale primo di questa F-algebra. Allora $(E \otimes_F K)/P$ è un dominio, il cui campo delle frazioni denotiamo con Γ_P. Abbiamo l'omomorfismo $s_P\colon a \mapsto a+P$ (con $a = a \otimes 1$) di E/F in $(E \otimes_F K)/P$ e quindi in Γ_P/F. Poiché E è un campo, esso è un monomorfismo. Analogamente si ha il monomorfismo $t_P\colon b \mapsto b+P$ di K/F in Γ_P/F. Poiché $E \otimes_F K$ è generato da E e K, il quoziente $(E \otimes_F K)/P$ è generato dalle sottoalgebre $s_P(E)$ e $t_P(K)$, e quindi Γ_P è generato come campo da $s_P(E)$ e $t_P(K)$. Dunque (Γ_P, s_P, t_P) è un composito di E/F e K/F.

Osserviamo poi che ideali primi distinti P e P' di $E \otimes_F K$ definiscono compositi non equivalenti (Γ_P, s_P, t_P) e $(\Gamma_{P'}, s_{P'}, t_{P'})$. Se fossero equivalenti, avremmo un isomorfismo u di Γ_P su $\Gamma_{P'}$ tale che $s_{P'} = us_P$ e $t_{P'} = ut_P$. Allora $u(a+P) = us_Pa = s_{P'}a = a+P'$ per $a \in E$ e $u(b+P) = b+P'$ per $b \in K$. Pertanto $u(\sum_i a_ib_i + P) = \sum_i a_ib_i + P'$, con $a_i \in E$, $b_i \in K$. Se $\sum_i a_ib_i \in P$, allora $\sum_i a_ib_i + P = 0$, sicché $\sum_i a_ib_i + P' = 0$ e $\sum_i a_ib_i \in P'$. Dunque $P \subset P'$ e per simmetria $P' \subset P$. Pertanto $P = P'$, contro l'ipotesi.

Sia ora (Γ, s, t) un composito qualsiasi di E/F e K/F. Gli omomorfismi s e t danno luogo all'omomorfismo $s \otimes t$ di $E \otimes_F K$ in Γ che manda $\sum_i a_ib_i$, $a_i \in E$, $b_i \in K$, nell'elemento $\sum_i s(a_i)t(b_i)$ di Γ. Poiché l'immagine è un dominio, il nucleo è un ideale primo P. Abbiamo quindi un isomorfismo u di $(E \otimes_F K)/P$ sulla sottoalgebra $s(E)t(K)$, che si prolunga a un isomorfismo u del campo delle frazioni Γ_P di $(E \otimes_F K)/P$ su $\Gamma = F(s(E), t(K))$. È chiaro che u è un'equivalenza di compositi. Abbiamo dunque stabilito una corrispondenza biunivoca fra l'insieme degli ideali primi di $E \otimes_F K$ e l'insieme delle classi di equivalenza dei compositi di E/F e K/F.

Resta da distinguere i compositi (Γ_P, s_P, t_P) che sono liberi. A questo scopo dimostreremo il teorema seguente.

Teorema 8.52. *Il composito (Γ_P, s_P, t_P) è libero se e solo se ogni elemento di P è un divisore dello zero in $E \otimes_F K$.*

Identificheremo E e K con le loro immagini in $E \otimes_F K$, considerandoli quindi come sottocampi di $E \otimes_F K$ con la seguente proprietà: se S e S' sono sottoinsiemi linearmente indipendenti rispettivamente di E/F e K/F, l'applicazione $(s, s') \mapsto ss'$ è una biiezione di $S \times S'$ su SS', e SS' è un sottoinsieme linearmente indipendente di $E \otimes_F K$.

Siano B e B' basi di trascendenza rispettivamente di E/F e K/F e siano M e M' i sottomonoidi dei monoidi moltiplicativi di E e K generati da B e B'. Poiché B e B' sono algebricamente indipendenti, M e M' sono linearmente indipendenti in E/F e in K/F, e quindi MM' è linearmente indipendente in $E \otimes_F K$. Ora il sottospazio FMM' generato da MM' è la sottoalgebra $F[B \cup B']$ ed è anche la sottoalgebra $F[B]F[B']$. Dunque MM' è una base di $F[B \cup B'] = F[B]F[B']$. Poiché $B \cup B'$ è algebricamente indipendente, $F[B \cup B']$ è un dominio. Il suo campo delle frazioni $F(B \cup B')$ contiene i sottocampi $F(B)$ e $F(B')$ e si vede subito che la sottoalgebra $F(B)F(B')$ generata da essi è l'insieme delle frazioni $a(cc')^{-1}$, con $a \in F[B \cup B'] = F[B]F[B']$, $0 \neq c \in F[B]$ e $0 \neq c' \in F[B']$.

Possiamo ora enunciare il lemma seguente.

Lemma 2. *Il composito (Γ_P, s_P, t_P) è libero se e solo se $F(B)F(B') \cap P = 0$.*

Dimostrazione. Per il lemma 1, (Γ_P, s_P, t_P) è libero se e solo se $s_P(B) \cap t_P(B') = \varnothing$ e $s_P(B) \cup$

$t_P(B')$ è algebricamente indipendente su F. Poiché $s_P(B) = \{b + P \mid b \in B\}$ e $t_P(B') = \{b' + P \mid b' \in B'\}$, queste condizioni valgono se e solo se le classi $q + P$, $q \in MM'$, sono linearmente indipendenti, con M e M' come sopra. Pertanto (Γ_P, s_P, t_P) è libero se e solo se $FMM' \cap P = 0$. Essendo $FMM' = F[B]F[B']$, tale condizione è $F[B]F[B'] \cap P = 0$. Poiché $F(B)F(B')$ consiste delle frazioni $a(cc')^{-1}$ con $a \in F[B]F[B']$, $0 \neq c \in F[B]$, $0 \neq c' \in F[B']$, si ha

$$F[B]F[B'] \cap P = 0 \quad \Longleftrightarrow \quad F(B)F(B') \cap P = 0.$$

Dunque (Γ_P, s_P, t_P) è libero se e solo se $F(B)F(B') \cap P = 0$. □

Ci occorre anche il seguente lemma.

Lemma 3. *$E \otimes_F K$ è intero su $F(B)F(B')$.*

Dimostrazione. Poiché B è una base di trascendenza di E, questo è algebrico, dunque intero, su $F(B)$. A maggior ragione E è intero su $F(B)F(B')$. Analogamente K è intero su $F(B)F(B')$. Poiché il sottoinsieme di $E \otimes_F K$ degli elementi interi su $F(B)F(B')$ è una sottoalgebra, ne segue che $E \otimes_F K = EK$ è intero su $F(B)F(B')$. □

Possiamo ora dare la *dimostrazione del teorema 8.52.* Supponiamo dapprima che ogni elemento di P sia un divisore dello zero in $E \otimes_F K$. Sia $a \in P \cap F(B)F(B')$. Allora a è un divisore dello zero in $E \otimes_F K$. Affermiamo che a è un divisore dello zero in $F(B)F(B')$. Per vederlo, siano $\{c_\alpha\}$ e $\{d_\beta\}$ basi rispettivamente di $E/F(B)$ e di $K/F(B')$, e siano $\{m_\gamma\}$ e $\{n_\delta\}$ basi rispettivamente di $F(B)/F$ e di $F(B')/F$. Allora $\{c_\alpha m_\gamma\}$ è una base di E/F e $\{d_\beta n_\delta\}$ è una base di K/F. Dunque $\{c_\alpha d_\beta m_\gamma n_\delta\}$ è una base di $E \otimes_F K$ su F. Ne segue che ogni elemento di $E \otimes_F K$ si scrive in modo unico come somma finita $\sum q_{\alpha\beta} c_\alpha d_\beta$ con $q_{\alpha\beta} \in F(B)F(B')$.

Ora esiste un elemento $\sum q_{\alpha\beta} c_\alpha d_\beta \neq 0$ tale che

$$\sum a q_{\alpha\beta} c_\alpha d_\beta = a\Big(\sum q_{\alpha\beta} c_\alpha d_\beta\Big) = 0.$$

Poiché $a \in F(B)F(B')$, ciò implica che ogni $aq_{\alpha\beta} = 0$ e, dato che $\sum q_{\alpha\beta} c_\alpha d_\beta \neq 0$, qualche $q_{\alpha\beta}$ è non nullo. Dunque a è un divisore dello zero in $F(B)F(B')$. Poiché $a \in F(B)F(B')$ e $F(B)F(B')$ è un dominio, ne segue che $a = 0$. Abbiamo dimostrato che, se ogni elemento di P è un divisore dello zero in $E \otimes_F K$, allora $P \cap F(B)F(B') = 0$, e per il lemma 2 (Γ_P, s_P, t_P) è libero. Viceversa, supponiamo (Γ_P, s_P, t_P) libero, sicché $P \cap F(B)F(B') = 0$. Sia $b \in P$. Allora b è intero su $F(B)F(B')$ e si ha una relazione $b^n + c_1 b^{n-1} + \cdots + c_n = 0$ con $c_i \in F(B)F(B')$. Possiamo supporre n minimo. Allora $c_n = -b^n - \cdots - bc_{n-1} \in P$, poiché $b \in P$. Dunque $c_n \in P \cap F(B)F(B')$ e perciò $c_n = 0$. Si ha quindi $b(b^{n-1} + c_1 b^{n-2} + \cdots + c_{n-1}) = 0$ e, per la minimalità di n, $b^{n-1} + c_1 b^{n-2} + \cdots + c_{n-1} \neq 0$, sicché b è un divisore dello zero. Il fatto che (Γ_P, s_P, t_P) sia libero implica dunque che ogni elemento di P è un divisore dello zero in $E \otimes_F K$. La dimostrazione è completa. □

Consideriamo ora un importante caso particolare di questo teorema, quello in cui F è separabilmente algebricamente chiuso in E. In tal caso, per il teorema 8.49, i divisori dello zero di $E \otimes_F K$ sono nilpotenti. Poiché vale anche il viceversa, $\mathrm{nilrad}(E \otimes_F K)$ è l'unico ideale primo di $E \otimes_F K$ costituito da divisori dello zero. Abbiamo pertanto il risultato seguente.

Teorema 8.53. *Se K/F è arbitraria e F è separabilmente algebricamente chiuso in E, a meno di equivalenza esiste un unico composito libero di E/F e K/F.*

Ciò si applica in particolare se E è un'estensione regolare di F. Allora $E \otimes_F K$ è un dominio per ogni K, sicché $\mathrm{nilrad}(E \otimes_F K) = 0$. In questo caso il composito libero di E/F e K/F è $E \cdot K$, che abbiamo definito come il campo delle frazioni di $E \otimes_F K$.

Consideriamo infine un caso molto semplice di compositi che servirà nella teoria delle valutazioni (si veda il ğ 9.9), quello in cui uno dei campi, diciamo E/F, ha dimensione finita. In

questo caso tutto ciò che ci occorre della trattazione precedente è la corrispondenza biunivoca fra l'insieme degli ideali primi P di $E \otimes_F K$ e le classi di equivalenza dei compositi (Γ_P, s_P, t_P). Osserviamo anche che, poiché $E \otimes_F K$ ha dimensione finita su K, questo anello è artiniano. Sono quindi applicabili i risultati ricavati nel ğ 7.11. Usando il fatto che un dominio di dimensione finita su un campo è un campo, vediamo che gli ideali primi di $E \otimes_F K$ sono massimali. Per il teorema 7.13 essi sono in numero finito. Inoltre la dimostrazione del teorema 7.13 mostra come determinare gli ideali massimali. Osserviamo pure che, se E è algebrico su F, l'estensione E/F ha per base di trascendenza l'insieme vuoto. Dalla definizione 8.7 segue che i compositi di E/F con qualsiasi K/F sono liberi.

Supponiamo ora che E abbia un elemento primitivo, diciamo $E = F(\theta)$. Ciò accade sempre se E/F è separabile e di dimensione finita (BAI, p. 291). Vale allora il seguente teorema.

Teorema 8.54. *Sia K/F arbitraria e sia $E = F(\theta)$, con θ algebrico su F di polinomio minimo $f(x)$ di grado n. Siano $f_1(x), \ldots, f_h(x)$ i fattori monici irriducibili di $f(x)$ in $K[x]$. Allora vi sono h compositi non equivalenti (Γ_i, s_i, t_i) di E/F e K/F, dove $\Gamma_i = K[x]/(f_i(x))$, s_i è il monomorfismo di E/F in Γ_i/F tale che $\theta \mapsto x + (f_i(x))$, e t_i è il monomorfismo $b \mapsto b + (f_i(x))$ di K/F in Γ_i/F. Ogni composito di E/F e K/F è equivalente a uno di questi.*

Dimostrazione. Abbiamo l'isomorfismo su F di $E = F(\theta)$ su $F[x]/(f(x))$ tale che $\theta \mapsto \bar{x} = x + (f(x))$. Come abbiamo visto a p. 546, $E \otimes_F K \cong K[x]/(f(x))$. Gli ideali massimali di $K[x]/(f(x))$ sono della forma $(f_i(x))/(f(x))$, dove $f_i(x)$ è un fattore monico irriducibile di $f(x)$ in $K[x]$. Allora

$$\Gamma_i = K[x]/(f_i(x)) \cong (K[x]/(f(x)))/((f_i(x))/(f(x)))$$

è un campo su F. Abbiamo il monomorfismo s_i di E/F in Γ_i/F tale che $\theta \mapsto x + (f_i(x))$ e il monomorfismo t_i di K/F in Γ_i/F tale che $b \mapsto b + (f_i(x))$, $b \in K$. Chiaramente $s_i(E)$ e $t_i(K)$ generano Γ_i. Quindi (Γ_i, s_i, t_i) è un composito di E/F e K/F. Il resto segue da quanto dimostrato sopra. □

Esercizi

1. Determinare i compositi su $\mathbb{Q}$ di $\mathbb{R}$ con (1) $\mathbb{Q}(\omega)$, dove ω è una radice cubica primitiva di 1, e (2) $\mathbb{Q}(\sqrt{2})$.
2. Determinare i compositi su $\mathbb{Q}$ di $\mathbb{Q}(\sqrt{-1})$ e $\mathbb{Q}(\sqrt{3})$.
3. Supporre che E/F e K/F siano estensioni di Galois di dimensione finita e che $E \otimes_F K$ sia un dominio, dunque un campo. L'estensione $(E \otimes_F K)/F$ è di Galois?

Riferimenti bibliografici

- E. Steinitz, «Algebraische Theorie den Körpern», *Journal für die reine und angewandte Mathematik*, vol. 137 (1909), pp. 167–309.
- N. Jacobson, *Lectures in Abstract Algebra III. The Theory of Fields and Galois Theory*, 1964. Nuova stampa, Springer-Verlag, New York.
- P. J. McCarthy, *Algebraic Extension of Fields*, Blaisdell, Waltham, Mass., 1966.
- D. J. Winter, *The Structure of Fields*, Springer-Verlag, New York, 1974.

9 Teoria delle valutazioni

La teoria delle valutazioni dei campi, che studieremo in questo capitolo, ha avuto, come la teoria degli ideali negli anelli commutativi, due origini: la teoria dei numeri e la geometria algebrica. Sul versante aritmetico il punto di partenza fu la scoperta dei numeri p-adici da parte di Hensel. Questi introdusse l'anello degli interi p-adici essenzialmente come abbiamo fatto nel capitolo 2: come limite inverso degli anelli $\mathbb{Z}/(p^n)$. Più tardi Kürschák (1913) introdusse la nozione di valutazione di un campo a valori reali e mostrò che il campo dei numeri p-adici di Hensel si poteva considerare come il completamento di $\mathbb{Q}$ rispetto alla valutazione p-adica. Sul versante della geometria algebrica la teoria sembra avere avuto origine con l'introduzione della nozione di posto da parte di Dedekind e Weber, che intendevano dare una definizione precisa della superficie di Riemann di una curva algebrica.

La teoria delle valutazioni stabilisce un saldo legame fra teoria dei numeri, algebra e analisi. Da un lato consente uno studio preciso delle funzioni algebriche, dall'altro porta a introdurre, nello studio di questioni aritmetiche, concetti analoghi a quelli dell'analisi classica.

Inizieremo dalle valutazioni a valori reali, che oggi si chiamano di solito *valori assoluti*. Se ne distinguono due tipi, archimedei e non archimedei. I secondi suggeriscono una generalizzazione alle valutazioni a valori in gruppi abeliani ordinati, introdotta da Krull nel 1934. Nel seguito riserviamo il termine «valutazione» alle valutazioni di Krull a valori in gruppi abeliani ordinati. Le valutazioni così intese equivalgono ad altre due nozioni: gli anelli di valutazione e i posti. Studieremo con qualche dettaglio il problema del prolungamento dei valori assoluti e delle valutazioni alle estensioni di campi, soprattutto alle estensioni di grado finito. In particolare considereremo questo problema per il campo $\mathbb{Q}$.

Definiremo l'importante nozione di campo locale, centrale nella teoria algebrica dei numeri, e daremo una caratterizzazione topologica di questi campi e delle algebre di divisione di dimensione finita sui campi locali. Il nostro metodo è elementare e consente, al tempo stesso, di determinare il gruppo di Brauer di un campo locale. Considereremo inoltre le forme quadratiche sui campi locali e definiremo per esse un invariante che, insieme al discriminante, ne fornisce una classificazione completa.

9.1 Valori assoluti

Supponiamo note le proprietà di $\mathbb{R}$ come campo ordinato che si studiano in un primo corso di analisi (per esempio, la completezza e l'esistenza dei logaritmi). Il concetto di valore assoluto su un campo generalizza direttamente il valore assoluto su $\mathbb{C}$.

Definizione 9.1. *Un valore assoluto* $|\ |$ *su un campo* F *è un'applicazione* $a \mapsto |a|$ *da* F *in* $\mathbb{R}$ *tale che*

1. $|a| \geq 0$ e $|a| = 0$ se e soltanto se $a = 0$;
2. $|ab| = |a|\,|b|$;
3. $|a + b| \leq |a| + |b|$ *(disuguaglianza triangolare).*

Come si è accennato, l'esempio classico è $\mathbb{C}$, dove $|a| = (\alpha^2 + \beta^2)^{1/2}$ per $a = \alpha + \beta\sqrt{-1}$, $\alpha, \beta \in \mathbb{R}$. Useremo la notazione $|\ |_\infty$ quando occorrerà distinguere questo valore assoluto dagli altri. Sui sottocampi $\mathbb{R}$ e $\mathbb{Q}$ esso si riduce al consueto valore assoluto. Elenchiamo alcuni esempi meno familiari.

Esempi

1. *Valore assoluto p-adico su* $\mathbb{Q}$. Fissiamo un primo $p \in \mathbb{Z}$. Per $0 \neq a \in \mathbb{Q}$ scriviamo $a = (b/c)p^k$, dove $k \in \mathbb{Z}$ e $(b,p) = (c,p) = 1$. L'intero k è univocamente determinato da a. Lo indichiamo con $v_p(a)$ e poniamo $v_p(0) = \infty$. Si verificano facilmente le proprietà

$$\begin{aligned} &\text{(i)} \quad v_p(a) = \infty \iff a = 0, \\ &\text{(ii)} \quad v_p(ab) = v_p(a) + v_p(b), \\ &\text{(iii)} \quad v_p(a+b) \geq \min(v_p(a), v_p(b)). \end{aligned}$$

   Sia ora γ reale con $0 < \gamma < 1$. Definiamo un valore assoluto p-adico su $\mathbb{Q}$ ponendo

$$|a|_p = \gamma^{v_p(a)}, \tag{1}$$

   dove $\gamma^\infty = 0$. È chiaro che si tratta di un valore assoluto ai sensi della definizione 9.1. Vale anzi, per $|\ | = |\ |_p$, la relazione più forte

$$|a+b| \leq \max(|a|, |b|). \tag{2}$$

2. Sia $F(x)$ il campo delle espressioni razionali in un'indeterminata x e sia $p(x)$ un polinomio primo in $F[x]$. Per $0 \neq a \in F(x)$ scriviamo $a = p(x)^k b(x)/c(x)$, con $k \in \mathbb{Z}$ e $(p(x), b(x)) = (p(x), c(x)) = 1$. Poniamo $v_p(a) = k$, $v_p(0) = \infty$ e $|a|_p = \gamma^{v_p(a)}$, dove γ è reale e $0 < \gamma < 1$. Valgono le prime due proprietà della definizione 9.1 e la (2), dunque $|a|_p = \gamma^{v_p(a)}$ definisce un valore assoluto su $F(x)$.

   Un caso particolare importante si ottiene con $F = \mathbb{C}$, $p(x) = x - r$, $r \in \mathbb{C}$. Ogni elemento $a \in \mathbb{C}(x)$ definisce nel modo usuale una funzione razionale sulla sfera di Riemann $\mathbb{C} \cup \{\infty\}$. Se $v_p(a) = k > 0$ la funzione ha uno zero di ordine k in r; se $v_p(a) = -k$, $k > 0$, ha un polo di ordine k in r. Infine, se $v_p(a) = 0$, non ha in r né uno zero né un polo. Il valore di $v_p(a)$ dà dunque informazioni sul comportamento di a in un intorno di r.

3. Otteniamo un altro valore assoluto su $F(x)$ come segue. Se $a \neq 0$, scriviamo $a = b(x)/c(x)$, dove $b(x) = b_0 + b_1 x + \cdots + b_m x^m$, $c(x) = c_0 + c_1 x + \cdots + c_n x^n$, con $b_i, c_i \in F$ e $b_m, c_n \neq 0$. Definiamo $v_\infty(a) = n - m$, $v_\infty(0) = \infty$ e $|a|_\infty = \gamma^{v_\infty(a)}$, con $\gamma \in \mathbb{R}$ e $0 < \gamma < 1$. Abbiamo

$$\begin{aligned} a &= \frac{x^m(b_0 x^{-m} + b_1 x^{-(m-1)} + \cdots + b_m)}{x^n(c_0 x^{-n} + c_1 x^{-(n-1)} + \cdots + c_n)} \\ &= \frac{b_0 x^{-m} + b_1 x^{-(m-1)} + \cdots + b_m}{c_0 x^{-n} + c_1 x^{-(n-1)} + \cdots + c_n}(x^{-1})^{n-m}. \end{aligned}$$

   La definizione di $|a|_\infty$ equivale quindi a prendere x^{-1} come generatore di $F(x)$ e ad applicare il procedimento dell'esempio 2 a $F[x^{-1}]$ con $p(x^{-1}) = x^{-1}$. Pertanto $|\ |_\infty$ è un valore assoluto. Nel caso $F = \mathbb{C}$, $v_\infty(a)$ descrive il comportamento all'infinito della funzione razionale definita da a.

Su ogni campo F si ha il *valore assoluto banale*, dato da $|0| = 0$ e $|a| = 1$ per $a \neq 0$. Elenchiamo alcune proprietà elementari che seguono direttamente dalla definizione:

$$\begin{gathered} |1| = 1, \qquad |u| = 1 \text{ se } u^m = 1 \ (m > 0), \qquad |-a| = |a|, \\ |a^{-1}| = |a|^{-1} \text{ se } a \neq 0, \qquad \big||a| - |b|\big|_\infty \leq |a - b|. \end{gathered}$$

Un valore assoluto su F definisce una topologia i cui aperti sono le unioni di intorni sferici: un tale intorno di a ha la forma $\{x \mid |x - a| < r\}$, con $r > 0$. Si vede facilmente che questa è

una topologia su F e che moltiplicazione, addizione e sottrazione sono funzioni continue di due variabili. Si definisce quindi, nel modo usuale, la convergenza delle successioni e delle serie. La successione $\{a_n \mid n = 1, 2, \ldots\}$ converge ad a se, per ogni $\varepsilon > 0$ reale, esiste un intero $N = N(\varepsilon)$ tale che $|a - a_n| < \varepsilon$ per tutti gli $n \geq N$. Si scrive anche $\lim a_n = a$ o $a_n \to a$ (oppure $a_n \xrightarrow{|\,|} a$ per indicare il valore assoluto). Si estendono le proprietà elementari della convergenza in $\mathbb{C}$: se $a_n \to a$, $b_n \to b$, allora $a_n \pm b_n \to a \pm b$, $a_n b_n \to ab$ e $|a_n| \to |a|$ in $\mathbb{R}$. Se $a_n \to a \neq 0$, allora $a_n \neq 0$ per $n > k$, con k abbastanza grande, e $a_{n+k}^{-1} \to a^{-1}$, e così via. Per una serie $\sum_{n=1}^{\infty} a_n$ scriviamo $\sum a_n = s$ se la successione delle somme parziali $s_n = a_1 + \cdots + a_n$ converge a s.

È naturale chiamare *equivalenti* due valori assoluti $|\ |_1$ e $|\ |_2$ quando definiscono la stessa topologia su F. Se, per esempio, due valori assoluti p-adici sono definiti dai parametri γ, γ', ossia $|a|_p = \gamma^{v_p(a)}$ e $|a|'_p = (\gamma')^{v_p(a)}$, allora $|a|'_p = |a|_p^s$, con $s = \log \gamma' / \log \gamma > 0$. Ogni intorno sferico di un punto per l'uno è un intorno sferico per l'altro. Vale lo stesso su qualunque campo F per due valori assoluti $|\ |$ e $|\ |' = |\ |^s$, dove s è un reale positivo. Osserviamo inoltre che la topologia definita da un valore assoluto è discreta se e soltanto se questo è banale. Il valore assoluto banale dà chiaramente la topologia discreta. Viceversa, se il valore assoluto è non banale, esiste a con $0 < |a| < 1$; allora $a^n \to 0$ e l'insieme $\{a^n\}$ non è chiuso in F. Il solo valore assoluto equivalente a quello banale è pertanto il valore assoluto banale stesso. Mostreremo ora che due valori assoluti non banali possono essere equivalenti soltanto se ciascuno è una potenza positiva dell'altro. Inoltre, per assicurare l'equivalenza basta una condizione in un solo senso. Entrambi i fatti seguono dal prossimo teorema.

Teorema 9.1. *Siano $|\ |_1, |\ |_2$ due valori assoluti su un campo F. Si supponga che $|\ |_1$ sia non banale e che, per $a \in F$, $|a|_1 < 1$ implichi $|a|_2 < 1$. Allora esiste un reale $s > 0$ tale che $|\ |_2 = |\ |_1^s$ (ossia $|a|_2 = |a|_1^s$ per ogni $a \neq 0$). Dunque i due valori assoluti sono equivalenti.*

Dimostrazione (Artin). Dall'ipotesi segue che $|a|_1 < |b|_1$ implica $|a|_2 < |b|_2$. In particolare, se $|a|_1 > 1$, anche $|a|_2 > 1$. Poiché $|\ |_1$ è non banale, scegliamo a_0 con $|a_0|_1 > 1$, e quindi $|a_0|_2 > 1$. Dato un qualunque a con $|a|_1 > 1$, poniamo $t = \log |a|_1 / \log |a_0|_1$. Allora $t > 0$ e $|a|_1 = |a_0|_1^t$. Affermiamo che $|a|_2 = |a_0|_2^t$. Scriviamo infatti $|a|_2 = |a_0|_2^{t'}$, con $t' > 0$. Se $t' \neq t$ esiste un razionale r strettamente compreso fra i due. Se $t < r < t'$, si avrebbe $|a_0|_2^r < |a|_2$; se $t' < r < t$, si avrebbe $|a_0|_2^r > |a|_2$. Ci basta perciò mostrare che, per $r > t$ razionale, $|a_0|_2^r > |a|_2$ e che, per $0 < r < t$ razionale, vale la disuguaglianza inversa. Scriviamo $r = m/n$ con m, n interi positivi. Se $r > t$, allora $|a|_1^n < |a_0|_1^m$, ossia $|a^n|_1 < |a_0^m|_1$. Segue che $|a^n|_2 < |a_0^m|_2$, quindi $|a|_2 < |a_0|_2^{m/n}$. Analogamente, se $m/n < t$, si ha $|a|_2 > |a_0|_2^{m/n}$. Dunque $|a|_2 = |a_0|_2^t$ e

$$t = \frac{\log |a|_2}{\log |a_0|_2} = \frac{\log |a|_1}{\log |a_0|_1}, \qquad \frac{\log |a|_2}{\log |a|_1} = \frac{\log |a_0|_2}{\log |a_0|_1}.$$

Otteniamo $|a|_2 = |a|_1^s$, con $s = \log |a_0|_2 / \log |a_0|_1 > 0$, per ogni a con $|a|_1 > 1$. Se $0 < |a|_1 < 1$, si applica il risultato ad a^{-1}; se $|a|_1 = 1$, lo si applica ad aa_0 e ad a_0. La relazione vale anche per $a = 0$. Come abbiamo visto, ne segue l'equivalenza dei valori assoluti. □

Il valore assoluto p-adico su $\mathbb{Q}$ e i valori assoluti su $F(x)$ visti negli esempi soddisfano la disuguaglianza triangolare più forte $|a + b| \leq \max(|a|, |b|)$. Un valore assoluto con questa proprietà si dice *non archimedeo*, altrimenti si dice *archimedeo*. Per distinguere i due casi basta esaminare il sottoanello fondamentale. Infatti si ha il seguente risultato.

Teorema 9.2. *Un valore assoluto su un campo F è non archimedeo se e soltanto se $|n1| \leq 1$ per ogni $n \in \mathbb{Z}$.*

Dimostrazione (Artin). Se $|\ |$ è non archimedeo, $|a_1 + \cdots + a_n| \leq \max_i |a_i|$. Pertanto $|1 + \cdots + 1| \leq |1| = 1$ e $|n1| \leq 1$ per ogni $n \in \mathbb{Z}$. Viceversa, supponiamo che ciò valga e siano $a, b \in F$. Per

ogni intero $n > 0$ si ha

$$\begin{aligned} |a+b|^n &= \left|a^n + \tbinom{n}{1}a^{n-1}b + \cdots + b^n\right| \\ &\le |a|^n + |a|^{n-1}|b| + \cdots + |b|^n \\ &\le (n+1)\max(|a|^n, |b|^n). \end{aligned}$$

Dunque $|a+b| \le (n+1)^{1/n}\max(|a|,|b|)$; poiché in $\mathbb{R}$ si ha $\lim(n+1)^{1/n} = 1$, segue che $|a+b| \le \max(|a|,|b|)$. □

Corollario 1. *Ogni valore assoluto su un campo di caratteristica $p \neq 0$ è non archimedeo.*

Dimostrazione. Se $n1$ è un elemento non nullo del sottoanello fondamentale, allora $(n1)^{p-1} = 1$, quindi $|n1| = 1$. Inoltre $|0| = 0$. La tesi segue dal teorema 9.2. □

Il valore assoluto banale è non archimedeo. Dal teorema 9.2 si vede anche che, se un valore assoluto è non archimedeo su un sottocampo di F, lo è su F. Otteniamo così il seguente corollario.

Corollario 2. *Se $|\ |$ è banale su un sottocampo, allora è non archimedeo.*

Esercizi

1. Mostrare che, se $|\ |$ è un valore assoluto e $0 < s < 1$, allora $|\ |^s$ è un valore assoluto. Mostrare anche che, se $|\ |$ è non archimedeo, $|\ |^s$ è un valore assoluto per ogni $s > 0$.

2. Mostrare che, se $|\ |$ è non archimedeo e $|a| > |b|$, allora $|a+b| = |a|$. Mostrare anche che da $a_1 + \cdots + a_n = 0$, per $n \ge 2$, segue $|a_i| = |a_j|$ per qualche $i \neq j$.

3. Sia F un campo con un valore assoluto non archimedeo e sia $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in F[x]$. Posto $M = \max(1, |a_1|, \ldots, |a_n|)$, mostrare che ogni zero ρ di f in F soddisfa $|\rho| \le M$.

4. Sia $|\ |$ un valore assoluto su E, banale su un sottocampo F tale che E/F sia algebrica. Mostrare che $|\ |$ è banale su E.

5. Siano $|\ |$ un valore assoluto su F e σ un automorfismo. Mostrare che $|a|_\sigma = |\sigma a|$ definisce un valore assoluto. Applicare il risultato a $\mathbb{Q}(\sqrt{2})$ e a $\mathbb{Q}(\sqrt{-1})$ con $\sigma \neq 1$. Stabilire in ciascun caso se $|\ |_\sigma$ e $|\ |$ sono o no equivalenti.

9.2 Il teorema di approssimazione

In questo paragrafo dimostreremo un teorema sull'approssimazione simultanea rispetto a valori assoluti non equivalenti, analogo al teorema cinese del resto della teoria degli anelli. Ne seguirà una forte proprietà di indipendenza per valori assoluti non equivalenti. Il risultato è il seguente.

Teorema di approssimazione (Artin–Whaples). *Siano $|\cdot|_1, \ldots, |\cdot|_n$ valori assoluti non banali, a due a due non equivalenti, su un campo F. Siano $a_1, \ldots, a_n$ elementi di F ed ε un numero reale positivo. Esiste allora $a \in F$ tale che*

$$|a - a_k|_k < \varepsilon, \qquad 1 \le k \le n. \tag{3}$$

Dimostreremo anzitutto il seguente teorema.

Teorema 9.3. *Siano $|\cdot|_1, \ldots, |\cdot|_n$ valori assoluti non banali, a due a due non equivalenti, su F. Per ogni k, $1 \le k \le n$, esiste $a_k \in F$ tale che*

$$|a_k|_k > 1, \qquad |a_k|_l < 1 \quad \text{se } l \neq k. \tag{4}$$

Dimostrazione. Basta dimostrarlo per $k = 1$. Dobbiamo dunque trovare a tale che $|a|_1 > 1$ e $|a|_l < 1$ per ogni $l > 1$. Sia dapprima $n = 2$. Per il criterio di equivalenza (teorema 9.1) esistono $b \in F$ con $|b|_1 < 1$ e $|b|_2 \geq 1$ e $c \in F$ con $|c|_2 < 1$ e $|c|_1 \geq 1$. Allora, ponendo $a = cb^{-1}$, abbiamo $|a|_1 > 1$ e $|a|_2 < 1$. Il risultato vale quindi per $n = 2$ e possiamo supporlo vero per $n - 1 \geq 2$. Abbiamo allora elementi b, c tali che

$$|b|_1 > 1, \quad |b|_2 < 1, \ \ldots, \ |b|_{n-1} < 1, \qquad |c|_1 > 1, \quad |c|_n < 1.$$

Distinguiamo due casi.

Caso I. $|b|_n \leq 1$. Consideriamo $a_r = b^r c$. Si ha $|a_r|_k = |b|_k^r |c|_k$. Questo valore è maggiore di 1 se $k = 1$ e minore di 1 se $k > 1$ e r è sufficientemente grande. Per uno qualunque di tali r poniamo $a = a_r$. Vale allora la (4).

Caso II. $|b|_n > 1$. Prendiamo $a_r = \frac{b^r}{1+b^r} c$. Se $2 \leq k \leq n-1$, si ha $|b|_k < 1$ e quindi $b^r \to 0$ rispetto a $|\cdot|_k$. Allora $a_r \to 0$ rispetto a $|\cdot|_k$ e $|a_r|_k < 1$ per r sufficientemente grande. Sia invece $k = 1$ oppure $k = n$. Allora $|b|_k > 1$, da cui $b^r/(1 + b^r) = 1/(1 + b^{-r}) \to 1$ e $a_r \to c$ rispetto a $|\cdot|_k$. Poiché $|c|_1 > 1$ e $|c|_n < 1$, si ha $|a_r|_1 > 1$ e $|a_r|_n < 1$ per r sufficientemente grande. Dunque per un opportuno $a = a_r$ abbiamo $|a|_1 > 1$, $|a|_2 < 1, \ldots, |a|_n < 1$. □

Possiamo ora dimostrare il teorema di approssimazione. Siano $|\cdot|_1, \ldots, |\cdot|_n$ non equivalenti e non banali e siano $a_1, \ldots, a_n \in F$. Per ogni k, $1 \leq k \leq n$, applichiamo il teorema 9.3 per ottenere b_k tale che $|b_k|_k > 1$ e $|b_k|_l < 1$ per ogni $l \neq k$. Si ha allora

$$\frac{b_k^r}{1 + b_k^r} \longrightarrow \begin{cases} 1 & \text{rispetto a } |\cdot|_k, \\ 0 & \text{rispetto a } |\cdot|_l, \quad l \neq k. \end{cases}$$

Pertanto $a_k b_k^r/(1+b_k^r)$ tende ad a_k rispetto a $|\cdot|_k$ e a zero rispetto a $|\cdot|_l$ per $l \neq k$. Di conseguenza $\sum_{k=1}^n a_k b_k^r/(1 + b_k^r)$ tende ad a_j rispetto a $|\cdot|_j$ per ogni j, $1 \leq j \leq n$. Per ogni $\varepsilon > 0$ possiamo quindi prendere

$$a = \sum_{k=1}^{n} \frac{a_k b_k^r}{1 + b_k^r}$$

con r sufficientemente grande e avremo le relazioni richieste $|a - a_k|_k < \varepsilon$, $1 \leq k \leq n$. □

Abbiamo visto che, se $|\cdot|_1$ e $|\cdot|_2$ sono equivalenti, esiste un reale positivo s tale che $|\cdot|_2 = |\cdot|_1^s$. D'altra parte il teorema di approssimazione mostra che, se $|\cdot|_1, \ldots, |\cdot|_n$ sono non equivalenti e non banali, non esiste una n-upla reale $(s_1, \ldots, s_n) \neq (0, \ldots, 0)$ tale che

$$|a|_1^{s_1} |a|_2^{s_2} \cdots |a|_n^{s_n} = 1$$

per ogni $a \in F^*$. Infatti possiamo supporre $s_1 = 1$. Per il teorema di approssimazione esiste per ogni i un a_i tale che $|a_i|_1 < 1/2^i$ e $|a_i - 1|_j < 1/2^i$ per $j > 1$. Allora $|a_i|_1 \to 0$ e $|a_i|_j \to 1$ per $j > 1$, e la relazione precedente non può valere per tutti gli a_i.

Esercizio.

1. Se p è primo, definiamo il *valore assoluto p-adico normalizzato* su $\mathbb{Q}$ mediante $|a|_p = p^{-v_p(a)}$. Sia $|\cdot|_\infty$ il valore assoluto usuale. Mostrare che $\prod_p |a|_p = |a|_\infty^{-1}$ per ogni $a \in \mathbb{Q}^*$, nel senso che, dato a, solo un numero finito di $|a|_p$ sono diversi da 1 e il loro prodotto è $|a|_\infty^{-1}$. Si può anche scrivere $\prod_q |a|_q = 1$, dove q percorre i primi $p \in \mathbb{Z}$ e ∞.

9.3 Valori assoluti su $\mathbb{Q}$ e $F(x)$

Determineremo tutti i valori assoluti su $\mathbb{Q}$ e tutti i valori assoluti sul campo $F(x)$, con x trascendente, che siano banali sul sottocampo F. Cominciamo con $\mathbb{Q}$.

Teorema 9.4. *Ogni valore assoluto archimedeo $|\cdot|$ su $\mathbb{Q}$ è equivalente al valore assoluto usuale $|\cdot|_\infty$.*

Dimostrazione (Artin). Siano n, n' interi maggiori di 1 e scriviamo

$$n' = a_0 + a_1 n + \cdots + a_k n^k, \qquad 0 \le a_i < n.$$

Allora

$$|n'| < n(1 + |n| + \cdots + |n|^k) \le n(k+1)\max(1, |n|^k).$$

Poiché $n' \ge n^k$, si ha $\log n' \ge k \log n$, ossia $k \le \log n'/\log n$, perciò

$$|n'| < n\left(\frac{\log n'}{\log n} + 1\right) \max\left(1, |n|^{\log n'/\log n}\right).$$

Sostituendo a n' la potenza $(n')^r$, con r intero positivo, otteniamo

$$|(n')^r| < n\left(\frac{r \log n'}{\log n} + 1\right) \max\left(1, |n|^{r \log n'/\log n}\right).$$

Ne segue

$$|n'| < \left[n\left(\frac{r \log n'}{\log n} + 1\right)\right]^{1/r} \max\left(1, |n|^{\log n'/\log n}\right).$$

Per costanti reali a, b, con $a > 0$, vale $\lim_{r\to\infty}(ra+b)^{1/r} = 1$, poiché $\lim_{r\to\infty} r^{-1}\log(ra+b) = 0$. L'ultima disuguaglianza dà quindi

$$|n'| \le \max\left(1, |n|^{\log n'/\log n}\right) \tag{5}$$

per ogni $n, n' > 1$. Poiché $|\cdot|$ è archimedeo, esiste n' tale che $|n'| > 1$ (teorema 9.2). Allora $|n'| \le |n|^{\log n'/\log n}$ e quindi $|n| > 1$ per ogni $n > 1$. La (5) dà allora, per ogni $n, n' > 1$,

$$|n'|^{1/\log n'} \le |n|^{1/\log n}.$$

Per simmetria si ha $|n'|^{1/\log n'} = |n|^{1/\log n}$. Dunque $\log|n'|/\log n' = \log|n|/\log n = s > 0$, cosicché $|n| = n^s$ per tutti gli interi $n > 1$. Ne segue che $|a| = |a|_\infty^s$ per ogni $a \ne 0$ in $\mathbb{Q}$, perciò $|\cdot|$ è equivalente a $|\cdot|_\infty$. □

Determiniamo ora i valori assoluti non archimedei su $\mathbb{Q}$.

Teorema 9.5. *Ogni valore assoluto non archimedeo e non banale su $\mathbb{Q}$ è un valore assoluto p-adico per qualche primo p.*

Dimostrazione. Si ha $|n| \le 1$ per ogni intero n. Se $|n| = 1$ per ogni $n \ne 0$ in $\mathbb{Z}$, allora $|\cdot|$ è banale. L'insieme P degli interi b tali che $|b| < 1$ contiene dunque elementi non nulli. Ora P è un ideale di $\mathbb{Z}$, poiché $|b_1 + b_2| \le \max(|b_1|, |b_2|) < 1$ per $b_i \in P$ e $|nb| = |n||b| < 1$ per $n \in \mathbb{Z}$, $b \in P$. Inoltre P è primo, poiché $|n| = |n'| = 1$ implica $|nn'| = 1$. Pertanto $P = (p)$ per qualche primo $p > 0$. Poniamo $\gamma = |p|$, cosicché $0 < \gamma < 1$. Per $r \ne 0$ in $\mathbb{Q}$ possiamo scrivere $r = p^k a/b$, con $k \in \mathbb{Z}$ e $a, b \notin (p)$. Allora $|a| = 1 = |b|$ e $|r| = \gamma^k = \gamma^{v_p(r)}$. Dunque $|\cdot|$ è il valore assoluto p-adico definito da γ. □

Consideriamo ora il caso di $F(x)$.

Teorema 9.6. *Sia $|\cdot|$ un valore assoluto non banale su $F(x)$, con x trascendente, che sia banale su F. Allora $|\cdot|$ è uno dei valori assoluti definiti negli esempi 2 e 3 del ğ9.1.*[35]

Dimostrazione. Poiché $|\cdot|$ è banale su F, è non archimedeo. Distinguiamo due casi.

Caso I. $|x| \leq 1$. Poiché $|\cdot|$ è non archimedeo e banale su F, si ha $|b| \leq 1$ per ogni $b \in F[x]$. Poiché non è banale su $F(x)$, deve esistere un $b \in F[x]$ tale che $0 < |b| < 1$. Si procede come nella dimostrazione del teorema 9.5. Sia P l'insieme dei $b \in F[x]$ per cui $|b| < 1$. È un ideale (p), dove $p = p(x)$ è un polinomio primo. Si vede allora che $|\cdot|$ è un valore assoluto determinato da $p(x)$ come nell'esempio 2 del ğ9.1.

Caso II. $|x| > 1$. Sia $b = b_0 + b_1 x + \cdots + b_m x^m$, con $b_i \in F$, $b_m \neq 0$. Allora $|b_m x^m| = |x|^m > |b_i x^i|$ per $i < m$, cosicché $|b| = |x|^m$ (esercizio 2 del ğ9.1). Ponendo $|x| = \gamma^{-1}$, $0 < \gamma < 1$, si verifica facilmente che $|\cdot|$ è il valore assoluto $|\cdot|_\infty$ definito nell'esempio 3 del ğ9.1. □

9.4 Completamento di un campo

Le nozioni familiari di convergenza, successione di Cauchy e completezza in $\mathbb{R}$ e in $\mathbb{C}$, già incontrate studiando le topologie definite dagli ideali di un anello (ğ7.18), si estendono ai campi con un valore assoluto. Per F e $|\cdot|$ arbitrari abbiamo le definizioni seguenti.

Definizione 9.2. Sia F un campo con un valore assoluto $|\cdot|$. Una successione $\{a_n\}$ di elementi di F si dice *successione di Cauchy* se, dato un reale $\varepsilon > 0$, esiste un intero positivo $N = N(\varepsilon)$ tale che

$$|a_m - a_n| < \varepsilon \tag{6}$$

per ogni $m, n \geq N$. Il campo F si dice *completo rispetto a* $|\cdot|$ se ogni successione di Cauchy di elementi di F converge (esiste $\lim a_n$).

Come nel caso di $\mathbb{C}$, è chiaro che, se $a_n \to a$, allora $\{a_n\}$ è una successione di Cauchy. Mostreremo che ogni campo F con un valore assoluto $|\cdot|$ ha un *completamento* $\widehat{F}$, nel senso che

1. $\widehat{F}$ è un'estensione di F ed è dotato di un valore assoluto che estende quello dato.
2. $\widehat{F}$ è completo rispetto a questo valore assoluto.
3. F è denso in $\widehat{F}$ rispetto alla topologia definita dal valore assoluto.

Poiché i passi della costruzione di $\widehat{F}$ sono quasi identici a quelli familiari per i numeri reali e per gli spazi metrici, ci limiteremo a delinearli e lasceremo le verifiche al lettore. Partiamo dall'insieme $C = C(F)$ delle successioni di Cauchy di elementi di F. Se ne può fare un anello commutativo che estende F. Per $\{a_n\}, \{b_n\} \in C$ definiamo $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ e $\{a_n\}\{b_n\} = \{a_n b_n\}$. Queste successioni appartengono a C. Per $a \in F$ sia $\{a\}$ la successione costante con tutti i termini uguali ad a. Allora $(C, +, \cdot, \{0\}, \{1\})$ è un anello commutativo contenente il sottoanello delle successioni costanti, isomorfo a F mediante $a \mapsto \{a\}$. Una successione $\{a_n\}$ si dice *infinitesima* se $a_n \to 0$. Sia B l'insieme delle successioni infinitesime. Si vede facilmente che B è un ideale di C. È chiaro che $B \cap \{F\}$ contiene solo la successione nulla, dove $\{F\}$ indica l'insieme delle successioni costanti $\{a\}$, $a \in F$. Dunque B è un ideale proprio di C.

Lemma. *B è un ideale massimale di C.*

Dimostrazione. Sia B' un ideale di C che contenga propriamente B e sia $\{a_n\} \in B' \setminus B$. Si tratta di una successione di Cauchy che non è infinitesima. Esistono allora un reale $\eta > 0$ e un

[35] Nell'enunciato sono richiamati gli esempi 1 e 2. Le due costruzioni usate nella dimostrazione sono quelle degli esempi 2 e 3, relativi a un polinomio primo e al punto all'infinito. [N.d.T.]

intero p tali che $|a_n| > \eta$ per ogni $n \geq p$. Poniamo $b_n = 1$ se $n < p$ e $b_n = a_n$ se $n \geq p$. Allora $\{a_n\} - \{b_n\} = \{c_n\} \in B$. Si verifica anche facilmente che $\{b_n^{-1}\} \in C$. Pertanto

$$\{1\} = \{b_n^{-1}\}\{b_n\} = \{b_n^{-1}\}\{a_n\} - \{b_n^{-1}\}\{c_n\} \in B'.$$

Ne segue $B' = C$, cosicché B è massimale. □

Poniamo $\widehat{F} = C/B$. È un campo. L'omomorfismo canonico di C su $\widehat{F}$ manda $\{F\}$ su un sottocampo che possiamo identificare con F. Identifichiamo così ogni $a \in F$ con la classe $\{a\} + B$ in C/B.

Introduciamo un valore assoluto $|\cdot|$ su $\widehat{F}$. Per $\{a_n\} \in C$, la disuguaglianza $\big||a_n| - |a_m|\big|_\infty \leq |a_n - a_m|$ mostra che $\{|a_n|\}$ è una successione di Cauchy di numeri reali. Esiste quindi $\lim |a_n|$ in $\mathbb{R}$. Se $\{b_n\} \in B$, si ha $b_n \to 0$ e $|b_n| \to 0$. Pertanto, se $\{a'_n\} \in \{a_n\} + B$, si ha $\lim |a'_n| = \lim |a_n|$. Definendo

$$\big|\{a_n\} + B\big| = \lim |a_n|$$

otteniamo dunque un'applicazione di $\widehat{F}$ in $\mathbb{R}$. Poiché $|a_n| \geq 0$, i suoi valori sono non negativi. Inoltre $|a_n| \to 0$ implica $a_n \to 0$, quindi $|\bar{a}| = 0$ per $\bar{a} \in \widehat{F}$ se e solo se $\bar{a} = 0$. Si verifica direttamente che $|\cdot|$ soddisfa anche le condizioni (2) e (3) della definizione 9.1. È quindi un valore assoluto su $\widehat{F}$. È chiaro anche che esso estende il valore assoluto su F, quando identifichiamo F, come sopra, con il sottoinsieme delle classi $\{a\} + B$.

Mostriamo che F è denso in $\widehat{F}$. Basta far vedere che ogni $\bar{a} \in \widehat{F}$ è limite di una successione di elementi di F. In effetti, se $\bar{a} = \{a_n\} + B$, si vede facilmente che $\lim a_n = \bar{a}$.

Sia ora $\{\bar{a}_n\}$ una successione di Cauchy in $\widehat{F}$. Per ogni n esiste $a_n \in F$ tale che $|\bar{a}_n - a_n| < 1/2^n$. Ne segue che $\{a_n\}$ è di Cauchy in F e che $\lim \bar{a}_n = \bar{a}$, dove $\bar{a} = \{a_n\} + B$. Dunque $\widehat{F}$ è completo e abbiamo dimostrato l'esistenza di un completamento di F.

Consideriamo ora l'unicità del completamento. Più in generale, siano $\widehat{F}_i$, $i = 1, 2$, due campi completi rispetto ai valori assoluti $|\cdot|_i$ e sia F_i un sottocampo denso di $\widehat{F}_i$. Supponiamo di avere un isomorfismo s di F_1 su F_2 che sia *isometrico*, ossia $|a|_1 = |sa|_2$ per $a \in F_1$. Allora s è un'applicazione continua di F_1 in $\widehat{F}_2$ e, poiché è isometrica e F_1 è denso in $\widehat{F}_1$, ha un'unica estensione a un'applicazione continua $\bar{s}$ di $\widehat{F}_1$ in $\widehat{F}_2$. È facile vedere che $\bar{s}$ è un omomorfismo. Poiché $\overline{s^{-1}}$ è un omomorfismo e $s^{-1}s = 1_{F_1}$, $ss^{-1} = 1_{F_2}$ implicano $\overline{s^{-1}}\bar{s} = 1_{\widehat{F}_1}$, $\bar{s}\,\overline{s^{-1}} = 1_{\widehat{F}_2}$, ne segue che $\bar{s}$ è un isomorfismo. È chiaro anche che $\bar{s}$ è unico ed è isometrico.

Teorema 9.7. *(1) Ogni campo F con un valore assoluto ha un completamento $\widehat{F}$. (2) Se $\widehat{F}_i$, $i = 1, 2$, è completo rispetto a un valore assoluto e F_i è un sottocampo denso di $\widehat{F}_i$, ogni isomorfismo isometrico di F_1 su F_2 si estende in uno e un solo modo a un isomorfismo isometrico di $\widehat{F}_1$ su $\widehat{F}_2$.*

Prendendo $s = 1_F$, ciò dimostra l'unicità del completamento a meno di un isomorfismo isometrico che sia l'identità su F.

Completando $\mathbb{Q}$ rispetto al valore assoluto usuale $|\cdot|_\infty$ si ottiene, classicamente, il campo $\mathbb{R}$ dei numeri reali. D'altra parte, il completamento di $\mathbb{Q}$ rispetto a un valore assoluto p-adico $|a|_p = \gamma^{v_p(a)}$, $0 < \gamma < 1$, si può identificare con il campo $\mathbb{Q}_p$ dei numeri p-adici definito alle pp. 74–75. Per vederlo, consideriamo dapprima la chiusura $\widehat{\mathbb{Z}}$ di $\mathbb{Z}$ nel completamento $\widehat{\mathbb{Q}}$ rispetto a $|\cdot|_p$. Un elemento $\alpha \in \widehat{\mathbb{Z}}$ è il limite in $\widehat{\mathbb{Q}}$ di una successione di interi a_i. Si può supporre che tale successione soddisfi $a_i \equiv a_j \pmod{p^i}$ per $i \leq j$ e determini quindi un elemento del limite inverso $\mathbb{Z}_p = \varprojlim \mathbb{Z}/(p^i)$. Si verifica direttamente che esiste un isomorfismo di $\widehat{\mathbb{Z}}$ con $\mathbb{Z}_p$ che manda $\lim a_i$ nell'elemento corrispondente di $\mathbb{Z}_p$. Possiamo quindi identificare questi due anelli. Poiché $\{|a|_p \mid a \in \mathbb{Q}\}$ è chiuso in $\mathbb{R}$, esso coincide con $\{|\alpha| \mid \alpha \in \widehat{\mathbb{Q}}\}$. Per ogni $\beta \neq 0$ in $\widehat{\mathbb{Q}}$ esiste dunque $e \in \mathbb{Z}$ tale che $|\beta| = |p^e|$, cosicché $\alpha = \beta p^{-e}$ soddisfa $|\alpha| = 1$. Allora $\alpha = \lim a_i$,

con $a_i = b_i/c_i$ e $(b_i, p) = 1 = (c_i, p)$. Esiste $x_i \in \mathbb{Z}$ tale che $x_i c_i \equiv b_i \pmod{p^i}$. Si ha quindi $|x_i - b_i/c_i| \leq |p^i|$, perciò $\alpha = \lim x_i \in \mathbb{Z}_p = \widehat{\mathbb{Z}}$. Ne segue che ogni elemento di $\widehat{\mathbb{Q}}$ è della forma αp^e, $\alpha \in \mathbb{Z}_p$, $e \leq 0$. Evidentemente $\widehat{\mathbb{Q}}$ è quindi il campo delle frazioni di $\mathbb{Z}_p$, ossia il campo $\mathbb{Q}_p$ dei numeri p-adici.

Esercizi. Negli esercizi 1–3 si suppone F completo rispetto a un valore assoluto $|\cdot|$.

1. Mostrare che, se $\sum a_n$ converge in F, allora $\lim a_n = 0$. Mostrare che vale il viceversa se $|\cdot|$ è non archimedeo.

2. Mostrare che, per k naturale positivo,

$$v_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \cdots$$

   e quindi $v_p(k!) < k/(p-1)$ (cfr. BAI, esercizio 15, p. 84). Servirsene per dimostrare che la serie di potenze

$$\exp z = \sum_{i=0}^{\infty} z^i/i!$$

   converge per ogni $z \in \mathbb{Q}_p$, $p \neq 2$, tale che $|z|_p < 1$.

3. Mostrare che $\exp(x+y) = (\exp x)(\exp y)$ se $|x|, |y| < 1$.

9.5 Estensioni di dimensione finita di campi completi. Il caso archimedeo

Uno dei problemi centrali della teoria delle valutazioni è il seguente: dato un campo F con un valore assoluto $|\cdot|$ e un'estensione di dimensione finita E/F, è possibile estendere $|\cdot|$ a un valore assoluto su E? Ci interessa anche determinare tutte le estensioni. Esamineremo ora il problema per F completo, soprattutto nel caso di un valore assoluto archimedeo. Dimostriamo anzitutto un teorema di unicità.

Teorema 9.8. *Sia $|\cdot|$ un valore assoluto non banale su F rispetto al quale F sia completo, e sia E un'estensione di dimensione finita di F. Se $|\cdot|$ si può estendere a un valore assoluto su E, tale estensione è unica ed è data da*

$$|a| = |N_{E/F}(a)|^{1/[E:F]}. \tag{7}$$

Inoltre E è completo.

Dimostrazione. Siano $u_1, \ldots, u_r$ elementi linearmente indipendenti di E e sia $\{a_n\}$ una successione di elementi della forma $a_n = \sum_{i=1}^{r} \alpha_{ni} u_i$, con $\alpha_{ni} \in F$. Allora $\{a_n\}$ è una successione di Cauchy se e solo se le r successioni $\{\alpha_{ni}\}$, $1 \leq i \leq r$, sono di Cauchy in F. In una direzione ciò è chiaro: se tutte le $\{\alpha_{ni}\}$ sono di Cauchy, anche $\{a_n\}$ lo è. Viceversa, supponiamo che $\{a_n\}$ sia di Cauchy. Per $r = 1$ è chiaro che $\{\alpha_{n1}\}$ è di Cauchy. Procediamo per induzione su r. Se $\{\alpha_{nr}\}$ è di Cauchy, lo è la successione $b_n = a_n - \alpha_{nr} u_r$, e poiché $b_n = \sum_{j=1}^{r-1} \alpha_{nj} u_j$ la tesi segue in questo caso dall'ipotesi induttiva. Supponiamo invece che $\{\alpha_{nr}\}$ non sia di Cauchy. Esiste allora un reale $\varepsilon > 0$ tale che per ogni intero positivo N vi siano interi $p, q \geq N$ con $|\alpha_{pr} - \alpha_{qr}| > \varepsilon$. Esistono quindi coppie di interi positivi (p_k, q_k), con $p_1 < p_2 < \cdots$, $q_1 < q_2 < \cdots$, tali che $|\alpha_{p_k r} - \alpha_{q_k r}| > \varepsilon$. L'inverso di $\alpha_{p_k r} - \alpha_{q_k r}$ esiste in F, e possiamo formare la successione

$$b_k = (\alpha_{p_k r} - \alpha_{q_k r})^{-1}(a_{p_k} - a_{q_k}). \tag{8}$$

Poiché $|\alpha_{p_k r} - \alpha_{q_k r}|^{-1} < \varepsilon^{-1}$ e $a_{p_k} - a_{q_k} \to 0$, abbiamo $b_k \to 0$. D'altra parte

$$b_k = \sum_{j=1}^{r-1} \beta_{kj} u_j + u_r. \tag{9}$$

Dunque, se $c_k = \sum_{j=1}^{r-1} \beta_{kj} u_j$, si ha $c_k \to -u_r$ e $\{c_k\}$ è di Cauchy. Per l'ipotesi induttiva ogni $\{\beta_{kj}\}$ è di Cauchy e, poiché F è completo rispetto a $|\cdot|$, si ha $\beta_{kj} \to \beta_j \in F$. Passando al limite nella (9) otteniamo $\sum_{j=1}^{r-1} \beta_j u_j + u_r = 0$, contro l'indipendenza lineare degli u_i. Abbiamo così provato che ogni $\{\alpha_{ni}\}$ è di Cauchy. È ora chiaro anche che, se $a_n \to 0$, ogni $\alpha_{ni} \to 0$. Prendendo $(u_1, \ldots, u_r)$ come base si vede inoltre che E è completo.

Resta da dimostrare la (7). Se non valesse, esisterebbe $a = \sum_{i=1}^{r} \alpha_i u_i$ tale che $|a^r| \neq |N_{E/F}(a)|$, con $r = [E : F]$. Sostituendo, se necessario, a con a^{-1}, possiamo supporre $|a^r| < |N_{E/F}(a)|$. Poniamo $b = a^r N_{E/F}(a)^{-1}$. Allora $|b| < 1$ e $N(b) = N_{E/F}(b) = 1$. Poiché $|b| < 1$, si ha $b^n \to 0$. Scrivendo $b^n = \sum_{i=1}^{r} \beta_{ni} u_i$, otteniamo quindi $\beta_{ni} \to 0$ per ogni i. Poiché l'applicazione norma è una funzione polinomiale da E in F, è continua. Pertanto $\beta_{ni} \to 0$ implica $1 = N(b^n) \to 0$. La contraddizione dimostra la (7). □

Determineremo ora i campi completi rispetto a una valutazione reale archimedea. Vedremo che le sole possibilità sono $\mathbb{R}$ e $\mathbb{C}$. Occorre il seguente risultato, applicabile nel caso archimedeo poiché tali campi hanno caratteristica zero.

Lemma. *Sia F un campo di caratteristica diversa da 2, completo rispetto a una valutazione reale $|\cdot|$, e sia E un'estensione quadratica di F. Allora la (7), ossia $|a| = |N_{E/F}(a)|^{1/2}$, definisce su E una valutazione che estende $|\cdot|$.*

Dimostrazione. E è galoisiano su F. Sia $a \mapsto \bar{a}$ l'automorfismo di E/F diverso dall'identità. Allora $T(a) = a + \bar{a}$, $N(a) = a\bar{a}$ e $a^2 - T(a)a + N(a) = 0$. Se $a \in F$, $N(a) = a^2$ e dalla definizione si vede che $a \mapsto |N_{E/F}(a)|^{1/2}$ estende il valore assoluto su F. Evidentemente $|a|$ definito dalla (7) è non negativo, e $|a| = 0$ se e solo se $N_{E/F}(a) = 0$, ossia se e solo se $a = 0$. La condizione $|ab| = |a||b|$ segue dalla moltiplicatività della norma. Resta da dimostrare $|a + b| \leq |a| + |b|$. Per la moltiplicatività basta provare $|a + 1| \leq |a| + 1$. Poiché la disuguaglianza vale in F, possiamo supporre $a \notin F$. Allora $E = F(a)$ e il polinomio minimo di a su F è $x^2 - T(a)x + N(a) = (x - a)(x - \bar{a})$. Dunque $N(a + 1) = (a + 1)(\bar{a} + 1) = N(a) + T(a) + 1$ e dobbiamo provare $|N(a + 1)| \leq (|N(a)|^{1/2} + 1)^2$, ossia

$$|1 + T(a) + N(a)| \leq 1 + 2|N(a)|^{1/2} + |N(a)|.$$

Poiché $|\alpha + \beta| \leq |\alpha| + |\beta|$ in F, basta mostrare $|T(a)| \leq 2|N(a)|^{1/2}$ o, equivalentemente, $|T(a)|^2 \leq 4|N(a)|$. Supponiamo invece $|T(a)|^2 > 4|N(a)|$. Mostreremo allora che $a \in F$, contro $E = F(a)$.

Consideriamo l'equazione $x^2 - \alpha x + \beta = 0$, con $\alpha = T(a)$, $\beta = N(a)$, le cui radici in E sono a e $\bar{a}$. Faremo vedere che essa ha una radice in F. Ne seguirà $a \in F$ e avremo la contraddizione cercata. L'equazione equivale a $x = \alpha - \beta x^{-1}$ e abbiamo $|\alpha|^2 > 4|\beta|$. Ne otterremo una soluzione come limite di una successione $\{\gamma_n\}$ in F. Definiamo per ricorsione

$$\gamma_1 = \tfrac{1}{2}\alpha, \qquad \gamma_{n+1} = \alpha - \beta\gamma_n^{-1}.$$

Perché ciò abbia senso, occorre mostrare che nessun γ_n è nullo. Abbiamo $|\gamma_1| \geq \frac{1}{2}|\alpha| > 0$, poiché $|2| \leq 2$, quindi $\gamma_1 \neq 0$. Supponendo $|\gamma_n| \geq \frac{1}{2}|\alpha|$, troviamo

$$\begin{aligned} |\gamma_{n+1}| = |\alpha - \beta\gamma_n^{-1}| &\geq |\alpha| - |\beta||\gamma_n|^{-1} \\ &\geq |\alpha| - 2|\beta||\alpha|^{-1} \geq |\alpha| - \tfrac{1}{2}|\alpha|^2|\alpha|^{-1} = \tfrac{1}{2}|\alpha|. \end{aligned}$$

Dunque $|\gamma_n| \geq \frac{1}{2}|\alpha| > 0$ per ogni n, cosicché $\gamma_n \neq 0$. Ora $\gamma_{n+2} - \gamma_{n+1} = \beta\gamma_{n+1}^{-1}\gamma_n^{-1}(\gamma_{n+1} - \gamma_n)$. Pertanto

$$|\gamma_{n+2} - \gamma_{n+1}| \leq \frac{4|\beta|}{|\alpha|^2}|\gamma_{n+1} - \gamma_n|.$$

Ponendo $r = 4|\beta|/|\alpha|^2 < 1$ si ottiene $|\gamma_{n+2} - \gamma_{n+1}| \leq r^n|\gamma_2 - \gamma_1|$. Tale disuguaglianza implica che $\{\gamma_n\}$ è di Cauchy. Esiste dunque $\gamma = \lim \gamma_n$ in F. Passando al limite nella relazione $\gamma_{n+1} = \alpha - \beta\gamma_n^{-1}$ otteniamo $\gamma = \alpha - \beta\gamma^{-1}$ e $\gamma^2 - \alpha\gamma + \beta = 0$. Ciò conclude la dimostrazione. □

Possiamo ora dimostrare il teorema seguente.

Teorema di Ostrowski. *I soli campi completi rispetto a un valore assoluto archimedeo sono* $\mathbb{R}$ *e* $\mathbb{C}$.

Dimostrazione (A. Ostrowski). Sia F completo rispetto al valore assoluto archimedeo $|\cdot|$. Allora F contiene $\mathbb{Q}$ e, poiché i valori assoluti archimedei di $\mathbb{Q}$ sono equivalenti al valore assoluto ordinario, la chiusura $\widehat{\mathbb{Q}}$ di $\mathbb{Q}$ in F si può identificare con $\mathbb{R}$ e la restrizione di $|\cdot|$ a $\mathbb{R}$ è equivalente al valore assoluto usuale. Se F contiene un elemento i tale che $i^2 = -1$, contiene un sottocampo $\mathbb{R}(i)$ che possiamo identificare con $\mathbb{C}$. Inoltre, per il teorema 9.8, la restrizione di $|\cdot|$ a $\mathbb{C}$ è equivalente all'usuale $|\cdot|_\infty$. Se F non contiene un tale i, possiamo aggiungerlo a F e ottenere $E = F(i)$. Per il lemma e il teorema 9.8 il valore assoluto $|\cdot|$ si estende in uno e un solo modo a E, che è completo rispetto al valore assoluto esteso. Le considerazioni precedenti si applicano a E in luogo di F e, se riusciamo a mostrare che $E = \mathbb{C}$, seguirà che $F = \mathbb{R}$. La dimostrazione è quindi ridotta a mostrare che, se F soddisfa le ipotesi, contiene $\mathbb{C}$ e la restrizione di $|\cdot|$ a $\mathbb{C}$ è equivalente a $|\cdot|_\infty$, allora $F = \mathbb{C}$.

Supponiamo che F contenga propriamente $\mathbb{C}$ e sia $a \in F \setminus \mathbb{C}$. Consideriamo l'applicazione $x \mapsto |x - a|$ di $\mathbb{C}$ in $\mathbb{R}$. Poiché la topologia indotta da $|\cdot|$ su $\mathbb{C}$ è quella usuale, si vede facilmente che l'applicazione è continua. Sia $r = \inf_{\gamma\in\mathbb{C}} |\gamma - a|$. Affermiamo che esiste $\gamma_0 \in \mathbb{C}$ tale che $|\gamma_0 - a| = r$. Anzitutto, restringendo γ agli elementi per cui $|\gamma - a| \leq r + 1$, l'estremo inferiore rimane r. Per due elementi γ_1, γ_2 di questo insieme si ha $|\gamma_1 - \gamma_2| \leq 2r + 2$. Ne segue che gli elementi γ con $|\gamma - a| \leq r + 1$ formano un insieme chiuso e limitato in $\mathbb{C}$. Per la continuità di $x \mapsto |x - a|$ esiste quindi $\gamma_0 \in \mathbb{C}$ tale che $|\gamma_0 - a| = r$ e pertanto $|\gamma - a| \geq |\gamma_0 - a|$ per ogni $\gamma \in \mathbb{C}$. Sia $D = \{\gamma \in \mathbb{C} \mid |\gamma - a| = r\}$. Tale insieme è non vuoto ed è chiuso per la continuità di $|x - a|$. L'argomento di prima mostra che è limitato. Mostreremo ora che D è aperto, ottenendo così una contraddizione.

Per provare che D è aperto mostreremo che, se $\gamma' \in D$, ogni γ con $|\gamma' - \gamma| < r$ appartiene a D. Sostituendo ad a l'elemento $\gamma' - a$ e chiamandolo ancora a, ciò equivale a mostrare che, se $|a| = r$ e $|\gamma| < r$, allora $|a - \gamma| = r$. Sia n un intero positivo e consideriamo $a^n - \gamma^n = (a - \gamma)(a - \epsilon\gamma)\cdots(a - \epsilon^{n-1}\gamma)$, dove ϵ è una radice primitiva n-esima di 1 in $\mathbb{C}$. Allora

$$|a - \gamma|\,|a - \epsilon\gamma|\cdots|a - \epsilon^{n-1}\gamma| = |a^n - \gamma^n| \leq |a|^n + |\gamma|^n.$$

Poiché $|a - \epsilon^k\gamma| \geq r$, segue

$$|a - \gamma|r^{n-1} \leq |a|^n\left(1 + \frac{|\gamma|^n}{|a|^n}\right) = r^n\left(1 + \frac{|\gamma|^n}{r^n}\right).$$

Dunque $|a - \gamma| \leq r(1 + |\gamma|^n/r^n)$ e, se $|\gamma| < r$, passando al limite si ha $|a - \gamma| \leq r$, poiché $1 + (|\gamma|/r)^n \to 1$. Perciò $|a - \gamma| = r$. Dunque D è aperto, chiuso e non vuoto. Poiché $\mathbb{C}$ è connesso, $D = \mathbb{C}$. Per due numeri complessi qualunque γ_1, γ_2 avremmo allora $|\gamma_1 - \gamma_2| \leq |\gamma_1 - a| + |\gamma_2 - a| = 2r$. Ciò è impossibile, e la dimostrazione è conclusa. □

Alla luce del teorema di Ostrowski il problema di estensione per i campi archimedei completi diventa immediato. Se F è un tale campo con valore assoluto $|\cdot|$, allora $F = \mathbb{C}$ oppure $F = \mathbb{R}$.

Nel primo caso F non ha estensioni algebriche proprie, nel secondo la sua unica estensione algebrica propria è $\mathbb{C}$. In entrambi i casi $|\cdot|$ è equivalente a $|\cdot|_\infty$ e, se $F = \mathbb{R}$ ed $E = \mathbb{C}$, l'estensione è data dalla (7) ed E è completo. Per potervi fare riferimento in seguito enunciamo questi risultati come teorema.

Teorema 9.9. *Sia F completo rispetto a un valore assoluto archimedeo $|\cdot|$ e sia E un'estensione di F di dimensione finita. Allora $|\cdot|$ si estende in uno e un solo modo a un valore assoluto su E, dato dalla (7). Inoltre E è completo rispetto a questo valore assoluto.*

Per il risultato analogo sui valori assoluti non archimedei attenderemo di aver generalizzato questa nozione a quella di valutazione in un gruppo abeliano ordinato. Esamineremo tale generalizzazione nel prossimo paragrafo. Dimostreremo poi un teorema di estensione per le valutazioni e, specializzandolo, otterremo il teorema di estensione per i valori assoluti non archimedei.

9.6 Valutazioni

Un valore assoluto non archimedeo $|\ |$ soddisfa la condizione $|a+b| \leq \max(|a|, |b|)$. L'addizione dei reali non interviene in nessuna delle condizioni che definiscono un tale valore assoluto: entrano in gioco soltanto la moltiplicazione e la relazione d'ordine nell'insieme dei reali non negativi. Questa osservazione porta a generalizzare il concetto di valore assoluto non archimedeo a quello di valutazione a valori in un qualsiasi gruppo ordinato a cui si aggiunge lo zero. Questa generalizzazione ha importanti applicazioni alla geometria algebrica; inoltre è più naturale del concetto originario, perché è proprio questa generalità che occorre per collegare le valutazioni alle proprietà interne del campo. Consideriamo anzitutto il concetto di gruppo abeliano ordinato.

Definizione 9.3. Un *gruppo abeliano ordinato* è una coppia (G, H) costituita da un gruppo abeliano G e da un sottoinsieme H tali che:

1. G è l'unione disgiunta $H \cup \{1\} \cup H^{-1}$, dove $H^{-1} = \{h^{-1} \mid h \in H\}$;
2. H è chiuso rispetto alla moltiplicazione di G.

Quando non vi sarà pericolo di confusione, parleremo del «gruppo abeliano ordinato G» o del gruppo G «ordinato da H». Possiamo usare H per definire una relazione d'ordine sull'insieme G ponendo $g_1 > g_2$ in G se $g_1^{-1} g_2 \in H$. È chiaro che questa relazione è transitiva. Inoltre l'ordine è totale (o lineare), perché per ogni (g_1, g_2), $g_i \in G$, si verifica una e una sola delle possibilità $g_1 > g_2$, $g_1 = g_2$, $g_2 > g_1$ (che scriviamo anche $g_1 < g_2$). L'ordine è inoltre compatibile con la moltiplicazione: $g_1 > g_2$ implica $gg_1 > gg_2$ per ogni g. Viceversa, dato un gruppo abeliano G con una relazione d'ordine totale $>$ compatibile con la moltiplicazione, otteniamo il gruppo ordinato (G, H), dove $H = \{h \mid h < 1\}$. Ciò fornisce una definizione equivalente dei gruppi abeliani ordinati. Osserviamo anche che, se (G, H) è un gruppo abeliano ordinato, lo è pure (G, H^{-1}). Evidentemente, se $g_1 > g_2$ in (G, H), allora $g_1 < g_2$ in (G, H^{-1}). Diciamo che (G, H^{-1}) si ottiene *invertendo l'ordine* in (G, H).

Valgono le consuete proprietà elementari: da $g_1 > g_1'$ e $g_2 > g_2'$ segue $g_1 g_2 > g_1' g_2'$, e da $g_1 > g_2$ segue $g_1^{-1} < g_2^{-1}$. Notiamo anche che non tutti i gruppi abeliani G possono essere ordinati: può accadere che G non contenga alcun sottoinsieme H che soddisfi le condizioni 1 e 2. Ciò accade, per esempio, se G ha torsione non banale. Infatti, se G è ordinato, da $g^n = 1$ in G per $n > 0$ segue $g = 1$.

Se G è ordinato da H e G_1 è un sottogruppo di G, allora G_1 è ordinato da $H_1 = G_1 \cap H$. La relazione d'ordine $>$ in G_1 è la restrizione a G_1 di quella in G. Se (G, H) e (G', H') sono gruppi abeliani ordinati, un *omomorfismo d'ordine* di G in G' è un omomorfismo di G in G' che manda H in H'. Se (G_i, H_i), $1 \leq i \leq n$, sono gruppi abeliani ordinati, $H_1 \times H_2 \times \cdots \times H_n$

non definisce in generale un ordine su $G_1 \times G_2 \times \cdots \times G_n$. Possiamo però ottenere un ordine in $G = G_1 \times G_2 \times \cdots \times G_n$, l'*ordine lessicografico* (corrispondente all'indicizzazione data $i \mapsto G_i$), prendendo come H l'insieme degli elementi della forma

$$(1_1, \ldots, 1_{r-1}, h_r, g_{r+1}, \ldots, g_n),$$

dove $1 \leq r \leq n$, 1_i è l'unità di G_i, $h_r \in H_r$ e i g_i sono arbitrari. È facile verificare che questo definisce un ordine su G. In tale ordine si ha

$$(g_1, g_2, \ldots, g_n) > (g'_1, g'_2, \ldots, g'_n)$$

se e solo se per qualche r, $1 \leq r \leq n$, vale $g_1 = g'_1, \ldots, g_{r-1} = g'_{r-1}$ e $g_r > g'_r$.

Abbiamo i seguenti esempi familiari: (1) $(\mathbb{R}, +, 0)$, il gruppo additivo dei reali con l'ordine consueto; (2) il gruppo moltiplicativo P dei reali positivi, dove il sottoinsieme H che definisce l'ordine è l'insieme dei reali positivi minori di 1 e l'applicazione $x \mapsto e^x$ da $\mathbb{R}$ in P è un isomorfismo d'ordine; (3) $\mathbb{Z}^{(n)}$, il gruppo additivo delle n-uple di interi, ordinato lessicograficamente.

Per definire valutazioni generali dei campi dobbiamo considerare gruppi abeliani ordinati con uno zero aggiunto: $V = G \cup \{0\}$, unione disgiunta, dove poniamo $00 = 0$ e, per ogni $g \in G$, $g > 0$, $0g = 0 = g0$. Possiamo ora dare la seguente definizione.

Definizione 9.4. Se F è un campo e V è un gruppo abeliano ordinato con zero aggiunto, una *V-valutazione* di F è un'applicazione φ di F in V tale che

$$\begin{aligned} &\text{(i)} && \varphi(a) = 0 \iff a = 0, \\ &\text{(ii)} && \varphi(ab) = \varphi(a)\varphi(b), \\ &\text{(iii)} && \varphi(a+b) \leq \max(\varphi(a), \varphi(b)). \end{aligned}$$

Se prendiamo come V l'insieme dei reali non negativi, cioè $V = \{0\} \cup G$ con G l'insieme dei reali positivi, otteniamo i valori assoluti non archimedei definiti in precedenza.

Nelle applicazioni si incontrano generalmente valutazioni in una forma nella quale il gruppo ordinato è scritto additivamente e l'ordine è invertito. Lo zero aggiunto è allora sostituito da un elemento ∞ tale che $\infty + \infty = \infty$ e $\infty > a$, $\infty + a = \infty$ per ogni a. La definizione di valutazione assume allora la forma seguente.

Definizione 9.4′. Se F è un campo e V è un gruppo additivo ordinato con ∞ aggiunto, una *V-valutazione esponenziale* di F è un'applicazione v di F in V tale che

$$\begin{aligned} &\text{(i}') && v(a) = \infty \iff a = 0, \\ &\text{(ii}') && v(ab) = v(a) + v(b), \\ &\text{(iii}') && v(a+b) \geq \min(v(a), v(b)). \end{aligned}$$

È chiaro che questa definizione equivale alla prima.

Se φ è una valutazione di F (nel senso della definizione 9.4) e, come di consueto, F^* denota il gruppo moltiplicativo degli elementi non nulli di F, allora $\varphi(F^*)$ è un sottogruppo del gruppo abeliano ordinato dato G. Lo chiamiamo *gruppo dei valori* di F (rispetto alla φ assegnata). Volendo, possiamo sostituire G con il gruppo dei valori $\varphi(F^*)$ senza alcuna perdita di generalità.

Come nel caso particolare dei valori assoluti non archimedei, si ha $\varphi(1) = 1$ per ogni valutazione φ, poiché $\varphi(1)^2 = \varphi(1^2) = \varphi(1)$. Inoltre $\varphi(-1)^2 = \varphi(1) = 1$ e, poiché G non ha elementi di ordine finito diversi da 1, otteniamo $\varphi(-1) = 1$. Dunque $\varphi(-a) = \varphi(-1)\varphi(a) = \varphi(a)$ e $\varphi(b^{-1}) = \varphi(b)^{-1}$. Inoltre $\varphi(a+b) = \varphi(b)$ se $\varphi(a) < \varphi(b)$.

Daremo ora alcuni esempi di valutazioni che non sono valori assoluti. La costruzione si basa su due lemmi. Dobbiamo anzitutto estendere la definizione 9.4 ai domini. Se D è un dominio e V un gruppo ordinato con zero, definiamo una V-valutazione di D come un'applicazione φ di D in V che soddisfi le condizioni (i)–(iii) della definizione 9.4. Vale allora il

Lemma 1. *Sia D un dominio e sia φ una V-valutazione su D. Allora φ ha un'unica estensione a una V-valutazione sul campo delle frazioni F di D.*

Dimostrazione. Sia $ab^{-1} = cd^{-1}$ per $a, b, c, d \in D$, $bd \neq 0$. Allora $ad = bc$ e $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$. Quindi $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$ e $ab^{-1} \mapsto \varphi(a)\varphi(b)^{-1}$ è un'applicazione ben definita da F in V. Evidentemente essa estende la valutazione φ di D. Indicandola ancora con φ, è chiaro che valgono la (i) e la (ii). Per dimostrare la (iii) basta mostrare che, per $a, b, d \in D$, $d \neq 0$, vale

$$\varphi(ad^{-1} + bd^{-1}) \leq \max(\varphi(ad^{-1}), \varphi(bd^{-1})).$$

Ciò equivale a $\varphi(a + b)\varphi(d)^{-1} \leq \max(\varphi(a)\varphi(d)^{-1}, \varphi(b)\varphi(d)^{-1})$, che si ottiene moltiplicando $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$ per $\varphi(d)^{-1}$. L'unicità dell'estensione è chiara, poiché $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$. □

Consideriamo ora un campo F con una V-valutazione esponenziale v, dove $V = G \cup \{\infty\}$. Formiamo $V' = G' \cup \{\infty\}$, con $G' = \mathbb{Z} \oplus G$ ordinato lessicograficamente: $(m, g) > (m', g')$ se $m > m'$ oppure se $m = m'$ e $g > g'$. Si ha il

Lemma 2. *La V-valutazione esponenziale v si può estendere a una V'-valutazione esponenziale v' di $F(x)$, con x indeterminata.*

Dimostrazione. Per il lemma 1 basta provare l'enunciato sostituendo a $F(x)$ l'anello dei polinomi $F[x]$. Sia $f(x) \neq 0$ in $F[x]$. Allora $f(x) = x^k(a_0 + a_1x + \cdots + a_nx^n)$ con $k \geq 0$, $a_i \in F$, $a_0 \neq 0$. Definiamo $v'(f) = (k, v(a_0)) \in G'$ e $v'(0) = \infty$. Allora v' estende v identificando $g \in G$ con $(0, g)$. Le condizioni (i′) e (ii′) della definizione 9.4′ sono chiare. Per provare la (iii′) basta supporre che f sia come sopra e $g(x) = x^l(b_0 + b_1x + \cdots + b_mx^m)$, con $l \geq 0$, $b_i \in F$, $b_0 \neq 0$. Possiamo anche supporre $v'(f) \geq v'(g)$. Allora o $k > l$, oppure $k = l$ e $v(a_0) \geq v(b_0)$. Nel primo caso $v'(f + g) = (l, v(b_0)) = v'(g) = \min(v'(f), v'(g))$. Nel secondo caso $v'(f + g) > \min(v'(f), v'(g))$ se $a_0 + b_0 = 0$, mentre $v'(f + g) = (k, v(a_0 + b_0)) \geq \min(v'(f), v'(g))$ se $a_0 + b_0 \neq 0$. Quindi la (iii′) vale in entrambi i casi. □

Possiamo ora partire dalla valutazione banale di F e applicare il lemma 2 per ottenere una valutazione esponenziale di $F(x_1)$, con x_1 indeterminata, il cui gruppo dei valori $v(F(x_1)^*)$ è $\mathbb{Z}$. Aggiungendo successivamente altre indeterminate otteniamo una valutazione esponenziale di $F(x_1, \ldots, x_n)$ con gruppo dei valori $\mathbb{Z}^{(n)}$ ordinato lessicograficamente. Osserviamo che $\mathbb{Z}^{(n)}$ per $n > 1$ non soddisfa l'assioma di Archimede, secondo cui, se g_1, g_2 sono elementi di $\mathbb{Z}^{(n)}$ con $g_1 > 0$, esiste un intero k tale che $kg_1 > g_2$. (Si prendano per esempio $g_1 = (0, 1, 0, \ldots)$ e $g_2 = (1, 0, \ldots)$.) Il gruppo additivo dei reali soddisfa invece l'assioma di Archimede. Quindi $\mathbb{Z}^{(n)}$ non è isomorfo, come gruppo ordinato, a un sottogruppo di questo gruppo, e la valutazione che abbiamo costruito non è un valore assoluto se $n > 1$.

Esercizio.

1. Sia (G, H) un gruppo abeliano ordinato, sia F un campo e sia $F[G]$ l'algebra di gruppo di G su F. Mostrare che $F[G]$ è un dominio. Per $f = \sum_i a_i g_i$, con $a_i \neq 0$ in F e $g_i \in G$ distinti, si ponga $\varphi(f) = \min_i g_i$ nell'ordine di G e si definisca $\varphi(0) = 0$. Mostrare che φ è una valutazione. Deducendo dal lemma 1, concludere che per ogni gruppo abeliano ordinato assegnato (G, H) esiste un campo con una valutazione il cui gruppo dei valori è (G, H).

9.7 Anelli di valutazione e posti

Al concetto di valutazione di un campo in un gruppo abeliano ordinato con zero sono equivalenti altri due concetti, quelli di anello di valutazione e di posto. Il primo nasce nel modo seguente. Sia φ una V-valutazione di un campo F e sia

$$R = \{a \in F \mid \varphi(a) \leq 1\}. \tag{10}$$

È un sottoanello di F, poiché per $a, b \in R$ si ha $\varphi(a-b) \leq \max(\varphi(a), \varphi(b))$, sicché $a - b \in R$, e $\varphi(ab) = \varphi(a)\varphi(b) \leq 1$, sicché $ab \in R$. Inoltre $1 \in R$. Supponiamo ora $a \notin R$. Allora $\varphi(a) > 1$ e $\varphi(a^{-1}) = \varphi(a)^{-1} < 1$. Vediamo dunque che R è un anello di valutazione (in F) nel senso della seguente definizione.

Definizione 9.5. Se F è un campo, un *anello di valutazione* in F è un sottoanello R di F tale che ogni elemento di F appartiene a R oppure è l'inverso di un elemento di R.

Se R è il sottoanello di F definito dalla (10), lo si chiama *anello di valutazione della valutazione* φ. Mostreremo ora che si può invertire la costruzione: ogni anello di valutazione R in F dà luogo a una valutazione. Sia U l'insieme delle unità di R, P l'insieme dei non invertibili, F^* il gruppo moltiplicativo degli elementi non nulli di F, $R^* = R \cap F^*$, $P^* = P \cap F^*$. Poiché U è un sottogruppo di F^*, possiamo formare il gruppo quoziente $G' = F^*/U$. Poniamo

$$H' = \{bU \mid b \in P^*\} \subseteq G'. \tag{11}$$

Allora (G', H') è un gruppo abeliano ordinato. Infatti, per $a \in F^*$ si ha $a \in R$ oppure $a^{-1} \in R$. Se sia a sia a^{-1} appartengono a R, allora $a \in U$ e $aU = U = 1$ in G'. Se $a \in R$ e $a^{-1} \notin R$, allora $a \in P^*$ e $aU \in H'$. Se $a \notin R$, allora $a^{-1} \in P^*$ e $aU \in (H')^{-1}$. È ora chiaro che vale la condizione 1 della definizione di gruppo abeliano ordinato. Siano poi $b_1, b_2 \in P^*$, cosicché i b_i sono elementi non nulli e non invertibili di R. Allora $b_1 b_2 \in P^*$ e quindi H' è chiuso rispetto alla moltiplicazione, e (G', H') è un gruppo abeliano ordinato. Aggiungiamo ora un elemento 0 a G' per ottenere $V' = G' \cup \{0\}$. Definiamo un'applicazione φ' di F in V' ponendo

$$\varphi'(0) = 0, \qquad \varphi'(a) = aU \in G' \quad \text{se } a \neq 0. \tag{12}$$

Mostriamo che si tratta di una V'-valutazione di F. Le condizioni (i) e (ii) della definizione 9.4 sono chiaramente soddisfatte. Anche la (iii) è chiara se $a = 0$ o $b = 0$. Se $a \neq 0$ e $b \neq 0$, allora $ab^{-1} \in R^*$ oppure $ba^{-1} \in R^*$. Possiamo supporre che valga la prima alternativa. Allora $\varphi'(ab^{-1}) \leq 1$ poiché $R^* = U \cup P^*$. Quindi $\varphi'(a) \leq \varphi'(b)$. Inoltre $ab^{-1} + 1 \in R$, perciò $\varphi'(ab^{-1} + 1) \leq 1$. Si ha allora

$$\varphi'(a+b) = \varphi'(b)\varphi'(ab^{-1} + 1) \leq \varphi'(b) = \max(\varphi'(a), \varphi'(b)).$$

Dunque φ' è una valutazione. Inoltre, poiché $\varphi'(a) \leq 1$ se e solo se $a \in R$, l'anello di valutazione associato a φ' è proprio l'anello R assegnato. Chiameremo φ' la *valutazione canonica* dell'anello di valutazione R.

Consideriamo ancora una qualsiasi valutazione φ di F in $V = G \cup \{0\}$, dove (G, H) è un gruppo abeliano ordinato. Sia R il corrispondente anello di valutazione e φ' la valutazione canonica di F determinata da R. Si ha $\varphi'(a) = aU$ per $a \neq 0$, con U come sopra. D'altra parte abbiamo l'omomorfismo $a \mapsto \varphi(a)$ da F^* in G, il cui nucleo è U. Otteniamo dunque un monomorfismo $\varphi'(a) \mapsto \varphi(a)$ da G' in G, che è un isomorfismo di G' sul gruppo dei valori di φ. Se $bU \in H'$, allora $b \in P^*$ e quindi $\varphi(b) < 1$. Ne segue che $\varphi'(a) \mapsto \varphi(a)$ conserva l'ordine. Vediamo ora che la valutazione data φ si può fattorizzare come $\eta\varphi'$, dove φ' è la valutazione canonica determinata da R e η è un isomorfismo d'ordine di G' sul gruppo dei valori di φ.

Diremo che due valutazioni φ_1, φ_2 sono *equivalenti* se esiste un isomorfismo d'ordine η del gruppo dei valori di φ_1 sul gruppo dei valori di φ_2 tale che $\varphi_2 = \eta\varphi_1$. È chiaro che ciò implica che φ_1 e φ_2 hanno lo stesso anello di valutazione. Inoltre abbiamo mostrato che ogni valutazione φ è equivalente alla valutazione canonica φ' determinata dal suo anello di valutazione R. Pertanto due valutazioni φ_1, φ_2 sono equivalenti se e solo se hanno lo stesso anello di valutazione.

Sia R un anello di valutazione in F. Possiamo dunque supporre che R sia il sottoinsieme di F degli elementi che soddisfano $\varphi(a) \leq 1$ per una valutazione φ di F. Sia P il sottoinsieme di R degli elementi b tali che $\varphi(b) < 1$. È chiaro allora che P è l'insieme dei non invertibili di R. Ora P è un ideale di R, poiché per $b_1, b_2 \in P$ si ha $\varphi(b_1 + b_2) \leq \max(\varphi(b_1), \varphi(b_2)) < 1$ e, per $a \in R$, $\varphi(b_1 a) = \varphi(b_1)\varphi(a) < 1$. Quindi R è un anello locale, P ne è l'ideale massimale e $\bar{R} = R/P$ è un campo. Questo campo si chiama il *campo residuo* di R o della valutazione φ. Abbiamo l'omomorfismo canonico $a \mapsto a + P$ di R sul campo $\bar{R}$. Ciò ci porta a introdurre un altro concetto equivalente alla valutazione in un gruppo ordinato e all'anello di valutazione.

Definizione 9.6. Se F e Δ sono campi, un *posto di F a valori in Δ* è un omomorfismo $\mathcal{P}$ di un sottoanello R di F in Δ tale che, se $a \notin R$, allora $a^{-1} \in R$ e $\mathcal{P}(a^{-1}) = 0$.

Evidentemente il sottoanello R che interviene nella definizione è un anello di valutazione. D'altra parte, se R è un qualsiasi anello di valutazione in F, abbiamo l'omomorfismo canonico di R sul campo residuo. Inoltre, se $a \notin R$, allora $\varphi(a) > 1$ e $\varphi(a^{-1}) < 1$, sicché a^{-1} è un elemento non invertibile di R. Allora $a^{-1} \in P$ e $a^{-1} + P = 0$. Dunque $a \mapsto a + P$ è un posto di F. Lo chiameremo *posto canonico* dell'anello di valutazione R. Come per le valutazioni, se $\mathcal{P}$ è un posto a valori in Δ, R l'anello di valutazione associato e $\mathcal{P}'$ il posto canonico di R, esiste un monomorfismo λ del campo residuo di R nel campo Δ per il quale vale la fattorizzazione $\mathcal{P} = \lambda\mathcal{P}'$. L'introduzione del concetto di posto permette di trasformare il problema dell'estensione di una valutazione di un campo F a un'estensione di F in un problema di estensione di omomorfismi. Tratteremo queste questioni nel prossimo paragrafo.

Osserviamo che tutto ciò che abbiamo fatto si può formulare anche in termini di V-valutazioni esponenziali. Se v è una tale valutazione, l'anello di valutazione corrispondente è

$$R = \{a \in F \mid v(a) \geq 0\}$$

e l'ideale massimale è

$$P = \{b \in F \mid v(b) > 0\}.$$

Per i nostri scopi sarà più comodo lavorare con le valutazioni φ. Tuttavia, come si è accennato, nelle applicazioni, specialmente alla teoria dei numeri, il lettore incontrerà di solito le valutazioni esponenziali.

Esercizi.

1. Sia $|\ |_p$ il valore assoluto p-adico di $\mathbb{Q}$ determinato da γ, $0 < \gamma < 1$, come nel ğ 9.1. Determinare il gruppo dei valori, l'anello di valutazione e l'ideale dei non invertibili per $\mathbb{Q}$ e per il suo completamento $\mathbb{Q}_p$. Mostrare che il campo residuo è isomorfo a $\mathbb{Z}/(p)$.

2. Sia $\mathcal{P}$ un posto su F a valori in Δ, con anello di valutazione R, e $\mathcal{P}'$ un posto su Δ a valori in Δ', con anello di valutazione R'. Mostrare che il composto $\mathcal{P}'\mathcal{P}$ è un posto a valori in Δ' con anello di valutazione $S = \{a \in R \mid \mathcal{P}(a) \in R'\}$.

3. Sia D un dominio fattoriale, F il suo campo delle frazioni e p un primo di D. Mostrare che la localizzazione $D_{(p)}$ è un anello di valutazione in F.

4. Sia $E = F(\xi_1, \ldots, \xi_m)$ il campo delle espressioni razionali in m indeterminate ξ_i. Mostrare che, per elementi assegnati $a_i \in F$, esiste un posto $\mathcal{P}$ su E a valori in F il cui anello di valutazione contiene F e per cui $\mathcal{P}(\xi_i) = a_i$.

9.8 Estensione degli omomorfismi e delle valutazioni

In questo paragrafo dimostreremo un teorema fondamentale sull'estensione di un omomorfismo di un sottoanello di un campo. Esso ci permetterà di dimostrare un teorema generale sull'estensione di una valutazione di un campo a una sua estensione qualsiasi. Alla base di tutto sta il seguente semplice risultato.

Lemma. *Siano R un sottoanello di un campo F, M un ideale proprio di R, a un elemento non nullo di F, e siano $R[a]$, $R[a^{-1}]$ i sottoanelli generati da R e rispettivamente da a e da a^{-1}. Allora l'ideale $MR[a]$ è proprio in $R[a]$ oppure $MR[a^{-1}]$ è proprio in $R[a^{-1}]$.*

Dimostrazione. In caso contrario esistono $m_i, n_j \in M$ tali che

$$1 = m_0 + m_1 a + \cdots + m_k a^k \tag{13}$$

e

$$1 = n_0 + n_1 a^{-1} + \cdots + n_l a^{-l}. \tag{14}$$

Poiché M è proprio in R, $k + l \geq 2$ e possiamo supporre $k + l$ minimo. Per simmetria possiamo anche supporre $k \geq l$. Allora $a^l(1 - n_0) = n_1 a^{l-1} + \cdots + n_l$ e $(1 - n_0) = (1 - n_0)m_0 + \cdots + (1 - n_0)m_k a^k$. Se nell'ultimo termine della seconda relazione sostituiamo ad $a^l(1 - n_0)$ l'espressione data dalla prima, otteniamo una relazione (13) con k minore. Ciò contraddice la minimalità di $k + l$ e dimostra il lemma. □

Il risultato principale sull'estensione di omomorfismi a posti è il seguente.

Teorema 9.10. *Sia R_0 un sottoanello di un campo F e sia $\mathcal{P}_0$ un omomorfismo di R_0 in un campo algebricamente chiuso Δ. Allora $\mathcal{P}_0$ si può estendere a un posto su F a valori in Δ.*

Dimostrazione. Consideriamo la famiglia degli omomorfismi in Δ di sottoanelli di F che estendono l'omomorfismo dato $\mathcal{P}_0$. Per il lemma di Zorn ne esiste uno massimale $\mathcal{P}$, definito su un sottoanello $R \supseteq R_0$. Mostreremo che R è un anello di valutazione, il che proverà il teorema. Sia M il nucleo di $\mathcal{P}$. Poiché $\mathcal{P}$ ha valori in un campo, R/M è un dominio e M è un ideale primo di R. Affermiamo che R è un anello locale con ideale massimale M. In caso contrario esiste $b \in R$, $b \notin M$, che non è un'unità. Allora $\mathcal{P}(b) \neq 0$ e il sottoinsieme degli elementi di F della forma ab^{-k}, $a \in R$, $k \geq 1$, è un sottoanello R' di F che contiene propriamente R. Esso si identifica con la localizzazione $R_{\langle b \rangle}$ (si veda p. 395). Ne segue che $\mathcal{P}$ si può estendere a un omomorfismo $\mathcal{P}'$ di R' in Δ. Ciò contraddice la massimalità di $\mathcal{P}$ e prova che R è locale con ideale massimale M. Allora R/M è un campo e quindi $\Gamma = \mathcal{P}(R)$ è un sottocampo di Δ.

Se R non è un anello di valutazione, esiste $a \in F$ tale che $a \notin R$ e $a^{-1} \notin R$. Per il lemma, $MR[a] \neq R[a]$ oppure $MR[a^{-1}] \neq R[a^{-1}]$. Possiamo supporre che valga la prima alternativa. Consideriamo gli anelli dei polinomi $R[x]$ e $\Gamma[x]$, con x indeterminata. L'omomorfismo $\mathcal{P}$ di R si può considerare come un epimorfismo di R su Γ. Esso si estende a un epimorfismo di $R[x]$ su $\Gamma[x]$ che manda x in x. Sia Z l'ideale di $R[x]$ dei polinomi $f(x)$ tali che $f(a) = 0$ e sia Z' la sua immagine in $\Gamma[x]$. Allora Z' è un ideale di $\Gamma[x]$ e, se $Z' = \Gamma[x]$, esiste $f(x) = \sum_{i=0}^{l} c_i x^i$, $c_i \in R$, tale che $\sum_i c_i a^i = 0$ e $\sum_i \mathcal{P}(c_i) x^i = 1$. Allora $\mathcal{P}(c_0) = 1$ e $\mathcal{P}(c_j) = 0$ per $j > 0$. Quindi $c_0 = 1 - m_0$ e $c_j = m_j$ con $m_0, m_j \in M$. La relazione $\sum_i c_i a^i = 0$ implica allora $1 \in MR[a]$, contro l'ipotesi. Dunque $Z' \neq \Gamma[x]$ e $Z' = (g(x))$, dove $g(x) = 0$ oppure $g(x)$ è un

polinomio monico di grado positivo. Nel primo caso scegliamo un $r \in \Delta$ qualunque, nel secondo un $r \in \Delta$ tale che $g(r) = 0$. Questo è possibile perché Δ è algebricamente chiuso. Abbiamo ora l'omomorfismo di $R[x]$ in Δ composto dell'omomorfismo di $R[x]$ in $\Gamma[x]$ con l'omomorfismo di $\Gamma[x]$ in Δ che è l'identità su Γ e manda x in r. L'omomorfismo di $R[x]$ in Δ ha la forma $h(x) = c_0 + c_1 x + \cdots \mapsto \mathcal{P}(c_0) + \mathcal{P}(c_1) r + \cdots$ e manda in 0 ogni $f(x) \in Z$. Abbiamo quindi l'omomorfismo di $R[x]/Z$ in Δ per cui $h(x) + Z \mapsto \mathcal{P}(c_0) + \mathcal{P}(c_1) r + \cdots$. Poiché Z è l'insieme dei polinomi tali che $f(a) = 0$, abbiamo l'omomorfismo $\mathcal{P}'$ di $R[a]$ in Δ tale che $h(a) \mapsto \mathcal{P}(c_0) + \mathcal{P}(c_1) r + \cdots$. Si tratta di un'estensione propria di $\mathcal{P}$, contro la sua massimalità. Dunque R è un anello di valutazione e la dimostrazione è completa. □

Applichiamo ora questo risultato alle valutazioni. Lavoriamo dapprima con gli oggetti canonici, definiti intrinsecamente. Supponiamo dunque di avere un campo F_0 e un anello di valutazione R_0 in F_0. Abbiamo la valutazione canonica φ_0' e il posto canonico $\mathcal{P}_0'$ associati a R_0. Se P_0 è il nucleo di $\mathcal{P}_0'$, allora P_0 è l'ideale dei non invertibili dell'anello locale R_0 e il campo residuo R_0/P_0 si può immergere in un campo algebricamente chiuso Δ. Possiamo allora considerare $\mathcal{P}_0'$ come un posto di F_0 a valori in Δ. Sia F un'estensione di F_0. Allora R_0 è un sottoanello di F, sicché per il teorema di estensione appena dimostrato $\mathcal{P}_0'$ si può estendere a un posto $\mathcal{P}$ su F a valori in Δ. Sia R l'anello di valutazione in F su cui $\mathcal{P}$ è definito, P l'ideale dei non invertibili di R. Sia U_0 l'insieme delle unità di R_0 e U quello delle unità di R. Si vede facilmente che $R_0 = R \cap F_0$, $P_0 = P \cap F_0$, $U_0 = U \cap F_0$. Ne segue che abbiamo un monomorfismo d'ordine s del gruppo ordinato $G_0' = F_0^*/U_0$ (ordinato dal sottoinsieme degli elementi bU_0, $b \in P_0^*$) nel gruppo ordinato $G' = F^*/U$, dato da

$$a_0 U_0 \longmapsto a_0 U, \qquad a_0 \in F_0^*. \tag{15}$$

Inoltre le definizioni mostrano che, se φ' è la valutazione canonica determinata da R, si ha

$$\varphi'(a_0) = s\varphi_0'(a_0), \qquad a_0 \in F_0. \tag{16}$$

In questo senso abbiamo esteso la valutazione canonica di F_0 alla valutazione canonica su F.

Una conseguenza immediata di questo risultato e della relazione fra valutazioni canoniche e arbitrarie è il seguente teorema di estensione per le valutazioni.

Teorema 9.11. *Sia φ_0 una valutazione su F_0 e sia F un'estensione di F_0. Allora esistono un gruppo ordinato G che estende il gruppo dei valori di F_0 e, ponendo $V = \{0\} \cup G$, una V-valutazione φ di F che estende φ_0.*

Dimostrazione. Siano R_0 l'anello di valutazione di φ_0 e φ_0' la valutazione canonica associata a R_0. Se applichiamo il risultato appena dimostrato e la relazione fra φ_0 e φ_0', vediamo che abbiamo una valutazione φ su F a valori in $V = \{0\} \cup G$ e un monomorfismo d'ordine t del gruppo dei valori di φ_0 in G tali che $\varphi(a_0) = t\varphi_0(a_0)$ per ogni $a_0 \in F_0$. Possiamo allora identificare il gruppo dei valori di F_0 con la sua immagine in G mediante t, e otteniamo il risultato enunciato. □

Nel caso delle estensioni di grado finito vale il seguente risultato.

Lemma. *Siano φ una valutazione di un campo F e F_0 un sottocampo tale che $[F : F_0] = n < \infty$. Allora il gruppo dei valori di F è isomorfo, come gruppo ordinato, a un sottogruppo del gruppo dei valori di F_0.*

Dimostrazione. Per ogni $a \neq 0$ in F si ha una relazione della forma $\alpha_1 a^{n_1} + \alpha_2 a^{n_2} + \cdots + \alpha_k a^{n_k} = 0$, con α_i elementi non nulli di F_0 e n_i interi tali che $[F : F_0] = n \geq n_1 > n_2 > \cdots > n_k \geq 0$. Se $\varphi(\alpha_i a^{n_i}) > \varphi(\alpha_j a^{n_j})$ per ogni $j \neq i$, allora $\varphi(\sum_j \alpha_j a^{n_j}) = \varphi(\alpha_i a^{n_i})$, contro l'uguaglianza $\sum_j \alpha_j a^{n_j} = 0$. Abbiamo quindi $\varphi(\alpha_i a^{n_i}) = \varphi(\alpha_j a^{n_j})$ per qualche coppia (i, j) con $i > j$. Allora $\varphi(a)^{n_i - n_j} = \varphi(\alpha_j \alpha_i^{-1})$ appartiene al gruppo dei valori G_0 di F_0. Ne segue che per ogni $a \neq 0$ si

ha $\varphi(a)^{n!} \in G_0$. Poiché il gruppo dei valori G di F non ha torsione, l'applicazione $g \mapsto g^{n!}$ è un monomorfismo d'ordine di G. Dunque G è isomorfo, come gruppo ordinato, a un sottogruppo di G_0. □

Possiamo servirci della dimostrazione di questo risultato e del teorema 9.11 per provare l'esistenza di estensioni dei valori assoluti non archimedei a estensioni di grado finito. Abbiamo il

Teorema 9.12. *Sia F_0 un campo con un valore assoluto non archimedeo $|\ |$ e sia F un'estensione di grado finito di F_0. Allora $|\ |$ si può estendere a un valore assoluto $|\ |$ di F, necessariamente non archimedeo.*

Dimostrazione. Il gruppo dei valori G_0 di F_0 è un sottogruppo del gruppo moltiplicativo dei reali positivi. Per il teorema 9.11 abbiamo un'estensione di $\varphi_0 = |\ |$ a una valutazione φ' di F il cui gruppo dei valori G estende G_0. La dimostrazione del lemma mostra che, se $n = [F : F_0]$, l'applicazione $g \mapsto g^{n!}$ è un monomorfismo d'ordine da G in G_0. Allora $g \mapsto (g^{n!})^{1/n!}$ è un monomorfismo d'ordine da G nei reali positivi che coincide con l'identità su G_0. Applicandolo a φ' otteniamo l'estensione $|\ |$ richiesta. □

Da questo risultato, dal teorema 9.8 e dal risultato precedente sui valori assoluti archimedei (teorema 9.9) discende immediatamente il

Corollario. *Sia F completo rispetto a un valore assoluto non banale $|\ |$ e sia E un'estensione di grado finito di F. Allora l'applicazione $a \mapsto |N_{E/F}(a)|^{1/[E:F]}$ è un valore assoluto su E che estende $|\ |$ su F. Inoltre questa è l'unica estensione di $|\ |$ da F a un valore assoluto su E, ed E è completo rispetto a essa.*

Esercizi.

1. Sia G un gruppo abeliano ordinato scritto additivamente. Per $a \in G$, si definisca $|a| = a$ se $a \geq 0$ e $|a| = -a$ se $a < 0$. Si dica *isolato* (o *convesso*) un sottogruppo K di G se, dato $a \in K$, K contiene ogni b tale che $|b| \leq a$. Mostrare che l'insieme dei sottogruppi isolati è totalmente ordinato per inclusione. Il tipo d'ordine di questo insieme si chiama il *rango* di G (si veda Hausdorff, *Mengenlehre*, 3ł ed., capitolo 3).

2. Mostrare che un gruppo ordinato G (scritto additivamente) ha rango uno se e solo se soddisfa il postulato di Archimede: se $a, b \in G$ e $a > 0$, esiste un intero positivo n tale che $na > b$.

3. Dimostrare che un gruppo ordinato ha rango uno se e solo se è isomorfo, come gruppo ordinato, a un sottogruppo del gruppo additivo ordinato dei reali. (Questo risultato mostra che le valutazioni a valori reali sono le valutazioni di rango uno, ossia le V-valutazioni per cui $V = \{0\} \cup G$ con G di rango uno.)

I due esercizi seguenti delineano una dimostrazione del Nullstellensatz di Hilbert basata sul teorema di estensione degli omomorfismi. In questi esercizi supponiamo F algebricamente chiuso.

4. Sia I un ideale primo di $F[x_1, \ldots, x_n]$. Sia E il campo delle frazioni del dominio $F[x_1, \ldots, x_n]/I$ e poniamo $\xi_i = x_i + I$, $1 \leq i \leq n$, in E. Allora $E = F(\xi_1, \ldots, \xi_n)$ e possiamo supporre che $\{\xi_1, \ldots, \xi_r\}$, $r \geq 0$, sia una base di trascendenza di E/F. Per ogni $i > r$ si scelga un polinomio

$$a_{i0}(x_1, \ldots, x_r)x^{m_i} + a_{i1}(x_1, \ldots, x_r)x^{m_i - 1} + \cdots + a_{im_i}(x_1, \ldots, x_r)$$

in $F[x_1, \ldots, x_r, x]$ tale che $a_{i0}(x_1, \ldots, x_r) \neq 0$ e

$$a_{i0}(\xi_1, \ldots, \xi_r)\xi_i^{m_i} + \cdots + a_{im_i}(\xi_1, \ldots, \xi_r) = 0.$$

Sia $g = g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$, $g \notin I$. Allora $g(\xi_1, \ldots, \xi_n) \neq 0$ ed esiste un polinomio

$$b_0(x_1, \ldots, x_r)x^m + \cdots + b_m(x_1, \ldots, x_r) \in F[x_1, \ldots, x_r, x]$$

tale che $g(\xi_1, \ldots, \xi_n)^{-1}$ sia uno zero di $b_0(\xi_1, \ldots, \xi_r)x^m + \cdots + b_m(\xi_1, \ldots, \xi_r)$. Mostrare che esiste un omomorfismo di F-algebre η di $F[\xi_1, \ldots, \xi_r]$ in F tale che

$$\eta\left(b_0(\xi_1, \ldots, \xi_r)\prod_{i>r} a_{i0}(\xi_1, \ldots, \xi_r)\right) \neq 0.$$

Servirsi del fatto che η si può estendere a un posto su E a valori in F per mostrare che esistono elementi $c_i \in F$, $1 \leq i \leq n$, tali che

$$f(c_1, \ldots, c_n) = 0 \quad \text{per ogni } f \in I, \qquad g(c_1, \ldots, c_n) \neq 0.$$

5. Usare il risultato dell'esercizio 4 e il teorema secondo cui il nilradicale di un ideale è l'intersezione degli ideali primi che lo contengono per dimostrare il Nullstellensatz di Hilbert.

I due esercizi seguenti intendono mostrare che, se $f(x)$ e $g(x)$ sono due polinomi monici irriducibili separabili a coefficienti in un campo completo non archimedeo F, e $f(x)$ e $g(x)$ sono sufficientemente vicini in un senso che preciseremo, allora i campi $F[x]/(f(x))$ e $F[x]/(g(x))$ sono isomorfi. Sia $\bar{F}$ la chiusura algebrica di F. Si osservi che, poiché ogni sottoinsieme finito di $\bar{F}$ è contenuto in un sottocampo di grado finito di $\bar{F}/F$, il valore assoluto $|\ |$ di F ha un'unica estensione a un valore assoluto su $\bar{F}$.

6. Sia $f(x) \in F[x]$ monico, irriducibile e separabile, $f(x) = \prod_{i=1}^n (x - \alpha_i)$ in $\bar{F}[x]$. Si ponga $\delta = \min_{i \neq j} |\alpha_i - \alpha_j|$. Mostrare che, se $\beta \in \bar{F}$ e $|\beta - \alpha_1| < \delta$, allora $F(\alpha_1) \subseteq F(\beta)$.

   Traccia. Si consideri $F(\alpha_1, \beta)/F(\beta)$. Sia $\varphi(x)$ il polinomio minimo di α_1 su $F(\beta)$. Possiamo supporre che $\varphi(x) = \prod_{i=1}^m (x - \alpha_i)$, $m \leq n$. Poiché $\bar{F}$ è la chiusura algebrica di $F(\beta)$, per ogni j, $1 \leq j \leq m$, esiste un automorfismo σ di $\bar{F}/F(\beta)$ tale che $\sigma\alpha_1 = \alpha_j$. Per l'unicità dell'estensione di $|\ |$ da F a $\bar{F}$, $|\sigma\gamma| = |\gamma|$ per ogni $\gamma \in \bar{F}$. Quindi $|\beta - \alpha_j| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1| < \delta$. Se $m > 1$, possiamo scegliere $j > 1$ e ottenere $|\alpha_j - \alpha_1| \geq \delta$, sicché $|\alpha_j - \alpha_1| > |\beta - \alpha_j| = |\beta - \alpha_1|$. Poiché $\beta - \alpha_j = (\beta - \alpha_1) + (\alpha_1 - \alpha_j)$, ciò contraddice l'esercizio 2 di p. 562. Dunque $m = 1$, $F(\alpha_1, \beta) = F(\beta)$ e $F(\alpha_1) \subseteq F(\beta)$.

7. (Lemma di Krasner.) Siano $F, \bar{F}, f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ come nell'esercizio 6. Sia $g(x) = x^n + b_1x^{n-1} + \cdots + b_n \in F[x]$. Mostrare che esiste $\varepsilon > 0$ tale che, se $|a_i - b_i| < \varepsilon$, $1 \leq i \leq n$, allora $F[x]/(f(x)) \simeq F[x]/(g(x))$. Quindi anche $g(x)$ è irriducibile e separabile.

   Traccia. Siano $M = \max(1, |a_i|)$, $\delta = \min_{i \neq j} |\alpha_i - \alpha_j|$, dove gli α_i sono gli zeri di $f(x)$ in $\bar{F}$. Sia $\varepsilon = \min(1, \delta^n/(M+1)^n)$. Supponiamo che i b_i soddisfino $|a_i - b_i| < \varepsilon$ e sia β uno zero di $g(x)$. Allora $|b_i| \leq |a_i| + 1 \leq M + 1$, sicché, per l'esercizio 3 di p. 562, $|\beta| \leq M + 1$ e

$$\prod_{i=1}^n |\beta - \alpha_i| = |f(\beta)| = |f(\beta) - g(\beta)| = \left|\sum_i (a_i - b_i)\beta^{n-i}\right| < \varepsilon(M+1)^n.$$

   Quindi per qualche i, diciamo $i = 1$, si ha $|\beta - \alpha_1| < \varepsilon^{1/n}(M+1) \leq \delta$. Per l'esercizio 6 si ha allora $F(\alpha_1) \subseteq F(\beta)$. Poiché $[F(\alpha_1) : F] = n$ e $[F(\beta) : F] \leq n$, si ha $F(\alpha_1) = F(\beta)$ e $F[x]/(f(x)) \simeq F[x]/(g(x))$.

8. (Kürschák.) Dimostrare che, se F è algebricamente chiuso e munito di un valore assoluto $|\ |$, il suo completamento $\widehat{F}$ è algebricamente chiuso.

   Traccia. Il caso in cui $|\ |$ è archimedeo segue facilmente dal teorema di Ostrowski. Supponiamo ora $|\ |$ non archimedeo. Mostriamo anzitutto che $\widehat{F}$ è perfetto. Ciò è chiaro se $\operatorname{char} F = 0$. Se $\operatorname{char} F = p$ e $a \in \widehat{F}$, sia $\{a_n\}$ una successione di elementi di F tale che $a_n \to a$. Allora $\{a_n^{1/p}\}$ è una successione di Cauchy, sicché $b = \lim a_n^{1/p}$ esiste in $\widehat{F}$ e $b^p = a$. Quindi $a^{1/p}$ esiste per ogni $a \in \widehat{F}$ e $\widehat{F}$ è perfetto.

   Supponiamo che $\widehat{F}$ non sia algebricamente chiuso. Allora esiste un polinomio $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \widehat{F}[x]$ irriducibile di grado $n > 1$. Questo è anche separabile. Poiché F è denso in $\widehat{F}$, il lemma di Krasner implica l'esistenza di un polinomio monico $g(x) \in F[x]$ irriducibile di grado n in $\widehat{F}[x]$, e quindi anche in $F[x]$. Ciò è impossibile, essendo F algebricamente chiuso.

9.9 Determinazione dei valori assoluti di un'estensione di dimensione finita

Torniamo al problema dell'estensione dei valori assoluti posto nel ğ 9.5. Dati un valore assoluto $|\cdot|$ su un campo F e un'estensione E/F di dimensione finita, determinare tutte le estensioni di $|\cdot|$ a valori assoluti su E. Il corollario del teorema 9.12 dà la risposta per F completo. Esiste una e una sola estensione del valore assoluto dato, ed è $|a| = |N_{E/F}(a)|^{1/n}$, con $n = [E : F]$. Inoltre E è completo.

Supponiamo ora F arbitrario. Sia $\widehat{F}$ il completamento di F rispetto a $|\cdot|$ e indichiamo con $|\cdot|$ il valore assoluto di $\widehat{F}$ che estende quello dato su F. Sia (Γ, s, t) un composto di $\widehat{F}/F$ ed E/F. Poiché $[E : F] = n < \infty$ e $\Gamma = s(\widehat{F})t(E)$, si ha $[\Gamma : s(\widehat{F})] \leq n < \infty$. Il valore assoluto $|\cdot|$ su $\widehat{F}$ si trasporta in un valore assoluto $|\cdot|_s$ su $s(\widehat{F})$ ponendo $|s(a)|_s = |a|$ per $a \in \widehat{F}$. Esso coincide con $|\cdot|$ su F, e $s(\widehat{F})$ è completo rispetto a $|\cdot|_s$. Poiché Γ ha dimensione finita su $s(\widehat{F})$, $|\cdot|_s$ ha un'unica estensione a un valore assoluto $|\cdot|_\Gamma$ su Γ. Restringendo questo a $t(E)$ e ponendo $|b|_\Gamma = |t(b)|_\Gamma$ per $b \in E$, otteniamo su E un valore assoluto che estende $|\cdot|$.

Abbiamo così un procedimento per associare a ogni composto (Γ, s, t) di $\widehat{F}/F$ ed E/F un valore assoluto su E che estende $|\cdot|$. Mostreremo che la corrispondenza è biunivoca se identifichiamo i composti equivalenti. Supponiamo dapprima che i composti (Γ_1, s_1, t_1) e (Γ_2, s_2, t_2) siano equivalenti. Abbiamo allora un isomorfismo u di Γ_1 su Γ_2 tale che $us_1 = s_2$, $ut_1 = t_2$. Per $c \in \Gamma_1$, $|u(c)|_{\Gamma_2}$ definisce un valore assoluto su Γ_1. Se $a \in \widehat{F}$, allora

$$|u(s_1(a))|_{\Gamma_2} = |s_2(a)|_{\Gamma_2} = |s_2(a)|_{s_2} = |a| = |s_1(a)|_{s_1}.$$

Dunque $|u(\cdot)|_{\Gamma_2}$ è un'estensione di $|\cdot|_{s_1}$. Lo stesso vale per $|\cdot|_{\Gamma_1}$ e, poiché l'estensione di $|\cdot|_{s_1}$ a Γ_1 è unica, $|u(\cdot)|_{\Gamma_2} = |\cdot|_{\Gamma_1}$. Ciò implica che (Γ_1, s_1, t_1) e (Γ_2, s_2, t_2) danno lo stesso valore assoluto su E che estende $|\cdot|$ su F.

Viceversa, supponiamo identici i valori assoluti su E definiti dai due composti. Allora per ogni $b \in E$, $|t_1(b)|_{\Gamma_1} = |t_2(b)|_{\Gamma_2}$. Osserviamo che la chiusura di $E_i = t_i(E)$, per $i = 1, 2$, nella topologia definita da $|\cdot|_{\Gamma_i}$, contiene $s_i(\widehat{F})$ e $t_i(E)$. Poiché è una sottoalgebra, contiene $\Gamma_i = s_i(\widehat{F})t_i(E)$. Dunque E_i è denso in Γ_i. L'applicazione $t_1(b) \mapsto t_2(b)$, $b \in E$, è un isomorfismo isometrico di $t_1(E)$ su $t_2(E)$. Per il teorema 9.2(2) essa si estende in modo unico a un isomorfismo isometrico u di Γ_1 su Γ_2. Evidentemente $ut_1 = t_2$. Inoltre, poiché u è l'identità su F e $s_i(\widehat{F})$ è il completamento di F rispetto a $|\cdot|_{s_i}$, la restrizione di u a $s_1(\widehat{F})$ è un isomorfismo isometrico di $s_1(\widehat{F})$ su $s_2(\widehat{F})$. Anche l'applicazione $s_1(a) \mapsto s_2(a)$ è un isomorfismo isometrico fra gli stessi campi ed è l'identità su F. Essa coincide perciò con la restrizione di u a $s_1(\widehat{F})$. Quindi $us_1(a) = s_2(a)$ per $a \in \widehat{F}$, e u è un'equivalenza di (Γ_1, s_1, t_1) con (Γ_2, s_2, t_2).

Resta da mostrare che ogni estensione di $|\cdot|$ a un valore assoluto su E si ottiene nel modo indicato da un composto. Sia $|\cdot|'$ un valore assoluto su E che estende $|\cdot|$ e sia E' il completamento di E rispetto a $|\cdot|'$. Come al solito indichiamo ancora con $|\cdot|'$ il valore assoluto su E' che estende $|\cdot|'$ su E. Il campo E' contiene $\widehat{F}$ ed E, quindi contiene $\widehat{F}E$, che è un dominio di dimensione finita su $\widehat{F}$. Dunque $\widehat{F}E$ è un campo di dimensione finita su $\widehat{F}$. Ne segue che $\widehat{F}E$ è completo rispetto a $|\cdot|'$. Quindi $E' = \widehat{F}E$ e si ha il composto (E', s, t), dove s, t sono le inclusioni di $\widehat{F}, E$. La data estensione $|\cdot|'$ si ottiene restringendo $|\cdot|'$ definito su E'.

Possiamo ora applicare la determinazione dei composti di due campi data nel ğ 8.19. I composti di $\widehat{F}$ ed E si ottengono prendendo $\Gamma_M = (\widehat{F} \otimes_F E)/M$, dove M è un ideale massimale di $\widehat{F} \otimes_F E$, e ponendo $s\colon a \mapsto a \otimes 1 + M,\ a \in \widehat{F}$, $t\colon b \mapsto 1 \otimes b + M,\ b \in E$. Ogni composto di $\widehat{F}/F$ ed E/F è equivalente a uno di questi, e i composti ottenuti da ideali massimali distinti sono inequivalenti. Per ottenere la corrispondente estensione di $|\cdot|$ a E poniamo $|a \otimes 1 + M|_s = |a|$, $a \in \widehat{F}$. Questo valore assoluto ha un'unica estensione $|\cdot|_{\Gamma_M}$ a Γ_M. Allora $|b|_M = |(1 \otimes b) + M|_{\Gamma_M}$, $b \in E$, definisce l'estensione a E di $|\cdot|$ su F.

Riassumiamo i risultati nel teorema seguente.

Teorema 9.13. *Sia F un campo munito di un valore assoluto $|\cdot|$, E un'estensione di dimensione finita di F e $\widehat{F}$ il completamento di F. Esiste una biiezione fra l'insieme degli ideali massimali M di $\widehat{F} \otimes_F E$ $(= E_{\widehat{F}})$ e l'insieme dei valori assoluti su E che estendono $|\cdot|$. Il valore assoluto $|\cdot|_M$ corrispondente a M è dato da $|b|_M = |(1 \otimes b) + M|_{\Gamma_M}$, $b \in E$, dove $\Gamma_M = (\widehat{F} \otimes_F E)/M$ e $|\cdot|_{\Gamma_M}$ è l'unica estensione a Γ_M del valore assoluto $|\cdot|_s$ su $\widehat{F} \otimes 1$ tale che $|a \otimes 1 + M|_s = |a|$, $a \in \widehat{F}$. Inoltre Γ_M è isomorfo al completamento di E rispetto a $|\cdot|_M$.*

Sia $\operatorname{rad} E_{\widehat{F}}$ il radicale di Jacobson di $E_{\widehat{F}} = \widehat{F} \otimes_F E$. Allora $E_{\widehat{F}}/\operatorname{rad} E_{\widehat{F}}$ è artiniano semiprimitivo, dunque

$$E_{\widehat{F}}/\operatorname{rad} E_{\widehat{F}} = \bar{I}_1 \oplus \bar{I}_2 \oplus \cdots \oplus \bar{I}_h, \tag{17}$$

dove gli $\bar{I}_j$ sono ideali minimali e sono campi su $\widehat{F}$ (p. 422). Gli ideali massimali di questa algebra sono gli ideali $\bar{M}_j = \bar{I}_1 + \cdots + \hat{\bar{I}}_j + \cdots + \bar{I}_h$, con l'addendo j-esimo omesso, $1 \le j \le h$, e $\bar{I}_j \cong (E_{\widehat{F}}/\operatorname{rad} E_{\widehat{F}})/\bar{M}_j$. Poiché $\operatorname{rad} E_{\widehat{F}}$ è l'intersezione degli ideali massimali di $E_{\widehat{F}}$, vi è una corrispondenza biunivoca fra questi e quelli di $E_{\widehat{F}}/\operatorname{rad} E_{\widehat{F}}$. Vi sono pertanto h ideali massimali distinti $M_1, \ldots, M_h$ di $E_{\widehat{F}}$, e $E_{\widehat{F}}/M_j \cong (E_{\widehat{F}}/\operatorname{rad} E_{\widehat{F}})/\bar{M}_j \cong \bar{I}_j$. Per il teorema 9.13 abbiamo dunque h estensioni di $|\cdot|$ a valori assoluti $|\cdot|_1, \ldots, |\cdot|_h$ su E, con $|\cdot|_j = |\cdot|_{M_j}$, e $\bar{I}_j$ è isomorfo al completamento $\widehat{E}_j$ di E rispetto a $|\cdot|_j$. Chiamiamo $n_j = [\widehat{E}_j : \widehat{F}]$ il *grado locale* di E/F in $|\cdot|_j$. Dalla (17) e dall'isomorfismo $\widehat{E}_j \cong \bar{I}_j$ segue la formula

$$\sum_{j=1}^{h} n_j = n - [\operatorname{rad} E_{\widehat{F}} : \widehat{F}], \tag{18}$$

dove $n = [E : F] = [E_{\widehat{F}} : \widehat{F}]$. Abbiamo quindi per i gradi locali la disuguaglianza

$$\sum_{j=1}^{h} n_j \le [E : F]. \tag{19}$$

Questi risultati assumono una forma concreta semplice se E ha un elemento primitivo, $E = F(u)$. In tal caso vale il seguente teorema.

Teorema 9.14. *Siano $|\cdot|$ un valore assoluto su F, $\widehat{F}$ il corrispondente completamento ed $E = F(u)$, con u algebrico su F di polinomio minimo $f(x)$ su F. Siano $f_1(x), \dots, f_h(x)$ i fattori monici irriducibili distinti di $f(x)$ in $\widehat{F}[x]$. Vi sono esattamente h estensioni di $|\cdot|$ a valori assoluti su E. I completamenti corrispondenti sono isomorfi ai campi $\widehat{F}[x]/(f_j(x))$, $1 \le j \le h$, e il grado locale n_j è* $\deg f_j(x)$.

Dimostrazione. Il campo E è isomorfo a $F[x]/(f(x))$, che ha la base $(1, \bar{x}, \dots, \bar{x}^{n-1})$, dove $\bar{x}^i = x^i + (f(x))$ e $n = \deg f(x)$. Questa è anche una base di $E_{\widehat{F}}/\widehat{F}$, sicché $E_{\widehat{F}} \cong \widehat{F}[x]/(f(x))$. Poiché $\widehat{F}[x]$ è un dominio a ideali principali, gli ideali massimali di $\widehat{F}[x]/(f(x))$ sono della forma $(g(x))/(f(x))$, dove $g(x)$ è un fattore monico irriducibile di $f(x)$ in $\widehat{F}[x]$. Dunque $\widehat{F}[x]/(f(x))$ ha h ideali massimali $(f_j(x))/(f(x))$. Il quoziente corrispondente è isomorfo a $\widehat{F}[x]/(f_j(x))$. Da ciò e dal teorema 9.13 seguono le asserzioni. □

Il teorema 9.14 si applica quando E/F è separabile, poiché un tale E ammette un elemento primitivo (*BAI*, p. 291). In questo caso il criterio della derivata (*BAI*, p. 231) mostra inoltre che $f(x) = f_1(x) \cdots f_h(x)$, dove gli $f_j(x)$ sono fattori irriducibili distinti. Si ha dunque il seguente corollario.

Corollario. *Sia E un'estensione separabile di dimensione finita di un campo F munito di un valore assoluto $|\cdot|$. Allora $[E : F] = \sum_{j=1}^{h} n_j$, dove $n_1, \dots, n_h$ sono i gradi locali.*

Come esempio, prendiamo $F = \mathbb{Q}$, $|\cdot|$ il valore assoluto usuale su $\mathbb{Q}$, ed $E = \mathbb{Q}(u)$, con $f(x)$ polinomio minimo di u. Qui $\widehat{F} = \mathbb{R}$ e in $\mathbb{R}[x]$ si ha la fattorizzazione

$$f(x) = \prod_{i=1}^{t} (x - \alpha_i) \prod_{j=1}^{s} g_j(x),$$

dove i g_j sono polinomi quadratici irriducibili. Non vi sono fattori multipli. Il numero delle estensioni di $|\cdot|$ a valori assoluti su E è dunque $t + s$, di cui t hanno grado locale uno e s grado locale due. La dimensione di E/F è $t + 2s$.

9.10 Indice di ramificazione e grado residuo. Valutazioni discrete

In questo paragrafo introduciamo le importanti nozioni di indice di ramificazione e di grado residuo di un'estensione di una valutazione, e quella di valutazione discreta. Sono discrete le valutazioni il cui gruppo dei valori è ciclico. Sono queste le valutazioni di maggiore interesse nella teoria dei numeri e nello studio delle funzioni algebriche di una variabile.

Sia E un campo con una valutazione φ e sia F un sottocampo. Siano S l'anello di valutazione di φ in E, Q l'ideale massimale di S, e R, P gli oggetti corrispondenti in F. Allora $R = S \cap F$ e $P = Q \cap F$. Abbiamo quindi il monomorfismo

$$a + P \longmapsto a + Q \tag{20}$$

di $\bar{R} = R/P$ in $\bar{S} = S/Q$. L'immagine è $(R + Q)/Q$, che si può identificare con $\bar{R}$ mediante l'isomorfismo (20) sulla sua immagine. Possiamo così considerare $\bar{R}$ immerso in $\bar{S}$ e considerare la dimensione

$$f = [\bar{S} : \bar{R}], \tag{21}$$

detta *grado residuo* di E/F rispetto a φ. È chiaro inoltre che il gruppo dei valori $\varphi(F^*)$ è un sottogruppo del gruppo dei valori $\varphi(E^*)$. Abbiamo perciò l'indice

$$e = [\varphi(E^*) : \varphi(F^*)], \tag{22}$$

detto *indice di ramificazione* di E/F rispetto a φ.

Consideriamo ora valori assoluti non archimedei o, equivalentemente, valutazioni con gruppo dei valori contenuto nel gruppo moltiplicativo dei reali positivi. Allora $S = \{a \in E \mid |a| \leq 1\}$ e $Q = \{b \in E \mid |b| < 1\}$. Supponiamo inoltre che $|\cdot|$ sia non banale. Mostriamo anzitutto che, se $[E : F] = n < \infty$, l'indice di ramificazione e il grado residuo sono finiti. Vale infatti la seguente proposizione.

Proposizione 9.1. $ef \leq n = [E : F]$.

Dimostrazione. Siano $u_1, \ldots, u_{f_1}$ elementi di S tali che le classi $u_i + Q$ in $\bar{S}$ siano linearmente indipendenti su $\bar{R} = (R + Q)/Q$. Ciò significa che, per $a_i \in R$, da $\sum_i a_i u_i \in Q$ segue $a_i \in Q$ per ogni i. Siano $b_1, \ldots, b_{e_1}$ elementi di E^* tali che le classi $|b_j||F^*|$ siano distinte nel gruppo quoziente $|E^*|/|F^*|$. Mostreremo che gli $e_1 f_1$ elementi $u_i b_j$ sono linearmente indipendenti su F. Moltiplicando i b_j per un opportuno elemento di F^*, possiamo portarli in Q. Supponiamo dunque $b_j \in Q$. Mostriamo anzitutto che, se $a_i \in F$ e $\sum_i a_i u_i \neq 0$, allora $|\sum_i a_i u_i| \in |F^*|$. Infatti qualche $a_i \neq 0$, e possiamo supporre $0 \neq |a_1| \geq |a_i|$ per tutti gli i. Allora $|\sum_i a_i u_i| = |a_1||\sum_i a_1^{-1} a_i u_i|$ e $|\sum_i a_1^{-1} a_i u_i| \leq 1$. Se fosse $|\sum_i a_1^{-1} a_i u_i| < 1$, avremmo $\sum_i a_1^{-1} a_i u_i \in Q$. Poiché $|a_1^{-1} a_i| \leq 1$, si ha $a_1^{-1} a_i \in R$ per ogni i, ma il coefficiente di u_1 è 1. La relazione contraddice la scelta degli u_i. Quindi $|\sum_i a_1^{-1} a_i u_i| = 1$ e $|\sum_i a_i u_i| = |a_1| \in |F^*|$.

Supponiamo ora di avere una relazione $\sum_{i,j} a_{ij} u_i b_j = 0$ con $a_{ij} \in F$. Se per qualche j si avesse $\sum_i a_{ij} u_i \neq 0$, la relazione implicherebbe l'esistenza di due indici distinti, diciamo $j = 1, 2$, tali che $|\sum_i a_{i1} u_i b_1| = |\sum_i a_{i2} u_i b_2| \neq 0$. Allora $\sum_i a_{i1} u_i \neq 0$ e $\sum_i a_{i2} u_i \neq 0$, sicché $|\sum_i a_{i1} u_i|$ e $|\sum_i a_{i2} u_i|$ appartengono a $|F^*|$. Ne seguirebbe $|b_1||F^*| = |b_2||F^*|$, contro la scelta dei b_j. Dunque la relazione implica $\sum_i a_{ij} u_i = 0$ per ogni j. Moltiplicando gli a_{ij} per un opportuno elemento non nullo di F, otteniamo una relazione $\sum_i a'_{ij} u_i = 0$ con $a'_{ij} \in R$ e, se qualche $a_{ij} \neq 0$, possiamo supporre che uno degli a'_{ij} non appartenga a Q. Ciò contraddice la scelta degli u_i e prova l'indipendenza su F degli $e_1 f_1$ elementi $u_i b_j$. Evidentemente ne segue $ef \leq n$. □

La disuguaglianza $ef \leq n$ si può precisare passando ai completamenti. Consideriamo il completamento $\widehat{E}$ di E, che contiene il completamento $\widehat{F}$ di F. Anzitutto $E, \widehat{E}$ hanno lo stesso gruppo dei valori. Sia $\hat{a} \in \widehat{E}^*$. Poiché E è denso in $\widehat{E}$, esiste $a \in E$ tale che $|a - \hat{a}| < |\hat{a}|$. Allora $|\hat{a}| = |a|$ e perciò $|\widehat{E}^*| = |E^*|$. Analogamente $|\widehat{F}^*| = |F^*|$. Quindi E/F e $\widehat{E}/\widehat{F}$ hanno lo stesso indice di ramificazione.

Siano $\widehat{S}, \widehat{R}$ gli anelli di valutazione di $\widehat{E}, \widehat{F}$ rispettivamente e $\widehat{Q}, \widehat{P}$ i corrispondenti ideali massimali. Abbiamo $S = \widehat{S} \cap E$, $Q = \widehat{Q} \cap E$, $R = \widehat{R} \cap F$, $P = \widehat{P} \cap F$. Se $\hat{a} \in \widehat{R}$, esiste $a \in F$ tale che $|\hat{a} - a| < 1$. Allora $\hat{a} - a \in \widehat{P}$, quindi $a \in \widehat{R} \cap F = R$. Dunque $\widehat{R} = R + \widehat{P}$ e si ha l'isomorfismo canonico

$$a + P \longmapsto a + \widehat{P} \tag{23}$$

del campo residuo $\bar{R} = R/P$ sul campo residuo $\widehat{R}/\widehat{P}$. Analogamente si ha l'isomorfismo $b + Q \mapsto b + \widehat{Q}$ di S/Q su $\widehat{S}/\widehat{Q}$. Esso è un isomorfismo semilineare di S/Q, considerato come spazio vettoriale su R/P, su $\widehat{S}/\widehat{Q}$, considerato come spazio vettoriale su $\widehat{R}/\widehat{P}$, rispetto all'isomorfismo (23) dei campi base. Dunque $[S/Q : R/P] = [\widehat{S}/\widehat{Q} : \widehat{R}/\widehat{P}]$ e, passando ai completamenti, rimangono invariati sia il grado residuo sia l'indice di ramificazione. D'altra parte $[E : F] = n$ è sostituito dal grado locale $\hat{n} = [\widehat{E} : \widehat{F}]$, che in generale sarà minore di $[E : F]$. Abbiamo la disuguaglianza più precisa $ef \leq \hat{n} \leq n$.

Risultati assai più precisi si ottengono quando $|\cdot|$ è discreto. Una valutazione φ si dice *discreta* se il suo gruppo dei valori è ciclico. Se non è banale, tale gruppo è ciclico infinito, e quindi si può realizzare nel gruppo moltiplicativo dei reali positivi. Dunque φ si può considerare un valore assoluto non archimedeo. I valori assoluti p-adici su $\mathbb{Q}$ sono discreti, poiché $|p|$ genera il gruppo

dei valori. Anche i valori assoluti su $F(x)$ banali su F sono discreti (p. 566). Ricordiamo inoltre che, se E è un'estensione di dimensione finita di F, il gruppo dei valori di E è isomorfo a un sottogruppo del gruppo dei valori di F (p. 582). Quindi, se una valutazione è discreta su F, anche ogni sua estensione a un campo estensione di dimensione finita è discreta.

Supponiamo $|\cdot|$ discreto e non banale su F e sia c il generatore di $|F^*|$ tale che $c < 1$. Prendiamo $\pi \in F^*$ con $|\pi| = c$. Allora $\pi \in P$. Per $a \in F^*$, si ha $|a| = |\pi|^k$ con $k \in \mathbb{Z}$, dunque $|a\pi^{-k}| = 1$ e $a\pi^{-k} = u$ è un'unità in R. Quindi $a = u\pi^k$. Evidentemente $a \in R$ se e solo se $k \geq 0$, e $a \in P$ se e solo se $k > 0$. Dunque $P = \pi R$. Si vede facilmente che i soli ideali non nulli di R sono $P^k = \pi^k R,\ k \geq 0$. L'anello di valutazione di un valore assoluto discreto è dunque un dominio a ideali principali. Inoltre questa proprietà è caratteristica, come mostra la proposizione seguente.

Proposizione 9.2. *Sia R un dominio locale a ideali principali (ossia un anello locale che è un dominio a ideali principali). Allora R è un anello di valutazione nel suo campo delle frazioni F e la corrispondente valutazione è discreta.*

Dimostrazione. Sia $\operatorname{rad} R = P = \pi R$. Essendo un dominio a ideali principali, R è fattoriale e, poiché πR è il solo ideale massimale, π e i suoi associati sono i soli elementi primi di R. Dunque ogni elemento non nullo di R si scrive in uno e un solo modo come $u\pi^k$, con u unità e $k \geq 0$. Quindi ogni elemento non nullo di F si scrive in uno e un solo modo come $v\pi^l$, con v unità di R e $l \in \mathbb{Z}$. Ne segue che R è un anello di valutazione in F e che la valutazione corrispondente è discreta. □

Alla luce della proposizione 9.2 e del risultato che la precede, è naturale chiamare un anello commutativo R con le proprietà indicate un *anello di valutazione discreta* (spesso abbreviato in DVR). Come vedremo nel capitolo 10, questi anelli hanno un ruolo importante nella teoria moltiplicativa degli ideali.

Proposizione 9.3. *Sia F completo rispetto a una valutazione discreta $|\cdot|$, sia E un'estensione di dimensione finita di F e si indichi con $|\cdot|$ l'unica estensione del valore assoluto a E. Allora $ef = n = [E : F]$.*

Dimostrazione. Sappiamo che $|\cdot|$ è discreto su E e che E è completo. Siano P, R, Q, S come prima e scegliamo π, Π tali che $P = \pi R,\ Q = \Pi S$. Allora $|\pi|$ e $|\Pi|$ generano rispettivamente $|F^*|$ e $|E^*|$. Poiché $[|E^*| : |F^*|] = e$, si ha $|\pi| = |\Pi|^e$, onde $\pi = u\Pi^e$ con u unità in S. Siano $u_1, \ldots, u_f \in S$ tali che le classi $u_i + Q$ formino una base di S/Q su R/P. Mostreremo che gli ef elementi

$$u_i\Pi^j, \qquad 1 \leq i \leq f, \quad 0 \leq j \leq e-1, \tag{24}$$

formano una base di E/F. È chiaro che le classi $|\Pi|^j|F^*|$, $0 \leq j \leq e-1$, sono distinte in $|E^*|/|F^*|$. La dimostrazione della proposizione 9.1 mostra dunque che gli $u_i\Pi^j$ sono linearmente indipendenti su F. Resta da mostrare che ogni elemento di E è combinazione lineare degli $u_i\Pi^j$ con coefficienti in F.

Mostriamo prima che ogni elemento di S si scrive come $\sum_{i,j} a_{ij}u_i\Pi^j$, con $a_{ij} \in R$. Sia $v \in S$, $v \neq 0$. Allora $|v| = |\Pi|^k$ per qualche $k \geq 0$. Scriviamo $k = m_1e + j_1$, dove $m_1 \geq 0$ e $0 \leq j_1 \leq e-1$. Allora $|v| = |\Pi^{m_1e+j_1}| = |\pi^{m_1}\Pi^{j_1}|$, onde $v = w\pi^{m_1}\Pi^{j_1}$ con $|w| = 1$, cioè $w \in S$. Esistono allora $a_{i1} \in R$ tali che $w - \sum_i a_{i1}u_i \in Q$, ossia $|w - \sum_i a_{i1}u_i| < 1$. Ponendo

$$v_1 = v - \left(\sum_i a_{i1}u_i\right)\pi^{m_1}\Pi^{j_1},$$

si ha $v_1 = (w - \sum_i a_{i1}u_i)\pi^{m_1}\Pi^{j_1}$ e $|v_1| < |v| = |\Pi|^k = |\Pi|^{m_1 e + j_1}$. Quindi $v = \sum_i b_{i1}u_i\Pi^{j_1} + v_1$ con $b_{i1} = a_{i1}\pi^{m_1} \in R$. Ripetiamo il procedimento con v_1 e otteniamo $v_1 = \sum_i b_{i2}u_i\Pi^{j_2} + v_2$, con $b_{i2} \in R$ e $|v_2| < |v_1|$. Sostituendo nell'espressione di v e iterando, otteniamo

$$v = \sum_{i=1}^{f}\sum_{j=0}^{e-1} c_{ij}^{(m)}u_i\Pi^j + v_m, \qquad m = 1, 2, \ldots,$$

dove $|v| > |v_1| > |v_2| > \cdots$ e $c_{ij}^{(m)} \in R$. Si ha allora $v_m \to 0$ e $\sum c_{ij}^{(m)}u_i\Pi^j \to v$. Poiché F è completo e gli ef elementi $u_i\Pi^j$ sono linearmente indipendenti, la dimostrazione del teorema 9.8 mostra che per ogni i, j esiste $\lim_m c_{ij}^{(m)} = c_{ij}$. Essendo $|c_{ij}^{(m)}| \leq 1$, si ha $|c_{ij}| \leq 1$, ossia $c_{ij} \in R$. Dunque $v = \sum c_{ij}u_i\Pi^j$ con tutti i $c_{ij} \in R$. Un elemento arbitrario v' di E può essere moltiplicato per un elemento non nullo di F in modo da ottenere un v con $|v| \leq 1$. Applicando il risultato appena provato per v, vediamo che v' è combinazione F-lineare degli $u_i\Pi^j$. La dimostrazione è conclusa. □

Possiamo ora dimostrare il risultato principale sui gradi residui e sugli indici di ramificazione.

Teorema 9.15. *Sia F un campo con un valore assoluto non archimedeo $|\cdot|$, sia E un'estensione di F tale che $[E : F] = n < \infty$, e siano $|\cdot|_1, \ldots, |\cdot|_h$ le estensioni di $|\cdot|$ a valori assoluti su E. Siano e_i, f_i l'indice di ramificazione e il grado residuo di E/F rispetto a $|\cdot|_i$. Allora $\sum_i e_i f_i \leq n$, e $\sum_i e_i f_i = n$ se $|\cdot|$ è discreto ed E/F è separabile.*

Dimostrazione. Sia $\widehat{E}_i$ il completamento di E rispetto a $|\cdot|_i$, che contiene il completamento $\widehat{F}$ di F rispetto a $|\cdot|$. Abbiamo visto che, posto $n_i = [\widehat{E}_i : \widehat{F}]$, si ha $e_i f_i \leq n_i$ e $\sum_i n_i \leq n$. Dunque $\sum_i e_i f_i \leq n$. Abbiamo anche visto che $\sum_i n_i = n$ se E/F è separabile e che $n_i = e_i f_i$ se $|\cdot|$ è discreto. Quindi $\sum_i e_i f_i = n$ quando $|\cdot|$ è discreto ed E/F è separabile. □[36]

Esercizi.

1. Determinare il gruppo dei valori, l'anello di valutazione e il suo ideale dei non invertibili per il campo $\mathbb{Q}_p$ dei numeri p-adici. Mostrare che il campo residuo è isomorfo a $\mathbb{Z}/(p)$. (Si veda l'esercizio 1, p. 560.)

2. Sia R un anello di valutazione in F. Mostrare che, se R è noetheriano, è un anello di valutazione discreta.

9.11 Lemma di Hensel

Dimostreremo ora un criterio di riducibilità per polinomi a coefficienti in un anello di valutazione, noto come *lemma di Hensel*. Nel testo tratteremo il caso più importante del lemma, in cui la valutazione è discreta e i polinomi sono monici. La forma generale è indicata negli esercizi. Le dimostrazioni qui date sono dovute a D. S. Rim. Il risultato essenziale è la proposizione seguente.

Proposizione 9.4. *Sia F completo rispetto a una valutazione discreta $|\cdot|$, sia R il suo anello di valutazione, P l'ideale massimale di R e $\bar{R} = R/P$. Se $f(x)$ è un polinomio monico irriducibile in $R[x]$, la sua immagine $\bar{f}(x)$ in $\bar{R}[x]$ è potenza di un polinomio irriducibile di $\bar{R}[x]$.*

[36] Un esempio in cui $n \neq \sum_i e_i f_i$ è stato dato da F. K. Schmidt, «Über die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körpererweiterungen», *Mathematische Zeitschrift*, vol. 41 (1936), pp. 443–450.

Dimostrazione. Sia E un campo di spezzamento di $f(x)$ su F. Allora $|\cdot|$ ha un'unica estensione a un valore assoluto $|\cdot|$ su E. Sia S l'anello di valutazione determinato dal valore assoluto su E e Q l'ideale massimale di S. Siano $a \in E$, $\sigma \in \mathrm{Gal}(E/F)$. Allora $N_{E/F}(\sigma a) = N_{E/F}(a)$. Quindi per la (7), $|\sigma a| = |a|$. Ne segue $\sigma(S) = S$ e $\sigma(Q) = Q$. Dunque σ determina l'automorfismo

$$\bar{\sigma}\colon \bar{a} \longmapsto \overline{\sigma a} \tag{25}$$

di S/Q. Esso è evidentemente l'identità su $\bar{R} = R/P$, sicché $\bar{\sigma} \in \mathrm{Gal}(\bar{S}/\bar{R})$, dove $\bar{S} = S/Q$. Il polinomio dato $f(x)$ è irriducibile in $F[x]$, poiché R è un dominio a ideali principali e quindi fattoriale (*BAI*, p. 148). In $E[x]$ abbiamo la fattorizzazione $f(x) = \prod_{i=1}^{n}(x - r_i)$. Sia $a_n = f(0) = \prod_i(-r_i)$. Allora $N_{E/F}(r_i) = ((-1)^n a_n)^e$, con $e = [E : F]/n$. Poiché $a_n \in R$, ne segue $|r_i| \leq 1$, onde $r_i \in S$. Applicando l'omomorfismo canonico di S su $\bar{S}$ si ottiene $\bar{f}(x) = \prod_i(x - \bar{r}_i)$. Siano $\bar{r}_i, \bar{r}_j$ due qualsiasi di queste radici. Poiché $f(x)$ è irriducibile in $F[x]$, esiste $\sigma \in \mathrm{Gal}(E/F)$ tale che $\sigma r_i = r_j$. Allora $\bar{\sigma}\bar{r}_i = \bar{r}_j$, il che implica che $\bar{r}_i, \bar{r}_j$ hanno lo stesso polinomio minimo su $\bar{R}$. Se questo è $\bar{g}(x)$, allora $\bar{f}(x)$ è una potenza di $\bar{g}(x)$. □

Possiamo ora dimostrare la seguente versione del lemma.

Lemma di Hensel. *Sia F completo rispetto a una valutazione discreta $|\cdot|$, R il suo anello di valutazione, P l'ideale dei non invertibili e $\bar{R} = R/P$. Supponiamo che $f(x)$ sia un polinomio monico in $R[x]$ tale che $\bar{f}(x) = \bar{\gamma}(x)\bar{\delta}(x)$ in $\bar{R}[x]$, dove $\bar{\gamma}(x), \bar{\delta}(x)$ sono monici e $(\bar{\gamma}(x), \bar{\delta}(x)) = 1$. Allora $f(x) = g(x)h(x)$ in $R[x]$, dove $g(x), h(x)$ sono monici, $\bar{g}(x) = \bar{\gamma}(x)$ e $\bar{h}(x) = \bar{\delta}(x)$.*

Dimostrazione. Abbiamo in $R[x]$ la fattorizzazione $f(x) = \prod_{i=1}^{s} f_i(x)^{e_i}$, dove gli $f_i(x)$ sono i fattori monici irriducibili distinti. Per la proposizione 9.4, $\bar{f}_i(x) = \bar{g}_i(x)^{k_i}$, con $\bar{g}_i(x)$ monico e irriducibile in $\bar{R}[x]$. Allora $\bar{f}(x) = \prod_{i=1}^{s} \bar{g}_i(x)^{e_i k_i}$ e, poiché $(\bar{\gamma}(x), \bar{\delta}(x)) = 1$, possiamo supporre che $\bar{\gamma}(x) = \prod_{j=1}^{r} \bar{g}_j(x)^{e_j k_j}$, $\bar{\delta}(x) = \prod_{l=r+1}^{s} \bar{g}_l(x)^{e_l k_l}$, con $\bar{g}_j(x) \neq \bar{g}_l(x)$ per gli indici j, l indicati. Poniamo $g(x) = \prod_{j=1}^{r} f_j(x)^{e_j}$ e $h(x) = \prod_{l=r+1}^{s} f_l(x)^{e_l}$. Allora $g(x)$ e $h(x)$ soddisfano le condizioni richieste. □

Il lemma di Hensel permette spesso di dedurre l'esistenza di radici di un'equazione $f(x) = 0$ in R dall'esistenza di radici di $\bar{f}(x)$ in $\bar{R}$. L'enunciato preciso è il seguente.

Corollario. *Siano $F, R, P, f(x)$, ecc., come nel lemma di Hensel. Se $\bar{f}(x)$ ha $\bar{\rho}$ come radice semplice in $\bar{R}$, allora $f(x)$ ha una radice r in R tale che $\bar{r} = \bar{\rho}$.*

Ciò è chiaro poiché $\bar{f}(x) = (x - \bar{\rho})\bar{\delta}(x)$, con $\bar{\delta}(\bar{\rho}) \neq 0$, sicché $(x - \bar{\rho}, \bar{\delta}(x)) = 1$.

Il lemma di Hensel si può usare anche insieme con il teorema 9.14 per determinare il numero delle estensioni di una valutazione p-adica di $\mathbb{Q}$ e i rispettivi gradi locali. Il secondo esercizio seguente ne dà un esempio.

Esercizi.

1. Mostrare che l'equazione $x^3 = 4$ ha una radice nel campo $\mathbb{Q}_5$ dei numeri 5-adici.
2. Determinare il numero delle estensioni e i gradi locali della valutazione p-adica di $\mathbb{Q}$, per $p = 3, 5, 11$, al campo delle radici quinte dell'unità.
3. Mostrare che $\mathbb{Q}_p$ ha p radici p-esime distinte di 1.[37]

   I tre esercizi seguenti conducono alla dimostrazione di una forma generale del lemma di Hensel.

[37] L'enunciato è così stampato nell'originale. Per p dispari non è vero. Il lemma di Hensel dà invece $p - 1$ radici $(p - 1)$-esime distinte dell'unità in $\mathbb{Q}_p$.

4. Sia R un anello di valutazione nel campo F. Un polinomio $f(x) \in R[x]$ si dice *primitivo* se qualche coefficiente di $f(x)$ è un'unità. Dimostrare il lemma di Gauss secondo cui il prodotto di due polinomi primitivi in $R[x]$ è primitivo. Mostrare che ogni polinomio non nullo in $F[x]$ si scrive come prodotto $cg(x)$, con $c \in F^*$ e $g(x)$ primitivo in $R[x]$. Mostrare che $c, g(x)$ sono determinati a meno di un'unità di R. Mostrare che, se $g(x)$ è primitivo e irriducibile in $R[x]$, è irriducibile in $F[x]$.

5. Siano F un campo e R un anello di valutazione in F tale che, per ogni estensione E di dimensione finita di F, esista un unico anello di valutazione S di E contenente R. (Osservare che ciò vale se F è completo rispetto al valore assoluto non archimedeo $|\cdot|$ e R è il corrispondente anello di valutazione.) Provare che la proposizione 9.4 vale per i polinomi monici in $R[x]$.

6. (*Lemma di Hensel.*) Siano F, R come nell'esercizio 5. Sia $f(x) \in R[x]$ e supponiamo $\bar{f}(x) = \bar{\gamma}(x)\bar{\delta}(x)$ in $\bar{R}[x]$, con $(\bar{\gamma}(x), \bar{\delta}(x)) = 1$ e $\deg \bar{\gamma}(x) > 0$. Allora $f(x) = g(x)h(x)$ in $R[x]$, con $\bar{g}(x) = \bar{\gamma}(x)$, $\bar{h}(x) = \bar{\delta}(x)$ e $\deg g(x) = \deg \bar{\gamma}(x)$.

7. Sia F un campo e sia $F^{\mathbb{Q}}$ l'insieme delle applicazioni di $\mathbb{Q}$ in F. Per $f \in F^{\mathbb{Q}}$ si definisca $\operatorname{Supp} f = \{\alpha \in \mathbb{Q} \mid f(\alpha) \neq 0\}$. Sia $P(F)$ il sottoinsieme di $F^{\mathbb{Q}}$ formato dalle f tali che (i) $\operatorname{Supp} f \subseteq \mathbb{Z}n^{-1}$ per qualche intero positivo n (dipendente da f), e (ii) $\operatorname{Supp} f$ è limitato inferiormente. Gli elementi di $P(F)$ si possono rappresentare come serie formali $\sum_{\alpha \in \operatorname{Supp} f} f(\alpha)t^{\alpha}$, dette *serie di Newton–Puiseux*. Per $f, g \in P(F)$ si definiscano $f+g, fg$ mediante $(f+g)(\alpha) = f(\alpha) + g(\alpha)$, $(fg)(\alpha) = \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma)$ (somma ben definita). Si ponga $0(\alpha) = 0$ per ogni α, e $1(\alpha) = 1$ per $\alpha = 0$, $1(\alpha) = 0$ per $\alpha \neq 0$. Verificare che $(P(F), +, \cdot, 0, 1)$ è un anello commutativo. Mostrare che ogni sottoinsieme finito $\{f_1, \ldots, f_r\}$ di $P(F)$ è contenuto in un sottoanello isomorfo a un campo di serie di Laurent $\sum_{i \geq k} a_i t^i$. Dedurne che $P(F)$ è un campo.

   Sia $v(0) = \infty$ e, per $f \neq 0$, sia $v(f)$ il minimo razionale in $\operatorname{Supp} f$. Verificare che $v(fg) = v(f) + v(g)$, $v(f+g) \geq \min(v(f), v(g))$. Mostrare che, per ogni razionale positivo λ, l'applicazione η_λ di $P(F)$ definita da $(\eta_\lambda f)(\alpha) = f(\lambda^{-1}\alpha)$ è un automorfismo di $P(F)$. (Simbolicamente, $\eta_\lambda \colon \sum f(\alpha)t^{\alpha} \mapsto \sum f(\alpha)t^{\lambda\alpha}$.) Si ha $v(\eta_\lambda f) = \lambda v(f)$.

8. (*Newton–Puiseux.*) Dimostrare che, se F è algebricamente chiuso di caratteristica zero, $P(F)$ è algebricamente chiuso. (*Traccia della dimostrazione, secondo un'esposizione di S. Abhyankar.* Occorre mostrare che un polinomio monico $g(x) \in P(F)[x]$ di grado $n > 1$ ha un fattore di grado m con $1 \leq m < n$. Applicando un opportuno automorfismo, possiamo supporre $g(x) \in F((t))[x]$. Sostituendo $g(x) = x^n + f_1 x^{n-1} + \cdots + f_n$, $f_i \in F((t))$, con $g(x - (1/n)f_1)$, possiamo supporre $f_1 = 0$. Supponiamo dapprima che tutti gli f_i appartengano a $F[[t]]$ e che per qualche i si abbia $f_i(0) \neq 0$, cioè che gli ordini siano tutti non negativi e almeno uno sia zero. Sia $\bar{g}(x) = x^n + f_2(0)x^{n-2} + \cdots + f_n(0)$. Osservare che $\bar{g}(x) \in F[x]$ non è potenza di un fattore lineare e applicare quindi il lemma di Hensel per mostrare che, se $n > 1$, $g(x)$ ha un fattore di grado m con $1 \leq m < n$. Sia ora $g(x)$ arbitrario della forma $x^n + f_2 x^{n-2} + \cdots + f_n$, con $f_i \in F((t))$. Possiamo supporre non nullo almeno un f_i. Sia $u = \inf\{v(f_i)/i \mid 2 \leq i \leq n\}$ e si scelga r, $2 \leq r \leq n$, tale che $v(f_r)/r = u$. Applicare l'automorfismo η_r ai coefficienti, seguito dall'automorfismo di $P(F)[x]$ che è l'identità sui coefficienti e manda x in $t^{v(f_r)}x$. Moltiplicando il polinomio risultante per $t^{-v(f_r)n}$ si ottiene un polinomio monico che soddisfa le condizioni del primo caso. La validità del risultato per quest'ultimo implica il risultato per $g(x)$.)

9.12 Campi locali

Un campo F munito di un valore assoluto $|\ |$ si dice *campo locale* se la coppia $(F, |\ |)$ soddisfa le condizioni seguenti.

1. Il valore assoluto $|\ |$ è non archimedeo, discreto e non banale.
2. F è completo rispetto a $|\ |$.
3. Il campo residuo di $|\ |$ è finito.

Esempi tipici sono $\mathbb{Q}_p$ e il campo $F((x))$ delle serie formali di Laurent in un'indeterminata su un campo finito F. Per il primo esempio ciò è stato indicato nell'esercizio 1 a p. 561. Il campo residuo è in questo caso $\mathbb{Z}/(p)$. Il secondo esempio si può considerare come il completamento del campo $F(x)$ delle espressioni razionali in x, con il valore assoluto $|\ |_\infty$ definito a p. 539. L'anello di valutazione R di $F(x)$ è l'insieme delle espressioni razionali $x^k b(x)/c(x)$ tali che $b(0) \neq 0$, $c(0) \neq 0$ e $k \geq 0$. L'ideale massimale P di R è l'insieme di questi elementi con $k > 0$. L'applicazione che manda un elemento di R nel suo valore in 0 è un omomorfismo di R su F di nucleo P. Quindi $R/P \cong F$. Ne segue che anche il campo residuo del completamento $\widehat{F(x)} = F((x))$ è isomorfo a F, sicché $F((x))$ è un campo locale.

Le proprietà (1), (2) e (3) si conservano passando a un'estensione di dimensione finita. Pertanto, se F è locale ed E è un campo di dimensione finita su F, anche E è locale.

È piuttosto facile determinare tutti i campi locali. Dimostriamo dapprima il lemma seguente.

Lemma 1. *Sia F un campo locale e sia $|R/P| = N_P$. Allora R contiene N_P radici distinte $\zeta_1, \zeta_2, \dots, \zeta_{N_P}$ di $x^{N_P} = x$ e questi elementi costituiscono un sistema di rappresentanti delle classi laterali di P nel gruppo additivo di R.*

Dimostrazione. Poiché N_P è la cardinalità del campo finito $\bar{R} = R/P$, esso è una potenza della caratteristica di $\bar{R}$ e $\bar{R}$ è un campo di spezzamento di $x^{N_P} - x$ sul campo primo (si veda BAI, p. 287). Sia ζ_0 un qualsiasi elemento di $\bar{R}$. Per il corollario al lemma di Hensel (p. 593) esiste un $\zeta \in R$ tale che $\zeta^{N_P} = \zeta$ e $\zeta + P = \zeta_0$. Se $\zeta_0' \neq \zeta_0$ è un altro elemento di $\bar{R}$ e $\zeta' \in R$ soddisfa $\zeta'^{N_P} = \zeta'$, $\zeta' + P = \zeta_0'$, allora $\zeta + P \neq \zeta' + P$. Possiamo quindi ottenere N_P elementi $\zeta_1, \zeta_2, \dots, \zeta_{N_P}$ tali che $\zeta_i^{N_P} = \zeta_i$ e con le classi $\zeta_i + P$ distinte. □

Poniamo $\Lambda = \{\zeta_1, \zeta_2, \dots, \zeta_{N_P}\}$. Sia π un elemento tale che $\pi R = P$. Allora $|\pi|$ genera il gruppo dei valori $|F^*|$. Più in generale, sia π_k un elemento tale che $|\pi_k| = |\pi|^k$, $k \in \mathbb{Z}$. In particolare possiamo prendere $\pi_k = \pi^k$. Sia $a \in F^*$. Affermiamo che si può scrivere

$$a = \alpha_{k_1}\pi_{k_1} + \alpha_{k_2}\pi_{k_2} + \cdots, \tag{26}$$

dove gli α_{k_i} appartengono a Λ, $k_1 < k_2 < \cdots$ e $\alpha_{k_i} \neq 0$. Sia $|a| = |\pi_{k_1}|$. Allora $a\pi_{k_1}^{-1} \in R$, $a\pi_{k_1}^{-1} \notin P$, quindi esiste un $\alpha_{k_1} \neq 0$ in Λ tale che $a\pi_{k_1}^{-1} \equiv \alpha_{k_1} \pmod{P}$. Si ha allora $|a - \alpha_{k_1}\pi_{k_1}| < |a|$. Se $a = \alpha_{k_1}\pi_{k_1}$, abbiamo la (26). Altrimenti ripetiamo l'argomento con $a - \alpha_{k_1}\pi_{k_1}$. Per induzione otteniamo $k_1 < k_2 < \cdots$ ed elementi non nulli $\alpha_{k_1}, \alpha_{k_2}, \dots$ di Λ tali che

$$|a| > |a - \alpha_{k_1}\pi_{k_1}| > |a - \alpha_{k_1}\pi_{k_1} - \alpha_{k_2}\pi_{k_2}| > \cdots.$$

Si ottiene così la (26). È inoltre chiaro che gli α per cui vale la (26) sono determinati in modo unico e che $a \in R$ se e solo se $k_1 \geq 0$.

Sia ora F_0 un sottocampo di F tale che (1) $F_0 \supset \Lambda$, (2) F_0 sia chiuso nella topologia di F e (3) $F_0 \cap P \neq 0$. Poniamo $R_0 = R \cap F_0$, $P_0 = P \cap F_0$. Diremo che un polinomio $f(x) = x^n + b_1 x^{n-1} + \cdots + b_n \in R_0[x]$ è un *polinomio di Eisenstein* in $R_0[x]$ se i b_i appartengono a P_0 e $b_n \notin P_0^2$. Si ha allora il seguente lemma.

Lemma 2. *Sia F_0 un sottocampo di F tale che (1) $F_0 \supset \Lambda$, (2) F_0 sia chiuso nella topologia di F e (3) $P_0 = F_0 \cap P \neq 0$. Sia π un elemento di R tale che $P = (\pi)$. Allora $F = F_0(\pi)$ e π è algebrico su F_0, con polinomio minimo un polinomio di Eisenstein su $R_0 = R \cap F_0$.*

Dimostrazione. È chiaro che F_0 è un sottocampo locale di F. Siano $P_0 = (\pi_0)$ in R_0 e $P = (\pi)$. Allora $|\pi_0| = |\pi|^e$ con $e \geq 1$. Per $k \in \mathbb{Z}$ si ha $k = eq + r$, dove $0 \leq r \leq e-1$. Posto $\pi_k = \pi_0^q \pi^r$, si ha dunque $|\pi_k| = |\pi^k|$. Come sopra, ogni $a \in F^*$ si può scrivere nella forma (26) usando questi π_k e, se $a \in R$, gli indici k nella (26) sono non negativi. Riordinando i termini della somma otteniamo

$$a = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}, \tag{27}$$

dove ogni a_i è della forma $\sum_q \alpha_q \pi_0^q$ e per $a \in R$ la somma è estesa a $q \geq 0$, sicché gli a_i appartengono a R_0. Ora $|a_i\pi^i|$, quando $a_i \neq 0$, è della forma $|\pi|^{es+i}$. Dunque $|a_i\pi^i| \neq |a_j\pi^j|$ per termini non nulli con $i \neq j$ e $0 \leq i, j \leq e-1$. Ne segue che, se $\sum_i a_i\pi^i = 0$, tutti gli a_i sono nulli. Pertanto $(1, \pi, \ldots, \pi^{e-1})$ è una base di F/F_0 e dunque $F = F_0(\pi)$. Applicando inoltre la (27) ad $a = \pi^e$, vediamo che π è algebrico con polinomio minimo della forma $f(x) = x^e + b_1x^{e-1} + \cdots + b_e$, dove $b_i \in R_0$. Allora $N_{F/F_0}(\pi) = \pm b_e$ e $|b_e| = |N_{F/F_0}(\pi)| = |\pi^e| = |\pi_0|$ (si veda la (7)). Dunque $b_e \in P_0$, $b_e \notin P_0^2$. Supponiamo che uno dei b_i non appartenga a P_0. Allora $\bar{f}(x) = g_0(x)x^j$ in $(R_0/P_0)[x]$, con $j \geq 1$ e $x \nmid g_0(x)$. Dal lemma di Hensel segue che $f(x)$ è riducibile. Questa contraddizione mostra che ogni $b_i \in P_0$ e quindi $f(x)$ è un polinomio di Eisenstein. □

Possiamo ora dimostrare il seguente teorema.

Teorema 9.16. *I campi locali sono i campi di serie formali di Laurent $F_0((x))$, dove F_0 è un campo finito, e le estensioni algebriche finite dei campi dei numeri p-adici.*

Dimostrazione. Supponiamo dapprima che F abbia caratteristica positiva. Allora R/P ha la stessa caratteristica. Sia $\Lambda = \{\zeta_1, \zeta_2, \ldots, \zeta_{N_P}\}$ l'insieme degli elementi di F tali che $\zeta_i^{N_P} = \zeta_i$. Poiché N_P è una potenza della caratteristica di F, ne segue che Λ è un sottocampo finito di F. Sia $\pi \in P$ tale che $P = (\pi)$. Abbiamo visto che ogni elemento di F ha la forma $\sum_{j \geq k} \alpha_j \pi^j$, $\alpha_j \in \Lambda$, e che questa espressione è unica. Dunque $F = \Lambda((\pi))$. Supponiamo ora che F abbia caratteristica 0. Allora F contiene $\mathbb{Q}$ e la valutazione non è banale su $\mathbb{Q}$, poiché R/P è finito, sicché $\mathbb{Z} \cap P \neq 0$. Pertanto F contiene $\mathbb{Q}_p$ per qualche p. Sia Λ come sopra e sia $F_0 = \mathbb{Q}_p(\Lambda)$. Allora F_0 soddisfa le condizioni del lemma 2, sicché $F = F_0(\pi)$ è algebrico su F_0. Quindi F è algebrico su $\mathbb{Q}_p$. □

Analizziamo ora la struttura di un'estensione E di dimensione finita di un campo locale F. Anche E è locale. Siano e ed f l'indice di ramificazione e il grado residuo del valore assoluto $|\ |$ di E che prolunga il valore assoluto dato su F. Allora $ef = n$. Mostreremo che E si costruisce a partire da F in due tappe, $E \supset W \supset F$, dove W è *non ramificato* su F, nel senso che l'indice di ramificazione associato a W/F è 1, ed E è *totalmente ramificato* su W, nel senso che il grado residuo corrispondente è 1.

Siano R, P, S, Q come di consueto (p. 568). Allora $[S/Q : R/P] = f$, quindi

$$N_Q = |S/Q| = |R/P|^f = N_P^f. \tag{28}$$

Inoltre il gruppo di Galois di S/Q su R/P è ciclico, con generatore

$$\bar{a} \longmapsto \bar{a}^{N_P}. \tag{29}$$

Denotiamo con Λ_E e Λ_F gli insiemi delle radici di $x^{N_Q} = x$ e $x^{N_P} = x$, rispettivamente in E e in F. Allora $\Lambda_E \supset \Lambda_F$. Poniamo $W = F(\Lambda_E)$. Si ha il lemma seguente.

Lemma 3. *$[W : F] = f$ e W/F è non ramificata.*

Dimostrazione. Si ha l'isomorfismo $\zeta \mapsto \bar{\zeta} = \zeta + Q$ del gruppo Λ_E^* degli elementi non nulli di Λ_E sul gruppo moltiplicativo del campo S/Q. Quindi, se ζ è una radice primitiva $(N_Q - 1)$-esima dell'unità in S, allora $\bar{\zeta}$ è una radice primitiva $(N_Q - 1)$-esima dell'unità di S/Q. Abbiamo $W = F(\zeta)$ e $S/Q = (R/P)(\bar{\zeta})$. Sia $g_0(x)$ il polinomio minimo di $\bar{\zeta}$ su R/P. Allora $\deg g_0(x) = [S/Q : R/P] = f$ e $x^{N_Q} - x = g_0(x)h_0(x)$ in $(R/P)[x]$. Per il lemma di Hensel, $x^{N_Q} - x = g(x)h(x)$, dove $g(x)$ e $h(x)$ sono monici in $R[x]$ e $\bar{g}(x) = g_0(x)$, $\bar{h}(x) = h_0(x)$. Se $g(\zeta) \neq 0$, allora $h(\zeta) = 0$ e $h_0(\bar{\zeta}) = 0$, il che è impossibile poiché $g_0(\bar{\zeta}) = 0$ e $x^{N_Q} - x$ ha radici distinte. Dunque $g(\zeta) = 0$. Poiché $g_0(x)$ è irriducibile in $(R/P)[x]$, $g(x)$ è irriducibile in $R[x]$ e quindi in $F[x]$. Allora $g(x)$ è il polinomio minimo di ζ su F e perciò $[W : F] = \deg g(x) = f$. Essendo $\Lambda_E \subset W$, è chiaro che il grado residuo della valutazione di W è f e, poiché $[W : F] = f$, ne segue che l'indice di ramificazione è 1. Dunque W è non ramificato. □

Ora W è un campo di spezzamento su F del polinomio $x^{N_Q} - x$, che ha radici distinte. Dunque W è di Galois su F. Sia $G = \mathrm{Gal}(W/F)$. Come nella dimostrazione della proposizione 9.4 (p. 573), ogni $\sigma \in G$ determina un automorfismo $\bar{\sigma}\colon \bar{a} \mapsto \overline{\sigma a}$ del campo residuo, appartenente a $\mathrm{Gal}((S/Q)/(R/P))$. Ora G manda Λ_E^* in sé e $\bar{G}$ manda il gruppo moltiplicativo di S/Q in sé. Poiché l'applicazione $a \mapsto \bar{a}$ su Λ_E^* è iniettiva e $W = F(\Lambda_E)$, ne segue che $\sigma \mapsto \bar{\sigma}$ è un monomorfismo. Poiché $|G| = [W : F] = [S/Q : R/P] = |\mathrm{Gal}((S/Q)/(R/P))|$, l'applicazione $\sigma \mapsto \bar{\sigma}$ è un isomorfismo del gruppo di Galois di W/F sul gruppo di Galois di S/Q su R/P. Quest'ultimo è ciclico. Quindi $\mathrm{Gal}(W/F)$ è un gruppo ciclico.

Poiché W è non ramificato, $|W^*| = |F^*|$ e dunque $[|E^*| : |W^*|] = e$. Pertanto e è l'indice di ramificazione di E su W ed è anche uguale a $[E : W]$. Quindi E è totalmente ramificato su W. Per il lemma 2, se Π è scelto in modo che $(\Pi) = Q$, allora $E = W(\Pi)$ e il polinomio minimo di Π su W è un polinomio di Eisenstein. Se E è non ramificato, chiaramente $E = W$. Si vede anche facilmente che, in ogni caso, W contiene ogni sottocampo non ramificato di E/F. Abbiamo dimostrato i risultati seguenti.

Teorema 9.17. *Sia F un campo locale ed E un'estensione di dimensione finita di F. Allora E contiene un unico sottocampo non ramificato massimale W. Si ha $[W : F] = f$, il grado residuo di E su F, e W è un campo ciclico su F. Il campo E è totalmente ramificato su W e $[E : W] = e$, l'indice di ramificazione. Inoltre, se Π è scelto in modo che $Q = (\Pi)$, allora $E = W(\Pi)$ e il polinomio minimo di Π su W è un polinomio di Eisenstein (su $S \cap W$).*

Vi è un altro risultato importante in queste considerazioni. Esso riguarda l'esistenza di un generatore distinto di $\mathrm{Gal}(W/F)$ per W non ramificato. Per il gruppo di Galois del campo finito S/Q su R/P si ha il generatore $\bar{a} \mapsto \bar{a}^{N_P}$. A esso corrisponde un automorfismo in $\mathrm{Gal}(W/F)$, detto *automorfismo di Frobenius* di W/F. È caratterizzato dalla proprietà di mandare ogni $\zeta \in \Lambda_E$ in ζ^{N_P}.

Esercizi

1. Con le notazioni del teorema 9.17, dimostrare che, se la caratteristica di S/Q non divide e, si può scegliere Π in modo che il suo polinomio minimo sia della forma $x^e - \pi$, $\pi \in P$.

2. Siano E, F come nell'esercizio 1, con $\mathrm{char}(S/Q) \nmid e$, e si supponga che E/F sia di Galois. Dimostrare che $\mathrm{Gal}(E/W)$ è ciclico di ordine e. Dedurne che $\mathrm{Gal}(E/F)$ è un'estensione di un gruppo ciclico mediante un gruppo ciclico. Dimostrare inoltre che, se E/F è un'estensione abeliana, allora $e \mid (N_Q - 1)$.

3. Dimostrare che, se R è un anello di valutazione, ogni polinomio di Eisenstein in $R[x]$ è irriducibile.

9.13 Anelli con divisione localmente compatti totalmente sconnessi

In questo paragrafo ci proponiamo di mostrare che i campi locali e, più in generale, le algebre con divisione di dimensione finita sui campi locali ammettono una semplice caratterizzazione topologica. Sono precisamente gli anelli topologici con divisione non discreti, totalmente sconnessi e localmente compatti. Con metodi topologici determineremo anche la struttura di questi anelli con divisione. Nel paragrafo successivo useremo tali risultati per determinare il gruppo di Brauer di un campo locale.

Per *anello topologico con divisione* D intendiamo un anello con divisione che sia uno spazio di Hausdorff, nel quale la sottrazione e la moltiplicazione siano applicazioni continue dello spazio prodotto nello spazio soggiacente D, e l'applicazione $x \mapsto x^{-1}$ sia continua sul sottospazio D^* degli elementi non nulli. Supponiamo che la topologia non sia discreta. Si vede facilmente che un anello topologico con divisione è connesso oppure totalmente sconnesso, il che significa che gli unici sottoinsiemi connessi non vuoti sono i singoletti. Ricordiamo che uno spazio è localmente compatto se ogni punto ha un intorno compatto. I campi localmente compatti, sia nel caso connesso sia in quello totalmente sconnesso, furono determinati nel 1931 da D. van Dantzig. Nel 1932 L. Pontrjagin dimostrò che gli anelli con divisione connessi localmente compatti sono i tre esempi classici, $\mathbb{H}$ (i quaternioni di Hamilton), $\mathbb{C}$ e $\mathbb{R}$. L'autore determinò nel 1936 quelli totalmente sconnessi, assumendo il primo assioma di numerabilità. Y. Otobe eliminò nel 1945 questa condizione e l'ipotesi di continuità di $x \mapsto x^{-1}$. Cominciamo col dimostrare il primo assioma di numerabilità per gli anelli con divisione localmente compatti mediante un semplice argomento tratto dalla seconda edizione dei *Topological Groups* di Pontrjagin. Seguiremo poi il metodo della nostra dimostrazione del 1936, con alcuni miglioramenti. Per le definizioni e i risultati topologici che enunceremo senza dimostrazione si può consultare il libro di Pontrjagin.[38]

Sia D un anello con divisione localmente compatto (non discreto), C un sottoinsieme compatto di D e W un intorno di 0. Poiché $a0 = 0$ per ogni a e la moltiplicazione è continua, per ogni $x \in C$ esistono intorni U_x di x e V_x di 0 tali che $U_x V_x = \{uv \mid u \in U_x,\ v \in V_x\} \subseteq W$. Per la compattezza di C, un numero finito di essi, $U_{x_1}, \ldots, U_{x_n}$, ricopre C. Ponendo $V = \bigcap_{i=1}^{n} V_{x_i}$ si ha $CV \subseteq W$.

Sia ora U un intorno compatto di 0. Esso è infinito, poiché D non è discreto. Sia $\{b_n\}$ una successione infinita di elementi distinti di U e poniamo $B_k = \{b_m \mid m \geq k\}$. Allora $B_1 \supseteq B_2 \supseteq \cdots$ e $\bigcap B_k = \varnothing$. Dunque qualche B_k non è chiuso e possiamo supporre che $B = \{b_n\}$ non sia chiuso. Sia $b \in \overline{B}$, la chiusura di B, con $b \notin B$. Allora b è un punto di accumulazione di B e $b \in U$. Mediante una traslazione possiamo supporre $b = 0$. Affermiamo che $\{Ub_n\}$ è una base di intorni di 0, ossia che per ogni intorno W di 0 esiste un n tale che $Ub_n \subseteq W$. Essendo U compatto, il risultato appena dimostrato dà un intorno V di 0 tale che $UV \subseteq W$. Poiché 0 è un punto di accumulazione di B, esiste un $b_n \in V \cap B$. Quindi $Ub_n \subseteq UV \subseteq W$. Ciò dimostra il primo assioma di numerabilità per D e ci permette di fondare le considerazioni topologiche sulla convergenza di successioni.

La nozione di successione di Cauchy in un gruppo abeliano topologico è chiara. Una successione $\{a_n\}$ è di Cauchy se per ogni intorno U di 0 esiste un intero N tale che $a_m - a_n \in U$ per tutti gli $m, n > N$. Tale successione converge se converge una sua sottosuccessione. Ne segue che ogni gruppo abeliano localmente compatto è completo, ossia ogni successione di Cauchy converge. Infatti, se $\{a_n\}$ è di Cauchy e U è un intorno compatto di 0, allora $a_{N+p} - a_N \in U$ per N abbastanza grande e $p = 1, 2, \ldots$. Una sottosuccessione di $\{a_{N+p} - a_N \mid p = 1, 2, \ldots\}$ converge e, poiché la successione è di Cauchy, esiste b tale che $\lim_{p\to\infty}(a_{N+p} - a_N) = b$. Allora $\lim_{n\to\infty} a_n = a_N + b$.

[38] Una buona bibliografia dei primi lavori sull'algebra topologica si trova nella recensione di H. Freudenthal al libro di Pontrjagin, in *Nieuw Archief voor Wiskunde*, vol. 20 (1940), pp. 311–316.

Sia ancora D un anello con divisione localmente compatto e siano U, V intorni compatti di 0 tali che $V \subsetneq U$. Esiste un intorno W di 0 tale che $WU \subseteq V$, sicché ogni $w \in W$ soddisfa

$$wU \subseteq V. \tag{30}$$

Mostreremo che, per ogni w che soddisfi (30), si ha $w^n \to 0$. Sia u un elemento non nullo di U. Poiché $w^n U \subseteq U$, abbiamo $w^n \in Uu^{-1}$ per $n = 1, 2, 3, \ldots$, e Uu^{-1} è compatto. Dato che la successione delle potenze $\{w^n\}$ è contenuta in un compatto, per provare che $w^n \to 0$ basta mostrare che 0 è l'unico possibile limite di una sua sottosuccessione. Supponiamo che $w^{n_i} \to z \neq 0$. Allora per gli esponenti $m_k = n_{i+1} - n_i$ si ha $w^{m_k} \to 1$. Quindi $\lim w^{m_k} u = u$ per ogni $u \in U$. Ogni $w^{m_k} u$ appartiene a wU, che è chiuso, dunque $u = \lim w^{m_k} u \in wU$. Ne segue $U \subseteq wU \subseteq V$, contro $V \subsetneq U$.

Scriveremo $a_n \to \infty$ se nessuna sottosuccessione di $\{a_n\}$ converge. Ci serviremo del fatto che W contiene elementi $w \neq 0$ tali che $w^n \to 0$ per dimostrare la proposizione seguente.

Proposizione 9.5. *Se D è un anello con divisione localmente compatto, una successione $\{a_n\}$ di elementi non nulli soddisfa $a_n \to \infty$ se e solo se $a_n^{-1} \to 0$.*

Dimostrazione. Per la continuità di $x \mapsto x^{-1}$ in D^*, da $a_n \to a \neq 0$ segue $a_n^{-1} \to a^{-1}$. Basta dunque provare che non si può avere contemporaneamente $a_n \to \infty$ e $a_n^{-1} \to \infty$. Supponiamo che ciò accada e sia U un intorno compatto di 0. Eliminando alcuni termini iniziali, possiamo supporre $a_n \notin U$ e $a_n^{-1} \notin U$ per $n = 1, 2, \ldots$. Sia $w \neq 0$ tale che $\lim w^n = 0$. Se, fissato j, si avesse $a_n w^j \in U$ per infiniti n, dalla compattezza di Uw^{-j} seguirebbe che una sottosuccessione di $\{a_n\}$ converge, contro l'ipotesi. Dunque per ogni j esiste n_j tale che $a_n w^j \notin U$ per $n > n_j$. Esiste pertanto una sottosuccessione $\{b_n\}$ di $\{a_n\}$ tale che $b_n w^n \notin U$. Poiché $w^n \to 0$, per ogni n esiste $k_n \geq n$ con $b_n w^{k_n} \notin U$ e $b_n w^{k_n+1} \in U$. Una sottosuccessione di $\{b_n w^{k_n+1}\}$ converge e possiamo supporre $b_n w^{k_n+1} \to z$. Allora $b_n w^{k_n} \to z w^{-1}$, e $z w^{-1} \neq 0$ poiché $b_n w^{k_n} \notin U$. Quindi $w^{-k_n} b_n^{-1} \to w z^{-1}$ e $b_n^{-1} = w^{k_n}(w^{-k_n} b_n^{-1}) \to 0$, in contraddizione con $a_n^{-1} \to \infty$. □

Sia G un gruppo abeliano localmente compatto totalmente sconnesso. Lo zero ammette una base di intorni costituita da sottoinsiemi compatti, aperti e chiusi di G (si veda Pontrjagin, op. cit., p. 87). Possiamo ora dimostrare il risultato seguente.

Proposizione 9.6. *Se G è un gruppo abeliano localmente compatto totalmente sconnesso, i suoi sottogruppi compatti e aperti (e quindi anche chiusi) formano una base di intorni di 0 in G.*

Dimostrazione. Poiché 0 ha una base di intorni compatti, aperti e chiusi, basta mostrare che ogni siffatto intorno U contiene un sottogruppo aperto di G. Prendiamo $V = U \cap (-U)$, dove $-U = \{-u \mid u \in U\}$, e $H = \{h \in G \mid h + V \subseteq V\}$. Allora H è un sottogruppo aperto di G contenuto in V, dunque $H \subseteq U$. □

Dimostriamo ora l'esistenza di sottoanelli compatti e aperti in un anello con divisione localmente compatto totalmente sconnesso.

Proposizione 9.7. *Sia D un anello con divisione localmente compatto totalmente sconnesso e sia H un sottogruppo compatto e aperto di D. L'insieme $R = \{a \in D \mid aH \subseteq H\}$ è un sottoanello compatto e aperto di D.*

Dimostrazione. È chiaro che R è un sottoanello e contiene un intorno aperto di 0, dunque è aperto e quindi chiuso. Se h è un elemento non nullo di H, si ha $R \subseteq Hh^{-1}$. Dalla compattezza di Hh^{-1} segue quella di R. □

Sia ora R un qualunque sottoanello compatto e aperto di D, e studiamone le proprietà aritmetiche. Per ogni $b \neq 0$ in R, bR e Rb sono rispettivamente un ideale destro aperto e un ideale sinistro aperto di R. Se I è un ideale destro (sinistro) non nullo, $I = \bigcup_{b \in I} bR$ (rispettivamente $\bigcup_{b \in I} Rb$), perciò I è aperto. Il quoziente R/I è compatto e discreto, quindi finito. Ne segue

che R è noetheriano a sinistra e a destra. Se B è un ideale non nullo di R, allora R/B è finito, perciò artiniano a sinistra e a destra. Osserviamo anche che gli ideali non nulli di R formano una base di intorni di 0. Se U è un intorno compatto di 0, esiste un intorno V di 0 tale che $RVR = \{ava' \mid a, a' \in R,\ v \in V\} \subseteq U$. Prendendo $z \neq 0$ in $V \cap R$, vediamo che RzR è un ideale non nullo di R contenuto in U (si può prendere U nella base dei sottogruppi aperti). Possiamo ora dimostrare il seguente teorema.

Teorema 9.18. *Sia R un sottoanello compatto e aperto dell'anello con divisione localmente compatto totalmente sconnesso D. Allora R è un anello locale. Posto $P = \operatorname{rad} R$, il quoziente R/P è un campo finito e $P = \{b \in R \mid b^n \to 0\}$. Inoltre $\{P^n \mid n = 1, 2, \ldots\}$ è una base di intorni di 0 in D.*

Dimostrazione. Sia $P = \{b \in R \mid bR \subsetneq R\}$. L'argomento che precede la proposizione 9.5 mostra che $b^n \to 0$ per ogni $b \in P$. Posto $N = R - P$, si ha $N = \{a \in R \mid aR = R\}$ ed N è un sottogruppo del gruppo moltiplicativo D^*, poiché ne è un sottomonoide e ogni suo elemento ha un inverso destro in N. Ne segue che, se $a \in R$ e $b \in P$, allora $ab, ba \in P$. Siano ora $b_1, b_2 \in P$ e supponiamo $a = b_1 + b_2 \notin P$. Allora $c_1 + c_2 = 1$, dove $c_i = b_i a^{-1} \in P$. Poiché gli ideali di R formano una base di intorni di 0 e $c_2^n \to 0$, la successione $1 + c_2,\ 1 + c_2 + c_2^2, \ldots$ è di Cauchy. Quindi in R esiste $1 + c_2 + c_2^2 + \cdots$, inverso di $1 - c_2 = c_1$. Si avrebbe $c_1^{-1}c_1 = 1 \in P$, contro la definizione di P. Dunque $b_1 + b_2 \in P$ se $b_i \in P$, e P è un ideale di R. Gli elementi di $N = R - P$ sono unità di R ed è chiaro che N ne è il gruppo delle unità. Quindi P è l'insieme dei non invertibili. Poiché P è un ideale, R è locale e P è il suo radicale. Essendo un ideale, P è aperto e R/P è finito. Per il teorema di Wedderburn (*BAI*, p. 453), l'anello con divisione R/P è un campo.

Abbiamo visto che gli ideali non nulli di R formano una base di intorni di 0. Per l'ultima affermazione basta pertanto mostrare che per ogni ideale non nullo B di R esiste n tale che $P^n \subseteq B$. Possiamo supporre B proprio. Allora $P \supseteq B$, poiché P è l'unico ideale massimale di R. Ora P/B è il radicale dell'anello finito R/B. Un anello finito è artiniano e il suo radicale è nilpotente. Dunque $(P/B)^n = 0$ per qualche intero n, ossia $P^n \subseteq B$. □

Sia R_1 un sottoanello compatto e aperto di D, sia P_1 il suo radicale e poniamo $R_2 = \{a \in D \mid aP_1 \subseteq P_1\}$. Allora R_2 è un sottoanello compatto e aperto di D che contiene R_1, e il suo radicale P_2 contiene P_1. Continuando il procedimento si ottiene una successione crescente di sottoanelli compatti $R_1 \subseteq R_2 \subseteq \cdots$ con radicali $P_1 \subseteq P_2 \subseteq \cdots$. Poniamo $R = \bigcup R_i$. Si tratta di un sottoanello aperto di D. Affermiamo che R/R_1 è finito. Altrimenti esisterebbero classi distinte $a_n + R_1$ con $a_n \in R$ per $n = 1, 2, 3, \ldots$. Supponiamo $a_n \to a$. Allora $a \in R$, poiché R è aperto e quindi chiuso. Dato che P_1 è un intorno di 0, esiste N tale che $a_n - a \in P_1$ per ogni $n \geq N$. Quindi $a_m - a_n \in P_1$ per $m, n > N$. Poiché $P_1 \subseteq R_1$, ciò dà $a_m + R_1 = a_n + R_1$, contro l'ipotesi che le classi siano distinte. Dunque $\{a_n\}$ non converge e, potendo sostituirle una qualunque sottosuccessione, si ha $a_n \to \infty$. Ne segue $a_n^{-1} \to 0$, sicché $a_n^{-1} \in P_1$ per n abbastanza grande, diciamo $n \geq N$. Dato che $R = \bigcup R_i$, esiste m tale che $a_N \in R_m$. Poiché $P_1 \subseteq P_m$, si avrebbe $1 = a_N a_N^{-1} \in P_m$. Ciò è impossibile, dunque R/R_1 è finito. Si ha $R_1/R_1 \subseteq R_2/R_1 \subseteq \cdots \subseteq R/R_1$ e, per la finitezza di R/R_1, risulta $R = R_m$ per qualche m. Abbiamo così dimostrato l'esistenza di un sottoanello compatto e aperto R di D il cui radicale P soddisfa

$$R = \{a \in D \mid aP \subseteq P\}. \tag{31}$$

Teorema 9.19. *Sia R un sottoanello compatto e aperto di D tale che (31) valga per il radicale P di R. Allora R è un anello di valutazione, nel senso che, se $a \in D$ e $a \notin R$, allora $a^{-1} \in R$. Inoltre R è massimale fra i sottoanelli compatti e aperti di D ed è l'unico sottoanello con queste proprietà.*

Dimostrazione. Se $a \notin R$, esiste $b_1 \in P$ tale che $ab_1 \notin P$. Se $ab_1 \notin R$, ripetiamo il procedimento.

Si ottengono infine n elementi $b_i \in P$ tali che $ab_1 \cdots b_n \in R - P$. Altrimenti si avrebbe una successione infinita $\{b_k\} \subseteq P$ con $ab_1 \cdots b_k \notin R$. Ma $\{P^n\}$ è una base di intorni di 0, quindi $\lim b_1 \cdots b_k = 0$ e perciò $\lim ab_1 \cdots b_k = 0$, contro $ab_1 \cdots b_k \notin R$ per ogni k. Abbiamo dunque un n tale che $ab_1 \cdots b_n = u$ è un'unità di R, donde $a^{-1} = b_1 \cdots b_n u^{-1} \in P \subseteq R$. Pertanto R è un anello di valutazione di D. Abbiamo pure dimostrato che, se $a \notin R$, si ha $a^{-1} \in P$ e, poiché $b^n \to 0$ per ogni $b \in P$, si ha $a^n \to \infty$ se $a \notin R$. Se $u \in R - P$, allora u^n non tende né a ∞ né a 0. Infatti $R - P$ è compatto, sicché ogni successione di potenze $\{u^{n_i}\}$ contiene una sottosuccessione convergente a un elemento di $R - P$, dunque non nullo. Da queste proprietà delle potenze risulta che

$$P = \{b \in D \mid b^n \to 0\}, \qquad R = \{a \in D \mid a^n \not\to \infty\}, \qquad D - R = \{a \in D \mid a^n \to \infty\}.$$

Se R' è un qualunque sottoanello compatto e aperto di D, allora $R' \cap (D - R) = \varnothing$, ossia $R' \subseteq R$. Dunque R è massimale ed è l'unico sottoanello compatto e aperto massimale di D. □

Possiamo usare l'anello di valutazione R per definire un valore assoluto su D (con la stessa definizione che per i campi). Abbiamo $\bigcap P^n = 0$. Per ogni $a \neq 0$ in R esiste quindi $k \geq 0$ tale che $a \in P^k - P^{k+1}$, dove $P^0 = R$. Definiamo $v(a) = k$. Se $a \notin R$, allora $a^{-1} \in P$ e poniamo $v(a) = -v(a^{-1})$. Poniamo inoltre $v(0) = \infty$ e $|a| = c^{v(a)}$, con c reale fissato, $0 < c < 1$. Vale il seguente teorema.

Teorema 9.20. *$|\cdot|$ è un valore assoluto non archimedeo su D. Si ha $|a| \geq 0$, con $|a| = 0$ se e solo se $a = 0$, e inoltre $|a + b| \leq \max(|a|, |b|)$ e $|ab| = |a||b|$.*

Dimostrazione. Basta dimostrare le corrispondenti affermazioni per v a valori in $\mathbb{Z} \cup \{\infty\}$, ossia $v(a) = \infty$ se e solo se $a = 0$, $v(a + b) \geq \min(v(a), v(b))$ e $v(ab) = v(a) + v(b)$. La prima è chiara dalla definizione. Siano $a, b \in D$ tali che $v(a) = v(b) = k \geq 0$ con k finito. Se $ab^{-1} \in P$, allora $a \in Pb \subseteq P^{k+1}$, contro $v(a) = k$. Perciò $ab^{-1} \notin P$ e analogamente $ba^{-1} \notin P$. Ne segue $ab^{-1} \in R - P$ e $v(ab^{-1}) = 0$. Se $v(a) = v(b) = k < 0$, si ha $v(a^{-1}) = v(b^{-1}) = -k > 0$, e di nuovo $v(ab^{-1}) = 0$. Scegliamo $\pi \in P - P^2$. Allora $\pi^k \in P^k$ per $k > 0$, dunque $v(\pi^k) \geq k$. Se $v(\pi^k) = l > k$, si può scrivere $\pi^k = \sum_j b_1^{(j)} \cdots b_l^{(j)}$ con $b_i^{(j)} \in P$ e ogni $b_1^{(j)} \notin P^2$, sicché $v(b_1^{(j)}) = 1 = v(\pi)$. Allora

$$\pi^{k-1} = \sum_j (\pi^{-1} b_1^{(j)}) b_2^{(j)} \cdots b_l^{(j)}, \qquad \pi^{-1} b_1^{(j)} \in R - P.$$

Quindi $v(\pi^{k-1}) > k - 1$. Si giunge così alla contraddizione $v(\pi) > 1$. Dunque $v(\pi^k) = k$. Insieme al risultato precedente ciò mostra che, se $v(a) = k \neq \infty$, esiste $u \in R - P$ tale che $a = u\pi^k$.

Osserviamo che la caratterizzazione degli insiemi P, $R - P$ e $D - R$ mediante le successioni di potenze dei loro elementi mostra che questi insiemi sono stabili per gli automorfismi interni di D. Siano $a, b \neq 0$ e $v(a) = k$, $v(b) = l \geq k$. Allora $a = u\pi^k$, $b = v\pi^l$, con u, v unità di R. Abbiamo $a + b = (u + v\pi^{l-k})\pi^k$ e $u + v\pi^{l-k} \in R$, dunque $v(a + b) \geq k = \min(v(a), v(b))$. Inoltre $ab = u\pi^k v\pi^l = uv'\pi^{k+l}$ con $v' = \pi^k v \pi^{-k} \in R - P$. Se $k + l > 0$, abbiamo visto che $\pi^{k+l} \in P^{k+l} - P^{k+l+1}$. Le stesse relazioni valgono per ab, perciò $v(ab) = k + l = v(a) + v(b)$. Ciò è chiaro anche per $k + l = 0$. Se invece $k + l < 0$, allora $(ab)^{-1} = b^{-1}a^{-1} = \pi^{-(k+l)}w$ con $w \in R - P$. Dunque $v((ab)^{-1}) = -(k + l)$ e ancora $v(ab) = k + l = v(a) + v(b)$. In ogni caso $v(ab) = v(a) + v(b)$. Abbiamo così le due relazioni $v(a+b) \geq \min(v(a), v(b))$ e $v(ab) = v(a)+v(b)$ per $a, b \neq 0$. Esse sono evidenti se $a = 0$ oppure $b = 0$, quindi valgono per tutti gli a, b. □

La definizione di $|\cdot|$ mostra che l'intorno sferico di 0 definito da $|a| \leq c^k$, con $k \geq 0$, è P^k. Dunque la topologia definita dalla valutazione coincide con quella data su D. Ne segue anche che D è completo rispetto a $|\cdot|$.

Sia F un sottocampo chiuso di D tale che $P_F = P \cap F \neq 0$. Allora il valore assoluto è non banale su F e F è completo. Inoltre, posto $R_F = R \cap F$, il campo R_F/P_F è isomorfo a un

sottocampo di R/P. Quindi R_F/P_F è finito e F è un campo locale. Si applicano pertanto i risultati del § 9.12.

Sia p la caratteristica di $\overline{R} = R/P$. Allora $|\overline{R}| = q = p^m$ con $m \geq 1$. Sia $\zeta_0 \in R$ tale che $\overline{\zeta}_0 = \zeta_0 + P$ sia una radice primitiva $(q-1)$-esima dell'unità. Mostreremo che R contiene un elemento ζ tale che $\zeta^{q-1} = 1$ e $\overline{\zeta} = \overline{\zeta}_0$. Allora ζ sarà una radice primitiva $(q-1)$-esima dell'unità in R. Si ha $\zeta_0^{q-1} - 1 \in P$ e, se $\zeta_0^{q-1} = 1$, possiamo prendere $\zeta = \zeta_0$. Altrimenti sia F la chiusura in D di $C(\zeta_0)$, dove C è il centro di D. Allora $P_F = P \cap F$ contiene $\zeta_0^{q-1} - 1 \neq 0$, dunque $P_F \neq 0$. Se $R_F = F \cap R$, allora $\overline{R}_F = R_F/P_F$ contiene $\zeta_0 + P_F$, che è una radice primitiva $(q-1)$-esima dell'unità. Per i risultati del paragrafo precedente R_F contiene un elemento ζ tale che $\zeta^{q-1} = 1$ e $\zeta + P_F = \zeta_0 + P_F$. Allora $\overline{\zeta} = \overline{\zeta}_0$.

Abbiamo visto che R e P sono stabili per gli automorfismi interni di D. Quindi ogni automorfismo interno determina un automorfismo di $\overline{R} = R/P$. In particolare, se $\pi \in P - P^2$, si ha l'automorfismo

$$\overline{\eta} : \bar{a} = a + P \longmapsto \overline{\pi a \pi^{-1}} \tag{32}$$

di $\overline{R} = R/P$. Poiché $|\overline{R}| = q = p^m$, esso ha la forma

$$\bar{a} \longmapsto \bar{a}^s, \qquad s = p^i. \tag{33}$$

Se invece $u \in R - P$, allora $\bar{u}\bar{a} = \bar{a}\bar{u}$ e $\overline{uau^{-1}} = \bar{a}$. Il corrispondente automorfismo di $\overline{R}$ è quindi l'identità. La condizione $\pi \in P - P^2$ determina π a meno di un fattore in $R - P$, perciò $\overline{\eta}$ è indipendente dalla scelta di π in $P - P^2$.

Mostreremo che si può scegliere π in modo che

$$\pi \zeta \pi^{-1} = \zeta^s. \tag{34}$$

Sia $G = \langle \zeta \rangle$, il sottogruppo di D^* generato da ζ. Se $\pi_0 \in P - P^2$ e $\lambda \in G$, allora $\overline{\pi_0 \lambda \pi_0^{-1}} = \bar{\lambda}^s$, quindi $\lambda^{-s} \pi_0 \lambda \pi_0^{-1} \equiv 1 \pmod{P}$ e $\lambda^{-s} \pi_0 \lambda \equiv \pi_0 \pmod{P^2}$. Allora

$$\pi = \sum_{\lambda \in G} \lambda^{-s} \pi_0 \lambda \tag{35}$$

soddisfa $\rho^{-s} \pi \rho = \pi$ per $\rho \in G$. Inoltre $\pi \equiv (q-1)\pi_0 \pmod{P^2}$ e, poiché $q1 \in P$, si ha $\pi \equiv -\pi_0 \pmod{P^2}$, quindi $\pi \in P - P^2$. Dall'uguaglianza $\rho^{-s} \pi \rho = \pi$ segue $\pi \rho \pi^{-1} = \rho^s$ per $\rho \in G$, e in particolare vale (34).

L'automorfismo interno $a \mapsto \pi a \pi^{-1}$ stabilizza G e induce $\overline{\eta}$ su $\overline{R}$. Poiché $\lambda \mapsto \bar{\lambda}$ è un isomorfismo di G sul gruppo moltiplicativo $\overline{R}^*$, la restrizione a G di $a \mapsto \pi a \pi^{-1}$ ha lo stesso ordine r di $\overline{\eta}$. Quindi π^r commuta con ogni $\lambda \in G$ ed è la minima potenza positiva di π con questa proprietà.

La dimostrazione delle pp. 571–572 mostra che ogni elemento di D si rappresenta mediante una serie di potenze in π con coefficienti in $K = \{0\} \cup G$. Più precisamente ogni elemento non nullo di D si scrive in uno e un solo modo come serie

$$a = (\lambda_0 + \lambda_1 \pi + \lambda_2 \pi^2 + \cdots) \pi^{-k}, \tag{36}$$

dove $\lambda_i \in K$, $\lambda_0 \neq 0$ e $k \in \mathbb{Z}$.[39] Ne risulta che un elemento a sta nel centro se e solo se commuta con π e con ogni $\lambda \in G$. Quindi il centro C è costituito dagli elementi

$$c = (\mu_0 + \mu_1 \pi^r + \mu_2 \pi^{2r} + \cdots) \pi^{-kr}, \tag{37}$$

[39]Nell'originale si legge $k \geq 1$. Poiché $-k = v(a)$, la rappresentazione enunciata per ogni $a \neq 0$ richiede $k \in \mathbb{Z}$.

dove i μ_i sono gli elementi di K tali che $\mu_i^s = \mu_i$. Evidentemente $C \cap P \neq 0$ e C è un campo locale. Il campo di estensione $W = C(\zeta)$ è stabile per l'automorfismo interno determinato da π. Detto σ l'automorfismo indotto in W/C, il campo C è l'insieme degli elementi fissi per σ. Dunque W/C è ciclica, con gruppo di Galois $\langle\sigma\rangle$. È chiaro inoltre che σ ha ordine r. Pertanto $[W : C] = r$. Poiché W è l'insieme degli elementi

$$b = (\lambda_0 + \lambda_1\pi^r + \lambda_2\pi^{2r} + \cdots)\pi^{-kr}, \tag{38}$$

con $\lambda_i \in K$,[40] l'indice di ramificazione di W su C è 1, perciò W è un'estensione non ramificata di C. Confrontando (36) e (38) si vede che ogni elemento di D si scrive in uno e un solo modo nella forma

$$w_0 + w_1\pi + \cdots + w_{r-1}\pi^{r-1}, \qquad w_i \in W. \tag{39}$$

La moltiplicazione in D è determinata da quella in W e dalle relazioni seguenti per $w \in W$,

$$\pi w = \sigma(w)\pi, \qquad \pi^r \in C. \tag{40}$$

Dunque D è un'algebra ciclica $D = (W, \sigma, \pi^r)$ e $[D : C] = r^2$. Abbiamo così dimostrato il seguente teorema di struttura per gli anelli con divisione localmente compatti totalmente sconnessi.

Teorema 9.21. *Sia D un anello con divisione localmente compatto totalmente sconnesso. Il centro C di D è un campo locale e D è un'algebra ciclica (W, σ, γ) su C, dove W è non ramificato e γ è un generatore dell'ideale massimale P_C dell'anello di valutazione di C.*

Naturalmente ciò mostra che D è un'algebra di dimensione finita su un campo locale. Abbiamo anche visto che un campo locale è un campo di serie di Laurent su un campo finito, oppure un'estensione di dimensione finita di un campo di numeri p-adici (teorema 9.16, p. 597). Pertanto D è un'algebra con divisione di dimensione finita su un campo di serie formali di Laurent $F_0((x))$, con F_0 finito, oppure un'algebra con divisione di dimensione finita su qualche campo p-adico $\mathbb{Q}_p$. Il primo caso si verifica se e solo se la caratteristica di D è un numero primo. Abbiamo inoltre visto che la topologia è quella del valore assoluto definito dall'unico sottoanello compatto e aperto massimale R di D. Si vede facilmente che questa topologia coincide con la topologia prodotto ottenuta considerando D come prodotto di un numero finito di copie di $F_0((x))$ oppure di $\mathbb{Q}_p$.

Non è difficile dimostrare il seguente inverso del teorema 9.21. Sia D un'algebra con divisione di dimensione finita su $F_0((x))$ o su $\mathbb{Q}_p$. Allora si può introdurre in D una topologia che ne faccia un anello con divisione non discreto, totalmente sconnesso e localmente compatto. Accenniamo alla dimostrazione. Sia $F = F_0((x))$ oppure $\mathbb{Q}_p$. Su F abbiamo la topologia di un valore assoluto definito come sopra, l'anello di valutazione R e il suo ideale massimale P (nel primo caso $R = F_0[[x]]$, nel secondo R è l'anello degli interi p-adici). Ora R si può considerare come limite inverso degli anelli finiti R/P^k (si veda p. 73), e la sua topologia si identifica con la topologia del limite inverso di insiemi finiti. Pertanto R è compatto e totalmente sconnesso. Ne segue che F è localmente compatto, totalmente sconnesso e non discreto. La continuità dell'applicazione $x \mapsto x^{-1}$ di F^* in sé si dimostra come nel caso del campo $\mathbb{R}$.

Sia ora A un'algebra di dimensione finita su F, munita della topologia prodotto. Allora A è localmente compatta, totalmente sconnessa e non discreta. Si vede subito che A è un anello topologico. Indichiamo con $N(a)$ il determinante della matrice $\rho(a)$ in una rappresentazione regolare di A. L'applicazione $a \mapsto N(a)$ di A in F è continua e l'insieme U degli elementi invertibili di A è l'aperto definito da $N(u) \neq 0$. Si vede facilmente che $u \mapsto u^{-1}$ è un'applicazione continua di U in sé. Nel caso particolare in cui $A = D$ sia un'algebra con divisione su F, si ha $U = D^*$ e A è un anello topologico con divisione nel senso definito all'inizio.

[40] La stampa indica $\lambda_i \in R$. Qui si tratta dei rappresentanti K introdotti prima della (36).

9.14 Il gruppo di Brauer di un campo locale

Applicheremo ora il teorema 9.21, le osservazioni che lo seguono e i risultati sulle algebre cicliche dati nel ğ 8.5 (p. 484) per determinare il gruppo di Brauer $\mathrm{Br}(F)$ di un campo locale F. Ricordiamo che, se E è un'estensione ciclica di un campo F, il sottogruppo del gruppo di Brauer di F costituito dalle classi delle algebre semplici centrali A di dimensione finita che hanno E come campo di spezzamento è isomorfo a $F^*/N(E^*)$, dove $N(E^*)$ è il gruppo delle norme $N_{E/F}(a)$ degli elementi non nulli $a \in E$. Si realizza l'isomorfismo scegliendo un generatore s di $G = \mathrm{Gal}(E/F)$ e definendo l'algebra ciclica (E, s, γ), $\gamma \in F^*$. Allora l'applicazione che manda $\gamma N(E^*)$ in $[(E, s, \gamma)]$, la classe di similitudine di (E, s, γ), è un isomorfismo di $F^*/N(E^*)$ sul gruppo di Brauer relativo $\mathrm{Br}(E/F)$. Sia K un sottocampo di E/F e sia $\bar{s}$ la restrizione di s a K. Allora $\bar{s}$ è un generatore del gruppo di Galois di K/F. Il suo ordine è $[K : F] = r$, e si ha $n = rm$, dove $n = [E : F]$ e $m = [E : K]$. Ogni algebra semplice centrale spezzata da K è spezzata da E e abbiamo il monomorfismo di $\mathrm{Br}(K/F)$ in $\mathrm{Br}(E/F)$ che manda la classe di $(K, \bar{s}, \gamma)$ in quella di (E, s, γ^m) (p. 485).

Sia ora F un campo locale. Determiniamo anzitutto il gruppo $F^*/N(W^*)$, dove W è un'estensione non ramificata di F. Ci occorrerà il seguente risultato.

Lemma. *Sia F_q un campo finito con q elementi e sia F_{q^n} un suo campo di estensione con q^n elementi. Ogni $a \in F_q^*$ è la norma di un elemento $b \in F_{q^n}^*$ che non è contenuto in alcun sottocampo proprio di F_{q^n} contenente F_q.*

Dimostrazione. L'automorfismo $x \mapsto x^q$ genera il gruppo di Galois di F_{q^n}/F_q. L'applicazione norma su $F_{q^n}^*$ è quindi

$$x \longmapsto x x^q \cdots x^{q^{n-1}} = x^{(q^n-1)/(q-1)}.$$

Il nucleo di questa applicazione è l'insieme degli elementi tali che $N_{F_{q^n}/F_q}(x) = 1$ e ha ordine $(q^n-1)/(q-1)$. Quindi l'immagine ha ordine $q-1$. Poiché essa è contenuta in F_q^*, che ha ordine $q-1$, è chiaro che l'applicazione norma di $F_{q^n}^*$ è suriettiva su F_q^*. Inoltre, per ogni $a \in F_q^*$, esistono $(q^n-1)/(q-1)$ elementi b tali che $N_{F_{q^n}/F_q}(b) = a$. D'altra parte, gli elementi b contenuti in sottocampi propri di F_{q^n} su F_q sono contenuti in sottocampi propri massimali. La cardinalità di ciascuno di questi è della forma q^m, dove m è un divisore proprio massimale di n, e sottocampi distinti hanno ordini distinti. Ne segue che il numero degli elementi non nulli contenuti nei sottocampi propri non supera $\sum_m (q^m - 1)$, dove la somma è estesa ai divisori propri massimali m di n. Questo numero è evidentemente minore di $(q^n-1)/(q-1) = 1 + q + \cdots + q^{n-1}$. Esiste dunque un $b \in F_{q^n}$ che non appartiene ad alcuno di quei sottocampi e per il quale $N_{F_{q^n}/F_q}(b) = a$. □

La condizione che b non sia contenuto in alcun sottocampo proprio di F_{q^n} su F_q equivale a $F_q(b) = F_{q^n}$. Ciò accade se e soltanto se il grado del polinomio minimo di b su F_q è n. Possiamo ora dimostrare la proposizione seguente.

Proposizione 9.8. *Sia W un'estensione non ramificata del campo locale F, sia R_F l'anello di valutazione di F e sia P_F il suo ideale degli elementi non invertibili. Allora ogni elemento $u \in R_F \setminus P_F$ è una norma da W.*

Dimostrazione. Sia $\bar{R}_F$ il campo residuo R_F/P_F e sia analogamente $\bar{R}_W = R_W/P_W$, dove R_W è l'anello di valutazione di W e P_W il suo ideale degli elementi non invertibili. Poiché W è non ramificata, abbiamo $[\bar{R}_W : \bar{R}_F] = n = [W : F]$. Per il lemma, posto $a = \bar{u} = u + P_F$, esiste $b \in \bar{R}_W$ tale che il polinomio minimo di b su $\bar{R}_F$ abbia grado n e $N_{\bar{R}_W/\bar{R}_F}(b) = a$. Se $\sigma \in \mathrm{Gal}(W/F)$, l'applicazione $\bar{\sigma}\colon \bar{x} \mapsto \overline{\sigma x}$, $x \in R_W$, appartiene a $\mathrm{Gal}(\bar{R}_W/\bar{R}_F)$, e $\sigma \mapsto \bar{\sigma}$ è un isomorfismo fra questi gruppi di Galois. Pertanto per ogni $v \in R_W$ si ha $\overline{N_{W/F}(v)} = N_{\bar{R}_W/\bar{R}_F}(\bar{v})$. Scegliendo $v \in R_W$ tale che $\bar{v} = b$, otteniamo quindi $\overline{N_{W/F}(v)} = a = \bar{u}$. Possiamo scegliere un

polinomio monico $f(x) \in R_F[x]$ di grado n tale che $\bar{f}(x)$ sia il polinomio minimo di $\bar{v} = b$. Poiché $\deg \bar{f}(x) = n$, questo è il polinomio caratteristico di b nella rappresentazione regolare e il suo termine costante è $(-1)^n N_{\bar{R}_W/\bar{R}_F}(\bar{v}) = (-1)^n \bar{u}$. Possiamo dunque supporre che il termine costante di $f(x)$ sia $(-1)^n u$. Poiché $\bar{f}(x)$ è separabile, possiamo applicare il lemma di Hensel e concludere che esiste un $v \in R_W$ tale che $f(v) = 0$. Poiché $\bar{f}(x)$ è irriducibile su $\bar{R}_F$, $f(x)$ è irriducibile in $F[x]$ ed è quindi il polinomio minimo di v su F. Avendo grado n, è anche il suo polinomio caratteristico. Il termine costante soddisfa dunque $(-1)^n u = (-1)^n N_{W/F}(v)$. Allora $u = N_{W/F}(v)$, come richiesto. □

Poiché W è non ramificata su F, possiamo scegliere $\pi \in F$ tale che $\pi \in P_W \setminus P_W^2$. Ogni $w \in W^*$ è allora della forma $u\pi^k$, con $u \in R_W \setminus P_W$ e $k \in \mathbb{Z}$. Si ha quindi $N_{W/F}(u\pi^k) = N_{W/F}(u)\pi^{kn}$ e $N_{W/F}(u) \in R_F \setminus P_F$. Viceversa, se $v = u\pi^{kn}$ con $u \in R_F \setminus P_F$, allora $\pi^{kn} = N_{W/F}(\pi^k)$ e la proposizione 9.8 mostra che u è una norma. Quindi v è una norma. Da questi risultati è chiaro che $F^*/N(W^*)$ è un gruppo ciclico di ordine n con generatore $\pi N(W^*)$. Allora $\mathrm{Br}(W/F)$ è un gruppo ciclico di ordine n. Otteniamo un isomorfismo fra $F^*/N(W^*)$ e $\mathrm{Br}(W/F)$ mandando la classe laterale $\pi^k N(W^*)$, $0 \leq k \leq n-1$, nella classe di algebre semplici centrali su F determinata dall'algebra ciclica (W, σ, π^k), dove σ è l'automorfismo di Frobenius di W/F.

Possiamo combinare questo risultato con quelli del paragrafo precedente per determinare $\mathrm{Br}(F)$. Si ha infatti il teorema seguente.

Teorema 9.22 (Hasse). *Il gruppo di Brauer di un campo locale è isomorfo al gruppo additivo dei numeri razionali modulo* 1*, ossia a* $\mathbb{Q}/\mathbb{Z}$.

Dimostrazione. Abbiamo visto che ogni algebra con divisione centrale D di dimensione finita sul campo locale F è un anello con divisione localmente compatto e totalmente sconnesso. Il teorema 9.21 mostra quindi che D ha come campo di spezzamento un'estensione non ramificata (e dunque ciclica) W/F. Ne segue che ogni classe $[A]$ di $\mathrm{Br}(F)$ è contenuta in $\mathrm{Br}(W/F)$ per qualche W. Allora $A \sim (W, \sigma, \pi^k)$, dove σ è l'automorfismo di Frobenius e $0 \leq k < n = [W : F]$. Scelto W, k è univocamente determinato. Mandiamo ora $[A]$ nel numero razionale $r = k/n$.

Vogliamo mostrare che il razionale così determinato è indipendente dalla scelta del campo di spezzamento. Dai risultati del ğ 9.12 si vede facilmente che per ogni intero positivo n esiste, a meno di isomorfismi, un'unica estensione non ramificata W/F con $[W : F] = n$. Inoltre, se W'/F è non ramificata e $[W' : F] = m$, allora W' è isomorfo a un sottocampo di W se e soltanto se $m \mid n$. Ne segue che basta mostrare che, se $W' \subseteq W$ è un campo di spezzamento di A, il numero razionale determinato da W' è lo stesso di quello determinato da W. Ora la restrizione $\bar{\sigma}$ a W' dell'automorfismo di Frobenius σ di W/F è l'automorfismo di Frobenius di W'/F. Quindi $A \sim (W', \bar{\sigma}, \pi^l)$ con $0 \leq l < m$, e il numero razionale determinato da A e da W' è l/m. Poiché $(W', \bar{\sigma}, \pi^l) \sim (W, \sigma, \pi^{ln/m}) \sim (W, \sigma, \pi^k)$, si ha $ln/m = k$ e $k/n = l/m$.

È chiaro inoltre che la nostra applicazione è suriettiva sull'insieme dei razionali $0 \leq r < 1$. Infatti $r = k/n$ con $0 \leq k < n$ e, se prendiamo come W l'estensione non ramificata di grado n su F, l'algebra ciclica (W, σ, π^k) è semplice centrale con campo di spezzamento W e viene mandata in $r = k/n$. Date due algebre semplici centrali A e B su F, possiamo scegliere un'estensione non ramificata W che sia campo di spezzamento per entrambe. Allora $A \sim (W, \sigma, \pi^k)$ e $B \sim (W, \sigma, \pi^l)$ con $0 \leq k, l < n$, e

$$A \otimes B \sim (W, \sigma, \pi^{k+l}) \sim (W, \sigma, \pi^m),$$

dove $0 \leq m < n$ e $m/n \equiv (k + l)/n \pmod{\mathbb{Z}}$. Ne segue che l'applicazione $\{A\} \mapsto (k/n) + \mathbb{Z}$ è un isomorfismo di $\mathrm{Br}(F)$ su $\mathbb{Q}/\mathbb{Z}$. □

Un'altra conseguenza importante dei nostri risultati è il teorema seguente.

Teorema 9.23. *L'esponente di un'algebra semplice centrale di dimensione finita su un campo locale coincide con il suo indice.*

Dimostrazione. Dobbiamo mostrare che, se D è un'algebra con divisione centrale su un campo locale F tale che $[D : F] = n^2$, allora l'ordine di $\{D\}$ è n. Per il teorema 9.21, $D = (W, \tau, \pi)$, dove τ è un generatore del gruppo di Galois di W/F e $\pi \in P_F \setminus P_F^2$. Allora l'esponente di D è l'ordine di $\pi N(W^*)$, che è evidentemente n. □

9.15 Forme quadratiche sui campi locali

Definiremo anzitutto un invariante, l'*invariante di Hasse*, di una forma quadratica non degenere su uno spazio vettoriale di dimensione finita su un campo qualsiasi F di caratteristica diversa da 2. Seguiremo un metodo dovuto a Witt, apparso in un suo bellissimo lavoro sulle forme quadratiche nel volume 176 (1937) del *Journal* di Crelle.

La definizione e le proprietà dell'invariante di Hasse si basano sulle algebre di quaternioni e sulle algebre di Clifford. Occorre richiamare alcuni risultati sulle algebre di quaternioni e ricavare alcune formule per i loro prodotti tensoriali. Abbiamo denotato con (a, b) l'algebra di quaternioni generata da due elementi i, j che soddisfano le relazioni

$$i^2 = a, \qquad j^2 = b, \qquad ij = -ji, \tag{41}$$

dove a e b sono elementi non nulli di F (p. 232). Nel trattare i prodotti tensoriali di algebre di quaternioni abbrevieremo $(a, b) \otimes_F (c, d)$ in $(a, b)(c, d)$ e, come di consueto, useremo $\sim$ per la similitudine di algebre semplici centrali. Si ha evidentemente

$$(a, b) \simeq (b, a). \tag{i}$$

È chiaro altresì che

$$(a, b) \simeq (as^2, bt^2) \tag{ii}$$

per $s \neq 0$, $t \neq 0$ qualsiasi.

Un'algebra di quaternioni (a, b) è un'algebra con divisione oppure si ha $(a, b) \simeq M_2(F)$, ossia $(a, b) \sim 1$ nel gruppo di Brauer $\mathrm{Br}(F)$. È evidente che $(1, b) \sim 1$ e quindi

$$(a^2, b) \sim 1. \tag{iii}$$

L'algebra (a, b) ha base $(1, i, j, k = ij)$. Se $x = x_0 + x_1 i + x_2 j + x_3 k$ e

$$T(x) = 2x_0, \qquad N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2, \tag{42}$$

allora $x^2 - T(x)x + N(x) = 0$. Con $(a, b)_0$ denotiamo il sottospazio degli elementi di traccia zero, $T(x) = 0$. Esso ha base (i, j, k) e la sua forma quadratica norma è $N(x) = -ax_1^2 - bx_2^2 + abx_3^2$. È chiaro che $(a, b) \sim 1$ se e soltanto se (a, b) contiene un elemento $z \neq 0$ tale che $z^2 = 0$. Ciò accade se e soltanto se esiste $z \neq 0$ con $T(z) = 0 = N(z)$. Quindi $(a, b) \sim 1$ se e soltanto se la forma quadratica norma su $(a, b)_0$ è *isotropa*, ossia se $-ax_1^2 - bx_2^2 + abx_3^2 = 0$ ha una soluzione diversa da $(0, 0, 0)$. Ne segue evidentemente

$$(a, -a) \sim 1. \tag{iv}$$

Poiché gli elementi non nulli di $(a, b)_0$ si possono caratterizzare come gli $x \in (a, b)$ tali che $x \notin F$ e $x^2 \in F$, è chiaro che un isomorfismo di (a, b) su (c, d) manda $(a, b)_0$ su $(c, d)_0$. Ne segue che, se $(a, b) \simeq (c, d)$, le forme quadratiche $-ax_1^2 - bx_2^2 + abx_3^2$ e $-cx_1^2 - dx_2^2 + cdx_3^2$ sono equivalenti. È facile applicare la teoria delle algebre di composizione per dimostrare il viceversa (si veda l'esercizio 2, p. 450 di BAI).

Se a non è un quadrato, abbiamo il campo $Z = F(\sqrt{a})$ e il suo automorfismo σ tale che $\sigma(\sqrt{a}) = -\sqrt{a}$. L'algebra di quaternioni (a, b) coincide allora con l'algebra ciclica (Z, σ, b) (p. 480). La formula del prodotto per le algebre cicliche (p. 475) dà quindi

$$(a, b)(a, c) \sim (a, bc) \tag{v}$$

se a non è un quadrato. La formula vale evidentemente anche se a è un quadrato, perché in tal caso tutte e tre le algebre sono simili a 1. Poiché $(a, b)(a, b) \sim 1$,

$$(a, a)(b, b) \sim (a, a)(a, b)(b, b)(a, b) \sim (a, ab)(b, ab) \sim (ab, ab).$$

Dunque

$$(a, a)(b, b) \sim (ab, ab). \tag{vi}$$

Iterando questa formula si ottiene

$$(a_1, a_1)(a_2, a_2) \cdots (a_r, a_r) \sim (a_1 \cdots a_r, a_1 \cdots a_r). \tag{vi$'$}$$

Consideriamo ora una forma quadratica Q su uno spazio vettoriale V di dimensione n su un campo F di caratteristica diversa da 2. La forma bilineare simmetrica associata B è definita da $B(x, y) = Q(x + y) - Q(x) - Q(y)$. Si ha allora $Q(x) = \frac{1}{2}B(x, x)$. Supporremo sempre che Q sia non degenere nel senso che B è non degenere. Definiamo il *discriminante* di Q come il discriminante di $\frac{1}{2}B$. Se $(v_1, \ldots, v_n)$ è una base ortogonale di V rispetto a Q (ossia rispetto a B), il discriminante $d = d(Q)$ determinato da questa base è dunque $\prod_{i=1}^{n}(\frac{1}{2}B(v_i, v_i)) = \prod_{i=1}^{n} Q(v_i)$.

Definiremo ora l'invariante di Hasse di Q come un certo elemento del gruppo di Brauer $\mathrm{Br}(F)$. Se $n = 1$, l'elemento è l'unità 1 di $\mathrm{Br}(F)$. Se $n > 1$, definiamo l'*invariante di Hasse di Q rispetto a una base ortogonale* $(v_1, \ldots, v_n)$ come l'elemento di $\mathrm{Br}(F)$ determinato dal prodotto tensoriale

$$\prod_{i<j}(Q(v_i), Q(v_j)). \tag{43}$$

Mostriamo che esso è indipendente dalla scelta della base ortogonale.

Proposizione 9.9. *Siano $(v_1, \ldots, v_n)$ e $(v_1', \ldots, v_n')$ basi ortogonali di V rispetto a Q. Allora*

$$\prod_{i<j}(Q(v_i), Q(v_j)) \sim \prod_{i<j}(Q(v_i'), Q(v_j')). \tag{44}$$

Dimostrazione (Witt). Sia U uno spazio vettoriale di dimensione n munito di una forma quadratica P per la quale esista una base ortogonale $(u_1, \ldots, u_n)$ tale che $P(u_i) = -1$, $1 \leq i \leq n$. Formiamo $W = U \oplus V$ e definiamo su W una forma quadratica R con $R(u + v) = P(u) + Q(v)$, $u \in U$, $v \in V$. Allora $W = U \perp V$ e le restrizioni di R a U e V sono rispettivamente P e Q. Mostreremo che, per ogni base ortogonale $(v_1, \ldots, v_n)$ di V, vale

$$\prod_{i<j}(Q(v_i), Q(v_j)) \sim C(W, R) \otimes_F (d, d), \tag{45}$$

dove $C(W, R)$ è l'algebra di Clifford di R e d è un discriminante di Q. È evidente che ne seguirà la (44). Poniamo $a_i = Q(v_i)$, $d_i = \prod_{j=1}^{i} a_j$, cosicché $d_n = d$. Mostriamo prima che

$$C(W, R) \simeq \prod_{i=1}^{n}(a_i, d_i). \tag{46}$$

Sappiamo che $C(W,R)$ è un'algebra semplice centrale generata dagli u_i, v_i, $1 \le i \le n$, e che valgono le relazioni $u_i^2 = -1$, $v_i^2 = a_i$, $u_i u_j = -u_j u_i$, $v_i v_j = -v_j v_i$ per $i \neq j$, e $u_i v_k = -v_k u_i$ per ogni i, k (pp. 229–230). Poniamo

$$w_1 = (v_1 u_1) \cdots (v_{n-1} u_{n-1}) v_n, \qquad w_2 = v_n u_n. \tag{47}$$

Poiché $(v_i u_i)^2 = -v_i^2 u_i^2 = a_i$, $(v_i u_i)(v_j u_j) = (v_j u_j)(v_i u_i)$, $v_n(v_i u_i) = (v_i u_i) v_n$ per $i < n$ e $v_n w_2 = -w_2 v_n$, si ha

$$w_1^2 = d = d_n, \qquad w_2^2 = a_n, \qquad w_1 w_2 = -w_2 w_1. \tag{48}$$

La sottoalgebra generata da w_1 e w_2 è dunque (a_n, d_n) e $C(W,R) \simeq (a_n, d_n) \otimes_F C'$, dove C' è il centralizzante in $C(W,R)$ della sottoalgebra generata da w_1 e w_2 (p. 233). Gli elementi u_i, v_i, $1 \le i \le n-1$, commutano con w_1 e w_2, e la sottoalgebra da essi generata è isomorfa all'algebra di Clifford $C(W', R')$, dove $W' = \sum_{j=1}^{n-1} F u_j + \sum_{j=1}^{n-1} F v_j$ e R' è la restrizione di R a W'. Poiché $[C(W',R') : F] = 2^{2(n-1)}$ e $[C' : F] = 2^{2n}/4 = 2^{2(n-1)}$, abbiamo $C' \simeq C(W',R')$ e $C(W,R) \simeq (a_n, d_n) \otimes C(W',R')$. La formula (46) segue ora per induzione su n. Da questa e dalle (v) e (vi′) si ricava

$$C(W,R) \sim \prod_{i \le j} (a_i, a_j) \sim (d,d) \prod_{i<j} (a_i, a_j). \tag{49}$$

Quindi $\prod_{i<j}(a_i, a_j) \sim C(W,R) \otimes (d,d)$. □

In virtù della proposizione 9.9 ha senso definire l'*invariante di Hasse* $s(Q)$ di Q come l'unità di $\mathrm{Br}(F)$ per $n = 1$ e, per $n > 1$, come l'elemento di $\mathrm{Br}(F)$ definito dalla (43).

L'invariante di Hasse è 1 oppure un elemento di ordine due del gruppo di Brauer. Se F è algebricamente chiuso o finito, $\mathrm{Br}(F) = 1$, sicché in tal caso l'invariante di Hasse è banale per ogni forma quadratica su F. Se $F = \mathbb{R}$ o è un campo locale, $\mathrm{Br}(F)$ ha un unico elemento di ordine due. Lo denoteremo con -1. Siano Q^+ e Q^- forme quadratiche rispettivamente definita positiva e definita negativa su uno spazio vettoriale di dimensione n su $\mathbb{R}$. Allora l'invariante di Hasse è $s(Q^\pm) = (\pm 1, \pm 1)^{n(n-1)/2} = (\pm 1)^{n(n-1)/2}$. Se $n \equiv 0 \pmod 4$, si ha $s(Q^+) = s(Q^-)$, ma le due forme non sono equivalenti. Mostreremo invece che il discriminante e l'invariante di Hasse costituiscono un sistema completo di invarianti per le forme quadratiche di dimensione fissata sui campi locali. Due tali forme sono equivalenti se e soltanto se hanno lo stesso discriminante e lo stesso invariante di Hasse.

Stabiliamo anzitutto alcuni risultati su campi base arbitrari di caratteristica diversa da 2.

Proposizione 9.10. *Sia $n \le 3$. Due forme quadratiche non degeneri su uno spazio vettoriale di dimensione n sono equivalenti se e soltanto se hanno lo stesso discriminante e lo stesso invariante di Hasse.*

Dimostrazione. La necessità della condizione è chiara, e la sufficienza è chiara per $n = 1$. Sia ora $n = 2$ e siano $\mathrm{diag}\{a,b\}$ e $\mathrm{diag}\{a',b'\}$ matrici diagonali delle due forme quadratiche. Supponiamo che $(a,b) \sim (a',b')$ e che ab e $a'b'$ differiscano per un fattore quadrato. Allora $(a,b) \simeq (a',b')$ e possiamo supporre che $ab = a'b'$. La condizione $(a,b) \sim (a',b')$ implica che le forme quadratiche $ax_1^2 + bx_2^2 - abx_3^2$ e $a'x_1^2 + b'x_2^2 - a'b'x_3^2$ siano equivalenti. Poiché $ab = a'b'$, dal teorema di cancellazione di Witt (BAI, p. 367) segue l'equivalenza di $ax_1^2 + bx_2^2$ e $a'x_1^2 + b'x_2^2$. Sia ora $n = 3$ e supponiamo $Q = ax_1^2 + bx_2^2 + cx_3^2$, $Q' = a'x_1^2 + b'x_2^2 + c'x_3^2$. Per ipotesi $(a,b)(a,c)(b,c) \sim (a',b')(a',c')(b',c')$ e $d = abc$ e $d' = a'b'c'$ differiscono per un fattore quadrato, sicché possiamo supporre $d = d'$. Basta mostrare che $-dQ$ e $-dQ'$, il cui discriminante è -1 modulo quadrati, sono equivalenti. Un semplice calcolo, che lasciamo per esercizio, mostra che $s(-dQ) \sim s(Q) \otimes (-d,-d)$. Dunque $s(-dQ) \sim s(-dQ')$ e basta provare il risultato per Q e Q'

di discriminante -1. Possiamo allora supporre $Q = ax_1^2 + bx_2^2 - abx_3^2$ e $Q' = a'x_1^2 + b'x_2^2 - a'b'x_3^2$. Ne segue

$$s(Q) = (a,b)(a,-ab)(b,-ab) \sim (a,b)(ab,-ab) \sim (a,b).$$

Dunque $(a,b) \simeq (a',b')$. Poiché Q e Q' sono rispettivamente gli opposti delle forme norma su $(a,b)_0$ e su $(a',b')_0$, ne segue che Q e Q' sono equivalenti. □

Dimostriamo ora la proposizione seguente.

Proposizione 9.11. *Sia F un campo tale che ogni forma quadratica su uno spazio vettoriale di dimensione cinque su F sia isotropa. Allora due forme quadratiche non degeneri su uno spazio vettoriale V su F sono equivalenti se e soltanto se hanno lo stesso discriminante e lo stesso invariante di Hasse.*

Dimostrazione. La necessità della condizione è chiara e la sufficienza vale, per la proposizione 9.10, se $\dim V \leq 3$. Supponiamo dunque $n \geq 4$. L'ipotesi implica che ogni forma quadratica non degenere P su uno spazio vettoriale U/F di dimensione quattro è *universale*, ossia rappresenta ogni elemento non nullo di F. Infatti, per $a \neq 0$ possiamo formare $U \oplus Fx$, $x \neq 0$, e definirvi una forma quadratica R mediante $R(u + \alpha x) = P(u) - \alpha^2 a$ per $u \in U$, $\alpha \in F$. Poiché R è isotropa, esiste $u + \alpha x \neq 0$ tale che $P(u) = \alpha^2 a$. Se $\alpha = 0$, allora $u \neq 0$, sicché P è isotropa e quindi universale. Se $\alpha \neq 0$, si ha $P(\alpha^{-1}u) = a$. Dunque P è universale. L'universalità delle forme quadratiche non degeneri sugli spazi di dimensione quattro implica che, se Q è una forma quadratica non degenere su uno spazio vettoriale V di dimensione $n \geq 4$, esiste una base ortogonale $(v_1, \ldots, v_n)$ con $Q(v_i) = 1$ per $i > 3$. Se R è la restrizione di Q a $Fv_1 + Fv_2 + Fv_3$, dalle definizioni e dalla formula $(1,a) \sim 1$ segue che Q e R hanno lo stesso discriminante e lo stesso invariante di Hasse. Se Q' è una seconda forma quadratica non degenere su uno spazio vettoriale di dimensione n, esiste una base ortogonale $(v_1', \ldots, v_n')$ con $Q'(v_i') = 1$ per $i > 3$. Le condizioni che $s(Q) = s(Q')$ e che Q e Q' abbiano lo stesso discriminante implicano le stesse condizioni per le restrizioni di Q e Q' a $Fv_1 + Fv_2 + Fv_3$ e a $Fv_1' + Fv_2' + Fv_3'$. Queste restrizioni sono dunque equivalenti e, di conseguenza, Q e Q' sono equivalenti. □

Ci occorre un altro risultato valido per campi generali.

Proposizione 9.12. *La forma quadratica $Q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$, con $d = a_1a_2a_3a_4 \neq 0$, è isotropa se e soltanto se $F(\sqrt{d})$ è un campo di spezzamento di $(-a_3a_4, -a_2a_4)$.*

Dimostrazione. Poniamo $a = -a_3a_4$, $b = -a_2a_4$, $c = a_2a_3a_4$. Allora cQ è equivalente a $dx_1^2 - ax_2^2 - bx_3^2 + abx_4^2$ e $-ax_2^2 - bx_3^2 + abx_4^2$ è la forma norma su $(a,b)_0 = (-a_3a_4, -a_2a_4)_0$. Supponiamo dapprima $\sqrt{d} \in F$, sicché $F(\sqrt{d}) = F$. In tal caso cQ è equivalente a $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$, la forma norma di (a,b), e $(a,b) \sim 1$ se e soltanto se questa forma norma, e quindi Q, è isotropa. Il risultato vale dunque in questo caso. Supponiamo poi $\sqrt{d} \notin F$. Allora $F(\sqrt{d})$ è un campo di spezzamento di (a,b) se e soltanto se si immerge come sottocampo di (a,b) (p. 221). Ciò equivale a dire che $(a,b)_0$ contiene un elemento u tale che $u^2 = d$. Questo accade se e soltanto se cQ, e quindi Q, è isotropa. Il risultato vale anche in questo caso. □

Supponiamo ora che F sia un campo locale. I risultati del paragrafo precedente mostrano che vi è un unico elemento di ordine due in $\mathrm{Br}(F)$. Esso ha un rappresentante che è un'algebra ciclica (W, σ, π), dove W è un'estensione quadratica non ramificata di F, σ è l'automorfismo di W/F diverso da 1 e π è un qualsiasi elemento di F tale che $\pi \in P \setminus P^2$, dove P è l'ideale degli elementi non invertibili dell'anello di valutazione R di W. Poiché supponiamo $\mathrm{char}\, F \neq 2$, si ha $W = F(\sqrt{a})$ e quindi $(W, \sigma, \pi) = (a, \pi)$. Abbiamo la seguente proposizione.

Proposizione 9.13. *Sia F un campo locale di caratteristica diversa da 2 e sia A un'algebra di quaternioni con divisione su F. Ogni estensione quadratica E/F è allora un campo di spezzamento di A.*

Dimostrazione. Si ha $A = (W, \sigma, \pi) = (a, \pi)$. L'estensione E/F è non ramificata oppure

totalmente ramificata. Nel primo caso $E \simeq W$, sicché A contiene un sottocampo isomorfo a E e quindi E è un campo di spezzamento. Supponiamo ora che E sia totalmente ramificata. Allora $E = F(b)$, dove b è radice di un polinomio di Eisenstein di secondo grado. Completando il quadrato possiamo supporre $b^2 = \pi' \in P \setminus P^2$.[41] Possiamo costruire l'algebra con divisione (W', σ', π'), dove W' è non ramificata e σ' è un automorfismo di periodo due. Allora $(W', \sigma', \pi') \simeq (W, \sigma, \pi) = A$, sicché anche in questo caso A contiene un sottocampo isomorfo a E ed E è un campo di spezzamento. □

Per il prossimo risultato sulle algebre di quaternioni è necessaria l'ipotesi più forte che il campo residuo R/P abbia caratteristica diversa da 2.

Proposizione 9.14. *Se F è un campo locale tale che* $\mathrm{char}(R/P) \neq 2$*, allora* $(-1,-1)/F \sim 1$.

(Ciò non vale sempre per $\mathrm{char}(R/P) = 2$. Per esempio $(-1,-1)/\mathbb{Q}_2 \not\sim 1$. Si veda l'esercizio 5.)

Dimostrazione. Il risultato è chiaro se -1 è un quadrato in F. Supponiamo dunque $W = F(\sqrt{-1}) \supsetneq F$. Ora W è non ramificata, poiché la riducibilità di x^2+1 in $(R/P)[x]$ implicherebbe per il lemma di Hensel l'esistenza di $\sqrt{-1}$ in F. Dunque $[(R_W/P_W) : (R/P)] = 2$, sicché il grado residuo di W/F è due e l'indice di ramificazione è 1, ossia W/F è non ramificata. Ne segue che, se $(-1,-1) \not\sim 1$, allora $(-1,-1) \simeq (-1,\pi)$ con $\pi \in P_W \setminus P_W^2$, $\pi \in F$. Ciò implica $-\pi \in N(W^*)$, in contraddizione con la descrizione di $N(W^*)$ data a p. 610. Pertanto $(-1,-1) \sim 1$. □

Possiamo ora dimostrare la proposizione seguente.

Proposizione 9.15. *Se F è un campo locale di caratteristica diversa da 2, ogni forma quadratica non degenere Q su uno spazio vettoriale di dimensione cinque su F è isotropa.*

Dimostrazione. Possiamo supporre $Q = \sum_{i=1}^5 a_i x_i^2$ e, moltiplicando Q per $\prod_i a_i$, possiamo supporre che $\prod_i a_i$ sia un quadrato. Supponiamo che Q non sia isotropa. Anche $\sum_{i=1}^4 a_i x_i^2$ non è isotropa. Per la proposizione 9.12, $F(\sqrt{a_1a_2a_3a_4})$ non è un campo di spezzamento di $(-a_3a_4, -a_2a_4)$. Quindi $(-a_3a_4, -a_2a_4) \not\sim 1$ e, per la proposizione 9.13, $a_1a_2a_3a_4$ è un quadrato. Dunque a_5 è un quadrato. Analogamente ciascun a_i è un quadrato e possiamo pertanto supporre che $Q = \sum_{i=1}^5 x_i^2$. Allora, ancora per la proposizione 9.12, $(-1,-1) \not\sim 1$. Ciò contraddice la proposizione 9.14 se la caratteristica del campo residuo di F è diversa da 2. Supponiamo ora che essa sia 2. Allora F contiene il campo $\mathbb{Q}_2$ dei numeri 2-adici e $\mathbb{Q}_2$ contiene $\sqrt{-7}$. Infatti, per il lemma di Hensel, $x^2 + x + 2$ è riducibile in $\mathbb{Q}_2$. Pertanto $\mathbb{Q}_2$ contiene $\frac{1}{2}(-1 + \sqrt{-7})$ e dunque contiene $\sqrt{-7}$. Ora

$$1^2 + 1^2 + 1^2 + 2^2 + (\sqrt{-7})^2 = 0,$$

cosicché $\sum_{i=1}^5 x_i^2$ è isotropa in $\mathbb{Q}_2$ e quindi in F. Ciò conclude la dimostrazione. □

Dalle proposizioni 9.11 e 9.15 otteniamo il teorema seguente.

Teorema 9.24. *Se F è un campo locale di caratteristica diversa da 2, due forme quadratiche non degeneri su uno spazio vettoriale V/F di dimensione n sono equivalenti se e soltanto se hanno lo stesso discriminante e lo stesso invariante di Hasse.*

Mostriamo poi che, se $n \geq 3$, i due invarianti sono indipendenti. La dimostrazione della proposizione 9.11 mostra che basta provarlo per $n = 3$. Un calcolo indicato nella dimostrazione della proposizione 9.10 mostra che, se $Q = ax_1^2 + bx_2^2 + cx_3^2$, si ha $s(Q) \sim (-da, -db)(-d, -d)$, dove $d = abc$. Da questa formula è chiaro che, per d dato, a e b si possono scegliere in modo che $s(Q) = \pm 1$. Si possono quindi scegliere a, b, c in modo che il discriminante sia un qualsiasi d e $s(Q)$ abbia uno qualsiasi dei due valori ± 1. Questo risultato e il teorema 9.24 implicano che

[41] Questo passaggio della dimostrazione originale vale quando la caratteristica residua è diversa da 2. Nel caso residuo 2 si può invece osservare che, per E/F totalmente ramificata, EW/E è quadratica non ramificata e la valutazione normalizzata di E dà $v_E(\pi) = 2$. Per la descrizione del gruppo delle norme a p. 610, π è dunque una norma da EW. L'algebra ciclica ottenuta per estensione degli scalari a E è pertanto spezzata. [N.d.T.]

il numero delle classi di equivalenza di forme quadratiche non degeneri su F, per $n \geq 3$ fissato, è $2|F^*/F^{*2}|$, dove F^{*2} è il sottogruppo dei quadrati di F^*. È facile vedere, con un argomento basato sul lemma di Hensel come nella dimostrazione della proposizione 9.8 sulle norme, che, se la caratteristica del campo residuo è diversa da 2, allora $|F^*/F^{*2}| = 4$. Pertanto il numero delle classi di equivalenza delle forme quadratiche non degeneri per $n \geq 3$ fissato è 8. Gli esercizi forniscono alcune indicazioni sul caso $n < 3$ e su quello in cui il campo residuo ha caratteristica due.

Esercizi

1. Mostrare che $ax_1^2 + bx_2^2$, con $ab \neq 0$, è isotropa se e soltanto se $ab = -d^2$ per qualche $d \in F$, e che $Q = ax_1^2 + bx_2^2 + cx_3^2$ è isotropa se e soltanto se $s(Q) \sim (-d, -d)$, con $d = abc$.

2. Sia F un'estensione di dimensione finita di $\mathbb{Q}_2$. Mostrare che $|F^*/F^{*2}| = 2^{[F:\mathbb{Q}_2]}$.[42]

3. Determinare il numero delle classi di equivalenza delle forme quadratiche non degeneri con $n = 2$ su un campo locale.

4. Sia F un campo tale che $(a, b) \sim 1$ per ogni algebra di quaternioni su F. Mostrare che due forme quadratiche non degeneri su uno spazio di dimensione n su F sono equivalenti se e soltanto se hanno lo stesso discriminante.

5. Mostrare che la forma quadratica $x_1^2 + x_2^2 + x_3^2$ su uno spazio vettoriale di dimensione tre su $\mathbb{Q}_2$ non è isotropa. Dedurne che $(-1, -1)/\mathbb{Q}_2 \not\sim 1$.

Riferimenti bibliografici

S. Kürschák, Über Limesbildung und allgemeine Körpertheorie, *Journal für die reine und angewandte Mathematik*, vol. 142 (1913), 211–253.

E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), 31–44.

O. F. G. Schilling, *The Theory of Valuations*, American Mathematical Society Surveys, Providence, R.I., 1950.

O. Zariski e P. Samuel, *Commutative Algebra II*, nuova stampa, Springer, New York, 1960.

E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

[42] La formula stampata omette un fattore 4. La cardinalità corretta è $2^{[F:\mathbb{Q}_2]+2}$; già per $F = \mathbb{Q}_2$ le classi modulo quadrati sono otto. [N.d.T.]

10 Domini di Dedekind

In questo capitolo studieremo i domini in cui ogni ideale proprio non nullo si può scomporre in uno e un solo modo come prodotto di ideali primi. Gli esempi più notevoli sono gli anelli degli elementi interi su $\mathbb{Z}$ dei campi di numeri, cioè delle estensioni di dimensione finita del campo $\mathbb{Q}$ (si veda BAI, pp. 278–281). Essi sono l'oggetto di studio della teoria algebrica dei numeri. Un'altra importante classe di esempi è data dagli anelli che intervengono nello studio delle curve algebriche. Qui si parte da un campo $F(x, y)$, dove F è un campo base (di solito algebricamente chiuso), x è trascendente su F e y è algebrico su $F(x)$. Il sottoanello degli elementi interi su $F[x]$ possiede allora la proprietà di fattorizzazione enunciata sopra.

Vi sono molti modi equivalenti di definire la classe dei domini, detti domini di Dedekind, nei quali vale il teorema fondamentale di fattorizzazione degli ideali in ideali primi (si veda il ğ 10.2). Prenderemo come punto di partenza una definizione basata sulle nozioni di ideale frazionario e di invertibilità. Quest'ultima equivale alla proiettività come modulo sull'anello dato.

Il fatto che i domini menzionati sopra siano di Dedekind si può dedurre da un teorema generale secondo cui, se D è un dominio di Dedekind con campo delle frazioni F ed E è un'estensione di dimensione finita di F, il sottoanello D' degli elementi di E interi su D è un dominio di Dedekind. Lo dimostreremo nel ğ 10.3. Nei ğğ 10.4 e 10.5 considereremo il problema centrale dello studio della fattorizzazione in D' delle estensioni degli ideali primi di D. Esso è strettamente legato al problema del prolungamento delle valutazioni da F a E trattato nel capitolo 9.

Oltre alla teoria degli ideali, considereremo la struttura dei moduli finitamente generati sui domini di Dedekind. Il caso particolare dei moduli senza torsione è classico e fu trattato per la prima volta da E. Steinitz (si veda il ğ 10.6).

Considereremo infine il gruppo delle classi di un dominio di Dedekind, definito nel ğ 7.9, e mostreremo nel ğ 10.6 che questo gruppo ha una realizzazione concreta come gruppo classico definito mediante gli ideali frazionari.

10.1 Ideali frazionari. Domini di Dedekind

Sia D un dominio e sia F il suo campo delle frazioni. È utile estendere la nozione di ideale di D a certi sottomoduli di F, come nella definizione seguente.

Definizione 10.1. *Se D è un dominio e F è il suo campo delle frazioni, un ideale frazionario (di D) è un D-sottomodulo non nullo I di F per cui esiste un elemento non nullo a di D tale che $aI \subset D$ (o, equivalentemente, $aI \subset I \cap D$).*

Gli ideali frazionari contenuti in D sono gli ideali non nulli di D. Essi si chiamano *ideali interi*. Se I è un ideale frazionario e a è un elemento non nullo di D tale che $aI \subset D$, allora aI è un ideale intero. Per ogni elemento non nullo b di F, $Db = \{db \mid d \in D\}$ è un ideale frazionario, poiché è chiaramente un D-sottomodulo di F e, se $b = ac^{-1}$, $a, c \in D$, si ha $c(Db) \subset D$. Un ideale frazionario della forma Db si chiama *ideale principale*.

Se I_1 e I_2 sono ideali frazionari, lo è anche la somma di moduli $I_1 + I_2$, poiché essa è un sottomodulo e, se $a_i I_i \subset D$ con $a_i \neq 0$ in D, allora $a_1 a_2 (I_1 + I_2) \subset D$. Anche l'intersezione $I_1 \cap I_2$ è un ideale frazionario, poiché è un D-sottomodulo e $I_1 \cap I_2 \neq 0$. Infatti, se $b_i \neq 0$ appartiene a I_i, esiste $a_i \neq 0$ in D tale che $a_i b_i \in D \cap I_i$. Allora $(a_1 b_1)(a_2 b_2) \neq 0$ appartiene a $I_1 \cap I_2$. Inoltre, se $a \neq 0$ soddisfa $aI_1 \subset D$, si ha $a(I_1 \cap I_2) \subset D$. Definiamo $I_1 I_2 = \{\sum_i b_{1i} b_{2i} \mid b_{1i} \in I_1,\ b_{2i} \in I_2\}$. Evidentemente questo è un D-sottomodulo di F e l'argomento usato per $I_1 \cap I_2$ mostra che $I_1 I_2$ è un ideale frazionario.

Ci occorrerà conoscere la forma degli omomorfismi di un ideale frazionario in D. Essa è data

dalla seguente proposizione.

Proposizione 10.1. *Sia f un D-omomorfismo dell'ideale frazionario I in D e sia b un qualsiasi elemento non nullo di I. Allora f ha la forma*

$$a \longmapsto b^{-1}f(b)a, \qquad a \in I. \tag{1}$$

Dimostrazione. Scegliamo un $d \neq 0$ in D tale che $dI \subset D$. Allora $db \in D$ e $da \in D$ per ogni $a \in I$. Si ha

$$daf(b) = f(dab) = dbf(a).$$

Quindi $af(b) = bf(a)$ e pertanto $f(a) = b^{-1}f(b)a$. Dunque f ha la forma data nella (1). □

Se I è un ideale frazionario, definiamo

$$I^{-1} = \{c \in F \mid cI \subset D\}. \tag{2}$$

È chiaro che I^{-1} è un D-sottomodulo di F. Poiché esiste $a \neq 0$ in D tale che $aI \subset D$, è chiaro che $I^{-1} \neq 0$. Inoltre, se $b \neq 0$ appartiene a $I \cap D$, allora $I^{-1}b \subset D$. Quindi I^{-1} è un ideale frazionario. Se I è l'ideale principale Db, con $b \neq 0$, è chiaro che $I^{-1} = Db^{-1}$. È chiaro anche che $I_1 \subset I_2$ implica $I_1^{-1} \supset I_2^{-1}$.

Se I è un ideale frazionario, $I^{-1}I \subset D$, e pertanto $I^{-1}I$ è un ideale intero. Diremo che I è *invertibile* se

$$I^{-1}I = D. \tag{3}$$

Se $I = Db \neq 0$, allora $I^{-1} = b^{-1}D$. Evidentemente $I^{-1}I = (b^{-1}D)(bD) = D$. Dunque ogni ideale principale è invertibile. Gli ideali frazionari formano, rispetto alla moltiplicazione, un monoide commutativo con unità D. Se I è invertibile, $I^{-1}I = D$, quindi I^{-1} è l'inverso di I nel monoide degli ideali frazionari. Viceversa, supponiamo che I abbia inverso J in questo monoide. Da $JI = D$ segue allora $J \subset I^{-1}$, dove I^{-1} è definito dalla (2). Poiché $I^{-1}I \subset D$, si ha $I^{-1}I = D$. Per l'unicità dell'inverso di un elemento di un monoide, $I^{-1} = J$. Gli ideali invertibili costituiscono dunque il gruppo delle unità del monoide degli ideali frazionari. Dimostriamo ora la proposizione seguente.

Proposizione 10.2. *Ogni ideale invertibile è finitamente generato.*

Dimostrazione. Sia I invertibile. Allora $I^{-1}I = D$ implica l'esistenza di elementi $c_i \in I^{-1}$, $b_i \in I$, tali che $\sum_{i=1}^{n} c_i b_i = 1$. Sia ora $b \in I$. Allora $b = b1 = \sum_i (bc_i)b_i$ e $a_i = bc_i \in D$. Dunque $I = \sum_i Db_i$ e $(b_1, \ldots, b_n)$ è un sistema di generatori di I. □

Stabiliamo ora l'equivalenza delle condizioni di invertibilità e di proiettività per gli ideali frazionari.

Proposizione 10.3. *Un ideale frazionario I è invertibile se e solo se è proiettivo.*

Dimostrazione. Supponiamo dapprima I invertibile. Allora $1 = \sum_{i=1}^{m} c_i b_i$ con $c_i \in I^{-1}$, $b_i \in I$. L'applicazione $f_i \colon a \mapsto ac_i$, $a \in I$, appartiene a $\hom_D(I, D)$ e $a = \sum_i (ac_i)b_i = \sum_i f_i(a)b_i$. Quindi I è D-proiettivo per il «lemma della base duale» (proposizione 3.11, p. 152). Viceversa, supponiamo I proiettivo. Abbiamo allora un sistema di generatori $\{b_\alpha\}$ di I e corrispondenti applicazioni $f_\alpha \in \hom_D(I, D)$ tali che, per ogni $a \in I$, $f_\alpha(a) = 0$ per tutti gli α tranne un numero finito e $a = \sum_\alpha f_\alpha(a)b_\alpha$. Nella proposizione 10.1 abbiamo mostrato che, se b è un elemento non nullo di I, allora f_α ha la forma $a \mapsto b^{-1}f_\alpha(b)a$. Poiché $f_\alpha(b) = 0$ per ogni α salvo, diciamo, $\alpha = 1, 2, \ldots, m$, si ha $f_\alpha = 0$ per $\alpha \neq 1, 2, \ldots, m$ e $a = \sum_{i=1}^{m} b^{-1}f_i(b)ab_i$. Allora $1 = \sum_i b^{-1}f_i(b)b_i$ e, poiché $b^{-1}f_i(b)a \in D$ per ogni $a \in I$, si ha $c_i = b^{-1}f_i(b) \in I^{-1}$. Dunque $1 = \sum_i c_i b_i$, con $c_i \in I^{-1}$, $b_i \in I$, e pertanto $I^{-1}I = D$. L'ideale I è quindi invertibile. □

Diciamo che un ideale frazionario I è un *divisore* dell'ideale frazionario J se esiste un ideale intero K tale che $J = IK$. Poiché $K \subset D$ e $DI \subset I$, ciò implica $J \subset I$. Se I è invertibile, vale l'importante proprietà inversa: se $I \supset J$, allora I è un divisore di J. Infatti $D = I^{-1}I \supset I^{-1}J$, sicché $K = I^{-1}J$ è intero. Inoltre $J = I(I^{-1}J) = IK$.

Ci interessano l'esistenza e l'unicità della fattorizzazione degli ideali in ideali primi. Per gli ideali interi invertibili vale la seguente proprietà di unicità.

Proposizione 10.4. *Sia I intero e invertibile e si supponga $I = P_1P_2\cdots P_m$, con i P_i ideali primi di D. Allora questa è l'unica fattorizzazione di I in prodotto di ideali primi.*

Dimostrazione. Osserviamo dapprima che, se M è un monoide commutativo e a è un'unità di M, ogni fattore di a è un'unità. Applicando l'osservazione al monoide moltiplicativo degli ideali frazionari, vediamo che i P_i sono invertibili. Sia ora $I = Q_1Q_2\cdots Q_n$ con i Q_j ideali primi. Allora $P_1 \supset Q_1\cdots Q_n$ e, poiché P_1 è primo, possiamo supporre $P_1 \supset Q_1$. Essendo P_1 invertibile, si ha $Q_1 = P_1R_1$ con R_1 intero. Allora $R_1 \supset Q_1$. Poiché Q_1 è primo, $P_1 \subset Q_1$ oppure $R_1 \subset Q_1$, e quindi $P_1 = Q_1$ oppure $R_1 = Q_1$. Nel secondo caso $R_1 = P_1R_1$ e, poiché $I = Q_1Q_2\cdots Q_n = P_1R_1Q_2\cdots Q_n$, R_1 è invertibile. Di qui $D = R_1^{-1}R_1 = R_1^{-1}R_1P_1 = P_1$, contro l'ipotesi che P_1 sia primo (e dunque proprio). Quindi $Q_1 = P_1$, sicché $P_1P_2\cdots P_m = P_1Q_2\cdots Q_n$ e, moltiplicando per P_1^{-1}, otteniamo $D = Q_2\cdots Q_n$ se $m = 1$ e $P_2\cdots P_m = Q_2\cdots Q_n$ se $m > 1$. Nel primo caso è anche $n = 1$ e nel secondo $n > 1$ e si può applicare l'induzione su m, poiché $P_2\cdots P_m$ è invertibile. □

Definiamo ora la classe di anelli di cui ci occuperemo in questo capitolo.

Definizione 10.2. *Un dominio D si chiama dominio di Dedekind se ogni ideale frazionario di D in F (campo delle frazioni di D) è invertibile.*

Per la proposizione 10.3 ciò equivale a supporre ogni ideale frazionario proiettivo. Dalla proposizione 10.2 è chiaro che ogni dominio di Dedekind è noetheriano. Si ha anche la seguente proprietà importante.

Proposizione 10.5. *Ogni ideale primo non nullo di un dominio di Dedekind è massimale.*

Dimostrazione. Sia I un ideale primo non nullo (cioè un ideale primo intero) del dominio di Dedekind D. Se I non è massimale, esiste un ideale J di D tale che $D \supsetneq J \supsetneq I$. Allora $I = JK$ con K intero. Poiché $J \neq I$, si ha $I \not\supset J$. Si ha anche $I \not\supset K$, poiché $K = DK \supset JK = I$, sicché $I \supset K$ implicherebbe $I = K$ e $K = JK$. Allora $D = KK^{-1} = JKK^{-1} = J$, contro $D \neq J$. Abbiamo dunque $I = JK$ con $J \not\subset I$ e $K \not\subset I$. Ciò contraddice l'ipotesi che I sia primo. □

Per i domini di Dedekind vale il seguente teorema fondamentale di fattorizzazione.

Teorema 10.1. *Ogni ideale intero proprio di un dominio di Dedekind si scrive in uno e un solo modo come prodotto di ideali primi.*

Dimostrazione. In virtù della proposizione 10.4 basta dimostrare che, se I è un ideale intero proprio del dominio di Dedekind D, allora I è un prodotto di ideali primi non nulli. Supponiamo che non sia così. L'insieme degli ideali interi propri che non sono prodotti di ideali primi è dunque non vuoto. Per la proprietà noetheriana di D, questo insieme contiene un elemento massimale I. Allora I non è primo e quindi non è massimale. Esiste pertanto un ideale I_1 di D tale che $D \supsetneq I_1 \supsetneq I$. Allora $I = I_1I_2$, dove I_2 è un ideale intero proprio. Abbiamo $I_2 \supset I$ e $I_2 = I$ implicherebbe $D = II^{-1} = I_1I_2I_2^{-1} = I_1$. Dunque $D \supsetneq I_i \supsetneq I$ per $i = 1, 2$. Per la massimalità di I, ciascun I_i è un prodotto di ideali primi. Ne risulta la contraddizione che $I = I_1I_2$ è un prodotto di ideali primi. □

Una conseguenza immediata è la seguente.

Corollario 1. *Si supponga $I = P_1P_2\cdots P_m$, con i P_i primi. Allora gli ideali interi diversi da D che contengono I hanno la forma $P_{i_1}P_{i_2}\cdots P_{i_r}$ con $1 \leq i_1 < i_2 < \cdots < i_r \leq m$.*

La dimostrazione è chiara. È chiaro pure che dal corollario 1 segue il risultato seguente.

Corollario 2. *Se I è un ideale intero di un dominio di Dedekind D, allora D/I è artiniano.*

È evidente che gli ideali frazionari di un dominio di Dedekind costituiscono un gruppo rispetto alla moltiplicazione, con D come unità e con I^{-1}, definito dalla (2), come inverso di I. Il teorema fondamentale di fattorizzazione dà la struttura di questo gruppo.

Teorema 10.2. *Il gruppo degli ideali frazionari di un dominio di Dedekind è prodotto diretto dei sottogruppi ciclici generati dagli ideali primi. Questi sottogruppi sono infiniti.*

Dimostrazione. Sia I un ideale frazionario diverso da D e sia a un elemento non nullo di D tale che $aI \subset D$. Allora aI è un ideale intero, sicché o $aI = D$ oppure aI è un prodotto di ideali primi. Anche aD è un ideale intero, quindi o $aD = D$ oppure aD è un prodotto di ideali primi. Poiché $I(aD) = aI$, si ha $I = (aI)(aD)^{-1}$. È allora chiaro che si può scrivere $I = P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$, con i P_i ideali primi e i k_i interi non nulli. Dal teorema 10.1 segue viceversa che, se i k_i sono interi non nulli e i P_i ideali primi distinti, allora $P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r} \neq D$. Ne segue che la rappresentazione di un ideale frazionario diverso da D come prodotto $P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$ è unica. Dunque il gruppo degli ideali frazionari è il prodotto diretto dei sottogruppi ciclici generati dai primi. È chiaro anche che questi gruppi sono infiniti. □

Esercizi

1. Dimostrare che ogni D-sottomodulo finitamente generato e non nullo di F è un ideale frazionario.

2. Dimostrare che, se D è di Dedekind, l'unico ideale frazionario I che soddisfa $I^2 = I$ è $I = D$.

3. Usare il teorema 10.1 per dimostrare che ogni dominio a ideali principali è fattoriale.

4. Dare un esempio di dominio fattoriale che non sia di Dedekind.

5. Sia $D = \mathbb{Z}[\sqrt{-3}]$, il sottoanello di $F = \mathbb{Q}(\sqrt{-3})$ costituito dagli elementi $a+b\sqrt{-3}$, $a, b \in \mathbb{Z}$. Sia I l'ideale frazionario di D dato da $D + Dw$, con $w = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ (una radice cubica primitiva di 1). Calcolare I^{-1} e II^{-1}. L'ideale I è invertibile?

6. Sia $D = \mathbb{Z}[\sqrt{-5}]$ con campo dei quozienti $F = \mathbb{Q}[\sqrt{-5}]$. Dimostrare che $I = D3 + D\sqrt{-5}$ è un D-modulo proiettivo che non è libero.[43]

7. Dimostrare che ogni dominio di Dedekind fattoriale è un dominio a ideali principali.

Negli esercizi rimanenti D è un dominio di Dedekind.

8. Siano I_1 e I_2 ideali interi di D e si scriva $I_j = P_1^{e_{j1}} \cdots P_g^{e_{jg}}$, con i P_i ideali primi distinti ed $e_{jk} \geq 0$. Dimostrare che $I_1 + I_2 = P_1^{\min(e_{11}, e_{21})} \cdots P_g^{\min(e_{1g}, e_{2g})}$ e $I_1 \cap I_2 = P_1^{\max(e_{11}, e_{21})} \cdots P_g^{\max(e_{1g}, e_{2g})}$.

9. Dimostrare che il reticolo degli ideali interi di D è distributivo (cfr. BAI, p. 463).

10. (Teorema cinese del resto per i domini di Dedekind.) Siano $I_1, \ldots, I_n$ ideali interi di un dominio di Dedekind D e $a_1, \ldots, a_n$ elementi di D. Dimostrare che il sistema di congruenze $x \equiv a_j \pmod{I_j}$, $1 \leq j \leq n$, ha una soluzione $x = a$ in D se e solo se, per ogni j, k,

[43] L'ideale è riportato come nell'originale. Con questi generatori si ha però $1 = 2 \cdot 3 + (\sqrt{-5})^2 \in I$, dunque $I = D$ è libero.

$1 \leq j, k \leq n$, si ha $a_j \equiv a_k \pmod{I_j + I_k}$. (Suggerimento. La necessità delle condizioni è chiara. Per la sufficienza si procede per induzione su n. Per $n = 2$ abbiamo $a_1 - a_2 = b_1 - b_2$, $b_j \in I_j$. Allora $a = a_1 - b_1 = a_2 - b_2$ soddisfa $a \equiv a_j \pmod{I_j}$, $j = 1, 2$. Per il passo induttivo si usa la legge distributiva $\bigcap_{j=1}^{n-1}(I_j + I_n) = (\bigcap_{j=1}^{n-1} I_j) + I_n$. Si vedano l'esercizio 9 e BAI, p. 461 e seguente.)

11. Sia I un ideale frazionario e J un ideale intero. Dimostrare che esiste un elemento $a \in I$ tale che $I^{-1}a + J = D$. (Suggerimento. Siano $P_1, \ldots, P_r$ gli ideali primi che dividono J. Per $1 \leq i \leq r$, scegliere $a_i \in IP_1 \cdots P_r P_i^{-1}$, $a_i \notin IP_1 \cdots P_r$, e porre $a = \sum_{i=1}^{r} a_i$. Allora $P_i \not\supset aI^{-1}$, $1 \leq i \leq r$, e $aI^{-1} + J = D$.)

12. Sia I un ideale frazionario e sia a un qualunque elemento non nullo di I. Dimostrare che esiste un $b \in I$ tale che $I = Da + Db$. (Suggerimento. Applicare l'esercizio 10 all'ideale dato I e a $J = aI^{-1}$.)

13. Sia I un ideale frazionario e J un ideale intero. Dimostrare che I/IJ e D/J sono D-moduli isomorfi.

14. Sia P un ideale primo non nullo di D. Dimostrare che, se $e \geq 1$, allora $D/P^e \supset P/P^e \supset \cdots \supset P^{e-1}/P^e \supset 0$ è una serie di composizione di D/P^e come D-modulo. Dimostrare che P^i/P^{i+1}, $i \geq 0$, è uno spazio vettoriale unidimensionale sul campo D/P.

15. Dimostrare che, se D ha soltanto un numero finito di ideali $P_1, \ldots, P_s$, allora è un dominio a ideali principali. (Suggerimento. Sia $I = P_1^{e_1} \cdots P_s^{e_s}$, con $e_i \geq 0$. Per ogni i scegliere $a_i \in IP_1 \cdots P_s P_i^{-1}$, $a_i \notin P_i^{e_i+1}$. Porre $a = \sum_{i=1}^{s} a_i$. Allora $a \in P_i^{e_i}$, $a \notin P_i^{e_i+1}$ e $I = Da$.)

10.2 Caratterizzazioni dei domini di Dedekind

Daremo diverse caratterizzazioni dei domini di Dedekind. La prima ricorre all'importante nozione di chiusura integrale introdotta nel §7.7. È facile vedere che ogni dominio fattoriale D è integralmente chiuso (esercizio 1 di questo paragrafo). Dimostriamo ora la seguente proposizione.

Proposizione 10.6. *Ogni dominio di Dedekind è integralmente chiuso.*

Dimostrazione. Sia D un dominio di Dedekind, F il suo campo delle frazioni e $u \in F$ un elemento intero su D. Sia $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ un polinomio monico a coefficienti in D tale che $f(u) = 0$, e poniamo $M = D1 + Du + \cdots + Du^{n-1}$. Se $u = bc^{-1}$ con $b, c \in D$, allora $c^{n-1}M \subseteq D$, cosicché M è un ideale frazionario. Evidentemente $M^2 = M$, da cui $M = D$ (si veda l'esercizio 2 del paragrafo precedente).[44] Allora $u \in M = D$ e D è integralmente chiuso. □

Abbiamo così stabilito tre proprietà di un dominio di Dedekind D:

1. D è noetheriano.
2. Ogni ideale primo non nullo di D è massimale.
3. D è integralmente chiuso.

Mostreremo che queste proprietà caratterizzano i domini di Dedekind. La dimostrazione si basa su alcuni lemmi che hanno interesse anche per sé stessi.

Lemma 1. *Ogni ideale frazionario su un dominio noetheriano D è finitamente generato come D-modulo.*

[44] Nell'originale si legge p. 604. Qui e nei due rinvii successivi al §10.1 si è tenuto conto della paginazione e della numerazione degli esercizi della seconda edizione. Nel teorema 10.4 si legge in origine «esercizio 14, p. 605» e nell'ultimo esercizio di questo paragrafo «esercizio 11, p. 605».

Dimostrazione. Sia I un ideale frazionario su D. Esiste $0 \neq a \in D$ tale che $I' = aI \subseteq D$. Allora I' è un ideale di D e, poiché D è noetheriano, un D-modulo finitamente generato. Anche $I = a^{-1}I'$ è quindi finitamente generato. □

Lemma 2. *Ogni ideale non nullo di un dominio noetheriano contiene un prodotto di ideali primi non nulli.*

Dimostrazione. Come nella dimostrazione del teorema 10.1, se il risultato fosse falso esisterebbe un ideale $I \neq 0$ massimale fra quelli che non contengono un prodotto di ideali primi non nulli. Allora I non è primo ed esistono ideali I_j, $j = 1, 2$, con $I_j \supsetneq I$ e $I_1 I_2 \subseteq I$. Per la massimalità di I ciascun I_j contiene un prodotto di ideali primi non nulli. Poiché $I \supseteq I_1 I_2$, si giunge a una contraddizione. □

Lemma 3. *Sia D un dominio noetheriano integralmente chiuso, F il suo campo delle frazioni e I un ideale frazionario su D. Allora*

$$S = \{s \in F \mid sI \subseteq I\} = D.$$

Dimostrazione. Sia $s \in S$. Poiché I è un D-modulo fedele finitamente generato e $sI \subseteq I$, per il lemma di p. 408 s è intero su D. Essendo D integralmente chiuso, $s \in D$. Dunque $S \subseteq D$. L'inclusione $D \subseteq S$ segue dalla definizione di ideale frazionario, onde $S = D$. □

Lemma 4. *Sia D un dominio noetheriano nel quale ogni ideale primo non nullo è massimale. Se I è un ideale non nullo di D e $I \subsetneq D$, allora $I^{-1} \supsetneq D$.*

Dimostrazione. Sia $0 \neq a \in I$. Abbiamo $D \supseteq I \supseteq aD$ e, per il lemma 2, $aD \supseteq P_1 P_2 \cdots P_m$, con i P_i primi non nulli. Scegliamo m minimo. Per la condizione noetheriana (o per il lemma di Zorn) esiste un ideale massimale $P \supseteq I$. Allora $P \supseteq I \supseteq aD \supseteq P_1 \cdots P_m$. Poiché P e i P_i sono primi e i primi non nulli sono massimali, $P = P_i$ per un certo i. Possiamo supporre $P = P_1$. Se $m = 1$, abbiamo $aD = I$, quindi $I^{-1} = a^{-1}D$. Essendo $I \subsetneq D$, si ha $a^{-1} \notin D$ e $I^{-1} = a^{-1}D \supsetneq D$. Sia ora $m > 1$. Per la minimalità di m, aD non contiene $P_2 \cdots P_m$. Scegliamo quindi $b \in P_2 \cdots P_m$, $b \notin aD$, e poniamo $c = a^{-1}b$. Allora $c \notin D$ e

$$cI \subseteq cP = a^{-1}bP \subseteq a^{-1}PP_2 \cdots P_m \subseteq a^{-1}(aD) = D.$$

Dunque $c \in I^{-1}$, $c \notin D$ e di nuovo $I^{-1} \supsetneq D$. □

Possiamo ora dimostrare il teorema seguente.

Teorema 10.3. *Un dominio D è di Dedekind se e solo se (1) D è noetheriano, (2) ogni suo ideale primo non nullo è massimale (equivalentemente, la dimensione di Krull di D è al più uno), (3) D è integralmente chiuso.*

Dimostrazione. Abbiamo già visto che ogni dominio di Dedekind soddisfa (1)–(3). Viceversa, sia D un dominio con queste proprietà e sia I un suo ideale frazionario. L'ideale frazionario $I^{-1}I$ è intero e $II^{-1}(II^{-1})^{-1} \subseteq D$, da cui $I^{-1}(II^{-1})^{-1} \subseteq I^{-1}$. Per il lemma 3 si ha $(II^{-1})^{-1} \subseteq D$. Poiché $II^{-1} \subseteq D$, dal lemma 4 segue $II^{-1} = D$. Ogni ideale frazionario è quindi invertibile e D è di Dedekind. □

La prossima caratterizzazione sarà in termini di localizzazioni. Sia D un dominio e S un sottomonoide del monoide moltiplicativo degli elementi non nulli di D. Nel campo delle frazioni F di D consideriamo il sottoanello D_S formato dagli elementi as^{-1} con $a \in D$, $s \in S$. È facile vedere che questo anello è isomorfo alla localizzazione di D rispetto a S definita nel §7.2. I risultati sulle localizzazioni dei §§7.2 e 7.3 si possono perciò applicare agli anelli D_S.

Sia I un ideale frazionario su D e poniamo $I_S = \{bs^{-1} \mid b \in I,\ s \in S\}$. Allora I_S è un D_S-sottomodulo non nullo di F e, se $0 \neq a \in D$ è tale che $aI \subseteq D$, abbiamo $aI_S \subseteq D_S$. Poiché F è evidentemente il campo delle frazioni di D_S, I_S è un ideale frazionario su D_S. Per due ideali

frazionari I_1, I_2 su D si ha

$$(I_1 + I_2)_S = I_{1S} + I_{2S}, \tag{4}$$

$$(I_1 I_2)_S = I_{1S} I_{2S}, \tag{5}$$

$$(I_1 \cap I_2)_S = I_{1S} \cap I_{2S}. \tag{6}$$

Le prime due uguaglianze sono chiare. Per la terza osserviamo che $(I_1 \cap I_2)_S \subseteq I_{1S} \cap I_{2S}$ è evidente. Se ora $a \in I_{1S} \cap I_{2S}$, scriviamo $a = a_1 s_1^{-1} = a_2 s_2^{-1}$ con $a_i \in I_i$, $s_i \in S$. Allora $b = a_1 s_2 = a_2 s_1 \in I_1 \cap I_2$ e $a = b(s_1 s_2)^{-1} \in (I_1 \cap I_2)_S$, onde (6).

Osserviamo poi che per ogni ideale frazionario I finitamente generato su D si ha

$$(I^{-1})_S = (I_S)^{-1}. \tag{7}$$

Infatti dalla definizione segue $(I_1 + I_2)^{-1} = I_1^{-1} \cap I_2^{-1}$. Inoltre, per ogni $b \neq 0$ in F, $(Db)_S = D_S b$. Quindi, se $I = Db_1 + \cdots + Db_m$ con generatori non nulli, allora $I_S = D_S b_1 + \cdots + D_S b_m$ e $(I_S)^{-1} = \bigcap_i D_S b_i^{-1}$. D'altra parte $I^{-1} = \bigcap_i D b_i^{-1}$ e per (6) si ha $(I^{-1})_S = \bigcap_i D_S b_i^{-1} = (I_S)^{-1}$. Ciò prova (7).

Sia ora I' un ideale frazionario su D_S. Esiste un elemento as^{-1}, con $0 \neq a \in D$, $s \in S$, tale che $as^{-1} I' \subseteq D_S$. Dunque $as^{-1} I'$ è un ideale non nullo contenuto nella localizzazione D_S. Per il ğ7.2 è della forma I_S con I ideale non nullo contenuto in D. Allora $I' = a^{-1} s I_S = ((a^{-1}s)I)_S$. Pertanto ogni ideale frazionario su D_S è della forma I_S per qualche ideale frazionario I su D.

Teorema 10.4. *Sia D un dominio.*

1. *Se D è di Dedekind, anche D_S lo è per ogni sottomonoide S del monoide moltiplicativo degli elementi non nulli di D.*
2. *Se D è di Dedekind e P è un suo ideale primo non nullo, D_P è un anello di valutazione discreta.*
3. *Se D è noetheriano e D_P è un anello di valutazione discreta per ogni ideale massimale P di D, allora D è di Dedekind.*

(Ricordiamo che, per un ideale primo P, $D_P = D_S$, dove S è il monoide moltiplicativo $D - P$.)

Dimostrazione. (1) Supponiamo D di Dedekind e sia I' un ideale frazionario su D_S. Allora $I' = I_S$ per un ideale frazionario I su D. Poiché D è di Dedekind, è noetheriano e dunque I è finitamente generato. Si ha $(I')^{-1} = (I_S)^{-1} = (I^{-1})_S$ per (7), e quindi

$$I'(I')^{-1} = I_S (I^{-1})_S = (II^{-1})_S = D_S$$

per (5). Dunque I' è invertibile e D_S è di Dedekind.

(2) La localizzazione D_P in $P \neq 0$ è un anello locale con unico ideale massimale P_P. Poiché D_P è di Dedekind, P_P è il suo unico ideale primo non nullo. Perciò D_P è un dominio a ideali principali (esercizio 15, p. 625) ed è quindi un anello di valutazione discreta (proposizione 9.2).

(3) Sia ora D noetheriano e supponiamo che D_P sia un anello di valutazione discreta per ogni ideale massimale P di D. Allora D_P è un dominio a ideali principali e quindi è di Dedekind. Ogni ideale frazionario I su D è finitamente generato poiché D è noetheriano. Pertanto $(I_P)^{-1} = (I^{-1})_P$, e $(II^{-1})_P = I_P (I^{-1})_P = I_P (I_P)^{-1} = D_P$ per ogni ideale massimale P. Applichiamo il principio del passaggio dal locale al globale. L'inclusione $II^{-1} \hookrightarrow D$ si localizza nell'inclusione

$(II^{-1})_P \hookrightarrow D_P$, suriettiva per ogni P. Per la proposizione 7.11 (2), p. 402, anche $II^{-1} \hookrightarrow D$ è suriettiva. Dunque $II^{-1} = D$ per ogni I e D è di Dedekind. □

La proprietà di fattorizzazione del teorema 10.1 caratterizza anch'essa i domini di Dedekind. Vale anzi il risultato più forte seguente.

Teorema 10.5. *Sia D un dominio nel quale ogni ideale intero proprio è un prodotto di ideali primi. Allora D è di Dedekind.*

Dimostrazione (Zariski–Samuel). Mostriamo anzitutto che ogni ideale primo invertibile P di D è massimale. Sia $a \in D$, $a \notin P$. Se $aD + P \neq D$, scriviamo $aD + P = P_1 \cdots P_m$, $a^2D + P = Q_1 \cdots Q_n$ con P_i, Q_j primi. Poiché $aD + P \supsetneq P$ e $a^2D + P \supsetneq P$ (essendo P primo), si ha $P_i \supsetneq P$, $Q_j \supsetneq P$ per tutti gli i, j. Passando al dominio $\bar{D} = D/P$ si ottiene $\bar{a}\bar{D} = \bar{P}_1 \cdots \bar{P}_m$ e $\bar{a}^2\bar{D} = \bar{Q}_1 \cdots \bar{Q}_n$, dove $x \mapsto \bar{x}$ è l'omomorfismo canonico. Gli ideali principali $\bar{a}\bar{D}$ e $\bar{a}^2\bar{D}$ sono invertibili, e i $\bar{P}_i$ e $\bar{Q}_j$ sono primi. Poiché $\bar{a}^2\bar{D} = (\bar{a}\bar{D})^2$, si ha $\bar{Q}_1 \cdots \bar{Q}_n = \bar{P}_1^2 \cdots \bar{P}_m^2$. Per la proposizione 10.4 le successioni di ideali primi $\{\bar{Q}_1, \ldots, \bar{Q}_n\}$ e $\{\bar{P}_1, \bar{P}_1, \ldots, \bar{P}_m, \bar{P}_m\}$ coincidono a meno dell'ordine. Lo stesso vale per le corrispondenti successioni di ideali di D contenenti P. Pertanto

$$(aD + P)^2 = P_1^2 \cdots P_m^2 = Q_1 \cdots Q_n = a^2D + P.$$

Quindi $P \subseteq (aD + P)^2 = a^2D + aP + P^2 \subseteq aD + P^2$. Per ogni $p \in P$ si può scrivere $p = ax + y$ con $x \in D$, $y \in P^2$. Allora $ax \in P$ e, siccome $a \notin P$, $x \in P$. Ne segue $P \subseteq aP + P^2 \subseteq P$, ossia $P = aP + P^2$. Moltiplicando per P^{-1} si ottiene $D = aD + P$, contro l'ipotesi. Dunque $aD + P = D$ per ogni $a \notin P$, e P è massimale.

Sia ora P un qualunque ideale primo non nullo di D e sia b un suo elemento non nullo. Abbiamo $P \supseteq bD$ e $bD = P_1P_2 \cdots P_m$, con i P_i primi e invertibili. Questi sono dunque massimali. Poiché P è primo, contiene un P_i e deve coincidere con esso; quindi è invertibile. Per ipotesi ogni ideale intero proprio è un prodotto di primi, dunque ogni ideale intero è invertibile. Ogni ideale frazionario I' è della forma aI con I intero e $a \neq 0$, e $I'(I')^{-1} = II^{-1} = D$. Ne segue che D è di Dedekind. □

Riassumiamo le caratterizzazioni ottenute.

Teorema 10.6. *Per un dominio D le seguenti condizioni sono equivalenti.*

(i) *D è di Dedekind.*

(ii) *D è noetheriano e integralmente chiuso, e ogni suo ideale primo non nullo è massimale.*

(iii) *Ogni ideale intero proprio di D si scrive in uno e un solo modo come prodotto di ideali primi, a meno dell'ordine dei fattori.*

(iv) *D è noetheriano e D_P è un anello di valutazione discreta per ogni ideale massimale P di D.*

Esercizi.

1. Dimostrare che ogni dominio fattoriale è integralmente chiuso.

2. Dimostrare che un dominio D è di Dedekind se e solo se è integralmente chiuso, è noetheriano e D/I è artiniano per ogni ideale intero I.

3. (H. Sah.) Mostrare che un dominio D è di Dedekind se e solo se possiede la proprietà seguente: per ogni ideale intero I di D e ogni $a \in I$ non nullo esiste $b \in I$ tale che $I = Da + Db$.

Traccia della dimostrazione. Per un dominio di Dedekind questa proprietà è stata indicata nell'esercizio 12, p. 625. Supponiamo ora che D la possegga. Allora D è noetheriano e si vede facilmente che ogni localizzazione D_S eredita la proprietà. Sia D un dominio locale dotato della proprietà e sia $P \neq 0$ il suo ideale massimale. Sia $I \neq 0$ un ideale di D. Allora $I = IP + Db$ per qualche $b \in I$. Per il lemma di Nakayama, $I = Db$. Dunque D è un dominio a ideali principali e quindi un anello di valutazione discreta. Concludere mediante il teorema 10.4 (3), p. 628.

Gli esercizi 4–7 mi sono stati comunicati da Tsuneo Tamagawa. Il primo è ben noto. In tutti questi esercizi D è di Dedekind con campo delle frazioni F, e x è un'indeterminata.

4. Per $f(x) \in D[x]$ si definisce il *contenuto* $c(f)$ come l'ideale di D generato dai coefficienti di f (cfr. BAI, p. 151). Provare che $c(fg) = c(f)c(g)$ per $f, g \in D[x]$.

5. Sia $S = \{f \in D[x] \mid c(f) = D\}$. Osservare che S è un sottomonoide del monoide moltiplicativo. Sia $D[x]_S$ il sottoanello di $F(x)$ formato dalle frazioni $f(x)/g(x)$ con $f(x) \in D[x]$ e $g(x) \in S$. Dimostrare che per $f(x), g(x) \in D[x]$, $g \neq 0$, la frazione $f(x)/g(x)$ appartiene a $D[x]_S$ se e solo se $c(f) \subseteq c(g)$.

6. Mostrare che $D[x]_S \cap F = D$. Se I' è un ideale di $D[x]_S$, provare che $I = I' \cap D$ è un ideale di D per il quale $ID[x]_S = I'$. Provare che $I \mapsto I' = ID[x]_S$ è una biiezione fra l'insieme degli ideali di D e quello degli ideali di $D[x]_S$.

7. Dimostrare che $D[x]_S$ è un dominio a ideali principali.

10.3 Estensioni intere di domini di Dedekind

Gli esempi classici di domini di Dedekind sono gli anelli degli interi su $\mathbb{Z}$ dei campi di numeri, cioè delle estensioni di grado finito di $\mathbb{Q}$, e gli anelli di interi dei campi di funzioni algebriche di una variabile. Dimostriamo in questo paragrafo che, se D è di Dedekind con campo delle frazioni F ed E è un'estensione di grado finito di F, allora il sottoanello D' degli elementi di E interi su D è di Dedekind. Ne segue la proprietà di Dedekind per i domini classici e quindi il teorema fondamentale sulla fattorizzazione unica degli ideali interi di questi domini in prodotti di ideali primi.

Dimostriamo dapprima la seguente proposizione.

Proposizione 10.7. *Siano D un dominio, F il suo campo delle frazioni, E un'estensione di grado finito di F e D' il sottoanello degli elementi di E interi su D. Ogni elemento di E è della forma rb^{-1}, con $r \in D'$ e $b \in D$.*

Dimostrazione. Sia $u \in E$ e sia $g(x) = x^m + a_1 x^{m-1} + \cdots + a_m \in F[x]$ un polinomio tale che $g(u) = 0$. Possiamo scrivere $a_i = c_i b^{-1}$, con $c_i, b \in D$. Allora

$$\begin{aligned} h(x) = b^m g(b^{-1}x) &= b^m(b^{-m}x^m + a_1 b^{-(m-1)}x^{m-1} + \cdots + a_m) \\ &= x^m + ba_1 x^{m-1} + b^2 a_2 x^{m-2} + \cdots + b^m a_m \end{aligned}$$

appartiene a $D[x]$ e $h(bu) = 0$. Dunque $r = bu \in D'$ e $u = b^{-1}r$, come richiesto. □

È evidente che E è il campo delle frazioni di D'. Poiché D' è l'anello degli interi di E su D, esso è integralmente chiuso in E. Pertanto D' è un dominio integralmente chiuso.

Supponiamo ora che D sia integralmente chiuso e dimostriamo la seguente proposizione.

Proposizione 10.8. *Siano D, E, F, D' come nella proposizione 10.7 e si supponga D integralmente chiuso. Siano $r \in E$ e $m(x), f(x)$ rispettivamente il polinomio minimo e il polinomio caratteristico di r su F. Le seguenti condizioni su r sono equivalenti.*

1. r è intero su D.

2. $m(x) \in D[x]$.

3. $f(x) \in D[x]$.

Se queste condizioni sono soddisfatte, $T_{E/F}(r)$ e $N_{E/F}(r)$ appartengono a D.

Dimostrazione. Poiché $f(x)$ è una potenza di $m(x)$, è chiaro che (2) $\Rightarrow$ (3). È anche evidente che (3) $\Rightarrow$ (1). Supponiamo ora che valga (1). Sia $\overline{F}$ una chiusura algebrica di F contenente E. In $\overline{F}[x]$ si ha $m(x) = \prod_i (x - r_i)$, con $r_1 = r$. Per ogni i esiste un automorfismo di $\overline{F}/F$ che manda r in r_i. Poiché r è intero su D, esiste un polinomio monico $g(x) \in D[x]$ tale che $g(r) = 0$. Applicando un automorfismo di $\overline{F}/F$ che manda r in r_i, otteniamo $g(r_i) = 0$. Ogni radice r_i di $m(x)$ è dunque intera su D. I coefficienti di $m(x)$ sono polinomi simmetrici nelle r_i e sono pertanto elementi di F interi su D. Poiché D è integralmente chiuso, essi appartengono a D. Così $m(x) \in D[x]$ e (1) $\Rightarrow$ (2). L'ultima affermazione è chiara, poiché $f(x) = x^n - T_{E/F}(r)x^{n-1} + \cdots + (-1)^n N_{E/F}(r)$. □

Per dimostrare il teorema sulle chiusure intere dei domini di Dedekind sarà essenziale la proposizione seguente.

Proposizione 10.9. *Siano D, E, F, D' come nella proposizione 10.8 e si supponga che E/F sia separabile e D noetheriano. Allora D' è un D-modulo finitamente generato.*

Dimostrazione. Poiché E/F è separabile, esistono $n = [E : F]$ monomorfismi distinti $\sigma_1, \ldots, \sigma_n$ di E/F nella chiusura algebrica $\overline{F}/F$. Inoltre, se $(u_1, \ldots, u_n)$ è una base di E/F, la matrice

$$A = \begin{pmatrix} \sigma_1(u_1) & \cdots & \sigma_1(u_n) \\ \sigma_2(u_1) & \cdots & \sigma_2(u_n) \\ \vdots & & \vdots \\ \sigma_n(u_1) & \cdots & \sigma_n(u_n) \end{pmatrix} \tag{8}$$

è invertibile (*BAI*, p. 292). Sappiamo anche che $T_{E/F}(u) = \sum_i \sigma_i(u)$ per $u \in E$ (*BAI*, p. 430). Si ha ${}^tAA = (T_{E/F}(u_i u_j))$. Quindi

$$d = \det(T_{E/F}(u_i u_j)) \neq 0. \tag{9}$$

Per la proposizione 10.7 esiste un $b_i \neq 0$ in D tale che $b_i u_i \in D'$. Possiamo pertanto supporre che $u_i \in D'$. Sia $r \in D'$ e scriviamo $r = \sum_i a_i u_i$, con $a_i \in F$. Allora $ru_j \in D'$ per $1 \leq j \leq n$ e $ru_j = \sum_i a_i u_i u_j$. Pertanto

$$T_{E/F}(ru_j) = \sum_i a_i T_{E/F}(u_i u_j) \in D. \tag{10}$$

Il sistema (10) nelle incognite a_i, $1 \leq i \leq n$, si risolve con la regola di Cramer. Ne segue che $a_i \in d^{-1}D$. Poiché ciò vale per ogni $r \in D'$, D' è contenuto nel D-modulo $M = \sum_i D(d^{-1}u_i)$. Abbiamo dunque incluso D' in un D-modulo finitamente generato. Poiché D è noetheriano, M è un D-modulo noetheriano. Il suo sottomodulo D' è quindi finitamente generato. □

Possiamo ora dimostrare il risultato principale del paragrafo.

Teorema 10.7. *Siano D un dominio di Dedekind, F il suo campo delle frazioni, E un'estensione di grado finito di F e D' il sottoanello degli elementi di E interi su D. Allora D' è di Dedekind.*

Dimostrazione. Supponiamo dapprima che E sia separabile su F. In questo caso dimostreremo che D' possiede le tre proprietà che caratterizzano i domini di Dedekind nel teorema 10.3: (1) D' è noetheriano, (2) ogni ideale primo non nullo di D' è massimale e (3) D' è integralmente chiuso.

La prima segue dalla proposizione 10.9, la quale implica che D' è un D-modulo noetheriano. A maggior ragione D' è noetheriano come D'-modulo. Sia ora P' un ideale primo non nullo di D'. Prendiamo $r \neq 0$ in P'. Per il polinomio caratteristico $f(x)$ di r si ha $f(r) = 0$. Ne segue che $N_{E/F}(r) \in P'$ e quindi, per la proposizione 10.8, $N_{E/F}(r) \in P = P' \cap D$. Poiché $N_{E/F}(r) \neq 0$, vediamo che $P \neq 0$. È anche chiaro che P è un ideale primo di D. Essendo D di Dedekind, P è un ideale massimale di D. Dal corollario alla proposizione 7.17, p. 410, concludiamo che P' è massimale in D'. Vale dunque (2). L'osservazione successiva alla proposizione 10.7 dà (3). Nel caso separabile D' è perciò di Dedekind.

Supponiamo ora che $\operatorname{char} F = p$ e che E sia puramente inseparabile su F. Poiché $[E : F] < \infty$, esiste $q = p^e$ tale che $u^{p^e} \in F$ per ogni $u \in E$. Sia $\overline{F}$ una chiusura algebrica di F contenente E. Indichiamo con $F^{1/q}$ (rispettivamente $D^{1/q}$) il sottocampo (rispettivamente sottoanello) di $\overline{F}$ costituito dagli elementi v tali che $v^q \in F$ (rispettivamente $v^q \in D$). Allora $v \mapsto v^q$ è un isomorfismo di $F^{1/q}$ su F che manda $D^{1/q}$ su D. Poiché D è di Dedekind, lo è anche $D^{1/q}$. Se $u \in D'$, si ha $u^q \in F$ e u^q è intero su D. Dunque $u^q \in D$ e $D' \subset D^{1/q}$. Proveremo ora che D' è di Dedekind mostrando che ogni ideale frazionario I di D' in E è invertibile. Poniamo $I' = D^{1/q}I$. Allora I' è un ideale frazionario di $D^{1/q}$. Esiste quindi un ideale frazionario J' di $D^{1/q}$ tale che $I'J' = D^{1/q}$. Da $I' = ID^{1/q}$ e $D^{1/q}J' = J'$ segue che esistono elementi $b_i \in I$, $c_i' \in J'$ con $\sum_i b_i c_i' = 1$. Allora $\sum_i b_i^q (c_i')^q = 1$, e dunque $\sum_i b_i c_i = 1$, dove $c_i = b_i^{q-1}(c_i')^q$. Ora $b_i^{q-1}(c_i')^q \in (I')^{q-1}(J')^q \subset J'$. Poiché $(c_i')^q \in F$ e $b_i \in E$, abbiamo $c_i = b_i^{q-1}(c_i')^q \in E$. Dunque $c_i \in J = J' \cap E$. È chiaro che $IJ \subset D^{1/q} \cap E$ e, poiché gli elementi di $D^{1/q}$ sono interi su D, si ha $D^{1/q} \cap E \subset D'$. Perciò $IJ \subset D'$ e $J \subset I^{-1}$. Poiché $c_i \in J$, $b_i \in I$ e $\sum_i c_i b_i = 1$, otteniamo $II^{-1} = D'$. Pertanto I è invertibile e D' è di Dedekind.

Il caso generale si ottiene combinando i due precedenti. Se E è un'estensione qualsiasi di grado finito di F, sia K il massimo sottocampo separabile di E/F. Allora E è puramente inseparabile su K. Per il primo caso $D'' = D' \cap K$ è di Dedekind e, poiché D' è l'insieme degli elementi di E interi su D'', per il secondo caso D' è di Dedekind. La dimostrazione è completa. □

Il risultato precedente si applica in particolare a $F = \mathbb{Q}$, $D = \mathbb{Z}$, e a $F = K(x)$, dove K è un campo qualsiasi, x un'indeterminata e $D = K[x]$. Infatti questi D sono domini a ideali principali, e dunque domini di Dedekind. Se E è un'estensione di grado finito di F, l'anello D' degli interi di E su D è di Dedekind. Nel caso $F = \mathbb{Q}$, $D = \mathbb{Z}$, E è un campo di numeri; negli altri casi E è un campo di funzioni algebriche di una variabile.

Esercizi

1. Con le notazioni del teorema 10.7, si supponga che E/F sia separabile e che D sia un dominio a ideali principali. Mostrare che D' è un D-modulo libero di rango $n = [E : F]$.

   Gli esercizi 3, 4 e 5 di *BAI*, p. 287, sono pertinenti a questo paragrafo.

2. (Sah.) Mostrare che, se D è un dominio di Dedekind, lo è anche l'anello $D((x))$ delle serie di Laurent su D. (Suggerimento. È facile vedere che $D((x))$ è un dominio. Per un ideale I di $D((x))$, sia $l(I)$ l'insieme dei coefficienti iniziali degli elementi di I. Allora $l(I)$ è un ideale e, se $l(I) = Da_1 + \cdots + Da_m$, dove a_i è il coefficiente iniziale di $f_i \in I$, allora $I = D((x))f_1 + \cdots + D((x))f_m$. Usare questo fatto e l'esercizio 3 di p. 630.)

10.4 Relazioni con la teoria delle valutazioni

Diamo dapprima una caratterizzazione, in termini di valutazioni, della chiusura intera di un sottoanello di un campo.

Teorema 10.8 (Krull). *Sia D un sottoanello di un campo F e sia D' la chiusura intera di D in F (il sottoanello degli elementi di F interi su D). Allora D' è l'intersezione degli anelli di valutazione di F contenenti D.*

Dimostrazione. Siano $u \in D'$, R un anello di valutazione di F contenente D e φ una valutazione di F con anello di valutazione R (per esempio, la valutazione canonica definita da R). Se $u \notin R$, si ha $\varphi(u^{-1}) < 1$. D'altra parte esiste una relazione $u^n + a_1 u^{n-1} + \cdots + a_n = 0$, $a_i \in D$, da cui

$$1 = -a_1 u^{-1} - a_2 u^{-2} - \cdots - a_n u^{-n}. \tag{11}$$

Poiché $a_i \in D \subset R$, si ha $\varphi(a_i) \leq 1$ e quindi $\varphi(a_i u^{-i}) < 1$. Essendo $\varphi(1) = 1$, si ottiene la contraddizione $1 \leq \max_i\{\varphi(a_i u^{-i})\} < 1$. Dunque $u \in R$ e $D' \subset \bigcap R$, dove l'intersezione è estesa a tutti gli anelli di valutazione di F contenenti D.

Supponiamo ora che $u \notin D'$. Allora u^{-1} non è invertibile nel sottoanello $D[u^{-1}]$ di F, perché in caso contrario il suo inverso sarebbe $u = a_0 + a_1 u^{-1} + \cdots + a_{n-1} u^{-(n-1)}$, con $a_i \in D$. Avremmo $u^n = a_0 u^{n-1} + a_1 u^{n-2} + \cdots + a_{n-1}$, contro l'ipotesi $u \notin D'$. Di conseguenza $u^{-1} D[u^{-1}]$ è un ideale proprio di $D[u^{-1}]$, contenuto in un ideale massimale P_0 di $D[u^{-1}]$. Allora $\Delta = D[u^{-1}]/P_0$ è un campo e l'omomorfismo canonico di $D[u^{-1}]$ su Δ si può considerare come un omomorfismo $\mathcal{P}_0$ di $D[u^{-1}]$ in una chiusura algebrica $\overline{\Delta}$ di Δ. Per il teorema 9.10 (p. 561) esiste un posto $\mathcal{P}$ a valori in $\overline{\Delta}$ che estende $\mathcal{P}_0$. Se R è l'anello di valutazione su cui è definito $\mathcal{P}$ e P il suo ideale massimale, allora P è il nucleo di $\mathcal{P}$. Abbiamo $R \supset D[u^{-1}] \supset D$ e $P \supset P_0$. Quindi $u^{-1} D[u^{-1}] \subset P_0 \subset P$, da cui $\mathcal{P}(u^{-1}) = 0$ e pertanto $u \notin R$. Abbiamo mostrato che da $u \notin D'$ segue $u \notin \bigcap R$ al variare di R fra gli anelli di valutazione di F contenenti D. Dunque $D' = \bigcap R$. □

Sia ora D di Dedekind con campo delle frazioni F. Essendo integralmente chiuso, D è l'intersezione degli anelli di valutazione di F che lo contengono. Affermiamo che questi anelli sono le localizzazioni D_P corrispondenti agli ideali primi P di D. Abbiamo visto che, per ogni ideale primo non nullo P di D, D_P è un anello di valutazione discreta. Anche D_0 è un anello di valutazione, essendo uguale a F. Sia ora $R \neq F$ un anello di valutazione di F contenente D, sia M il suo ideale massimale e poniamo $P = M \cap D$. Allora P è un ideale primo di D e, se $P = 0$, ogni elemento non nullo di D è invertibile in R. Essendo F il campo delle frazioni di D, ne seguirebbe $F = R$, contro l'ipotesi. Dunque P è un ideale primo intero non nullo di D. L'anello di valutazione D_P ha ideale massimale $P_P = PD_P$. Se $a \in D \setminus P$, allora $a \in R \setminus M$ e $a^{-1} \in R$. Dunque $R \supset D_P$. Inoltre, poiché $M \supset P$, vale $M = RM \supset D_P P$. È facile vedere che, se R_1, R_2 sono anelli di valutazione con ideali massimali M_1, M_2, da $R_1 \supset R_2$ e $M_1 \supset M_2$ seguono $R_1 = R_2$ e $M_1 = M_2$. Perciò $R = D_P$ e $M = PD_P$. Gli anelli di valutazione di F che contengono D e sono diversi da F sono precisamente le localizzazioni D_P negli ideali primi non nulli P di D. Per il teorema 10.8, $D = \bigcap D_P$.

Un ideale primo $P \neq 0$ di un dominio di Dedekind D determina una valutazione esponenziale v_P del campo delle frazioni F di D, in modo analogo alla valutazione esponenziale v_p di $\mathbb{Q}$ definita da un numero primo p. Se $a \neq 0$ appartiene a F, scriviamo $Da = P^k P_1^{k_1} \cdots P_l^{k_l}$, dove $P, P_1, \ldots, P_l$ sono ideali primi distinti e $k, k_i \in \mathbb{Z}$. Poniamo $v_P(a) = k$ e inoltre $v_P(0) = \infty$. Come nel caso particolare di $\mathbb{Q}$, si verifica subito che v_P è una valutazione esponenziale di F. Preso quindi un numero reale γ, $0 < \gamma < 1$, la formula $|a|_P = \gamma^{v_P(a)}$ definisce un valore assoluto non archimedeo su F. Lo chiamiamo un *valore assoluto P-adico* su F. L'anello di valutazione di $|\cdot|_P$ contiene evidentemente la localizzazione D_P e il suo ideale massimale contiene PD_P. Pertanto l'anello di valutazione di $|\cdot|_P$ è D_P e il suo ideale massimale è PD_P.

Poiché D_P è di Dedekind e PD_P è il suo unico ideale primo non nullo, gli ideali interi non nulli di D_P sono i $P^k D_P$, $k \geq 0$. Evidentemente $P^k \subset P^k D_P \cap D$. Reciprocamente, se $a \in P^k D_P \cap D$, con $k \geq 1$, si ha $a = bc^{-1}$ con $b \in P^k$, $c \in D \setminus P$. Quindi $ac \equiv 0 \bmod P^k$ e $c \not\equiv 0 \bmod P$.

Quest'ultima condizione implica che $c + P$ è invertibile in D/P. Allora $c + P^k$ è invertibile in D/P^k (p. 195). Ne segue $a \in P^k$. Perciò $P^k D_P \cap D = P^k$ per $k \geq 0$.

Sia $|\cdot|$ un valore assoluto non archimedeo con anello di valutazione D_P. Affermiamo che $|\cdot| = |\cdot|_P$ per una valutazione P-adica determinata da P. Osserviamo infatti che $PD_P = \pi D_P$, dove $\pi \in PD_P$, $\pi \notin P^2 D_P$. Allora $P^k D_P = \pi^k D_P$ per $k \geq 0$, e ogni elemento non nullo di D_P si scrive $u\pi^k$, con u invertibile in D_P e $k \geq 0$. Si ha $|u\pi^k| = \gamma^k$, dove $|\pi| = \gamma$, $0 < \gamma < 1$. Quindi, se $a \in P^k \setminus P^{k+1}$, vale $a \in P^k D_P \setminus P^{k+1} D_P$ e $|a| = \gamma^k$. D'altra parte, evidentemente $Da = P^k P_1^{k_1} \cdots P_l^{k_l}$ con $P_1, \ldots, P_l$ primi diversi da P. Se $|\cdot|_P$ è la valutazione P-adica determinata da γ, allora $|a|_P = |a|$ per $a \in D$. Quindi $|\cdot| = |\cdot|_P$.

Mostriamo ora che il campo residuo D_P/P_P di $|\cdot|_P$ è canonicamente isomorfo a D/P. Da $P = P_P \cap D$ si ottiene il monomorfismo $a + P \mapsto a + P_P$ di D/P in D_P/P_P. Se $a, b \in D$ e $b \notin P$, poiché D/P è un campo esiste $c \in D$ tale che $cb \equiv a \bmod P$. Allora $ab^{-1} \equiv c \bmod P_P$ e dunque $a + P \mapsto a + P_P$ è suriettivo su D_P/P_P. Tale applicazione è quindi un isomorfismo.

Raccogliamo questi risultati nella seguente proposizione.

Proposizione 10.10. *Sia D un dominio di Dedekind con campo delle frazioni F. (1) Ogni anello di valutazione di F contenente D è della forma D_P, con P ideale primo di D. (2) Ogni valore assoluto non archimedeo di F con anello di valutazione D_P, $P \neq 0$, è una valutazione P-adica. (3) L'applicazione $a + P \mapsto a + P_P$ è un isomorfismo di D/P su D_P/P_P.*

Sia ora E un'estensione di grado finito di F e sia D' l'anello degli interi di E su D. Allora D' è di Dedekind. Se P è un ideale primo intero non nullo di D, l'ideale che esso genera in D' è $D'P$. Si ha $D'P \neq D'$. Infatti, per il teorema di esistenza degli ideali primi sovrastanti (p. 411), esiste un ideale primo P' di D' tale che $P' \cap D = P$. Quindi $P' \supset PD'$ e $PD' \neq D'$. Può accadere che l'ideale esteso PD' non sia primo. Si ha comunque una fattorizzazione

$$PD' = (P_1')^{e_1} \cdots (P_g')^{e_g}, \tag{12}$$

dove i P_i' sono ideali primi distinti di D' e gli e_i sono positivi.

Nel capitolo 9 (p. 585) abbiamo studiato il problema generale dell'estensione di un valore assoluto di un campo F a un'estensione di grado finito. Tratteremo ora il caso particolare di un valore assoluto P-adico del campo delle frazioni F di un dominio di Dedekind con un altro metodo, basato sulla fattorizzazione (12). Dimostriamo dapprima il seguente teorema.

Teorema 10.9. *Siano D un dominio di Dedekind, F il suo campo delle frazioni, E un'estensione di grado finito di F e D' il sottoanello degli elementi di E interi su D. Siano P un ideale primo intero non nullo di D, $|\cdot|_P$ un valore assoluto P-adico di F e (12) la fattorizzazione di PD' in ideali primi di D'. Per ciascun P_i' esiste un unico valore assoluto P_i'-adico $|\cdot|_{P_i'}$ su E che estende $|\cdot|_P$. Inoltre $|\cdot|_{P_i'}$ e $|\cdot|_{P_j'}$ sono inequivalenti se $i \neq j$, e i valori assoluti $|\cdot|_{P_i'}$ sono le sole estensioni di $|\cdot|_P$ a valori assoluti su E.*

Dimostrazione. Sia $0 \neq a \in F$ e scriviamo $Da = P^k P_1^{k_1} \cdots P_l^{k_l}$, dove P e i P_j sono ideali primi distinti e $k, k_j \in \mathbb{Z}$. Allora $v_P(a) = k$ e, per la (12),

$$\begin{aligned} D'a &= (D'P)^k (D'P_1)^{k_1} \cdots (D'P_l)^{k_l} \\ &= (P_1')^{e_1 k} (P_2')^{e_2 k} \cdots (P_g')^{e_g k} \cdots , \end{aligned} \tag{13}$$

dove i termini dopo $(P_g')^{e_g k}$ provengono dalle fattorizzazioni dei $D'P_j$ in ideali primi di D'. Se P_1 e P_2 sono ideali primi distinti di D, allora $P_1 + P_2 = D$ e quindi $D'P_1 + D'P_2 = D'$. Ciò implica che gli ideali primi di D' che dividono $D'P_1$ sono diversi da quelli che dividono $D'P_2$. Ne segue che $v_{P_j'}(a) = e_j k$. Se dunque $|\cdot|_P = \gamma^{v_P(\cdot)}$ con $0 < \gamma < 1$, avremo $|\cdot|_P = |\cdot|_{P_j'}$ su F se e solo se $|\cdot|_{P_j'} = (\gamma^{1/e_j})^{v_{P_j'}(\cdot)}$. Ciò dimostra la prima affermazione.

Abbiamo visto che l'anello di valutazione di $|\cdot|_{P'_j}$ (o di $v_{P'_j}$) è $D'_{P'_j}$. Questi anelli sono distinti per scelte diverse di j, quindi $|\cdot|_{P'_i}$ e $|\cdot|_{P'_j}$ sono inequivalenti per $i \neq j$. Sia ora $|\cdot|'$ un qualunque valore assoluto di E che estende $|\cdot|_P$, e sia R' il suo anello di valutazione. Allora $R' \supset D_P$ e, poiché D' è la chiusura intera di D in E, il teorema 10.8 dà $R' \supset D'$. Per la proposizione 10.10(1), $R' = D'_{P'}$ per un ideale primo P' di D'. Poiché la valutazione si restringe a quella di D_P, si ha $P' \supset P$, e quindi $P' = P'_i$ per qualche i. Per la proposizione 10.10(2), $|\cdot|'$ è una valutazione P'_i-adica. □

Ricordiamo che l'indice di ramificazione di $|\cdot|_{P'_i}$ rispetto a $|\cdot|_P$ è l'indice $[|E^*|_{P'_i} : |F^*|_P]$ (p. 589). Poiché $|F^*|_P$ è il sottogruppo di $\mathbb{R}^*$ generato da γ e $|E^*|_{P'_i}$ è quello generato da γ^{1/e_i}, l'indice di ramificazione è e_i.

Ricordiamo anche che il grado residuo f_i di $|\cdot|_{P'_i}$ rispetto a $|\cdot|_P$ è la dimensione $[D'_{P'_i}/P'_{iP'_i} : D_P/P_P]$, dove D_P/P_P è immerso in $D'_{P'_i}/P'_{iP'_i}$ mediante il monomorfismo $x + P_P \mapsto x + P'_{iP'_i}$ (p. 589). Si ha anche un monomorfismo $a + P \mapsto a + P'_i$, $a \in D$, di D/P in D'/P'_i, cosicché è definita la dimensione $[D'/P'_i : D/P]$. Ora abbiamo gli isomorfismi $\sigma\colon a + P \mapsto a + P_P$ e $s\colon x + P'_i \mapsto x + P'_{iP'_i}$, rispettivamente di D/P su D_P/P_P e di D'/P'_i su $D'_{P'_i}/P'_{iP'_i}$. Si ha $s((a + P)(x + P'_i)) = s(ax + P'_i) = ax + P'_{iP'_i}$, e anche

$$\sigma(a + P)s(x + P'_i) = (a + P_P)(x + P'_{iP'_i}) = ax + P'_{iP'_i}.$$

Dunque s è un isomorfismo semilineare di D'/P'_i, considerato su D/P, su $D'_{P'_i}/P'_{iP'_i}$, con isomorfismo associato dei campi σ. Ne segue che il grado residuo f_i coincide con la dimensione $[D'/P'_i : D/P]$.

I risultati sull'indice di ramificazione e sul grado residuo si possono enunciare come segue.

Teorema 10.10. *Con le notazioni del teorema 10.9, siano $|\cdot|_P$ un valore assoluto P-adico di F e $|\cdot|_{P'}$ un valore assoluto P'_i-adico di E che estende $|\cdot|_P$. Allora e_i è l'indice di ramificazione e $[D'/P'_i : D/P]$ è il grado residuo di $|\cdot|_{P'_i}$ rispetto a $|\cdot|_P$.*

Da questo risultato e dal teorema principale sui gradi residui e sugli indici di ramificazione (teorema 9.15, p. 592) segue immediatamente il seguente teorema.

Teorema 10.11. *Con le notazioni del teorema 10.9 si ha $\sum_i e_i f_i \leq n = [E : F]$, dove $f_i = [D'/P'_i : D/P]$. Inoltre $\sum_i e_i f_i = n$ se E/F è separabile.*

In particolare il numero g degli ideali primi di D' contenenti $D'P$ è al più n. Il risultato fornisce inoltre informazioni assai più precise sulla fattorizzazione (12).

Esercizi

1. Sia E il campo ciclotomico $\mathbb{Q}(\zeta)$, dove ζ è una radice primitiva ℓ-esima dell'unità e ℓ è primo. Siano $D = \mathbb{Z}$ e D' la chiusura intera di $\mathbb{Z}$ in E. Mostrare che $\ell D' = ((\zeta - 1)D')^{\ell-1}$ e che $(\zeta - 1)D'$ è un ideale primo di D'. (Suggerimento. $[E : \mathbb{Q}] = \ell - 1$ e $f(x) = x^{\ell-1} + x^{\ell-2} + \cdots + 1$ è il polinomio minimo di ζ. Si ha $f(x) = \prod_{i=1}^{\ell-1}(x - \zeta^i)$ in $E[x]$ e ogni ζ^i, $1 \leq i \leq \ell - 1$, è una radice primitiva ℓ-esima di 1. Si veda *BAI*, p. 154. Sostituendo 1 in $f(x)$ si ottiene $\ell = \prod_{i=1}^{\ell-1}(1 - \zeta^i)$. Inoltre $(1 - \zeta^i)/(1 - \zeta) = 1 + \zeta + \cdots + \zeta^{i-1} \in D'$. Mostrare che $1 + \zeta + \cdots + \zeta^{i-1}$ è invertibile in D', sicché $\ell D' = ((\zeta - 1)D')^{\ell-1}$. Mostrare che ℓ non è invertibile in D' e usare il teorema 10.11 per concludere che $(\zeta - 1)D'$ è primo.)

   I tre esercizi seguenti mostrano che, nel caso particolare del teorema 10.11 in cui E/F è galoisiana, la fattorizzazione (12) è $PD' = (P'_1 \cdots P'_g)^e$ e tutti i gradi residui sono uguali. Dunque $n = [E : F] = efg$.

2. Sia E/F galoisiana, con $\mathrm{Gal}(E/F) = G$. Mostrare che ogni $\sigma \in G$ manda D' in sé. Mostrare che, se P' è un ideale primo di D', anche $\sigma P'$ è un ideale primo. Mostrare che $\sigma\colon a + P' \mapsto \sigma a + \sigma P'$ è un isomorfismo di D'/P' su $D'/\sigma P'$.

3. Sia P un ideale primo non nullo di D e sia $PD' = (P'_1)^{e_1} \cdots (P'_g)^{e_g}$ la fattorizzazione di PD' in ideali primi di D', con $P'_i \neq P'_j$ se $i \neq j$. Mostrare che, per $\sigma \in G$, vale $\{\sigma P'_1, \ldots, \sigma P'_g\} = \{P'_1, \ldots, P'_g\}$ e che G agisce transitivamente sull'insieme degli ideali primi $\{P'_1, \ldots, P'_g\}$. (Suggerimento. Per dimostrare la transitività si mostri che, se P' è un ideale primo di D' tale che $P' \cap D = P$, ogni ideale primo Q di D' tale che $Q \cap D = P$ è uno degli ideali $\sigma P'$, $\sigma \in G$. In caso contrario, per la proposizione 7.1, p. 390, $Q \not\subset \bigcup_{\sigma\in G} \sigma P'$. Esiste dunque $a \in Q$ tale che $\sigma a \notin P'$ per ogni $\sigma \in G$. Allora $N_{E/F}(a) = \prod_{\sigma\in G} \sigma a \notin P'$. Ciò è assurdo, poiché $N_{E/F}(a) \in Q \cap D = P$.)

4. Usare i risultati degli esercizi 2 e 3 per mostrare che $e_i = e_j$ per ogni i, j e che i campi D'/P'_i e D'/P'_j sono isomorfi su D/P. Concludere che $[D'/P'_i : D/P] = [D'/P'_j : D/P]$. Ponendo $e = e_i$, $f = f_i = [D'/P'_i : D/P]$, mostrare che $n = efg$.

10.5 Ideali primi ramificati e discriminante

Come nel paragrafo precedente, sia D un dominio di Dedekind, F il suo campo delle frazioni, E un'estensione di dimensione finita di F e D' il sottoanello degli elementi di E interi su D. Sia P un ideale primo non nullo di D e sia $PD' = (P'_1)^{e_1} \cdots (P'_g)^{e_g}$, dove i P'_i sono ideali primi distinti di D', come nella (12). Consideriamo l'anello $\overline{D'} = D'/PD'$, che possiamo anche riguardare come modulo su D' e, per restrizione, come modulo su D. Poiché P annulla $\overline{D'}$, quest'ultimo si può considerare anche come spazio vettoriale su $\overline{D} = D/P$. L'azione di $a + P$, $a \in D$, su $x + PD'$, $x \in D'$, è data da $(a + P)(x + PD') = ax + PD'$. Considerando insieme la struttura di anello e quella di spazio vettoriale su $\overline{D}$, otteniamo l'algebra $\overline{D'}$ su $\overline{D}$. Ne studieremo ora la struttura. Il risultato principale è il seguente.

Teorema 10.12. *Sia D un dominio di Dedekind con campo delle frazioni F, sia E un'estensione di dimensione finita di F e sia D' il sottoanello di E costituito dagli elementi interi su D. Sia P un ideale primo non nullo di D e $PD' = (P'_1)^{e_1} \cdots (P'_g)^{e_g}$, dove i P'_i sono ideali primi distinti di D' ed $e_i > 0$. Allora $\overline{D'} = D'/PD'$ è un'algebra sul campo $\overline{D} = D/P$ con $(a+P)(x+PD') = ax + PD'$, per $a \in D$, $x \in D'$. La sua dimensione è $[\overline{D'} : \overline{D}] = \sum_{i=1}^{g} e_i f_i$, dove f_i è il grado residuo $[D'/P'_i : \overline{D}]$. Si ha $[\overline{D'} : \overline{D}] \leq n = [E : F]$, con uguaglianza se E/F è separabile. L'algebra $\overline{D'}$ è somma diretta di g ideali isomorfi alle algebre $D'/(P'_i)^{e_i}$. Il radicale di $\overline{D'}$ è $P'_1 \cdots P'_g/PD'$ e $\overline{D'}/\operatorname{rad}\overline{D'}$ è somma diretta di g ideali isomorfi ai campi D'/P'_i.*

Dimostrazione. Poniamo $A'_i = (P'_i)^{-e_i}(P'_1)^{e_1} \cdots (P'_g)^{e_g}$. Allora

$$\sum_i A'_i = D', \qquad A'_i \cap \sum_{j\neq i} A'_j = D'P. \tag{14}$$

Ne segue

$$\overline{D'} = D'/PD' = A'_1/PD' \oplus \cdots \oplus A'_g/PD', \tag{15}$$

e inoltre

$$A'_i/PD' = A'_i/(A'_i \cap (P'_i)^{e_i}) \cong (A'_i + (P'_i)^{e_i})/(P'_i)^{e_i} = D'/(P'_i)^{e_i}.$$

Pertanto

$$\overline{D'} \cong D'/(P'_1)^{e_1} \oplus \cdots \oplus D'/(P'_g)^{e_g}. \tag{16}$$

Abbiamo la catena di ideali

$$D' \supset P_i' \supset (P_i')^2 \supset \cdots \supset (P_i')^{e_i}, \qquad 1 \le i \le g, \tag{17}$$

ciascuno dei quali è minimale fra gli ideali che contengono propriamente il successivo. Quindi

$$D'/(P_i')^{e_i} \supset P_i'/(P_i')^{e_i} \supset \cdots \supset 0 \tag{18}$$

è una serie di composizione per $D'/(P_i')^{e_i}$ come D'-modulo. I fattori di composizione sono isomorfi a D'/P_i', $P_i'/(P_i')^2, \ldots, (P_i')^{e_i-1}/(P_i')^{e_i}$. Ognuno è annullato da P_i' e si può dunque considerare come spazio vettoriale sul campo D'/P_i'. Poiché questi spazi vettoriali non hanno sottospazi propri non nulli, hanno dimensione uno su D'/P_i'. I fattori di composizione sono fra loro isomorfi come D'-moduli, quindi anche come D-moduli e come spazi vettoriali su $\overline{D}$. Ne segue $[(P_i')^{j-1}/(P_i')^j : \overline{D}] = [D'/P_i' : \overline{D}] = f_i$ per $j = 1, \ldots, e_i$. Per la (18) abbiamo $[D'/(P_i')^{e_i} : \overline{D}] = e_i f_i$. La (16) dà allora $[\overline{D'} : \overline{D}] = \sum_{i=1}^{g} e_i f_i$. Nel teorema 10.11 abbiamo dimostrato che $\sum e_i f_i \le n$, con uguaglianza se E/F è separabile. Dunque $[\overline{D'} : \overline{D}] \le n$ ed è uguale a n se E/F è separabile.

Sia $e = \max\{e_i\}$. Allora $(P_1' P_2' \cdots P_g')^e \subseteq D'P$. Quindi $P_1' \cdots P_g'/D'P$ è un ideale nilpotente in $\overline{D'} = D'/D'P$ e

$$\overline{D'}/(P_1' \cdots P_g'/D'P) \cong D'/(P_1' \cdots P_g') \cong D'/P_1' \oplus \cdots \oplus D'/P_g'.$$

Poiché ogni D'/P_i' è un campo, segue $P_1' \cdots P_g'/D'P = \operatorname{rad} \overline{D'}$ e $\overline{D'}/\operatorname{rad} \overline{D'}$ è somma diretta di g ideali isomorfi ai campi D'/P_i'. □

Definizione 10.4. Un ideale primo non nullo P di D si dice *non ramificato* in D' se $D'P = P_1' \cdots P_g'$, dove i P_i' sono ideali primi distinti di D' e ogni D'/P_i' è separabile su $\overline{D} = D/P$. Negli altri casi P si dice *ramificato* in D'.

Per il teorema 10.12, P è non ramificato in D' se e solo se $\overline{D'} = D'/D'P$ è somma diretta di campi separabili su $\overline{D} = D/P$. Mostreremo che, se E/F è separabile, soltanto un numero finito di ideali primi P di D si ramifica in D' e, in linea di principio, determineremo quali siano. A questo scopo diamo la definizione seguente.

Definizione 10.5. Siano D, F, E, D' come sopra e supponiamo E/F separabile. L'*ideale discriminante* $d_{D'/D}$ di D' su D è l'ideale generato da tutti gli elementi

$$\det(T_{E/F}(u_i u_j)), \tag{19}$$

dove $(u_1, \ldots, u_n)$ è una base di E/F formata da elementi $u_i \in D'$.

Nella dimostrazione della proposizione 10.9 abbiamo visto che $\det(T_{E/F}(u_i u_j)) \neq 0$ per ogni base $(u_1, \ldots, u_n)$ di un'estensione separabile E/F. Il risultato principale sulla ramificazione è il seguente.

Teorema 10.13. *Sia D un dominio di Dedekind con campo delle frazioni F, sia E un'estensione separabile di dimensione finita di F e sia D' il sottoanello degli elementi di E interi su D. Un ideale primo non nullo P di D si ramifica in D' se e solo se P divide il discriminante $d_{D'/D}$.*

Ciò implica naturalmente che i primi ramificati sono in numero finito. Per dimostrare il teorema 10.13 ci occorre un criterio, espresso mediante la traccia, affinché un'algebra commutativa A di dimensione finita su un campo F sia somma diretta di ideali che siano estensioni separabili di F.

Se A è un'algebra di dimensione finita su un campo F, definiamo su A/F la *forma bilineare traccia* $T(a, b)$ mediante

$$T(a, b) = T_{A/F}(ab), \tag{20}$$

dove $T_{A/F}$ è la traccia definita dalla rappresentazione regolare. Poiché $T_{A/F}$ è lineare e $T_{A/F}(ab) = T_{A/F}(ba)$, la forma $T(a,b)$ è bilineare simmetrica (*BAI*, pp. 424, 426). Ricordiamo inoltre che $T(a,b)$ è non degenere se e solo se $\det(T(u_i,u_j)) \neq 0$ per una qualunque base $(u_1,\dots,u_n)$ di A/F. Ci occorre il lemma seguente.

Lemma. *Se A è un'algebra commutativa di dimensione finita su un campo F, allora A/F è somma diretta di ideali che sono campi separabili su F se e solo se la forma bilineare traccia $T(a,b)$ è non degenere su A.*

Dimostrazione. Supponiamo dapprima $A = E_1 \oplus \cdots \oplus E_g$, dove ogni E_i è un'estensione separabile di F. Sia $(u_{i1},\dots,u_{in_i})$ una base di E_i. Allora $(u_{11},\dots,u_{1n_1},\dots,u_{g1},\dots,u_{gn_g})$ è una base di A/F e

$$\det(T(u_{ik},u_{jl})) = \prod_{i=1}^{g} \det(T_i(u_{ik},u_{il})), \tag{21}$$

dove T_i indica la forma bilineare traccia su E_i. Avendo dimostrato che T_i è non degenere (p. 612 nell'originale), concludiamo dalla formula che T è non degenere su A.

Viceversa, supponiamo T non degenere su A. Mostriamo dapprima che A è semiprimitiva. Sia $z \in \operatorname{rad} A$. Allora $za = az$ è nilpotente per ogni $a \in A$. Poiché la traccia di una trasformazione lineare è la somma delle sue radici caratteristiche, una trasformazione nilpotente ha traccia nulla. Quindi $T(a,z) = 0$ per ogni a, e dalla non degenerazione di T segue $z = 0$. Si ha dunque $\operatorname{rad} A = 0$ e A è semiprimitiva. Allora $A = E_1 \oplus \cdots \oplus E_g$ con E_i estensioni di F. Per la (21), la forma bilineare traccia T_i è non degenere su ogni E_i. D'altra parte, se E/F è un'estensione inseparabile di dimensione finita, la funzione traccia è identicamente nulla su E. Infatti $E \supsetneq S$, dove S è il massimo sottocampo separabile di E/F. Allora E è puramente inseparabile su S ed esiste un sottocampo K di E contenente S tale che $[E:K] = p$, la caratteristica. Il polinomio minimo su K di un qualunque $a \in E$ è della forma $x^p - \alpha$ oppure $x - \alpha$. In entrambi i casi il polinomio caratteristico ha la forma $x^p - \beta$ (nel secondo caso $\beta = \alpha^p$). Dunque $T_{E/K}(a) = 0$ per ogni a. Per la transitività della traccia (*BAI*, p. 426) si ha $T_{E/F}(a) = T_{K/F}(T_{E/K}(a)) = 0$. La forma bilineare traccia di un'estensione inseparabile è quindi identicamente nulla. Ne segue che ogni E_i è separabile. □

Dimostrazione del teorema 10.13. Supponiamo dapprima che D sia un dominio a ideali principali. Per la proposizione 10.9, D' è finitamente generato come D-modulo. Poiché è privo di torsione e D è a ideali principali, D' è un D-modulo libero. Ogni elemento di E è della forma $r^{-1}u$, con $r \in D$, $u \in D'$, perciò il rango di D' su D è $n = [E:F]$. Sia $(v_1,\dots,v_n)$ una D-base di D'. Allora $\det(T(v_i,v_j))$ genera $d_{D'/D}$, sicché dobbiamo mostrare che $\overline{D'}$ è somma diretta di estensioni separabili di $\overline{D}$ se e solo se P non contiene $\det(T(v_i,v_j))$. Dato che $(v_1,\dots,v_n)$ è una D-base di D', si ha $PD' = \sum Pv_i$ e, posto $\bar{v}_i = v_i + PD'$, la famiglia $(\bar{v}_1,\dots,\bar{v}_n)$ è una base di $\overline{D'}$ su $\overline{D}$. Se $a \mapsto \rho(a)$ è la rappresentazione matriciale regolare di E/F relativa alla base $(v_1,\dots,v_n)$, la rappresentazione matriciale regolare di $\overline{D'}/\overline{D}$ nella base $(\bar{v}_1,\dots,\bar{v}_n)$ è $\bar{a} \mapsto \overline{\rho(a)}$, con $\bar{a} = a + PD'$. Ne segue $\det(T(\bar{v}_i,\bar{v}_j)) = \det(T(v_i,v_j)) + P$. Per il lemma, $\overline{D'}$ è somma diretta di campi separabili su $\overline{D}$ se e solo se $\det(T(v_i,v_j)) \notin P$. Ciò conclude la dimostrazione per D a ideali principali.

Il caso generale si riduce a quello appena trattato localizzando rispetto all'ideale primo P di D. Poiché ci interessa localizzare sia D' sia D e P non è un ideale primo di D', indichiamo esplicitamente il monoide di localizzazione con $S = D - P$. Formiamo D_S e D'_S. Per la proposizione 7.16, D'_S è la chiusura integrale di D_S in E. Poiché $P'_i \cap D = P$, abbiamo $P'_i \cap S = \varnothing$, quindi P'_{iS} è un ideale primo di D'_S. Si ha $P_S D'_S = (P'_{1S})^{e_1} \cdots (P'_{gS})^{e_g}$ e i P'_{iS} sono distinti. Poiché $P'_{iS} \cap D' \subseteq P'_{iP'_i} \cap D' = P'_i$, si ha $P'_{iS} \cap D' = P'_i$. Come nella dimostrazione del teorema 10.10, esiste un'applicazione semilineare di D'_S/P'_{iS} su D_S/P_S in D'/P'_i su D/P, che è un isomorfismo

di anelli. Pertanto D'_S/P'_{iS} è separabile su D_S/P_S se e solo se D'/P'_i è separabile su D/P. Così P si ramifica in D' se e solo se P_S si ramifica in D'_S.

Mostriamo ora che $d_{D'_S/D_S} = (d_{D'/D})_S$. Sia $(u_1, \ldots, u_n)$ una base di E/F con $u_i \in D'$. Allora $u_i \in D'_S$ e $\det(T(u_i, u_j)) \in d_{D'_S/D_S}$. Quindi $d_{D'/D} \subseteq d_{D'_S/D_S}$ e $(d_{D'/D})_S \subseteq d_{D'_S/D_S}$. Sia invece $(u'_1, \ldots, u'_n)$ una base di E/F con $u'_i \in D'_S$. Possiamo scrivere $u'_i = u_i s^{-1}$ con $u_i \in D'$, $s \in D - P$, e allora $\det(T(u'_i, u'_j)) = s^{-2n} \det(T(u_i, u_j)) \in (d_{D'/D})_S$. Perciò $d_{D'_S/D_S} \subseteq (d_{D'/D})_S$ e si ha l'uguaglianza. È anche chiaro che P divide $d_{D'/D}$ se e solo se P_S divide $(d_{D'/D})_S = d_{D'_S/D_S}$. Il teorema si riduce così al caso degli anelli D_S e D'_S. Poiché D_S è a ideali principali, si applica la prima parte della dimostrazione. □

Esempio. Sia m un intero libero da quadrati, $E = \mathbb{Q}(\sqrt{m})$ e D' la chiusura integrale di $\mathbb{Z}$ in E. Se $m \equiv 2$ o $3 \pmod 4$, D' ha base $(1, \sqrt{m})$ su $\mathbb{Z}$; se $m \equiv 1 \pmod 4$, ha base $(1, (1+\sqrt{m})/2)$ (esercizi 4 e 5, p. 287 di *BAI*). Nel primo caso il discriminante $d_{D'/\mathbb{Z}}$ è quindi l'ideale principale generato da

$$\begin{vmatrix} 2 & 0 \\ 0 & 2m \end{vmatrix} = 4m.$$

I primi ramificati (i primi p di $\mathbb{Z}$ per i quali l'estensione di $p\mathbb{Z}$ è il quadrato di un ideale primo di D') sono dunque 2 e i divisori primi di m. Nel secondo caso, $m \equiv 1 \pmod 4$, il discriminante è l'ideale principale generato da

$$\begin{vmatrix} 2 & 1 \\ 1 & (m+1)/2 \end{vmatrix} = m.$$

Quindi i primi ramificati sono i divisori primi di m.

Esercizi

1. Con le notazioni dell'esempio, mostrare che, se p è dispari e pD è non ramificato in D', allora pD' è primo oppure è prodotto di due ideali primi distinti in D' secondo che il simbolo di Legendre (m/p) sia -1 oppure 1. Mostrare che, se $m \equiv 1 \pmod 4$, allora $2D'$ è primo oppure è prodotto di due ideali primi in D' secondo che $m \equiv 5$ oppure $m \equiv 1 \pmod 8$. (*Suggerimento.* Usare i teoremi 10.9 e 9.14.)

2. Sia E il campo ciclotomico $\mathbb{Q}(\zeta)$, dove ζ è una radice primitiva ℓ-esima dell'unità ed ℓ è primo, come nell'esercizio 1 di p. 618, nel quale si è dimostrato che $(\zeta - 1)D'$ è primo in D'. Mostrare che $[D'/(\zeta-1)D' : \mathbb{Z}/\ell\mathbb{Z}] = 1$ e quindi $|D'/(\zeta-1)D'| = \ell$. Mostrare che $D' = \mathbb{Z}[\zeta] + (\zeta - 1)D'$. Usare l'esercizio 2 di p. 276 di *BAI* per provare che $|\det(T(\zeta^i, \zeta^j))| = \ell^{\ell-2}$, con $0 \le i, j \le \ell - 2$. Dedurne che $D' \subseteq \ell^{-(\ell+2)}\mathbb{Z}[\zeta]$ e che $\ell^{\ell+2}D' \subseteq \mathbb{Z}[\zeta] \subseteq D'$. Usare questi risultati per provare che $D' = \mathbb{Z}[\zeta]$ e che $\ell\mathbb{Z}$ è l'unico ideale primo di $\mathbb{Z}$ che si ramifica in D'.

3. Mostrare che un'algebra commutativa A di dimensione finita su un campo F è somma diretta di campi separabili se e solo se A_E è semiprimitiva per ogni estensione E di F. (Quest'ultima proprietà è stata discussa a p. 374, dove è stata chiamata separabilità.)

10.6 Moduli finitamente generati su un dominio di Dedekind

In questo paragrafo estenderemo la teoria dei moduli finitamente generati su un dominio a ideali principali, trattata in BAI (ğğ 3.6–3.9, pp. 179–194), ai moduli finitamente generati su un dominio di Dedekind. Ricordiamo che, se M è un modulo su un dominio D, il sottoinsieme

T degli elementi $x \in M$ per cui esiste un $a \neq 0$ tale che $ax = 0$ è un sottomodulo, detto *sottomodulo di torsione* di M. Il modulo M si dice *senza torsione* se $T = 0$. Ogni sottomodulo di un modulo senza torsione è senza torsione. Quindi, poiché ogni modulo libero è senza torsione, ogni sottomodulo di un modulo libero è senza torsione. È chiaro anche che, se T è il sottomodulo di torsione di un modulo M, allora M/T è senza torsione. Ricaveremo ora due risultati meno immediati sui moduli senza torsione.

Proposizione 10.11. *Ogni modulo finitamente generato senza torsione M su un dominio D è isomorfo a un sottomodulo di un modulo libero di rango finito.*

Dimostrazione. Sia $\{u_1, \dots, u_r\}$ un sistema di generatori di M. Supponiamo $M \neq 0$ e $u_i \neq 0$. Possiamo supporre che esista un s, $1 \leq s \leq r$, tale che $\{u_1, \dots, u_s\}$ siano linearmente indipendenti su D, nel senso che $\sum_{i=1}^{s} d_i u_i = 0$ vale soltanto se tutti i d_i sono nulli, ma che $\{u_1, \dots, u_s, u_{s+j}\}$ siano linearmente dipendenti su D per ogni j, $1 \leq j \leq r - s$. Allora il sottomodulo $\sum_{i=1}^{s} Du_i$ di M è libero e quindi il risultato vale se $s = r$. Se invece $s < r$, per ogni j esiste un $d_j \neq 0$ in D tale che $d_j u_{s+j} \in \sum_{i=1}^{s} Du_i$. Allora $du_{s+j} \in \sum_{i=1}^{s} Du_i$ per $d = \prod_j d_j \neq 0$ e pertanto $dM \subset \sum_{i=1}^{s} Du_i$. Dunque il D-endomorfismo $x \mapsto dx$ di M manda M nel sottomodulo libero $\sum_{i=1}^{s} Du_i$. Poiché M è senza torsione, questa applicazione è un monomorfismo. Quindi M è isomorfo a un sottomodulo del modulo libero $\sum_{i=1}^{s} Du_i$. □

Otterremo ora una generalizzazione del teorema secondo cui ogni sottomodulo di un modulo libero finitamente generato su un dominio a ideali principali è libero (teorema 3.7 di BAI, p. 179).

Proposizione 10.12. *Sia R un anello, non necessariamente commutativo, tale che ogni suo ideale sinistro sia un R-modulo proiettivo. Allora ogni sottomodulo M del modulo libero $R^{(n)}$ è somma diretta di $m \leq n$ sottomoduli isomorfi a ideali sinistri di R. Pertanto M è proiettivo.*

Dimostrazione. Per $n = 1$ il risultato è chiaro, poiché i sottomoduli di $R = R^{(1)}$ sono ideali sinistri. Supponiamo dunque $n > 1$. Sia S il sottomodulo di $R^{(n)}$ degli elementi della forma $(x_1, \dots, x_{n-1}, 0)$. Evidentemente $S \cong R^{(n-1)}$. Consideriamo ora l'R-omomorfismo $p\colon y = (y_1, \dots, y_n) \mapsto y_n$ di M in R. L'immagine è un ideale sinistro I di R e il nucleo è isomorfo a un sottomodulo N di $R^{(n-1)}$. Si ha una successione esatta

$$0 \longrightarrow N \longrightarrow M \xrightarrow{p} I \longrightarrow 0. \tag{22}$$

Poiché I è proiettivo, questa successione esatta si spezza (p. 150), quindi $M \cong N \oplus I$. Essendo $N \subset R^{(n-1)}$, possiamo concludere per induzione che N è isomorfo a una somma diretta di al più $n - 1$ ideali sinistri. Allora M è isomorfo a una somma diretta di $m \leq n$ ideali sinistri di R. Poiché ogni ideale sinistro è proiettivo, ne segue che M è proiettivo. □

Supponiamo ora che M sia un modulo finitamente generato su un dominio di Dedekind D. La proprietà usata per definire D è che ogni suo ideale frazionario è invertibile e dunque proiettivo (proposizione 10.3). In particolare ogni ideale intero di D è proiettivo e, poiché 0 è banalmente proiettivo, ogni ideale di D è un modulo proiettivo. Quindi D soddisfa l'ipotesi della proposizione 10.12. Sia T il sottomodulo di torsione di M e poniamo $\bar{M} = M/T$. Allora $\bar{M}$ è finitamente generato e senza torsione. Per la proposizione 10.11, $\bar{M}$ è dunque isomorfo a un sottomodulo di un modulo libero di rango finito. Per la proposizione 10.12, $\bar{M}$ è allora proiettivo. Poiché si ha la successione esatta $0 \to T \to M \to \bar{M} \to 0$ e $\bar{M}$ è proiettivo, $M \cong \bar{M} \oplus T$. Allora T è un'immagine omomorfa di M e quindi anch'esso è finitamente generato. È chiaro che abbiamo ridotto il problema di classificare i D-moduli finitamente generati a meno di isomorfismo allo stesso problema per i moduli senza torsione e per i moduli di torsione.

Consideriamo dapprima i moduli senza torsione. Abbiamo visto che ognuno di questi moduli è proiettivo. D'altra parte, se M è proiettivo, esso è un addendo diretto di un modulo libero e, poiché D è un dominio, i moduli liberi, e quindi i moduli proiettivi su D, sono senza torsione. Dunque M è finitamente generato senza torsione su D se e solo se è finitamente generato e

proiettivo.

Per determinare condizioni di isomorfismo di due tali moduli, possiamo supporre che essi abbiano la forma $M = I_1 \oplus \cdots \oplus I_n$, con gli I_j ideali interi. Benché ciò non accresca la generalità, è un po' più naturale supporre che gli I_j siano ideali frazionari. Consideriamo la localizzazione M_{D^*} determinata dal monoide D^* degli elementi non nulli di D. Si ha $M_{D^*} \cong D_{D^*} \otimes_D M \cong I_{1D^*} \oplus \cdots \oplus I_{nD^*}$ e, poiché D_{D^*} è il campo delle frazioni F di D e $I_{jD^*} = F$, M_{D^*} è uno spazio vettoriale di dimensione n su F. Dunque $M_{D^*} \cong F^{(n)}$. La dimensione n è il *rango* di M su D come definito nel ğ 7.7 (corollario, p. 415). L'applicazione canonica $x \mapsto x/1$ di M in M_{D^*} è un monomorfismo. Si ottiene dunque un isomorfismo di M con il D-sottomodulo di $F^{(n)}$ costituito dai vettori $(x_1, \ldots, x_n)$ con $x_j \in I_j$. Possiamo quindi supporre che M sia questo insieme di vettori.

Se η è un isomorfismo di M su un secondo modulo finitamente generato senza torsione M', esso ha un unico prolungamento a una trasformazione lineare biiettiva di M_{D^*}/F su M'_{D^*}/F. Ne segue che M e M' hanno lo stesso rango n e possiamo supporre anche che M' sia il D-sottomodulo di $F^{(n)}$ costituito dai vettori $(x'_1, \ldots, x'_n)$ con $x'_j \in I'_j$, ideale frazionario in F, $1 \leq j \leq n$. Tenendo conto della forma di una trasformazione lineare biiettiva di $F^{(n)}$, vediamo che η ha la forma

$$(x_1, \ldots, x_n) \longmapsto (x'_1, \ldots, x'_n) = (x_1, \ldots, x_n)A, \tag{23}$$

dove $A = (a_{ij}) \in \mathrm{GL}_n(F)$, il gruppo delle matrici invertibili $n \times n$ a elementi in F. Si ha $x'_k = \sum_j x_j a_{jk} \in I'_k$ e, se $A^{-1} = (b_{ij})$, si ha $x_j = \sum_k x'_k b_{kj} \in I_j$ per $x'_k \in I'_k$, $1 \leq k \leq n$. Viceversa, se $A \in \mathrm{GL}_n(F)$ soddisfa queste condizioni, la (23) è un isomorfismo di M su M'.

Se $n = 1$, le condizioni precedenti implicano che due ideali frazionari I e I' sono isomorfi se e solo se esiste un $a \neq 0$ in F tale che $I' = Ia$. Possiamo enunciare questo risultato in termini del *gruppo delle classi* del dominio di Dedekind D, che definiamo come il gruppo quoziente $\mathcal{F}/\mathcal{D}$, dove $\mathcal{F}$ è il gruppo moltiplicativo degli ideali frazionari di D e $\mathcal{D}$ è il sottogruppo degli ideali principali aD, $a \neq 0$ in F. Gli ideali I e $aI = (aD)I$ si dicono appartenenti alla stessa classe. Abbiamo dunque mostrato che I e I' sono D-moduli isomorfi se e solo se appartengono alla stessa classe. È chiaro che si ha una corrispondenza biunivoca fra le classi di isomorfismo degli ideali frazionari, e quindi dei moduli senza torsione di rango uno, e gli elementi del gruppo delle classi $\mathcal{F}/\mathcal{D}$.

Dimostriamo ora il seguente lemma.

Lemma. *Siano I_1 e I_2 ideali frazionari. Allora $M = I_1 \oplus I_2 \cong D \oplus I_1 I_2$.*

Dimostrazione. Usiamo l'esercizio sugli ideali coprimi (esercizio 11, p. 625).[45] Secondo questo risultato, se $a_1 \neq 0$ appartiene a I_1 e $J = a_1 I_1^{-1} \subset D$, esiste un $a_2 \in I_2$ tale che $a_1 I_1^{-1} + a_2 I_2^{-1} = D$. Abbiamo quindi $b_i \in I_i^{-1}$ tali che $a_1 b_1 + a_2 b_2 = 1$. Allora la matrice

$$A = \begin{pmatrix} b_1 & -a_2 \\ b_2 & a_1 \end{pmatrix} \tag{24}$$

è invertibile, con $A^{-1} = \left(\begin{smallmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{smallmatrix}\right)$. Se $x_j \in I_j$, si ha $y_1 = x_1 b_1 + x_2 b_2 \in D$ e $y_2 = -x_1 a_2 + x_2 a_1 \in I_1 I_2$. D'altra parte, se $y_1 \in D$ e $y_2 = c_1 c_2$, $c_j \in I_j$, allora $x_1 = a_1 y_1 - b_2 c_1 c_2 \in I_1$ e $x_2 = a_2 y_1 + b_1 c_1 c_2 \in I_2$. Dunque $(x_1, x_2) \mapsto (x_1, x_2)A$ è un isomorfismo di $I_1 \oplus I_2$ su $D \oplus I_1 I_2$. □

Possiamo ora dimostrare il teorema principale sui moduli finitamente generati senza torsione su un dominio di Dedekind.

[45] Nell'originale il rinvio è all'esercizio 10 di p. 605.

Teorema 10.14. *Ogni modulo finitamente generato senza torsione M su un dominio di Dedekind è isomorfo a una somma diretta di un numero finito di ideali interi. Condizioni necessarie e sufficienti perché $M = I_1 \oplus \cdots \oplus I_n$ e $M' = I'_1 \oplus \cdots \oplus I'_m$, dove gli I_j e gli I'_k sono ideali frazionari, siano isomorfi sono $m = n$ e l'appartenenza di $I_1 \cdots I_n$ e $I'_1 \cdots I'_m$ alla stessa classe.*

Dimostrazione. Abbiamo già osservato la validità della prima affermazione. Supponiamo ora $M \cong M'$ con M e M' come nell'enunciato. Allora $m = n$ e si ha una matrice $A = (a_{ij}) \in \mathrm{GL}_n(F)$ tale che, se $x_j \in I_j$, $1 \le j \le n$, allora $x'_k = \sum_{j=1}^n x_j a_{jk} \in I'_k$. Inoltre, se $A^{-1} = (b_{ij})$ e $x'_k \in I'_k$ per $1 \le k \le n$, allora $x_j = \sum_k x'_k b_{kj} \in I_j$. La prima condizione implica che $x_j a_{jk} \in I'_k$ per ogni $x_j \in I_j$. Quindi $I_j a_{jk} \subset I'_k$, sicché $(I'_k)^{-1} I_j a_{jk} \subset D$ e $a_{jk} \in I_j^{-1} I'_k$. Pertanto, se $(k_1, \dots, k_n)$ è una permutazione di $1, 2, \dots, n$, allora

$$a_{1k_1} \cdots a_{nk_n} \in \Big(\prod_j I_j\Big)^{-1} \Big(\prod_k I'_k\Big).$$

Ne segue che $\det A \in (\prod_j I_j)^{-1}(\prod_k I'_k)$ e $(\det A) \prod_j I_j \subset \prod_j I'_j$. Analogamente $(\det A^{-1}) \prod_j I'_j \subset \prod_j I_j$. Dunque $\prod_j I'_j = (\det A) \prod_j I_j$, sicché $\prod_j I_j$ e $\prod_j I'_j$ appartengono alla stessa classe. Viceversa, supponiamo $m = n$ e che $\prod_j I_j$ e $\prod_j I'_j$ appartengano alla stessa classe. Per il lemma,

$$\begin{aligned} M &= I_1 \oplus I_2 \oplus \cdots \oplus I_n \\ &\cong D \oplus I_1 I_2 \oplus I_3 \oplus \cdots \oplus I_n \\ &\cong D \oplus D \oplus I_1 I_2 I_3 \oplus I_4 \oplus \cdots \oplus I_n \\ &\cong \cdots \cong D \oplus \cdots \oplus D \oplus \prod_j I_j. \end{aligned}$$

Analogamente $M' \cong D \oplus \cdots \oplus D \oplus \prod_j I'_j$. Poiché $\prod_j I_j$ e $\prod_j I'_j$ sono nella stessa classe, sono isomorfi e quindi $M \cong M'$. □

Consideriamo ora la struttura di un modulo di torsione finitamente generato M su D. Per studiarlo, lo sostituiremo con un modulo strettamente legato a esso su un dominio a ideali principali. Sia $I = \operatorname{ann}_D M$. Se $M = Dx_1 + Dx_2 + \cdots + Dx_n$, allora

$$I = \bigcap_i \operatorname{ann} x_i \supset \prod_i \operatorname{ann} x_i \neq 0.$$

Dunque $I = \operatorname{ann}_D M \neq 0$. Siano $\{P_1, \dots, P_r\}$ gli ideali primi divisori di I e poniamo

$$S = D - \bigcup_{i=1}^r P_i = \bigcap_{i=1}^r (D - P_i).$$

Allora S è un sottomonoide del monoide moltiplicativo di D e possiamo formare l'anello D_S e il D_S-modulo $M_S = D_S \otimes_D M$. Ogni ideale primo di D_S è della forma P_S, dove P è un ideale primo tale che $P \cap S = \varnothing$ (p. 401). Allora $P \subset \bigcup_i P_i$ e quindi $P \subset P_i$ per qualche i (proposizione 7.1, p. 390), il che implica $P = P_i$ per $P \neq 0$. Dunque D_S è un dominio di Dedekind con un numero finito di ideali primi non nulli $P'_i = P_{iS}$, $1 \le i \le r$. Un tale dominio è a ideali principali (esercizio 15, p. 625). Inoltre M_S è un D_S-modulo di torsione, poiché $I_S \neq 0$ e $I_S M_S = 0$.

Il teorema fondamentale sui moduli finitamente generati su un dominio a ideali principali (BAI, p. 187) si applica al D_S-modulo M_S. Secondo tale teorema, $M_S = D_S y_1 \oplus \cdots \oplus D_S y_m$, dove $\operatorname{ann}_{D_S} y_1 \supset \operatorname{ann}_{D_S} y_2 \supset \cdots \supset \operatorname{ann}_{D_S} y_m$. Inoltre $\operatorname{ann}_{D_S} y_i \supset I_S \neq 0$ e $\operatorname{ann}_{D_S} y_i$ è un ideale proprio di D_S. Potremo applicare questo risultato per determinare la struttura di M come D-modulo, poiché si può ricostruire M da M_S mediante il lemma seguente.

Lemma. *Sia I un ideale non nullo di D, siano $P_1, \dots, P_r$ gli ideali primi divisori di I in D e sia $S = \bigcap_i (D - P_i)$. Sia N un D-modulo tale che $IN = 0$. Allora $N \cong (D/I) \otimes_D N_S$ come D-moduli.*

Dimostrazione. Abbiamo

$$(D/I) \otimes_D N_S \cong (D/I) \otimes_D (D_S \otimes_D N) \cong ((D/I) \otimes_D D_S) \otimes_D N \cong (D/I)_S \otimes_D N.$$

Si vede subito che gli elementi $s+I$, $s \in S$, sono invertibili in D/I, il che implica $(D/I)_S \cong D/I$. Dunque $(D/I)_S \otimes_D N \cong (D/I) \otimes_D N \cong N$, poiché $IN = 0$. □

Possiamo ora dimostrare il seguente teorema di struttura.

Teorema 10.15. *Sia M un modulo di torsione finitamente generato su un dominio di Dedekind D. Allora M è isomorfo a una somma diretta di moduli ciclici $Dz_1 \oplus \cdots \oplus Dz_m$ tali che $\operatorname{ann} z_1 \supset \operatorname{ann} z_2 \supset \cdots \supset \operatorname{ann} z_m \neq 0$. Inoltre gli ideali $\operatorname{ann} z_i$, $1 \leq i \leq m$, sono determinati in modo unico.*

Dimostrazione. Sia S come sopra. Allora $M_S = D_S y_1 \oplus \cdots \oplus D_S y_m$, dove $\operatorname{ann}_{D_S} y_1 \supset \cdots \supset \operatorname{ann}_{D_S} y_m$. Posto $I'_j = \operatorname{ann}_{D_S} y_j$, si ha $D_S y_j \cong D_S/I'_j$. Sia $I_j = \{a \in D \mid a/s \in I'_j \text{ per qualche } s \in S\}$. Allora $I_{jS} = I'_j$ (p. 401) e D/I_j è un D-modulo ciclico, Dz_j, tale che $(D/I_j)_S \cong D_S/I_{jS} = D_S/I'_j$. Inoltre $\operatorname{ann}_D z_j = I_j$ e $I_1 \supset \cdots \supset I_m$. Consideriamo ora il modulo $N = Dz_1 \oplus \cdots \oplus Dz_m$. Abbiamo $N_S = (Dz_1)_S \oplus \cdots \oplus (Dz_m)_S \cong D_S y_1 \oplus \cdots \oplus D_S y_m = M_S$. Quindi, per il lemma, $M \cong N = Dz_1 \oplus \cdots \oplus Dz_m$. Anche l'unicità si ottiene usando la localizzazione rispetto a S e il corrispondente risultato di unicità nel caso di un dominio a ideali principali (BAI, p. 192). Lasciamo i particolari al lettore. □

I teoremi 10.14 e 10.15, insieme al fatto che ogni modulo finitamente generato su un dominio di Dedekind D è somma diretta del suo sottomodulo di torsione e di un modulo senza torsione, costituiscono una generalizzazione diretta del teorema fondamentale sui moduli finitamente generati su un dominio a ideali principali. Se D è un dominio a ideali principali, il gruppo delle classi $\mathcal{F}/\mathcal{D}$ è banale e i risultati mostrano che M è somma diretta di copie di D e di moduli ciclici $Dz_1, \dots, Dz_m$ con annullatori non nulli $I_1, \dots, I_m$ tali che $I_1 \supset \cdots \supset I_m$. Questo è il teorema fondamentale nella forma data in BAI, p. 187. Un dominio di Dedekind è a ideali principali se e solo se $\mathcal{F}/\mathcal{D} = 1$. Il gruppo $\mathcal{F}/\mathcal{D}$ misura quanto D si discosti dall'essere un dominio a ideali principali. È un gruppo classico della teoria algebrica dei numeri. In tale teoria si dimostra con metodi trascendenti che il gruppo delle classi è finito. D'altra parte L. Claborn (*Pacific J. of Math.*, vol. 18 (1966), pp. 219–222) ha dimostrato che ogni gruppo abeliano è il gruppo delle classi di un opportuno dominio di Dedekind.

Mostreremo ora che il gruppo delle classi coincide con il *gruppo delle classi proiettive*, che abbiamo definito nel ğ 7.4. Quest'ultimo, denotato con $\operatorname{Pic} D$, è l'insieme delle classi di isomorfismo dei moduli proiettivi fedeli finitamente generati di rango uno, con moltiplicazione definita dal prodotto tensoriale. Poiché D è un dominio, i D-moduli proiettivi di rango uno sono automaticamente fedeli. Gli elementi di $\operatorname{Pic} D$ si possono quindi rappresentare mediante gli ideali frazionari e, come abbiamo visto, due tali ideali sono isomorfi se e solo se appartengono alla stessa classe. Si ha pertanto l'applicazione biiettiva $[I] \mapsto I\mathcal{D}$ di $\operatorname{Pic} D$ su $\mathcal{F}/\mathcal{D}$, dove $[I]$ denota la classe di isomorfismo dell'ideale frazionario I. Ora abbiamo l'omomorfismo canonico di moduli da $I_1 \otimes I_2$ in $I_1 I_2$ che manda $a_1 \otimes a_2$ in $a_1 a_2$. Localizzando in tutti gli ideali massimali si vede che è un isomorfismo. Dunque $I_1 \otimes I_2 \cong I_1 I_2$ e perciò $[I] \mapsto I\mathcal{D}$ è un isomorfismo di gruppi fra $\operatorname{Pic} D$ e il gruppo delle classi.

Riferimenti bibliografici

- O. Zariski e P. Samuel, *Commutative Algebra*, vol. I, D. van Nostrand, 1958. Nuova stampa, Springer-Verlag, New York, 1975.
- S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.
- S. Lang, *Introduction to Algebraic and Abelian Functions*, Addison-Wesley, Reading, Mass., 1972.
- G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.

11 Campi formalmente reali

Nel capitolo 5 di *Basic Algebra I* abbiamo studiato le equazioni, le condizioni di non annullamento e le disuguaglianze polinomiali in un campo reale chiuso. Abbiamo definito tale un campo ordinato in cui ogni polinomio di grado dispari in una indeterminata ha una radice e ogni elemento positivo possiede una radice quadrata. Abbiamo dimostrato che, se R è reale chiuso, allora $R(\sqrt{-1})$ è algebricamente chiuso. Il nostro problema principale era costruire un algoritmo per stabilire se un sistema di equazioni, condizioni di non annullamento e disuguaglianze polinomiali in più incognite ammette soluzione in un campo reale chiuso. Nel caso di una sola equazione polinomiale in un'incognita, il metodo classico di J. C. F. Sturm risolve il problema. Abbiamo esposto questo metodo e ne abbiamo sviluppato un'ampia estensione al caso generale dei sistemi in più incognite. Ne consegue, come indicato in BAI, il teorema di Tarski: in termini approssimativi, un sistema di equazioni, condizioni di non annullamento e disuguaglianze polinomiali che ha soluzione in un campo reale chiuso ha soluzione in ogni campo reale chiuso (per l'enunciato preciso si veda BAI, p. 340).

Riprendiamo ora lo studio dei campi reali chiusi da un diverso punto di vista, quello dei campi formalmente reali introdotti da Artin e Schreier. La proprietà che li definisce è che -1 non sia somma di quadrati nel campo, o, equivalentemente, che da $\sum a_i^2 = 0$, con gli a_i nel campo, segua $a_i = 0$ per ogni i. È evidente che ogni campo ordinato è formalmente reale. D'altra parte, come vedremo, ogni campo formalmente reale ammette un ordinamento. Un campo è dunque formalmente reale se e solo se può essere ordinato.

La teoria di Artin e Schreier dei campi formalmente reali è un ingrediente essenziale della soluzione data da Artin a uno dei problemi posti da Hilbert al Congresso internazionale dei matematici di Parigi del 1900. Si tratta del diciassettesimo problema di Hilbert, sulle funzioni razionali semidefinite positive. Sia $f(x_1, \ldots, x_n)$ una funzione razionale a coefficienti reali che assume soltanto valori non negativi, in tutti i punti reali in cui è definita. È necessariamente una somma di quadrati di espressioni razionali a coefficienti reali? Artin diede nel 1927 una risposta affermativa. Nel 1955 A. Robinson elaborò una nuova dimostrazione fondata sulla teoria dei modelli. Esporremo il teorema di Artin seguendo un approccio essenzialmente modellistico che si basa sul teorema di Tarski ricordato sopra.

Il teorema di Artin non dà informazioni sul numero di quadrati necessari per esprimere una data $f(x_1, \ldots, x_n)$. Hilbert aveva dimostrato nel 1893 che ogni funzione razionale semidefinita positiva in due variabili è somma di quattro quadrati. Nel 1966, in un lavoro inedito, J. Ax mostrò che in tre variabili bastano otto quadrati e congetturò che per tali funzioni di n variabili ne bastassero 2^n. A. Pfister lo dimostrò nel 1967 con un metodo interamente nuovo e ingegnoso. Ne daremo la dimostrazione.

Concluderemo con una bella caratterizzazione dei campi reali chiusi dovuta ad Artin e Schreier. È notevole che la dimostrazione di questo teorema abbia dato inizio allo studio delle estensioni cicliche di grado p^e di campi di caratteristica p.

11.1 Campi formalmente reali

Ricordiamo che un campo F si dice *ordinato* se è assegnato un sottoinsieme P di F, l'insieme degli elementi positivi, chiuso rispetto alla somma e al prodotto e tale che F sia l'unione disgiunta di P, $\{0\}$ e $-P = \{-p \mid p \in P\}$ (BAI, p. 307). Allora, ponendo $a > b$ se $a - b \in P$, si ottiene un ordine totale su F. Se $a > b$, si ha inoltre $a + c > b + c$ per ogni c e $ap > bp$ per ogni $p \in P$. Per $a \neq 0$, $a^2 = (-a)^2 > 0$. Dunque se $\sum a_i^2 = 0$ in F, ogni a_i è nullo. Equivalentemente, -1 non è somma di quadrati in F. Ne segue che F ha caratteristica zero.

Seguendo Artin e Schreier introduciamo la definizione seguente.

Definizione 11.1. *Un campo F si dice formalmente reale se -1 non è somma di quadrati in F.*

È chiaro che ogni campo che ammette un ordinamento è formalmente reale. Il viceversa è un teorema di Artin e Schreier, che dimostreremo con un argomento dovuto a Serre, basato sul lemma seguente.

Lemma 1. *Sia P_0 un sottogruppo del gruppo moltiplicativo F^* di un campo F, chiuso rispetto alla somma e contenente tutti i quadrati non nulli. Sia $a \in F^*$ tale che $-a \notin P_0$. Allora $P_1 = P_0 + P_0 a = \{b + ca \mid b, c \in P_0\}$ è un sottogruppo di F^* chiuso rispetto alla somma.*

Dimostrazione. P_1 è evidentemente chiuso rispetto alla somma. Per $b_i, c_i \in P_0$, $i = 1, 2$, si ha

$$(b_1 + c_1 a)(b_2 + c_2 a) = (b_1 b_2 + c_1 c_2 a^2) + (b_1 c_2 + b_2 c_1)a \in P_1,$$

poiché entrambi i coefficienti appartengono a P_0. Osserviamo poi che $0 \notin P_1$: da $b + ca = 0$, con $b, c \in P_0$, seguirebbe $-a = bc^{-1} \in P_0$, contro l'ipotesi. Inoltre

$$(b + ca)^{-1} = (b + ca)(b + ca)^{-2} = b(b + ca)^{-2} + c(b + ca)^{-2} a \in P_1,$$

poiché $b(b + ca)^{-2}$ e $c(b + ca)^{-2}$ appartengono a P_0. Dunque P_1 è un sottogruppo di F^*. □

Sia ora F formalmente reale e sia P_0 l'insieme delle somme $\sum a_i^2$ con tutti gli $a_i \neq 0$. Esso è chiuso rispetto alla somma e, poiché $(\sum_i a_i^2)(\sum_j b_j^2) = \sum_{i,j}(a_i b_j)^2$, anche rispetto al prodotto. Contiene tutti i quadrati non nulli e quindi, se $a = \sum a_i^2$ con $a_i \neq 0$, si ha $a^{-1} = aa^{-2} \in P_0$. Dunque P_0 soddisfa le condizioni del lemma e l'insieme dei sottoinsiemi P' che soddisfano tali condizioni non è vuoto. Per il lemma di Zorn questo insieme di sottoinsiemi di F ammette un elemento massimale P. Dal lemma segue allora che per ogni $a \in F^*$ si ha $a \in P$ oppure $-a \in P$. Dunque $F = P \cup \{0\} \cup (-P)$, dove $-P = \{-p \mid p \in P\}$. Poiché $0 \notin P$ e P è chiuso rispetto alla somma, $P \cap (-P) = \varnothing$ e $0 \notin -P$. I tre insiemi sono dunque disgiunti e, poiché P è chiuso rispetto alla somma e al prodotto, esso determina un ordinamento di F. Abbiamo così dimostrato il seguente teorema.

Teorema 11.1. *Un campo F si può ordinare (mediante un sottoinsieme P) se e solo se è formalmente reale.*

In BAI (p. 308) abbiamo detto *reale chiuso* un campo ordinato R tale che (1) ogni elemento positivo di R abbia una radice quadrata in R e (2) ogni polinomio di grado dispari in una indeterminata a coefficienti in R abbia una radice in R. Abbiamo visto che l'ordinamento di un campo reale chiuso R è unico e che ogni suo automorfismo è un automorfismo d'ordine (teorema 5.1, p. 308). Abbiamo inoltre dimostrato un'estensione del cosiddetto teorema fondamentale dell'algebra: se R è reale chiuso, $R(\sqrt{-1})$ è algebricamente chiuso (teorema 5.2, p. 309). Diamo ora una caratterizzazione dei campi reali chiusi in termini di realtà formale.

Teorema 11.2. *Un campo R è reale chiuso se e solo se è formalmente reale e nessuna sua estensione algebrica propria è formalmente reale.*

Premettiamo alla dimostrazione il seguente lemma.

Lemma 2. *Se F è formalmente reale, l'estensione $F(r)$ è formalmente reale qualora $r = \sqrt{a}$ per un elemento $a > 0$ di F, oppure r sia algebrico su F con polinomio minimo di grado dispari.*

Dimostrazione. Sia dapprima $r = \sqrt{a}$, $a > 0$. Se $F(r)$ non fosse formalmente reale, si avrebbe $r \notin F$ ed esisterebbero $a_i, b_i \in F$ tali che $-1 = \sum(a_i + b_i r)^2$. Ne seguirebbe $\sum a_i^2 + a \sum b_i^2 = -1$, impossibile perché $a > 0$.

Nel secondo caso, sia $f(x)$ il polinomio minimo di r. Il grado $m = \deg f(x)$ è dispari. Ragioniamo per induzione su m. Se $F(r)$ non fosse formalmente reale, esisterebbero polinomi $g_i(x)$ di

grado minore di m tali che $\sum g_i(r)^2 = -1$. Allora $\sum g_i(x)^2 = -1 + f(x)g(x)$ per un $g(x) \in F[x]$. Poiché F è formalmente reale e il coefficiente direttivo di $g_i(x)^2$ è un quadrato, il grado di $-1 + f(x)g(x)$, uguale al grado di $\sum g_i(x)^2$, è pari e minore di $2m$. Quindi $\deg g(x)$ è dispari e minore di m. Il polinomio $g(x)$ ha perciò un fattore irriducibile $h(x)$ di grado dispari. Sia s una radice di $h(x)$. Per l'ipotesi induttiva $F(s)$ è formalmente reale, ma sostituendo s nella relazione $\sum g_i(x)^2 = -1 + f(x)g(x)$ si ottiene $\sum g_i(s)^2 = -1$, assurdo. □

Dimostrazione del teorema 11.2. Supponiamo R reale chiuso. Allora $C = R(\sqrt{-1})$ è algebricamente chiuso e $C \neq R$. Il campo C è una chiusura algebrica di R e ogni estensione algebrica di R si può considerare un campo intermedio di C/R. Se è propria, coincide quindi con C, che non è formalmente reale perché contiene $\sqrt{-1}$.

Viceversa, sia R formalmente reale e supponiamo che nessuna sua estensione algebrica propria abbia la stessa proprietà. Se $a \in R$ è positivo, per il lemma 2 il campo $R(\sqrt{a})$ è formalmente reale e dunque coincide con R; pertanto $\sqrt{a} \in R$. Sia poi $f(x) \in R[x]$ di grado dispari. Scegliamo un suo fattore irriducibile $g(x)$ di grado dispari e consideriamo un'estensione $R(r)$ con $g(r) = 0$. Per il lemma 2, $R(r)$ è formalmente reale. Dunque $R(r) = R$, sicché $r \in R$ e $f(r) = 0$. Abbiamo verificato le due proprietà che definiscono un campo reale chiuso. □

Mostriamo infine che la proprietà fondamentale dei campi reali chiusi R, secondo cui $\sqrt{-1} \notin R$ e $C = R(\sqrt{-1})$ è algebricamente chiuso, caratterizza tali campi.

Teorema 11.3. *Un campo R è reale chiuso se e solo se $\sqrt{-1} \notin R$ e $C = R(\sqrt{-1})$ è algebricamente chiuso.*

Dimostrazione. Basta mostrare che, se R ha le proprietà indicate, è reale chiuso. Mostriamo anzitutto che in R la somma di due quadrati è un quadrato. Siano a, b elementi non nulli di R e scegliamo $u \in C$ con $u^2 = a + bi$, $i = \sqrt{-1}$. L'automorfismo $x + iy \mapsto x - iy$ $(x, y \in R)$ di C/R ha per campo dei punti fissi R. Ora

$$a^2 + b^2 = (a + bi)(a - bi) = u^2\bar{u}^2 = (u\bar{u})^2$$

con $u\bar{u} \in R$. Dunque $a^2 + b^2$ è un quadrato in R. Per induzione lo stesso vale per ogni somma di quadrati. Poiché -1 non è un quadrato in R, non può essere somma di quadrati e R è formalmente reale. D'altra parte, essendo C algebricamente chiuso, la prima parte della dimostrazione del teorema 11.2 mostra che nessuna estensione algebrica propria di R è formalmente reale.[46] Dunque R è reale chiuso per il teorema 11.2. □

Esercizi.

1. Dimostrare che, se F è formalmente reale e le x_i sono indeterminate, anche $F(x_1, \ldots, x_n)$ è formalmente reale.

2. Definire un ordinamento di un dominio D come per un campo: si assegna un sottoinsieme P chiuso rispetto alla somma e al prodotto e tale che D sia l'unione disgiunta di P, $\{0\}$ e $-P$. Mostrare che un ordinamento di un dominio si estende in modo unico al suo campo delle frazioni.

3. Sia F un campo ordinato. Dimostrare che $F[x]$, con x indeterminata, ammette l'ordinamento definito ponendo $a_0x^n + a_1x^{n-1} + \cdots > 0$ se $a_0 > 0$.

4. Un campo ordinato F si dice *archimedeo* se per ogni $a > 0$ in F esiste un intero positivo n con n $(= n1)$ maggiore di a. Dimostrare che $F(x)$, con x indeterminata e con l'ordinamento ottenuto mediante gli esercizi 2 e 3, non è archimedeo.

[46] Nella conclusione di questa dimostrazione l'originale reca «real closed». La proprietà appena dimostrata, richiamata nel teorema 11.2, è «formally real».

5. Provare che ogni campo ordinato archimedeo è isomorfo, come campo ordinato, a un sottocampo di $\mathbb{R}$.

6. (T. Springer.) Sia Q una forma quadratica anisotropa su uno spazio vettoriale di dimensione finita V su un campo F di caratteristica diversa da 2. Sia E/F un'estensione di grado dispari e sia Q_E l'estensione di Q a V_E. Dimostrare che Q_E è anisotropa. (*Suggerimento.* Basta supporre $E = F(\rho)$. Ragionare per induzione su $[E : F]$ come nella seconda parte della dimostrazione del lemma 2.)

11.2 Chiusure reali

Definizione 11.2. Sia F un campo ordinato. Un'estensione R di F si chiama *chiusura reale* di F se (1) R è reale chiuso e algebrico su F, e (2) l'(unico) ordine di R estende l'ordine dato di F.

Un risultato centrale della teoria di Artin–Schreier dei campi formalmente reali è l'esistenza e l'unicità di una chiusura reale di ogni campo ordinato F. Per dimostrarlo useremo il teorema di Sturm (*BAI*, p. 312), che permette di determinare il numero delle radici in un campo reale chiuso R di un polinomio $f(x) \in R[x]$. Sia $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ e sia $M = 1 + |a_1| + \cdots + |a_n|$, con $|\cdot|$ definito nel modo consueto. Tutte le radici di $f(x)$ in R appartengono all'intervallo $-M < x < M$ (*BAI*, esercizio 4, p. 311). Definiamo la successione standard di $f(x)$ ponendo

$$\begin{aligned} f_0(x) &= f(x), \qquad f_1(x) = f'(x), \quad \text{la derivata di } f(x), \\ f_{i-1}(x) &= g_i(x)f_i(x) - f_{i+1}(x), \qquad \deg f_{i+1} < \deg f_i \end{aligned} \tag{1}$$

per $i \geq 1$, fino a ottenere $f_{s+1} = 0$. Per il teorema di Sturm, il numero delle radici di $f(x)$ in R è $V_{-M} - V_M$, dove V_a è il numero delle variazioni di segno in $f_0(a), f_1(a), \ldots, f_s(a)$. Possiamo così dimostrare il lemma seguente.

Lemma. *Per $i = 1, 2$ siano R_i un campo reale chiuso e F_i un sottocampo di R_i. Sia $a \mapsto \bar{a}$ un isomorfismo d'ordine di F_1 su F_2, dove l'ordine di F_i è quello indotto da R_i. Se $f(x)$ è un polinomio monico in $F_1[x]$ e $\bar{f}(x)$ il corrispondente polinomio in $F_2[x]$, allora $f(x)$ ha in R_1 lo stesso numero di radici che $\bar{f}(x)$ ha in R_2.*

Dimostrazione. Con M come sopra, il primo numero è $V_{-M} - V_M$ e il secondo è $V_{-\bar{M}} - V_{\bar{M}}$, calcolato per la successione standard di $\bar{f}(x)$. Poiché $a \mapsto \bar{a}$ è un isomorfismo d'ordine di F_1 su F_2, è chiaro che i due numeri coincidono. □

Possiamo ora dimostrare il seguente importante teorema.

Teorema 11.4. *Ogni campo ordinato ha una chiusura reale. Se F_1, F_2 sono campi ordinati con chiusure reali rispettivamente R_1, R_2, ogni isomorfismo d'ordine di F_1 su F_2 ha un'unica estensione a un isomorfismo di R_1 su R_2, e questa estensione conserva l'ordine.*

Dimostrazione. Siano F un campo ordinato, $\bar{F}$ una chiusura algebrica di F ed E il sottocampo di $\bar{F}$ ottenuto aggiungendo a F le radici quadrate di tutti gli elementi positivi di F. Allora E è formalmente reale. Altrimenti E conterrebbe elementi a_i tali che $\sum_i a_i^2 = -1$. Gli a_i appartengono a un sottocampo generato su F da un numero finito di radici quadrate di elementi positivi di F. Applicando per induzione la prima parte del lemma 2 del § 11.1, si vede che questo sottocampo è formalmente reale, in contraddizione con $\sum_i a_i^2 = -1$ per a_i nel sottocampo. Consideriamo ora l'insieme dei sottocampi formalmente reali di $\bar{F}$ che contengono E. Tale insieme è induttivo, quindi per il lemma di Zorn ammette un elemento massimale R. Affermiamo

che R è reale chiuso. Altrimenti esisterebbe un'estensione algebrica propria R' di R formalmente reale (teorema 11.2). Poiché $\bar{F}$ è una chiusura algebrica di R, potremmo supporre $R' \subseteq \bar{F}$, onde $\bar{F} \supseteq R' \supsetneq R$. Ciò contraddice la massimalità di R. Dunque R è reale chiuso. Sia ora $a \in F$, $a > 0$. Allora $a = b^2$ con $b \in E \subseteq R$, onde $a > 0$ nell'ordine definito in R. L'ordine di R estende quindi quello di F, sicché R è una chiusura reale di F.

Siano ora F_1, F_2 campi ordinati, R_i una chiusura reale di F_i, e sia $\sigma\colon a \mapsto \bar{a}$ un isomorfismo d'ordine di F_1 su F_2. Vogliamo mostrare che σ si può estendere a un isomorfismo Σ di R_1 su R_2. La definizione di Σ è facile. Sia $r \in R_1$, sia $g(x)$ il suo polinomio minimo su F_1, e siano $r_1 < r_2 < \cdots < r_k = r < \cdots < r_m$ le radici di $g(x)$ in R_1 disposte in ordine crescente. Per il lemma, $\bar{g}(x)$ ha esattamente m radici in R_2, che possiamo disporre in ordine crescente $\bar{r}_1 < \bar{r}_2 < \cdots < \bar{r}_m$. Definiamo Σ come l'applicazione che manda r nella k-esima di queste radici. È facile vedere che Σ è biiettiva ed è chiaro che estende σ.

Mostrare che Σ è un isomorfismo richiede però qualche accortezza. A tal fine proviamo che per ogni sottoinsieme finito S di R_1 esistono un sottocampo E_1 di R_1/F_1 e un monomorfismo η di E_1/F_1 in R_2/F_2 che estende σ e conserva l'ordine degli elementi di S. Ossia, se $S = \{s_1 < s_2 < \cdots < s_n\}$, allora $\eta s_1 < \eta s_2 < \cdots < \eta s_n$. Siano $T = S \cup \{\sqrt{s_{i+1} - s_i} \mid 1 \leq i \leq n-1\}$ ed $E_1 = F_1(T)$. Evidentemente E_1 ha dimensione finita su F_1 e quindi $E_1 = F_1(w)$. Sia $f(x)$ il polinomio minimo di w su F_1. Per il lemma, $\bar{f}(x)$ ha una radice $\bar{w}$ in R_2, e abbiamo un monomorfismo η di E_1/F_1 in R_2/F_2 che manda w in $\bar{w}$. Si ha

$$\eta(s_{i+1}) - \eta(s_i) = \eta(s_{i+1} - s_i) = \eta\big((\sqrt{s_{i+1} - s_i})^2\big) = (\eta\sqrt{s_{i+1} - s_i})^2 > 0.$$

Quindi η conserva l'ordine degli s_i. Siano ora r, s due elementi qualsiasi di R_1 e applichiamo il risultato appena dimostrato all'insieme finito S delle radici in R_1 dei polinomi minimi di $r, s, r+s, rs$. Poiché η conserva l'ordine in S, si ha $\eta(r) = \Sigma(r)$, $\eta(s) = \Sigma(s)$, $\eta(r+s) = \Sigma(r+s)$, $\eta(rs) = \Sigma(rs)$. Quindi $\Sigma(r+s) = \eta(r+s) = \eta(r) + \eta(s) = \Sigma(r) + \Sigma(s)$, e analogamente $\Sigma(rs) = \Sigma(r)\Sigma(s)$. Dunque Σ è un isomorfismo.

Resta da mostrare che Σ è unico e conserva l'ordine. Sia Σ' un isomorfismo di R_1 su R_2. Poiché Σ' manda quadrati in quadrati e gli elementi positivi di R_i sono i quadrati non nulli, è chiaro che Σ' conserva l'ordine. Se inoltre Σ' estende σ, dalla definizione di Σ è chiaro che $\Sigma' = \Sigma$. La dimostrazione è conclusa. □

Se R_1, R_2 sono due chiusure reali di un campo ordinato F, l'identità su F si estende in modo unico a un isomorfismo d'ordine di R_1 su R_2. In questo senso la chiusura reale di F è unica.

Si vede facilmente che il campo $\mathbb{Q}$ dei numeri razionali ha un unico ordinamento. La sua chiusura reale $\mathbb{R}_0$ si chiama *campo dei numeri algebrici reali*. Il campo $\mathbb{C}_0 = \mathbb{R}_0(\sqrt{-1})$ è la chiusura algebrica di $\mathbb{Q}$. È il *campo dei numeri algebrici*.

Esercizi.

1. Sia F un campo ordinato ed E un'estensione reale chiusa il cui ordine estende quello di F. Mostrare che E contiene una chiusura reale di F.

2. Sia F un campo ordinato ed E un'estensione tale che le sole relazioni della forma $\sum_i a_i b_i^2 = 0$, con $a_i > 0$ in F e $b_i \in E$, siano quelle con tutti i $b_i = 0$. Mostrare che E ammette un ordinamento che estende quello di F.

11.3 Elementi totalmente positivi

Quali elementi di un campo dato si possono scrivere come somme di quadrati? Considereremo questa interessante questione nel presente paragrafo e nei due successivi. Otteniamo anzitutto

un criterio generale basato sulla definizione seguente.

Definizione 11.3. Un elemento a di un campo F si dice *totalmente positivo* se $a > 0$ per ogni ordinamento di F.

Si intende che, se F non ammette ordinamenti, ogni suo elemento è totalmente positivo. Ciò avviene dunque se F non è formalmente reale. In tal caso $-1 = \sum_i a_i^2$ con $a_i \in F$ e, se $\operatorname{char} F \neq 2$, la relazione

$$a = \left(\frac{1+a}{2}\right)^2 - \left(\frac{1-a}{2}\right)^2 = \left(\frac{1+a}{2}\right)^2 + \sum_i a_i^2 \left(\frac{1-a}{2}\right)^2 \tag{2}$$

mostra che ogni elemento di F è somma di quadrati. Ci servirà questa osservazione nella dimostrazione del criterio seguente.

Teorema 11.5. *Sia F un campo di caratteristica diversa da 2. Un elemento $a \neq 0$ di F è totalmente positivo se e solo se a è una somma di quadrati.*

Dimostrazione. Se $0 \neq a = \sum_i a_i^2$, evidentemente $a > 0$ in ogni ordinamento di F. Viceversa, supponiamo che $a \neq 0$ non sia somma di quadrati in F. Sia $\bar{F}$ una chiusura algebrica di F e consideriamo l'insieme dei sottocampi E di $\bar{F}/F$ nei quali a non è somma di quadrati. Per il lemma di Zorn ve n'è uno massimale, che chiameremo R. Per l'osservazione precedente R è formalmente reale e perciò può essere ordinato. Affermiamo che $-a$ è un quadrato in R. Altrimenti il sottocampo $R(\sqrt{-a})$ di $\bar{F}/F$ conterrebbe propriamente R, sicché a sarebbe somma di quadrati in $R(\sqrt{-a})$. Avremmo dunque $b_i, c_i \in R$ tali che $a = \sum_i (b_i + c_i\sqrt{-a})^2$. Ne seguirebbero $\sum_i b_i c_i = 0$ e $a = \sum_i b_i^2 - a\sum_i c_i^2$. Quindi $a(1 + \sum_i c_i^2) = \sum_i b_i^2$ e $1 + \sum_i c_i^2 \neq 0$, poiché R è formalmente reale. Posto $c = 1 + \sum_i c_i^2$, avremmo allora

$$a = \sum_i b_i^2 c^{-1} = \sum_i b_i^2 \left(1 + \sum_j c_j^2\right) c^{-2},$$

sicché a sarebbe somma di quadrati in R, contro la definizione di R. Dunque $-a = b^2$ per un $b \in R$, e $a = -b^2$ è negativo in ogni ordinamento di R. Tali ordinamenti inducono ordinamenti di F, per i quali $a < 0$. Dunque a non è totalmente positivo. □

Applichiamo anzitutto il risultato per determinare quali elementi di un campo di numeri F siano somme di quadrati. Abbiamo $F = \mathbb{Q}(r)$, con r algebrico su $\mathbb{Q}$. Se $\mathbb{R}_0$ è il campo dei numeri algebrici reali (la chiusura reale di $\mathbb{Q}$), allora $\mathbb{C}_0 = \mathbb{R}_0(\sqrt{-1})$ è una chiusura algebrica di $\mathbb{Q}$ e di F. Posto $n = [F : \mathbb{Q}]$, si hanno n monomorfismi distinti di $F/\mathbb{Q}$ in $\mathbb{C}_0/\mathbb{Q}$. Sono determinati dalle assegnazioni $r \mapsto r_i$, $1 \leq i \leq n$, dove gli r_i sono le radici del polinomio minimo $g(x)$ di r su $\mathbb{Q}$. Siano $r_1, \ldots, r_h$ quelli contenuti in $\mathbb{R}_0$. Li chiamiamo *coniugati reali* di r e poniamo $h = 0$ se nessun r_i appartiene a $\mathbb{R}_0$. Sia σ_i, $1 \leq i \leq h$, il monomorfismo di $F/\mathbb{Q}$ tale che $\sigma_i r = r_i$. Ciascun σ_i definisce un ordinamento di F stabilendo che $a > 0$ in F se $\sigma_i a > 0$ nell'unico ordinamento di $\mathbb{R}_0$. Affermiamo che questi h ordinamenti sono distinti e sono i soli ordinamenti di F.

Supponiamo dapprima che gli ordinamenti definiti da σ_i, σ_j coincidano. Allora $\sigma_j\sigma_i^{-1}$ è un isomorfismo che conserva l'ordine del sottocampo $\mathbb{Q}(r_i)$ di $\mathbb{R}_0$ sul sottocampo $\mathbb{Q}(r_j)$. Poiché $\mathbb{R}_0$ è algebrico su $\mathbb{Q}(r_i)$ e su $\mathbb{Q}(r_j)$, è la chiusura reale di entrambi. Per il teorema 11.4, $\sigma_j\sigma_i^{-1}$ si estende a un automorfismo σ di $\mathbb{R}_0$. Ma $\mathbb{R}_0$ è la chiusura reale di $\mathbb{Q}$, dunque ancora per il teorema 11.4 il suo unico automorfismo è l'identità. Ne segue $\sigma = 1$ e $\sigma_j = \sigma_i$. Sia ora dato un ordinamento di F e sia R la chiusura reale determinata da esso. Poiché R è algebrico su $\mathbb{Q}$, è anche una chiusura reale di $\mathbb{Q}$. Abbiamo quindi un isomorfismo d'ordine di $R/\mathbb{Q}$ su $\mathbb{R}_0/\mathbb{Q}$.

La sua restrizione a F coincide con uno degli σ_i, perciò l'ordinamento dato coincide con quello definito da tale σ_i.

È chiaro che gli σ_i così definiti sono precisamente i monomorfismi di F in $\mathbb{R}_0$. Abbiamo quindi provato il teorema seguente.

Teorema 11.6. *Sia F un campo di numeri algebrici e sia $\mathbb{R}_0$ il campo dei numeri algebrici reali. Vi è una corrispondenza biunivoca fra gli ordinamenti di F e i monomorfismi di F in $\mathbb{R}_0$. Nell'ordinamento determinato dal monomorfismo σ_i, si ha $a > 0$ per $a \in F$ se $\sigma_i a > 0$ in $\mathbb{R}_0$.*

Una conseguenza immediata dei teoremi 11.5 e 11.6 è il seguente risultato, dovuto a Hilbert e a E. Landau.

Teorema 11.7. *Sia F un campo di numeri algebrici e siano $\sigma_1, \ldots, \sigma_h$ ($h \geq 0$) i diversi monomorfismi di F nel campo $\mathbb{R}_0$ dei numeri algebrici reali. Un elemento $a \neq 0$ di F è somma di quadrati in F se e solo se $\sigma_i a > 0$ per $1 \leq i \leq h$.*[47]

Esercizi.

1. Sia F un campo ordinato ed E un'estensione. Mostrare che, se $b \in E$ non può scriversi nella forma $\sum_i a_i b_i^2$ con $a_i \geq 0$ in F e $b_i \in E$, esiste un ordinamento di E che estende quello di F e nel quale $b < 0$.

2. Siano F un campo ordinato, R la sua chiusura reale ed E un'estensione di dimensione finita di F. Dimostrare la seguente generalizzazione del teorema 11.6. Vi è una corrispondenza biunivoca fra gli ordinamenti di E che estendono quello di F e i monomorfismi di E/F in R/F.

3. (*I. Kaplansky–M. Kneser.*) Sia F un campo di caratteristica diversa da 2 che non sia formalmente reale. Supponiamo $|F^*/F^{*2}| = n < \infty$. Mostrare che ogni forma quadratica non degenere in n variabili è universale. (*Traccia della dimostrazione.* Sia $a_1, a_2, \ldots$ una successione di elementi non nulli di F e sia M_k l'insieme dei valori della forma quadratica $a_1 x_1^2 + \cdots + a_k x_k^2$, per $x_i \in F$. Mostrare che esiste $k \leq n$ tale che $M_{k+1} = M_k$. Allora $M_{k+1} = a_{k+1}F^2 + M_k = M_k$, dove F^2 è l'insieme dei quadrati degli elementi di F. Iterando $M_k = a_{k+1}F^2 + M_k$ si ottiene $M_k = a_{k+1}(F^2 + \cdots + F^2) + M_k$. Concludere che $M_k = F + M_k$ e $M_k = F$.)

11.4 Il diciassettesimo problema di Hilbert

Fra i ventitré problemi irrisolti che Hilbert propose in una conferenza al Congresso internazionale dei matematici di Parigi del 1900 figurava il problema delle funzioni razionali semidefinite positive. Sia f una funzione razionale di n variabili reali a coefficienti razionali, semidefinita positiva nel senso che $f(a_1, \ldots, a_n) \geq 0$ per tutte le n-uple reali $(a_1, \ldots, a_n)$ per cui f è definita. È necessariamente possibile scrivere f come somma di quadrati di funzioni razionali a coefficienti razionali? Per funzione razionale di n variabili reali a coefficienti razionali intendiamo un'applicazione $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$, dove $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$ e g, h sono polinomi nelle indeterminate x_i a coefficienti razionali. Il dominio di definizione della funzione è l'aperto di Zariski definito da $h(a_1, \ldots, a_n) \neq 0$, e due funzioni razionali si considerano uguali se assumono gli stessi valori in ogni punto di un aperto di Zariski non vuoto.

[47] Nell'enunciato originale manca la precisazione $a \neq 0$. L'elemento 0 è sempre somma di quadrati.

Nel 1927 Artin, servendosi in modo essenziale della teoria di Artin–Schreier dei campi formalmente reali, diede risposta affermativa alla domanda di Hilbert dimostrando il seguente risultato più forte.

Teorema di Artin. *Sia F un sottocampo di $\mathbb{R}$ che ammette un unico ordinamento e sia f una funzione razionale a coefficienti in F tale che $f(a_1, \ldots, a_n) \geq 0$ per tutti gli $a_i \in F$ per i quali f è definita. Allora f è somma di quadrati di funzioni razionali a coefficienti in F.*

Esempi di campi che ammettono un unico ordinamento sono $\mathbb{Q}$, $\mathbb{R}$ e ogni campo di numeri che abbia un solo coniugato reale (un'unica immersione reale).

Nel teorema di Artin la condizione che F sia un sottocampo di $\mathbb{R}$ può essere sostituita dall'ipotesi che F abbia un ordinamento archimedeo. Si vede facilmente che questa condizione equivale, a meno di isomorfismo, all'ipotesi $F \subseteq \mathbb{R}$ del teorema di Artin. Dimostreremo un risultato un po' più forte, nel quale la proprietà archimedea di F sarà sostituita da una condizione di densità nella chiusura reale. Se F è un sottocampo di un campo ordinato E, diciamo che F è *denso* in E se per ogni $a, b \in E$ con $a < b$ esiste $c \in F$ tale che $a < c < b$. Si vede facilmente che $\mathbb{Q}$ è denso in questo senso in $\mathbb{R}$, e ciò implica che ogni sottocampo di $\mathbb{R}$ è denso in $\mathbb{R}$. Il teorema seguente è quindi una generalizzazione del teorema di Artin.

Teorema 11.8. *Sia F un campo ordinato tale che (1) F abbia un unico ordinamento e (2) F sia denso nella sua chiusura reale. Sia f una funzione razionale a coefficienti in F tale che $f(a_1, \ldots, a_n) \geq 0$ per ogni $(a_1, \ldots, a_n) \in F^{(n)}$ per cui f è definita. Allora f è una somma di quadrati di funzioni razionali a coefficienti in F.*

Daremo una dimostrazione di tipo modellistico del teorema 11.8 basata sul risultato seguente, dimostrato in BAI, p. 340.

Siano R_1 e R_2 campi reali chiusi con un sottocampo ordinato comune F, ossia tali che gli ordinamenti indotti su F da R_1 e R_2 coincidano. Sia S un insieme finito di equazioni polinomiali, condizioni di non annullamento ($f \neq 0$) e disuguaglianze ($f > 0$) a coefficienti in F. Allora S ha una soluzione in R_1 se e solo se ne ha una in R_2.

Dimostrazione del teorema 11.8. L'insieme delle funzioni razionali di n variabili a coefficienti in F forma un campo rispetto alle usuali operazioni di addizione e moltiplicazione. Se p_i, $1 \leq i \leq n$, indica la funzione $p_i(a_1, \ldots, a_n) = a_i$, abbiamo un isomorfismo del campo $F(x_1, \ldots, x_n)$, con x_i indeterminate, sul campo delle funzioni razionali che manda x_i in p_i. Quest'ultimo campo è dunque $F(p_1, \ldots, p_n)$. Supponiamo che $f \in F(p_1, \ldots, p_n)$ non sia somma di quadrati. Per il teorema 11.5 esiste allora un ordinamento di $F(p_1, \ldots, p_n)$ per il quale $f < 0$. Scriviamo $f = gh^{-1}$ con $g, h \in F[p_1, \ldots, p_n]$. Allora $gh < 0$. Ponendo

$$k(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)h(x_1, \ldots, x_n),$$

si ha $k(p_1, \ldots, p_n) < 0$. Pertanto la disuguaglianza $k(x_1, \ldots, x_n) < 0$ ammette la soluzione $(p_1, \ldots, p_n)$ in $F(p_1, \ldots, p_n)$ e, a maggior ragione, nella sua chiusura reale R. Consideriamo ora la chiusura reale R_0 di F. Poiché F ha un unico ordinamento, gli ordinamenti di F indotti da R_0 e da R coincidono. Inoltre $k(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Per il risultato citato esistono quindi $a_i \in R_0$ tali che $k(a_1, \ldots, a_n) < 0$ e, di conseguenza, $f(a_1, \ldots, a_n) < 0$. Per completare la dimostrazione basta mostrare che gli a_i si possono scegliere in F.

Lemma. *Sia F un campo ordinato denso nella sua chiusura reale R. Supponiamo che, per $k(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$, esistano $a_i \in R$ tali che $k(a_1, \ldots, a_n) < 0$. Esistono allora $b_i \in F$ tali che $k(b_1, \ldots, b_n) < 0$.*

Dimostrazione. Procediamo per induzione su n. Per $n = 1$ scegliamo $a' < a$ (dove $a = a_1$) in modo che l'intervallo $[a', a]$ non contenga radici di k. Allora $k(x) < 0$ per ogni $x \in [a', a]$ (BAI, p. 310), e in questo intervallo possiamo scegliere $x = b \in F$. Si ha così $k(b) < 0$. Supponiamo

ora che il risultato valga per $n-1$ variabili. Il caso di una variabile mostra che esiste $b_1 \in F$ tale che $k(b_1, a_2, \ldots, a_n) < 0$. Dal caso di $n-1$ variabili segue poi che esistono $b_2, \ldots, b_n \in F$ tali che $k(b_1, b_2, \ldots, b_n) < 0$. □

Osservazione. K. McKenna ha dimostrato il seguente inverso del teorema 11.8. Se F è un campo ordinato nel quale ogni funzione razionale f semidefinita positiva, nel senso che $f(a_1, \ldots, a_n) \geq 0$ per ogni $(a_1, \ldots, a_n)$ per cui è definita, è somma di quadrati, allora F ha un unico ordinamento ed è denso nella sua chiusura reale.

Esercizi.

1. (J. Keisler.) Sia F ordinato e si munisca l'estensione $F(x)$, con x trascendente, dell'ordinamento dell'esercizio 4 del §11.1. Mostrare che $F(x)$ non è denso nella sua chiusura reale, provando che l'intervallo $[\sqrt{x}, 2\sqrt{x}]$ non contiene elementi di $F(x)$.

2. Sia R reale chiuso e sia $f(x) \in R[x]$ tale che $f(a) \geq 0$ per ogni $a \in R$. Mostrare che $f(x)$ è somma di due quadrati in $R[x]$.

3. (C. Procesi.) Sia R un campo reale chiuso, V una varietà algebrica irriducibile definita su R e F il campo delle funzioni razionali su V (si veda l'esercizio 7, pp. 429–430). Siano $h_1, \ldots, h_k \in F$ e sia X l'insieme dei punti ρ di V per i quali $h_i(\rho) \geq 0$ per ogni i. Mostrare che, se $g \in F$ soddisfa $g(\rho) \geq 0$ per ogni $\rho \in X$ in cui g è definita, allora g ha la forma

$$\sum{}' s_{i_1 \cdots i_j} h_{i_1} \cdots h_{i_j},$$

   dove $\sum'$ indica la somma sugli indici tra 1 e k presi in ordine strettamente crescente e gli $s_{i_1 \cdots i_j}$ sono somme di quadrati in F.

   Traccia della dimostrazione. La conclusione equivale al fatto che g sia somma di quadrati in $F_1 = F(\sqrt{h_1}, \ldots, \sqrt{h_k})$. Senza perdita di generalità possiamo supporre che g e gli h_i siano polinomi nelle funzioni coordinate $p_1, \ldots, p_n$ (come nella dimostrazione del teorema di Artin). Abbiamo cioè polinomi $g(x_1, \ldots, x_n)$, $h_j(x_1, \ldots, x_n)$, $1 \leq j \leq k$, nelle indeterminate x_i, a coefficienti in R, tali che $g = g(p_1, \ldots, p_n)$ e $h_j = h_j(p_1, \ldots, p_n)$. Se g non è somma di quadrati in F_1, esiste un ordinamento di F_1 per cui $g < 0$. Siano $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$ generatori dell'ideale primo di $R[x_1, \ldots, x_n]$ che definisce V. In F_1, e quindi in una sua chiusura reale R_1, abbiamo

$$f_1(p_1, \ldots, p_n) = 0, \ \ldots, \ f_m(p_1, \ldots, p_n) = 0,$$
$$h_1(p_1, \ldots, p_n) \geq 0, \ \ldots, \ h_k(p_1, \ldots, p_n) \geq 0, \qquad g(p_1, \ldots, p_n) < 0.$$

   Esistono di conseguenza $a_1, \ldots, a_n \in R$ tali che $f_1(a_1, \ldots, a_n) = 0, \ldots, f_m(a_1, \ldots, a_n) = 0$, $h_1(a_1, \ldots, a_n) \geq 0, \ldots, h_k(a_1, \ldots, a_n) \geq 0$ e $g(a_1, \ldots, a_n) < 0$. Ciò contraddice l'ipotesi.

4. (J. J. Sylvester.) Sia $f(x) \in R[x]$, con R reale chiuso e x indeterminata, e sia $A = R[x]/(f(x))$. Sia $T(a, b)$ la forma bilineare traccia su A/R e sia $Q(a) = T(a, a)$ la forma quadratica corrispondente. Mostrare che il numero di radici distinte di $f(x)$ in R è la segnatura di Q (BAI, p. 359).

5. Sia F un campo, $f(x)$ un polinomio monico in $F[x]$ e sia $f(x) = \prod_{i=1}^{n}(x - r_i)$ in un campo di spezzamento E/F di $f(x)$. Poniamo $s_j = \sum_{i=1}^{n} r_i^j$, cosicché $s_j \in F$. La matrice

$$\begin{pmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{pmatrix}$$

si chiama *bezoutiana* di $f(x)$. Mostrare che il suo determinante è il discriminante della forma traccia $T(a,b)$ su $A = F[x]/(f(x))$ rispetto alla base $\overline{1}, \bar{x}, \ldots, \overline{x^{n-1}}$, dove $\overline{x^i} = x^i + (f(x))$.

6. (Sylvester.) Con le notazioni degli esercizi 4 e 5, sia b_k la somma dei minori principali (ossia diagonali) di ordine k della bezoutiana di $f(x)$, cosicché il polinomio caratteristico della bezoutiana è $x^n - b_1 x^{n-1} + \cdots + (-1)^n b_n$. Mostrare che tutte le radici di $f(x)$ appartengono a R se e solo se $b_i \geq 0$ per ogni i.

7. (Procesi.) Sia R un campo reale chiuso e sia g una funzione razionale simmetrica di n variabili a coefficienti in R, tale che $g(a_1, \ldots, a_n) \geq 0$ per ogni $(a_1, \ldots, a_n) \in R^{(n)}$ per cui g è definita. Sia b_k la somma dei minori principali di ordine k della bezoutiana di $f(x) = \prod_{i=1}^n (x - \rho_i)$. Mostrare che g è della forma $\sum' s_{i_1 \cdots i_j} b_{i_1} \cdots b_{i_j}$, dove $\sum'$ indica la somma sugli indici in ordine strettamente crescente, da 1 a n, e gli $s_{i_1 \cdots i_j}$ sono somme di quadrati di funzioni simmetriche.[48]

11.5 La teoria di Pfister delle forme quadratiche

Se un elemento di un campo è somma di quadrati, possiamo affermare che è somma di n quadrati per un n assegnato? Non è difficile vedere che, se R è un campo reale chiuso, ogni elemento di $R(x)$ che sia somma di quadrati è somma di due quadrati. Hilbert dimostrò che una funzione razionale semidefinita positiva di due variabili su $\mathbb{R}$ è somma di quattro quadrati. Nel paragrafo successivo dimostreremo il teorema di Pfister secondo il quale, se R è reale chiuso, ogni elemento di $R(x_1, \ldots, x_n)$ che sia somma di quadrati è somma di 2^n quadrati. Negli esercizi del § 11.6 daremo anche una traccia della dimostrazione di un teorema di Cassels secondo il quale esistono elementi di $R(x_1, \ldots, x_n)$ che sono somme di quadrati ma non si possono scrivere come somme di meno di n quadrati. Non si conosce, al momento in cui scriviamo, il valore esatto del minimo numero $k(n)$ tale che ogni elemento di $R(x_1, \ldots, x_n)$ che sia somma di quadrati sia somma di $k(n)$ quadrati. I risultati indicati danno le disuguaglianze $n \leq k(n) \leq 2^n$.

La dimostrazione del teorema di Pfister si fonda su alcuni risultati sulle forme quadratiche che presentano anche un notevole interesse autonomo. Dedichiamo questo paragrafo alla loro esposizione.

Ci occupiamo esclusivamente di forme quadratiche Q su spazi vettoriali V di dimensione finita su un campo F di caratteristica diversa da 2. Come al solito, scriviamo $B(x,y) = Q(x+y) - Q(x) - Q(y)$. Poiché la caratteristica è diversa da 2, conviene sostituire $B(x,y)$ con $Q(x,y) = \frac{1}{2}B(x,y)$. Allora $Q(x,x) = Q(x)$. Indicheremo che V ha una base $(u_1, \ldots, u_n)$ ortogonale rispetto a Q, con $Q(u_i) = b_i$, scrivendo

$$Q \sim \operatorname{diag}\{b_1, b_2, \ldots, b_n\}. \tag{3}$$

Scriveremo inoltre

$$\operatorname{diag}\{b_1, \ldots, b_n\} \sim \operatorname{diag}\{c_1, \ldots, c_n\} \tag{4}$$

se le forme quadratiche $\sum_{i=1}^n b_i x_i^2$ e $\sum_{i=1}^n c_i x_i^2$ sono equivalenti.

Introduciamo alcune nozioni e alcuni risultati sulle forme quadratiche che finora non abbiamo considerato. Per prima cosa consideriamo il prodotto tensoriale di forme quadratiche. Per

[48] Nell'originale si legge «da 1 a k». Qui k designa l'ordine del minore e le quantità disponibili sono $b_1, \ldots, b_n$. I minori sono quelli principali dell'esercizio 6. [N.d.T.]

$i = 1, 2$, sia V_i uno spazio vettoriale su F e Q_i una forma quadratica su V_i. Mostreremo che su $V_1 \otimes V_2$ si definisce una forma quadratica $Q_1 \otimes Q_2$ tale che

$$(Q_1 \otimes Q_2)(v_1 \otimes v_2) = Q_1(v_1)Q_2(v_2) \tag{5}$$

per $v_i \in V_i$. Sia $(u_1^{(i)}, \dots, u_{n_i}^{(i)})$ una base di V_i/F. Allora $(u_i^{(1)} \otimes u_j^{(2)})$ è una base di $V_1 \otimes V_2$ e su questo spazio abbiamo una forma quadratica Q tale che

$$Q(u_i^{(1)} \otimes u_j^{(2)}, u_k^{(1)} \otimes u_l^{(2)}) = Q_1(u_i^{(1)}, u_k^{(1)})Q_2(u_j^{(2)}, u_l^{(2)}). \tag{6}$$

Se $v_1 = \sum a_i u_i^{(1)}$ e $v_2 = \sum b_j u_j^{(2)}$, allora

$$\begin{aligned} Q(v_1 \otimes v_2) &= Q(v_1 \otimes v_2, v_1 \otimes v_2) \\ &= Q\left(\sum_{i,j} a_i b_j u_i^{(1)} \otimes u_j^{(2)}, \sum_{k,l} a_k b_l u_k^{(1)} \otimes u_l^{(2)}\right) \\ &= \sum_{i,j,k,l} a_i a_k b_j b_l Q_1(u_i^{(1)}, u_k^{(1)}) Q_2(u_j^{(2)}, u_l^{(2)}) \\ &= \left(\sum_{i,k} a_i a_k Q_1(u_i^{(1)}, u_k^{(1)})\right)\left(\sum_{j,l} b_j b_l Q_2(u_j^{(2)}, u_l^{(2)})\right) \\ &= Q_1(v_1)Q_2(v_2). \end{aligned}$$

Ponendo $Q = Q_1 \otimes Q_2$ si ottiene (5). Poiché i vettori $v_1 \otimes v_2$ generano $V_1 \otimes V_2$, la forma bilineare precisata dalla (6), e quindi la forma quadratica $Q_1 \otimes Q_2$, è unica.[49]

Se $(u_1^{(i)}, \dots, u_{n_i}^{(i)})$ è una base ortogonale per V_i, allora $(u_j^{(1)} \otimes u_k^{(2)})$ è una base ortogonale per $V_1 \otimes V_2$. Se $Q_i \sim \operatorname{diag}\{b_1^{(i)}, \dots, b_{n_i}^{(i)}\}$, abbiamo

$$\begin{aligned} Q_1 \otimes Q_2 \sim \operatorname{diag}\{&b_1^{(1)}b_1^{(2)}, \dots, b_1^{(1)}b_{n_2}^{(2)}, b_2^{(1)}b_1^{(2)}, \dots, b_2^{(1)}b_{n_2}^{(2)}, \\ &\dots, b_{n_1}^{(1)}b_1^{(2)}, \dots, b_{n_1}^{(1)}b_{n_2}^{(2)}\} \\ = \operatorname{diag}\{&b_1^{(1)}, \dots, b_{n_1}^{(1)}\} \otimes \operatorname{diag}\{b_1^{(2)}, \dots, b_{n_2}^{(2)}\}, \end{aligned} \tag{7}$$

dove il prodotto tensoriale di matrici è quello definito a p. 250. In modo analogo si definisce il prodotto tensoriale di più di due forme quadratiche e si ha la seguente generalizzazione di (7). Se $Q_i \sim \operatorname{diag}\{b_1^{(i)}, \dots, b_{n_i}^{(i)}\}$, allora

$$Q_1 \otimes \cdots \otimes Q_r \sim \operatorname{diag}\{b_1^{(1)}, \dots, b_{n_1}^{(1)}\} \otimes \cdots \otimes \operatorname{diag}\{b_1^{(r)}, \dots, b_{n_r}^{(r)}\}. \tag{8}$$

Conviene inoltre definire la somma diretta di due forme quadratiche. Se Q_i è una forma quadratica su V_i, per $i = 1, 2$, si definisce $Q_1 \oplus Q_2$ come la forma quadratica su $V_1 \oplus V_2$ tale che

$$(Q_1 \oplus Q_2)(v_1, v_2) = Q_1(v_1) + Q_2(v_2).$$

È chiaro che $Q_1 \oplus Q_2$ è ben definita. Se identifichiamo V_1, V_2 nel modo consueto con sottospazi di $V_1 \oplus V_2$, questi sono ortogonali rispetto alla forma bilineare di $Q_1 \oplus Q_2$. Se $(u_1^{(i)}, \dots, u_{n_i}^{(i)})$ è

[49] L'originale attribuisce l'unicità alla sola (5). La (6) specifica anche i valori della forma bilineare su coppie di tensori puri. La distinzione è necessaria, perché forme quadratiche diverse possono coincidere su tutti i tensori puri.

una base ortogonale per V_i, allora $(u_1^{(1)}, \ldots, u_{n_1}^{(1)}, u_1^{(2)}, \ldots, u_{n_2}^{(2)})$ è una base ortogonale per $V_1 \oplus V_2$. Abbiamo

$$Q_1 \oplus Q_2 \sim \operatorname{diag}\{b_1^{(1)}, \ldots, b_{n_1}^{(1)}, b_1^{(2)}, \ldots, b_{n_2}^{(2)}\} \tag{9}$$

se $Q_i \sim \operatorname{diag}\{b_1^{(i)}, \ldots, b_{n_i}^{(i)}\}$. Se B, C sono matrici, conviene indicare con $B \oplus C$ la matrice $\left(\begin{smallmatrix} B & 0 \\ 0 & C \end{smallmatrix}\right)$. Con questa notazione possiamo riscrivere la (9) nella forma

$$Q_1 \oplus Q_2 \sim \operatorname{diag}\{b_1^{(1)}, \ldots, b_{n_1}^{(1)}\} \oplus \operatorname{diag}\{b_1^{(2)}, \ldots, b_{n_2}^{(2)}\}.$$

Consideriamo ora i risultati di Pfister sulle forme quadratiche da cui si ricava il teorema sulle somme di quadrati enunciato all'inizio del paragrafo. Il nostro punto di partenza è una generalizzazione in senso debole del teorema di A. Hurwitz sulle somme di quadrati (si veda *BAI*, pp. 438–451). Hurwitz dimostrò che esistono identità della forma

$$\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right) = \sum_{i=1}^{n} z_i^2,$$

con gli z_i bilineari nelle x e nelle y, se e solo se $n = 1, 2, 4$ oppure 8. Pfister ha dimostrato che, per ogni n potenza di due, il prodotto di due somme di n quadrati in un campo F è ancora somma di n quadrati in F. Dunque, rinunciando a richiedere che gli z_i dipendano in modo bilineare dalle x e dalle y, abbiamo $(\sum_{i=1}^n x_i^2)(\sum_{i=1}^n y_i^2) = \sum_{i=1}^n z_i^2$ per ogni n potenza di due. Più in generale, consideriamo forme quadratiche Q che siano *moltiplicative*, nel senso che, dati due vettori qualunque x, y, esista un vettore z tale che $Q(x)Q(y) = Q(z)$. Una condizione più forte è data dalla definizione seguente.

Definizione 11.4. Una forma quadratica Q si dice *fortemente moltiplicativa* se è equivalente a cQ per ogni $c \neq 0$ rappresentato da Q.

Ciò significa che esiste una trasformazione lineare biiettiva η di V tale che $cQ(x) = Q(\eta x)$ per ogni x. Se $Q(y) = c$, abbiamo allora $Q(x)Q(y) = Q(z)$ per $z = \eta x$, dunque una forma fortemente moltiplicativa è moltiplicativa. Se Q ha indice di Witt massimo (*BAI*, p. 369) su uno spazio di dimensione pari, in coordinate Q si può scrivere come $\sum_{i=1}^n x_i^2 - \sum_{i=n+1}^{2n} x_i^2$. Si verifica facilmente che Q è fortemente moltiplicativa. La forma $Q = x_1^2 - x_2^2 - x_3^2$ su uno spazio vettoriale reale di dimensione tre è invece moltiplicativa, ma non fortemente moltiplicativa. La moltiplicatività segue dal fatto che ogni forma universale possiede questa proprietà. Per il teorema di Sylvester (*BAI*, p. 359), Q non è equivalente a $-Q$. Per una forma quadratica Q su V/F indichiamo con F_Q^* l'insieme degli elementi non nulli di F rappresentati da Q. È chiaro che F_Q^* è chiuso rispetto alla moltiplicazione se e solo se Q è moltiplicativa. Poiché $Q(x) = c \neq 0$ implica $Q(c^{-1}x) = c^{-1}$, vediamo che Q è moltiplicativa se e solo se F_Q^* è un sottogruppo di F^*.

Passiamo a dedurre i risultati di Pfister. Diamo anzitutto un criterio di equivalenza nel caso binario.

Lemma 1. *Si ha* $\operatorname{diag}\{b_1, b_2\} \sim \operatorname{diag}\{c_1, c_2\}$ *se e solo se* c_1 *è rappresentato da* $b_1x_1^2 + b_2x_2^2$ *e* b_1b_2 *e* c_1c_2 *differiscono per un fattore quadrato.*

Dimostrazione. Poiché b_1b_2 è un discriminante di $Q = b_1x_1^2 + b_2x_2^2$ e i b_i sono rappresentati da Q, è chiaro che le condizioni sono necessarie. Supponiamo ora che valgano. Per la prima esiste un vettore y tale che $Q(y) = c_1$. Allora $\operatorname{diag}\{b_1, b_2\} \sim \operatorname{diag}\{c_1, c\}$ e $c_1c = k^2b_1b_2$, $k \in F^*$. Inoltre $c_1c_2 = l^2b_1b_2$. Ne segue $c_2 = n^2c$ e possiamo sostituire c con c_2. Dunque $\operatorname{diag}\{b_1, b_2\} \sim \operatorname{diag}\{c_1, c_2\}$. □

Dimostriamo ora il lemma fondamentale.

Lemma 2. *Sia Q una forma quadratica fortemente moltiplicativa e sia $a \in F^*$. Se $Q_a \sim \operatorname{diag}\{1, a\}$, allora $Q_a \otimes Q$ è fortemente moltiplicativa.*

Dimostrazione. È chiaro che $Q_a \otimes Q$ è equivalente a $Q \oplus aQ$. Basta quindi mostrare che quest'ultima è fortemente moltiplicativa. Usiamo ora $\sim$ anche per l'equivalenza fra forme quadratiche. Se $Q_1 \sim \operatorname{diag}\{a, b\}$, indichiamo $Q_1 \otimes Q_2$ con $\operatorname{diag}\{a, b\} \otimes Q_2 \sim aQ_2 \oplus bQ_2$. Sia $k \in F^*$ rappresentato da $Q \oplus aQ$. Abbiamo $k = b + ac$ dove b, c sono rappresentati da Q (eventualmente in modo banale se b oppure c è zero). Distinguiamo tre casi.

Caso I. $c = 0$. Allora $k = b$ e $Q \sim bQ$. Quindi $Q \oplus aQ \sim bQ \oplus abQ = b(Q \oplus aQ) = k(Q \oplus aQ)$.

Caso II. $b = 0$. Allora $k = ac$ e $k(Q \oplus aQ) = kQ \oplus kaQ = acQ \oplus a^2cQ \sim aQ \oplus Q$, poiché $cQ \sim Q$ per ipotesi e $Q \sim a^2Q$ per ogni $a \in F^*$. Quindi $k(Q \oplus aQ) \sim Q \oplus aQ$.

Caso III. $bc \neq 0$. Abbiamo $Q \oplus aQ \sim bQ \oplus acQ \sim \operatorname{diag}\{b, ac\} \otimes Q$. Poiché $k = b + ac$ è rappresentato da $bx_1^2 + acx_2^2$ e bac e k^2abc differiscono per un quadrato, il lemma 1 dà $\operatorname{diag}\{b, ac\} \sim \operatorname{diag}\{k, kabc\}$. Ne segue

$$\begin{aligned}\operatorname{diag}\{b, ac\} \otimes Q &\sim \operatorname{diag}\{k, kabc\} \otimes Q \sim k \operatorname{diag}\{1, abc\} \otimes Q \\ &\sim kQ \oplus kabcQ \sim kQ \oplus kaQ = k(Q \oplus aQ).\end{aligned}$$

In tutti i casi abbiamo $Q \oplus aQ \sim k(Q \oplus aQ)$, dunque $Q \oplus aQ$ è fortemente moltiplicativa. □

È chiaro che la forma $Q_0 = x^2 \sim \operatorname{diag}\{1\}$ è fortemente moltiplicativa. Applicando ripetutamente il lemma 2 otteniamo quindi il teorema seguente.

Teorema 11.9. *Se $a_i \in F^*$, allora*

$$Q \sim \operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} \tag{10}$$

è una forma quadratica fortemente moltiplicativa. In particolare $\sum_{i=1}^{2^n} x_i^2 \sim \operatorname{diag}\{1, 1\} \otimes \cdots \otimes \operatorname{diag}\{1, 1\}$ (n fattori) è fortemente moltiplicativa.

Chiameremo le forme del teorema 11.9 *forme di Pfister di dimensione* 2^n. Dimostriamo ora per queste forme una specie di teorema di fattorizzazione.

Teorema 11.10. *Scriviamo*

$$\operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} = \operatorname{diag}\{1\} \oplus D \tag{11}$$

e sia Q una forma quadratica tale che $Q \sim D$. Supponiamo che $b_1 \neq 0$ sia rappresentato da Q. Allora esistono $b_2, \ldots, b_n \in F^*$ tali che

$$\operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} \sim \operatorname{diag}\{1, b_1\} \otimes \cdots \otimes \operatorname{diag}\{1, b_n\}. \tag{12}$$

Dimostrazione. Procediamo per induzione su n. Se $n = 1$, allora $b_1 = a_1c^2$ e perciò $\operatorname{diag}\{1, a_1\} \sim \operatorname{diag}\{1, b_1\}$. Supponiamo il risultato valido per n e consideriamo

$$\operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} \otimes \operatorname{diag}\{1, a\} = \operatorname{diag}\{1\} \oplus D'. \tag{13}$$

Supponiamo che $b_1 \neq 0$ sia rappresentato da $Q' \sim D'$. Allora $b_1 = b_1' + ab$, dove b_1' è rappresentato da $Q \sim D$ e b è rappresentato da $x^2 \oplus Q \sim \operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\}$.

Caso I. $b = 0$. Allora $b_1' \neq 0$ e l'ipotesi induttiva dà elementi $b_2, \ldots, b_n \in F^*$ per i quali vale (12). Quindi

$$\begin{aligned}&\operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} \otimes \operatorname{diag}\{1, a\} \\ &\quad \sim \operatorname{diag}\{1, b_1\} \otimes \cdots \otimes \operatorname{diag}\{1, b_n\} \otimes \operatorname{diag}\{1, a\}.\end{aligned}$$

Caso II. $b_1' = 0$. Allora $b \neq 0$, $b_1 = ab$ e, scrivendo $H = \operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\}$, abbiamo

$$H \otimes \operatorname{diag}\{1, a\} \sim H \oplus aH \sim H \oplus abH \sim \operatorname{diag}\{1, ab\} \otimes H$$

per il teorema 11.9.

Caso III. $bb_1' \neq 0$. L'equivalenza stabilita nel caso II ci permette di sostituire a con ab. Per il caso I esistono poi $b_2, \ldots, b_n \in F^*$ tali che

$$\begin{aligned}&\operatorname{diag}\{1, a_1\} \otimes \cdots \otimes \operatorname{diag}\{1, a_n\} \otimes \operatorname{diag}\{1, ab\}\\ &\quad \sim \operatorname{diag}\{1, b_1'\} \otimes \operatorname{diag}\{1, b_2\} \otimes \cdots \otimes \operatorname{diag}\{1, b_n\} \otimes \operatorname{diag}\{1, ab\}.\end{aligned}$$

Ora

$$\begin{aligned}\operatorname{diag}\{1, ab\} \otimes \operatorname{diag}\{1, b_1'\} &\sim \operatorname{diag}\{1, ab, b_1', abb_1'\}\\ &\sim \operatorname{diag}\{1, abb_1'\} \oplus \operatorname{diag}\{b_1', ab\}\\ &\sim \operatorname{diag}\{1, abb_1'\} \oplus \operatorname{diag}\{b_1, b_1abb_1'\} \quad \text{(lemma 1)}\\ &\sim \operatorname{diag}\{1, b_1\} \otimes \operatorname{diag}\{1, b_1'ab\}.\end{aligned}$$

Sostituendo nella prima equivalenza otteniamo il risultato anche in questo caso. □

Possiamo ora dedurre il risultato principale, che riguarda la rappresentazione delle somme di quadrati mediante valori di forme di Pfister.

Teorema 11.11. *Supponiamo che ogni forma di Pfister di dimensione* 2^n *rappresenti ogni somma non nulla di due quadrati in* F*. Allora ogni forma di Pfister di dimensione* 2^n *rappresenta ogni somma non nulla di* k *quadrati in* F*, per* k *arbitrario.*

Dimostrazione. Procediamo per induzione su k. Ogni forma di Pfister rappresenta 1, dunque il caso $k = 1$ è chiaro e il caso $k = 2$ è l'ipotesi. Supponiamo il risultato valido per $k \geq 2$. Basta mostrare che, se Q è una forma di Pfister di dimensione 2^n e a è una somma di k quadrati tale che $c = 1 + a \neq 0$, allora c è rappresentato da Q. A tale scopo basta dimostrare che $Q \oplus (-cQ)$ rappresenta 0 in modo non banale. Infatti avremmo allora vettori u, v, almeno uno dei quali non nullo, tali che $Q(u) = cQ(v)$. Se $Q(u) = 0$ oppure $Q(v) = 0$, entrambi sono nulli, dunque Q rappresenta 0 in modo non banale. Allora Q è universale e quindi rappresenta c. Se $Q(u) \neq 0$ e $Q(v) \neq 0$, entrambi appartengono a F_Q^*, perciò $c = Q(u)Q(v)^{-1} \in F_Q^*$ e c è rappresentato da Q.

Scriviamo ora $Q = x^2 \oplus Q'$. Poiché Q rappresenta a, abbiamo $a = a_1^2 + a'$, dove Q' rappresenta a'. Si ha $\operatorname{diag}\{1, -c\} \otimes Q \sim Q \oplus (-cQ) \sim x^2 \oplus Q' \oplus (-cQ)$ e $Q' \oplus (-cQ)$ rappresenta $a' - (1 + a_1^2 + a') = -(1 + a_1^2)$. Se questo elemento è zero, allora $c = a'$ è rappresentato da Q. Possiamo dunque supporre $1 + a_1^2 \neq 0$. Per il teorema 11.10,

$$\operatorname{diag}\{1, -c\} \otimes Q \sim \operatorname{diag}\{1, -1 - a_1^2\} \otimes Q'',$$

dove Q'' è una forma di Pfister di dimensione 2^n. Per ipotesi Q'' rappresenta $1 + a_1^2$. Ne segue che $\operatorname{diag}\{1, -1 - a_1^2\} \otimes Q''$ rappresenta 0 in modo non banale. Lo stesso vale allora per $Q \oplus (-cQ) \sim \operatorname{diag}\{1, -1 - a_1^2\} \otimes Q''$, e la dimostrazione è completa. □

11.6 Somme di quadrati in $R(x_1, \ldots, x_n)$, con R campo reale chiuso

Consideriamo ora il campo $R(x_1, \ldots, x_n)$ delle espressioni razionali in n indeterminate $x_1, \ldots, x_n$ su un campo reale chiuso R. Vogliamo mostrare che il teorema 11.11 si può applicare al campo $F = R(x_1, \ldots, x_n)$. A tale scopo occorre invocare un teorema dimostrato da C. C. Tsen nel 1936 e riscoperto da S. Lang nel 1951. Per enunciarlo ci serve la seguente definizione.

Definizione 11.5. Un campo F si dice *campo C_i* se, per ogni intero positivo d, ogni polinomio omogeneo f di grado d, a coefficienti in F, in più di d^i indeterminate, possiede uno zero non banale in F.

Per zero non banale, dette m le indeterminate, intendiamo un elemento $(a_1, \dots, a_m) \in F^{(m)}$ tale che $(a_1, \dots, a_m) \neq (0, \dots, 0)$ e $f(a_1, \dots, a_m) = 0$. Il teorema che ci occorre è il seguente.

Teorema di Tsen–Lang. *Se F è algebricamente chiuso e le x_j sono indeterminate, allora $F(x_1, \dots, x_n)$ è un campo C_n.*

Si vede subito che ogni campo algebricamente chiuso è un campo C_0. Supponiamo ora che F non sia algebricamente chiuso. Esiste allora un'estensione E/F tale che $[E : F] = n > 1$, con n finito. Sia $(u_1, \dots, u_n)$ una base di E/F e sia ρ la rappresentazione matriciale regolare determinata da questa base (*BAI*, p. 424). Allora, posto $u = \sum a_i u_i$, con $a_i \in F$, si ha

$$N_{E/F}(u) = \det\Big(\sum a_i \rho(u_i)\Big) \neq 0$$

a meno che tutti gli a_i siano nulli. Siano $x_1, \dots, x_n$ indeterminate e poniamo $N(x_1, \dots, x_n) = \det(\sum x_i \rho(u_i))$. Questo polinomio è omogeneo di grado n e $N(a_1, \dots, a_n) = N_{E/F}(u)$. Pertanto N ammette soltanto lo zero banale $(0, \dots, 0)$ e F non è un campo C_0. Dunque un campo è C_0 se e solo se è algebricamente chiuso.

I campi C_1 furono introdotti da Artin, che li denominò *quasi algebricamente chiusi*. In una serie di esercizi di *BAI* abbiamo indicato come provare che ogni campo finito è C_1 (esercizi 2–7, p. 137).

La dimostrazione del teorema di Tsen–Lang procede per induzione. Sia per provare il passo iniziale, secondo cui $F(x)$ è C_1 se F è algebricamente chiuso, sia per il passo induttivo, ci serviremo del seguente risultato, conseguenza del teorema 7.29, p. 453.

Lemma 1. *Siano F un campo algebricamente chiuso e $f_1, \dots, f_r$ polinomi senza termine costante in n indeterminate, a coefficienti in F. Se $n > r$, il sistema di equazioni $f_1(x_1, \dots, x_n) = 0, \dots, f_r(x_1, \dots, x_n) = 0$ possiede una soluzione non banale in $F^{(n)}$.*

Ci occorre anche un risultato analogo per sistemi di equazioni polinomiali in un campo C_i, che ricaveremo fra poco. Diamo prima la seguente definizione.

Definizione 11.6. Un polinomio a coefficienti in F si dice *normico di ordine i* ($i > 0$) per F se è omogeneo di grado $d > 1$ in d^i indeterminate e possiede soltanto lo zero banale in F.

Il ragionamento precedente mostra che, se F non è algebricamente chiuso, esistono polinomi normici di ordine 1 per F. Per un campo F qualunque e un'indeterminata t si vede facilmente che $F(t)$ non è algebricamente chiuso (per esempio, $\sqrt{t} \notin F(t)$). Esistono quindi polinomi normici di ordine 1 per $F(t)$. Vale inoltre il seguente lemma.

Lemma 2. *Se esiste un polinomio normico di ordine i per F, esiste un polinomio normico di ordine $i + 1$ per $F(t)$, dove t è un'indeterminata.*

Dimostrazione. Sia $N(x_1, \dots, x_{d^i})$ un polinomio normico di ordine i per F, di grado d. Affermiamo che

$$\begin{aligned} N(x_1, \dots, x_{d^i}) + N(x_{d^i+1}, \dots, x_{2d^i})t + \cdots \\ + N(x_{(d-1)d^i+1}, \dots, x_{d^{i+1}})t^{d-1} \end{aligned} \tag{14}$$

è normico di ordine $i + 1$ per $F(t)$. Poiché è omogeneo di grado d in d^{i+1} indeterminate, basta dimostrare che in $F(t)$ ha soltanto lo zero banale. Sia dunque $(a_1, \dots, a_{d^{i+1}})$ uno zero non banale

di (14). Per omogeneità possiamo supporre che gli a_i appartengano a $F[t]$ e che non siano tutti divisibili per t. Sia a_k il primo che non lo è e supponiamo che $jd^i+1 \le k \le (j+1)d^i$. Dividendo per t^j otteniamo

$$N(a_{jd^i+1}, \dots, a_{(j+1)d^i}) \equiv 0 \pmod{t}.$$

Riducendo modulo t, ricaviamo $N(\bar{a}_{jd^i+1}, \dots, \bar{a}_{(j+1)d^i}) = 0$, dove $\bar{a}$ denota il termine costante di a. Poiché $\bar{a}_k \neq 0$, ciò contraddice l'ipotesi che N sia normico e conclude la dimostrazione. □

Se $N(x_1, \dots, x_{d^i})$ è un polinomio normico di ordine i e grado d, allora

$$N\big(N(x_1, \dots, x_{d^i}),\, N(x_{d^i+1}, \dots, x_{2d^i}),\, \dots,\, N(x_{d^{2i}-d^i+1}, \dots, x_{d^{2i}})\big) \tag{15}$$

è omogeneo di grado d^2 in d^{2i} indeterminate. Inoltre ha soltanto lo zero banale in F, dunque (15) è normico. Poiché $d > 1$, iterando il procedimento possiamo ricavare da un polinomio normico assegnato polinomi normici di grado arbitrariamente elevato. Useremo questa osservazione nella dimostrazione dell'analogo del lemma 1 per i campi C_i.

Lemma 3 (Artin). *Sia F un campo C_i per il quale esista un polinomio normico di ordine $i > 0$. Siano $f_1, \dots, f_r$ polinomi omogenei di grado d nelle indeterminate $x_1, \dots, x_n$, a coefficienti in F. Se $n > rd^i$, i polinomi f_j hanno uno zero comune non banale in F.*

Dimostrazione. Sia N un polinomio normico di ordine i per F e supponiamo che il suo grado sia e. Il numero delle indeterminate di N è e^i, che possiamo scrivere nella forma $e^i = rs + t$, con $s > 0$ e $0 \le t < r$. Sostituiamo alle prime r indeterminate di N rispettivamente $f_1(x_1, \dots, x_n), \dots, f_r(x_1, \dots, x_n)$, alle r successive $f_1(x_{n+1}, \dots, x_{2n}), \dots, f_r(x_{n+1}, \dots, x_{2n})$, e così via. Alle ultime t indeterminate sostituiamo degli zeri. Otteniamo il polinomio

$$\begin{aligned} M = N\big(&f_1(x_1, \dots, x_n), \dots, f_r(x_1, \dots, x_n),\\ &f_1(x_{n+1}, \dots, x_{2n}), \dots, f_r(x_{n+1}, \dots, x_{2n}), \dots, 0, \dots, 0\big), \end{aligned}$$

omogeneo in ns indeterminate, di grado ed. Desideriamo che $ns > (ed)^i = d^i(rs + t)$, ossia $(n - rd^i)s > d^i t$. Poiché $n > rd^i$ e $0 \le t < r$, basta scegliere e abbastanza grande, cosa possibile per l'osservazione che precede il lemma. Per questa scelta di e, la proprietà C_i assicura che M ammette uno zero non banale in F. Poiché N è normico, ne segue subito che gli f_j ammettono uno zero comune non banale in F. □

Per uniformità di enunciato, nel lemma seguente conveniamo di considerare 1 come un polinomio normico di ordine 0. Abbiamo allora il seguente risultato.

Lemma 4. *Sia F un campo C_i, $i \ge 0$, per il quale esista un polinomio normico di ordine i. Allora $F(t)$, con t indeterminata, è un campo C_{i+1}.*

Dimostrazione. Sia $f(x_1, \dots, x_n)$ un polinomio omogeneo di grado d a coefficienti in $F(t)$, con $n > d^{i+1}$. Dobbiamo provare che f ha uno zero non banale in $F(t)$. Possiamo supporre, senza perdita di generalità, che i coefficienti di f siano polinomi in t. Sia r il grado di f rispetto a t. Poniamo

$$x_j = x_{j0} + x_{j1}t + \cdots + x_{js}t^s, \qquad 1 \le j \le n,$$

dove gli x_{jk} sono indeterminate. Allora

$$f = f_0 + f_1 t + \cdots + f_{sd+r}t^{sd+r},$$

dove gli f_ℓ sono polinomi omogenei di grado d nelle $n(s+1)$ indeterminate x_{jk}, a coefficienti in F. Il polinomio f avrà uno zero non banale in $F(t)$ se gli f_ℓ hanno uno zero comune non banale in F. Per i lemmi 1 e 3 ciò accade se $n(s+1) > (sd + r + 1)d^i$. Poiché $n > d^{i+1}$, la disuguaglianza è soddisfatta prendendo s abbastanza grande. □

La dimostrazione del teorema di Tsen–Lang è ora chiara. Il lemma 4 per $i = 0$ mostra anzitutto che, se F è algebricamente chiuso, $F(x_1)$ è un campo C_1. Poi, applicando ripetutamente il lemma 2, vediamo che esiste un polinomio normico di ordine i per $F(x_1, \ldots, x_i)$. Applicazioni successive del lemma 4 mostrano infine che $F(x_1, \ldots, x_n)$ è un campo C_n. □

Applichiamo il risultato per $d = 2$. Se F è un campo algebricamente chiuso, ogni forma quadratica su uno spazio vettoriale V di dimensione $2^n + 1$ su $F(x_1, \ldots, x_n)$ rappresenta lo zero in modo non banale. Ne segue che ogni forma quadratica su uno spazio di dimensione 2^n su $F(x_1, \ldots, x_n)$ è universale. Ci serviremo di questo fatto per dimostrare il prossimo teorema.

Teorema 11.12. *Sia R un campo reale chiuso e sia Q una forma di Pfister su uno spazio vettoriale di dimensione 2^n sul campo $R(x_1, \ldots, x_n)$. Allora Q rappresenta ogni somma non nulla di due quadrati in $R(x_1, \ldots, x_n)$.*

Dimostrazione. Sia Q una forma di Pfister su uno spazio vettoriale V di dimensione 2^n su $R(x_1, \ldots, x_n)$. Dobbiamo provare che, se $b = b_1^2 + b_2^2 \neq 0$, con $b_i \in R(x_1, \ldots, x_n)$, allora b è rappresentato da Q. Poiché Q rappresenta 1, il risultato è chiaro quando $b_1 b_2 = 0$. Supponiamo quindi $b_1 b_2 \neq 0$. Sia $C = R(i)$, $i^2 = -1$, e consideriamo l'estensione $C(x_1, \ldots, x_n)$ di $R(x_1, \ldots, x_n)$ e lo spazio vettoriale

$$\widetilde{V} = V_{C(x_1,\ldots,x_n)} = C(x_1, \ldots, x_n) \otimes_{R(x_1,\ldots,x_n)} V.$$

Se (e_1, e_2) è una base di C/R, essa è anche una base di $C(x_1, \ldots, x_n)$ su $R(x_1, \ldots, x_n)$. Ogni elemento di $\widetilde{V}$ si scrive, in uno e un solo modo, come $e_1 u_1 + e_2 u_2$, con $u_i \in V$ (identificato, come al solito, con un sottospazio di $\widetilde{V}$). La forma quadratica Q ha un'unica estensione a una forma quadratica $\widetilde{Q}$ su $\widetilde{V}$. Evidentemente $\widetilde{Q}$ è una forma di Pfister. Poniamo ora $q = b_1 + b_2 i$. Allora $(1, q)$ è una base dell'estensione razionale e

$$q^2 - 2b_1 q + b = q^2 - 2b_1 q + (b_1^2 + b_2^2) = 0.$$

Esiste un vettore $w = u_1 + q u_2$, con $u_i \in V$, tale che $\widetilde{Q}(w) = q$. Dunque

$$Q(u_1) + 2qQ(u_1, u_2) + q^2 Q(u_2) = q.$$

Poiché $(1, q)$ è una base di $C(x_1, \ldots, x_n)/R(x_1, \ldots, x_n)$ e $q^2 - 2b_1 q + b = 0$, otteniamo $Q(u_1) = bQ(u_2)$. Ne segue che b è rappresentato da Q. □

Combinando il teorema di Artin (p. 640) con i teoremi 11.11 e 11.12, otteniamo il risultato principale.

Teorema 11.13. *Sia R un campo reale chiuso. Ogni funzione razionale semidefinita positiva in n variabili su R è somma di 2^n quadrati.*

Più in generale, gli stessi teoremi mostrano che ogni funzione razionale semidefinita positiva in n variabili su R può essere rappresentata da una forma di Pfister di dimensione 2^n. È degno di nota che, per dimostrare il teorema 11.13, sia stato necessario usare forme di Pfister diverse dalla somma di quadrati.

Esercizi

1. (J. W. S. Cassels.) Sia F un campo di caratteristica diversa da 2, e sia x un'indeterminata. Sia $p(x) \in F[x]$ somma di n quadrati in $F(x)$. Si dimostri che $p(x)$ è somma di n quadrati in $F[x]$.

(*Traccia della dimostrazione.* Il risultato è chiaro se $p = 0$. Inoltre, se $-1 = \sum_{j=2}^{n} a_j^2$, con $a_j \in F$, si ha

$$p = \left(\frac{p+1}{2}\right)^2 + \sum_{j=2}^{n} \left(\frac{a_j(p-1)}{2}\right)^2.$$

Possiamo dunque supporre che $p \neq 0$ e che $Q = \sum_{i=1}^{n} x_i^2$ sia anisotropa su F e quindi su $F(x)$. Esistono polinomi $f_0(x), f_1(x), \ldots, f_n(x)$ tali che $f_0(x) \neq 0$ e

$$p(x) f_0(x)^2 = f_1(x)^2 + \cdots + f_n(x)^2. \tag{16}$$

Fra tutte le scelte ammissibili prendiamo $f_0(x)$ di grado minimo e supponiamo che $\deg f_0(x) > 0$. Scriviamo

$$f_i(x) = f_0(x) g_i(x) + r_i(x), \tag{17}$$

con $\deg r_i(x) < \deg f_0(x)$ (poniamo $\deg 0 = -\infty$). Sia Q' la forma quadratica data da $\mathrm{diag}\{-p, 1, \ldots, 1\}$, con n unità. Allora (16) dà $Q'(f) = 0$, dove $f = (f_0, \ldots, f_n)$. Se $g = (g_0 = 1, g_1, \ldots, g_n)$ e $Q'(g) = 0$, il risultato è provato. Supponiamo dunque $Q'(g) \neq 0$. Ne segue che f e g sono linearmente indipendenti su $F(x)$. Allora $h = Q'(g,g) f - 2Q'(f,g) g \neq 0$ e $Q'(h) = 0$. Se $h_0 = 0$, la forma Q rappresenta lo zero in modo non banale su $F(x)$, quindi su F, contro l'ipotesi. Perciò $h_0 \neq 0$. Gli h_i sono polinomi in x e

$$h_0 = Q'(g,g) f_0 - 2Q'(f,g) = \frac{Q'(f_0 g - f)}{f_0} = \frac{1}{f_0} \sum_{i=1}^{n} r_i(x)^2.$$

Allora $\deg h_0 < \deg f_0$, una contraddizione.)

2. (Cassels.) Siano F, x come nell'esercizio 1 e sia $x^2 + d$, con $d \in F$, somma di $n > 1$ quadrati in $F(x)$. Si dimostri che o -1 è somma di $n-1$ quadrati in F, oppure d è somma di n quadrati in F.

3. (Cassels.) Si usino gli esercizi 1 e 2 per dimostrare che, se R è reale chiuso, $x_1^2 + \cdots + x_n^2$ non è somma di $n-1$ quadrati in $R(x_1, \ldots, x_n)$.

4. (T. Motzkin.) Sia R reale chiuso, siano x, y indeterminate e sia

$$p(x,y) = 1 + x^2(x^2 - 3)y^2 + x^2 y^4.$$

Si verifichino le identità[50]

$$\begin{aligned} p(x,y) &= \frac{(1 - x^2y^2)^2 + x^2(1-y^2)^2 + x^2(1-x^2)^2 y^2}{1 + x^2} \\ &= \frac{(1 + x^2 - 2x^2y^2)^2 + \big(x(1-x^2)y\big)^2}{(1+x^2)^2} \\ &\quad + \big(x(1-x^2)y^2\big)^2 + \big(x^2(1-x^2)y\big)^2 \end{aligned}.$$

Pertanto $p(x,y)$ è somma di quattro quadrati in $R(x)[y]$. Si dimostri che $p(x,y)$ non è somma di quadrati in $R[x,y]$.

5. Si dimostri che ogni estensione algebrica di un campo C_i è un campo C_i.

[50] Nella seconda frazione della stampa originale il primo quadrato contiene $1 - x^2 - 2x^2y^2$ e l'ultimo contiene $x^2(1-x^2)y^2$. Qui si correggono il segno di x^2 e l'esponente di y nell'ultimo termine.

11.7 La caratterizzazione di Artin–Schreier dei campi reali chiusi

Concludiamo lo studio dei campi reali chiusi dimostrando una bella caratterizzazione di questi campi dovuta ad Artin e Schreier. Abbiamo visto che un campo R è reale chiuso se e solo se $\sqrt{-1} \notin R$ e $C = R(\sqrt{-1})$ è algebricamente chiuso (teorema 11.3, p. 654).[51] Artin e Schreier dimostrano il seguente teorema, assai più forte.

Teorema 11.14. *Sia C un campo algebricamente chiuso e sia R un suo sottocampo proprio di codimensione finita ($[C : R] < \infty$). Allora R è reale chiuso e $C = R(\sqrt{-1})$.*

Dimostriamo dapprima alcuni lemmi elementari sui campi di caratteristica $p \neq 0$. I primi due sono già comparsi in *BAI*, ma per comodità ne riportiamo qui gli enunciati e le dimostrazioni.

Lemma 1. *Sia F un campo di caratteristica p e sia a un elemento di F che non è una potenza p-esima. Allora, per ogni $e \geq 1$, il polinomio $x^{p^e} - a$ è irriducibile in $F[x]$.*

Dimostrazione. Se E è un campo di spezzamento di $x^{p^e} - a$, in $E[x]$ abbiamo la fattorizzazione $x^{p^e} - a = (x-r)^{p^e}$. Perciò, se $g(x)$ è un fattore monico di grado positivo di $x^{p^e} - a$ in $F[x]$, allora $g(x) = (x-r)^k$, con $k = \deg g(x)$. Si ha dunque $r^k \in F$ e $r^{p^e} = a \in F$. Sia $p^f = (p^e, k)$ il massimo comune divisore. Esistono interi m, n tali che $p^f = mp^e + nk$. Allora $r^{p^f} = (r^{p^e})^m (r^k)^n \in F$. Se $k < p^e$, si ha $f < e$ e, posto $b = r^{p^f}$, si ottiene $b^{p^{e-f}} = a$, contro l'ipotesi che a non sia una potenza p-esima in F. □

Lemma 2. *Se F è un campo di caratteristica p e $a \in F$ non è della forma $u^p - u$, con $u \in F$, allora $x^p - x - a$ è irriducibile in $F[x]$.*

Dimostrazione. Se r è una radice di $x^p - x - a$ in un suo campo di spezzamento E, anche $r+1, r+2, \ldots, r+(p-1)$ sono radici di $x^p - x - a$. Si ha pertanto la fattorizzazione

$$x^p - x - a = \prod_{i=0}^{p-1} (x - r - i)$$

in $E[x]$. Se $g(x) = x^k - bx^{k-1} + \cdots$ è un fattore di grado positivo di $x^p - x - a$ in $F[x]$, allora $kr + l \cdot 1 = b$ per un intero l. Da $k < p$ seguirebbe perciò $r \in F$. Essendo $r^p - r = a$, ciò contraddice l'ipotesi. □

Lemma 3. *Siano F e a come nel lemma 2 e sia E un campo di spezzamento di $x^p - x - a$. Esiste un'estensione K/E tale che $[K : E] = p$.* (Si confronti il teorema 8.32, p. 510.)

Dimostrazione. Si ha $E = F(r)$, dove $r^p = r + a$. Affermiamo che l'elemento $ar^{p-1} \in E$ non è della forma $u^p - u$, con $u \in E$. Infatti ogni u si scrive $u_0 + u_1 r + \cdots + u_{p-1} r^{p-1}$ con $u_i \in F$, e dalla condizione $u^p - u = ar^{p-1}$ e dalla relazione $r^p = r + a$ si ottiene

$$\begin{aligned} u_0^p + u_1^p (r+a) + u_2^p (r+a)^2 + \cdots + u_{p-1}^p (r+a)^{p-1} \\ - u_0 - u_1 r - \cdots - u_{p-1} r^{p-1} = ar^{p-1}. \end{aligned}$$

Poiché $(1, r, \ldots, r^{p-1})$ è una base, ne segue la relazione $u_{p-1}^p - u_{p-1} = a$, contro l'ipotesi su a. Dal lemma 2 segue ora che $x^p - x - ar^{p-1}$ è irriducibile in $E[x]$. Pertanto, se K è il campo di spezzamento di questo polinomio su E, allora $[K : E] = p$. □

Possiamo ora dare la dimostrazione del teorema.

Dimostrazione del teorema 11.14. Poniamo $C' = R(\sqrt{-1}) \subset C$. Mostreremo che $C' = C$. Il risultato seguirà allora dal teorema 11.3. Ora C è la chiusura algebrica di C'. Pertanto ogni estensione algebrica di C' è isomorfa a un sottocampo di C/C' e il suo grado è limitato da $[C : C']$. La prima conclusione che possiamo trarne è che C' è perfetto. In caso contrario la

[51] Nell'originale il rinvio è a p. 634. Il teorema 11.3 si trova a p. 654.

caratteristica sarebbe un primo p e C' conterrebbe un elemento che non è una potenza p-esima in C'. Per il lemma 1, per ogni $e \geq 1$ esisterebbe un'estensione algebrica di C' di grado p^e. Avendo escluso questa possibilità, vediamo che C' è perfetto. Allora C è algebrico separabile su C' e, poiché è algebricamente chiuso, è un'estensione galoisiana di grado finito di C'. Sia $G = \mathrm{Gal}(C/C')$, cosicché $|G| = [C : C']$.

Supponiamo che $C \neq C'$. Allora $|G| \neq 1$. Sia p un divisore primo di $|G|$. Il gruppo G contiene un sottogruppo ciclico H di ordine p. Se E è il sottocampo degli elementi fissi per H, allora C è un'estensione ciclica di grado p di E. Se p fosse la caratteristica, avremmo $C = E(r)$, dove il polinomio minimo di r su E sarebbe della forma $x^p - x - a$ (*BAI*, p. 308). Per il lemma 3 esisterebbe un'estensione di grado p di C. Ciò contraddice il fatto che C è algebricamente chiuso. Dunque la caratteristica è diversa da p e, poiché C è algebricamente chiuso, esso contiene p radici p-esime distinte dell'unità. Queste sono le radici di $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$. Poiché i polinomi irriducibili di $E[x]$ hanno grado che divide $[C : E] = p$, i fattori irriducibili di $x^p - 1$ in $E[x]$ sono lineari. Quindi le p radici p-esime dell'unità appartengono a E. Allora $C = E(r)$, dove il polinomio minimo di r su E è $x^p - a$, con $a \in E$ (*BAI*, p. 308).

Consideriamo ora il polinomio $x^{p^2} - a$. Esso si fattorizza come $\prod_{i=1}^{p^2}(x - u^i s)$, dove u è una radice primitiva p^2-esima dell'unità e $s^{p^2} = a$. Se un qualche $u^i s$ appartenesse a E, avremmo $(u^i s)^p \in E$ e $((u^i s)^p)^p = a$, contro l'irriducibilità di $x^p - a$ in $E[x]$. Ne segue che i fattori irriducibili di $x^{p^2} - a$ in $E[x]$ hanno grado p. Se b è il termine costante di uno di essi, preso con il segno $(-1)^p$, allora $b = s^p v$, con v una potenza di u. Poiché $(s^p)^p = a$, si ha $s^p \notin E$ e, poiché $[C : E] = p$, otteniamo $C = E(s^p) = E(bs^{-p}) = E(v)$. Siccome E contiene tutte le radici p-esime dell'unità, v è una radice primitiva p^2-esima dell'unità.

Sia P il sottocampo primo di C e consideriamo il sottocampo $P(v)$ di C. Se $P = \mathbb{Q}$, sappiamo che il campo ciclotomico delle radici p^r-esime dell'unità ha grado $\varphi(p^r)$ su $\mathbb{Q}$ (*BAI*, p. 272). Questo numero tende all'infinito al crescere di r. Se P ha caratteristica finita ℓ, abbiamo visto che $\ell \neq p$. Il campo delle radici p^r-esime dell'unità su P contiene allora almeno p^r elementi, e di nuovo il suo grado su P tende all'infinito con r. In entrambi i casi esiste pertanto un r tale che $P(v)$ contiene una radice primitiva p^r-esima dell'unità ma nessuna radice primitiva p^{r+1}-esima. Poiché v è una radice primitiva p^2-esima, $r \geq 2$. Il campo C contiene un elemento w che è una radice primitiva p^{r+1}-esima dell'unità. Consideriamo il campo ciclotomico $P(w)$. Sia $K = \mathrm{Gal}(P(w)/P)$. Se P è finito, sappiamo che K è ciclico (*BAI*, p. 291). Lo stesso vale se $P = \mathbb{Q}$, salvo il caso $p = 2$, $r \geq 2$. Se K è ciclico, ha un unico sottogruppo di ordine p e quindi, per la corrispondenza di Galois, $P(w)$ contiene un unico sottocampo sul quale ha grado p. Mostreremo ora che $P(w)$ ha due sottocampi di questo tipo. Ciò implicherà che $p = 2$ e che la caratteristica è zero.

Sia $h(x)$ il polinomio minimo di w su E. Poiché $v \notin E$, si ha $w \notin E$ e $C = E(w)$. Perciò $\deg h(x) = p$. Inoltre $h(x)$ divide $x^{p^{r+1}} - 1 = \prod_{i=1}^{p^{r+1}}(x - w^i)$, quindi i suoi coefficienti appartengono al sottocampo $D = E \cap P(w)$. Ne segue $[P(w) : D] = p$. Consideriamo poi il sottocampo $D' = P(z)$, dove $z = w^p$. L'elemento w è una radice di $x^p - z \in D'[x]$, e questo polinomio è irriducibile oppure ha una radice in D' (*BAI*, esercizio 1 di p. 248). Nel primo caso $[P(w) : D'] = p$. Nel secondo, poiché z è una radice primitiva p^r-esima dell'unità, D' contiene p radici p-esime distinte dell'unità e quindi $x^p - z$ è un prodotto di fattori lineari in $D'[x]$. Allora $w \in D'$ e $D' = P(w)$. Ma $P(v)$ contiene una radice primitiva p^r-esima dell'unità e quindi contiene z. Se $D' = P(w)$, allora $P(v)$ conterrebbe la radice primitiva p^{r+1}-esima w, contro la scelta di r. Pertanto $[P(w) : D'] = p$.

Ora $D' \neq D$. Altrimenti D conterrebbe una radice primitiva p^r-esima dell'unità e E ne

conterrebbe una. Allora E conterrebbe v,[52] contro il fatto che $[C : E] = [E(v) : E] = p$. Dunque D e D' sono sottocampi distinti di $P(w)$, entrambi di codimensione p in $P(w)$. Come abbiamo visto, ciò implica che la caratteristica è zero e che $p = 2$. Ora $C = E(v)$ e v è una radice primitiva $2^2 = 4$-esima dell'unità. Pertanto $v = \pm\sqrt{-1}$. Poiché E contiene $\sqrt{-1}$, ciò contraddice $[C : E] = 2$. La dimostrazione è completa. □

Riferimenti bibliografici

E. Artin e O. Schreier, *Algebraische Konstruktion reeller Körper*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 5 (1927), pp. 85–99.

E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, ivi, pp. 100–115.

T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Mass., 1973.

[52] Nell'originale si legge w. Qui occorre v, di ordine p^2, poiché $r \geq 2$.

Indice analitico

I numeri rinviano alle pagine dell'edizione inglese. Le voci sono ordinate secondo i termini italiani. Nel PDF integrale ogni numero porta all'inizio del paragrafo corrispondente.

A

Abhyankar, S., 595
Aggiunto rispetto a una forma sesquilineare, 209
Aggiunzione, 49
Albert, A. A., 502
Algebra, 44, 137–148
  affine, 519
  centrale, 215
  esterna, 141
  filtrata, 147
  centrale semplice di dimensione finita, 215–226
  libera, 44
  graduata, 141, 147
  moduli e rappresentazioni, 211
  dei polinomi, 43
  separabile, 374
  simile, 227
  teoria della struttura, 210–215
  simmetrica, 141
  tensoriale, 139
Algebra di Clifford, 228
  nota storica, 245
  involuzione principale, 239
  struttura, 234
Algebra di Clifford pari, 236
Algebra di gruppo, 251–252
  centro, 260
Algebra di Lie degli endomorfismi, 531
Algebra di Lie ristretta (p-algebra di Lie), 531
Algebra di quaternioni, 232, 611–615
Algebra di Weyl, 192
Algebra esterna, 141, 235
Algebra graduata, 147, 384
Algebra inviluppante, 213
Algebra inviluppante universale di un'algebra di Lie, 142–143
Algebra libera, 44
Algebra quoziente, 61
Algebra separabile, 374
Algebra simmetrica, 141–142
Algebra spezzata, 220
Algebra tensoriale, 140
Algebre cicliche, 484–485
Algebre di Boole, 75–76
Altezza di un ideale primo, 456
Amitsur, S. A., 393
Anelli con divisione localmente compatti totalmente sconnessi, 599–608
  teorema di struttura, 607
Anelli simili nel senso di Morita, 179
Anello artiniano, 103, 202–210
  commutativo, 425–427
Anello degli endomorfismi, 96, 185
Anello degli interi algebrici, 284
Anello delle moltiplicazioni, 203
Anello di Rees, 438
Anello di valutazione, 577
  discreta, 591
Anello graduato associato a un ideale, 448
Anello libero, 86
Anello locale, 111
  regolare, 454
Anello noetheriano, 420–425
Anello primitivo, 187
  commutativo, 189
  destro, 195
Anello regolare (nel senso di von Neumann), 196
Anello semiprimitivo, 187, 203
Annullatore di un modulo, 186
Antiautomorfismi di $\mathrm{End}_\Delta V$, 210
Antiderivazione, 379
Antirappresentazione, 195
Applicazione semilineare, 205
Applicazione universale, 42
Artin, E., 184, 312, 483, 501, 651, 660–662, 651, 670, 671
Artin, E. e Schreier, O., 501, 509, 650, 674–677
Artin, E. e Whaples, G., 563
Artin, E., Nesbitt, C. J. e Thrall, R. M., 483
Artin, M., 526
Asano, K., 306
Assioma della scelta, 2
Assioma dello scambio, 123
Assiomatizzazione di Zermelo–Fraenkel della teoria degli insiemi, 1, 3
Aumentazione, 145, 651
Automorfismo di Frobenius, 506, 599
Ax, J., 631

B

Baer, R., 157, 543
Barsotti, J., 544
Base, 123
Base di trascendenza, 516
  separante, 527
Base di trascendenza separante, 527
Beauville, A., 523
Bergman, G., 195
Bezoutiante, 663
Bialgebra, 145
Bifuntore, 20

Bimoduli, 133–137
  invertibili, 182
Birkhoff, G., 52, 69, 92
Bordo, 332
Bourbaki, N., 197
Brauer, R., 245, 247, 305–312, 313–314, 495
Burnside, W., 215, 246, 247, 284, 524

C

Campi formalmente reali, 651–655
Campi locali, 595–599
  gruppo di Brauer, 608–611
  forme quadratiche, 591–598, 611–618
Campo algebricamente chiuso, 427, 464
Campo C_r, 669
Campo di spezzamento
  di un'algebra centrale semplice, 220–221
  di un gruppo, 264
  di un insieme di polinomi, 467
Campo di spezzamento separabile (di un'algebra centrale semplice), 495–498
Campo ordinato, 651
Campo quasi algebricamente chiuso, 670
Campo reale chiuso, 632–633, 653–654
  caratterizzazione, 674
Carattere, 269
  di un gruppo abeliano, 280–281
  di un prodotto diretto, 279–280
  generalizzato, 306
  irriducibile, 269
  lineare, 280
  realizzabile su un sottocampo, 315
  tavola, 277–278
  unità, 271
Cartan, E., 184, 245
Cartan, H. e Eilenberg, S., 326, 387
Cartier, P., 544
Cassels, J. W. S., 673, 674
Categoria abeliana, 330
Categoria (definizione), 9–10
  abeliana, 330
  additiva, 328
  discreta, 12
  duale, 13
  equivalente, 27
  isomorfa, 26
  dei moduli, 95–100, 177–183
  degli oggetti sopra o sotto un oggetto, 14
  prodotto di categorie, 13
  piccola, 12
Cayley, A., 184
Chevalley, C., 244
Chevalley, C. e Eilenberg, S., 326
Chiusura algebrica, 464
  esistenza, 466
  isomorfismo, 468
  separabile, 490
Chiusura algebrica separabile, 490
Chiusura normale, 490
Chiusura perfetta, 494
Chiusura reale di un campo ordinato, 655–657
Ciclo, 332
Claborn, L., 648
Classi, 6
Clemens, C. H., 523
Clifford, W. K., 244
Coalgebra, 144–145
  duale, 146
Cobordo, 333
Cociclo, 333
Codominio, 9
Cogeneratore, 177
Cohen, P. J., 1, 7
Colliot-Thélène, J. L., 523
Complesso, 331
  di catene (positivo), 333
  di cocatene (negativo), 333
  sopra un modulo, 339
  sotto un modulo, 341
Complesso di Amitsur, 334
Complesso di Koszul, 383
Completamenti, 455–461, 566–569
Completa riducibilità dei moduli sugli anelli artiniani semisemplici, 208
Componente omogenea, 121
Componente primaria isolata, 434
Componenti semplici di un anello artiniano semisemplice, 204
Composizione circolare, 194
Composti liberi di campi, 551
Composto di campi, 550
Condizione della catena ascendente, 101
Condizione della catena discendente, 101
Condizione del massimo, 101
Condizione del minimo, 101
Congruenza, 61
  delle identità, 91
Contenuto, 630
Contesto di Morita (dati di pre-equivalenza), 164–171
  anello associato, 171
Controvariante (funtore hom), 38
Conucleo, 96, 329
Coomologia dei gruppi, 355–363
Coomologia delle algebre, 370–375
Coprodotto, 34
Corisoluzione, 341
  iniettiva, 341
Corrispondenza, 53
  diagonale, 53
  inversa, 53
Corrispondenza di Jacobson–Bourbaki, 468–471

Corro, D. R., 323
Covariante (funtore hom), 38
Curtis, C. e Reiner, I., 325

D

Dati di pre-equivalenza (contesto di Morita), 164–171
Decomposizione di Peirce, 197
Decomposizione primaria (di moduli e ideali), 433–440
Decomposizione primaria irridondante, 436
Decomposizione primaria normale, 437
Decomposizione sottodiretta di Ω-algebre, 69
Dedekind, R., 282, 388, 557
Dedekind, R. e Weber, H., 557
DeMeyer e Ingraham, 462
Denso, 197
Derivazione, 147, 226, 530–540
  superiore, 147
  interna, 373, 496
  a valori in un modulo, 373
Derivazione superiore, 540
Determinante di gruppo, 282
Diagonalizzazione, 145
Diagramma di pullback, 36
Diagramma di pushout, 37
Diciassettesimo problema di Hilbert, 651
Dickson, L. E., 254, 472, 476
Dimensione di Krull, 450–455
Dimensione di un modulo completamente riducibile, 125
Dimensione globale, 377–378
Dimensione omologica, 375–378
Dipendente, 118, 123
Dipendenza algebrica, 514–515
Dipendenza intera, 408–412
Dirac, P. A. M., 245
Discriminante di una forma quadratica, 232, 613
Discriminante (ideale), 640
Disgiunzione lineare, 525
Divisore dello zero di un modulo, 433
Divisore (ideale), 622
Dominio, 9
  integralmente chiuso, 412
Dominio di Dedekind, 623
  caratterizzazioni, 625–631
  estensione intera, 631–634
Dominio integralmente chiuso, 412
Doppio centralizzante, 257–258

E

Eckmann, B., 326
Eckmann, B. e Schopf, A., 160
Eilenberg, S. e Mac Lane, S., 8, 326, 368
Eklof, P., 77
Elementi totalmente positivi, 657–660
Elemento puramente inseparabile, 491
Elemento quasi-regolare, 194
Epimorfismo, 15
  in **Grp** e in R-**mod**, 16
  in **Ring**, 17
Equivalenza delle categorie **mod**-R e **mod**-$M_n(R)$, 29–31, 170
Equivalenza di categorie, 27
Esponente
  di un'algebra centrale semplice, 497
  di un gruppo, 270
  di un'estensione puramente inseparabile, 495
Estensione
  del campo base, 220
  di campi completi, 569–573, 582–583
  di gruppi, 363–369
  di omomorfismi a posti, 580–585
  di moduli, 348–350
Estensione algebrica normale, 489
  struttura, 492–494
Estensione algebrica separabile, 491
Estensione di Galois, 474
Estensione di Kummer, 498–501
Estensione essenziale, 161
Estensione non ramificata, 598
Estensione puramente inseparabile, 491
Estensione puramente trascendente, 516
Estensione ramificata, 599
Estensione regolare, 549
Estensione separabile, 529
Estensione separabilmente generata, 527
Estensione totalmente ramificata, 598
Ext, 346–353

F

Feit, W., 246, 320, 326
Feit, W. e Thompson, J., 246
Filtro, 76
  principale, 78
  proprio, 76
Finitamente generato, 103
Forma antihermitiana, 209
Forma bilineare traccia, 641
Forma hermitiana, 209
Forma non degenere, 209
Forma quadratica, 228–229
  su campi locali, 611–618
  moltiplicativa, 665
  fortemente moltiplicativa, 666
Forma quadratica di Pfister, 667
Forma sesquilineare, 209
  aggiunto relativo a una forma, 210
Freccia, 10
Freudenthal, H., 600
Frobenius, G., 184, 225, 246
Funtore, 19

di abelianizzazione, 20
additivo, 97
controvariante, 19
diagonale, 21
di dualità, 21
fedele, 22
di dimenticanza, 20
pieno, 22
identità, 20
di inclusione, 20
potenza, 20
di proiezione, 21
rappresentabile, 37–40
Funtore aggiunto, 48
Funtore derivato, 342–346
Funtore esatto, 98
Funtore fedele, 22
Funtore prodotto tensoriale, 129–130
Funtori hom, 37–40
controvariante, 38
covariante, 38
Funzione di classe, 269
indotta, 306
Funzione razionale omogenea, 517

G

Generatore di una categoria di moduli, 173, 175
Gerstenhaber, M., 544
G-modulo, 355
regolare, 356
Goldschmidt, D. M. e Isaacs, I. M., 306, 325
Gradi di separabilità e inseparabilità, 495
Grado
di un'algebra centrale semplice, 222
di una parola, 78
Grado di trascendenza, 516
Grado residuo, 588, 638
Graves, J. J., 184
Griffiths, P. A., 523
Grothendieck, A., 9
Gruppi abeliani localmente compatti totalmente sconnessi, 602
Gruppi di Frobenius, 317–325
Gruppo abeliano ordinato, 575
sottogruppo isolato, 583
Gruppo con operatori, 56
Gruppo degli ideali frazionari, 624
Gruppo dei caratteri, 281
Gruppo dei valori, 575
Gruppo delle classi, 626
Gruppo delle classi proiettive, 419–420
Gruppo di Brauer, 226–228, 475–484, 495
di un campo locale, 608–611
Gruppo di Clifford, 238
rappresentazione vettoriale, 238
Gruppo di Clifford pari, 238
Gruppo di coomologia, 333
Gruppo diedrale, 261–262, 289
Gruppo di Galois di un'estensione semplice puramente trascendente, 522
Gruppo d'inerzia, 304
Gruppo di permutazioni k volte transitivo, 278
Gruppo elementare, 305
Gruppo fortemente indecomponibile, 117
Gruppoide, 12
Gruppo libero, 89
Gruppo lineare proiettivo, 256
Gruppo ortogonale ridotto, 240
Gruppo quasi-elementare, 307
Gruppo spinoriale, 240

H

Hajja, M., 524
Halmos, P. R., 1, 7
Hartshorne, R., 523
Hasse, H., 483, 610
Hausdorff, F., 583
Hensel, K., 557
Herstein, I. N., 245
Hilbert, D., 327, 476, 659
Hochschild, G., 326, 370, 374
Hopf, H., 326
Huppert, B., 369

I

Ideale, 65
frazionario, 620
intero, 620
invertibile, 621
massimale, 68
nil, 195
nilpotente, 191, 202
primo, 389, 434
principale, 620
Ideale nilpotente, 191
Ideale primario, 434
Ideale primitivo, 192
Ideale primo, 389
associato a un sottomodulo primario, 434
Ideale primo associato, 437
Ideale quasi-regolare, 194
Idealizzatore, 199
Idempotenti ortogonali, 110
Indice di ramificazione, 588, 637–638
Indice di Schur, 316
Indice di Witt, 241
Indipendente, 118, 123
Ingraham, *Vedi* DeMeyer e Ingraham
Insieme, 1
diretto, 59
Insieme diretto, 59
Insieme numerabile infinito, 3

Insieme parzialmente ordinato, 57
Insiemi ben ordinati, 3
Insiemi finiti, 3
Intero algebrico, 284
Invariante di Arf, 244
Invariante di Hasse, 613
Inviluppo iniettivo, 163
Iskovskikh, V. A., 523
Isomorfismi di anelli artiniani semplici, 206
Isomorfismo di aggiunzione, 49
Isomorfismo di $H^2(G, F^*)$ con $\mathrm{Br}(E/F)$, 481
Isomorfismo (in una categoria), 12
Isomorfismo isometrico, 568
Isomorfismo naturale, 23
Isomorfismo semilineare, 205

J

Jacobi, C. G. J., 323
Jacobson, N., 542, 600
Janusz, G. J., 649

K

Kan, D., 48
Kaplansky, I., 462
Kaplansky, I. e Kneser, M., 659–660
Keisler, L., 662
Koszul, J. L., 326, 379
Krull, W., 392, 488, 558, 634
Kürschák, S., 557, 584, 618

L

Λ-gruppo, 104
  indecomponibile, 117
  fortemente indecomponibile, 117
Λ-gruppo quoziente, 104
Λ-sottogruppo, 104
Lam, T. Y., 677
Landau, D., 659
Lang, S., 669
Lasker, E., 388
Legge di reciprocità quadratica, 323
Lemma dei cinque, 100
Lemma della base duale, 152–153
Lemma del serpente, 337
Lemma di Artin–Rees, 441–442
Lemma di Banaschewski, 307
Lemma di evitamento dei primi, 391
Lemma di Fitting, 113–114
Lemma di Gauss, 594
Lemma di Hensel, 593, 594, 595
Lemma di Krasner, 584
Lemma di Nakayama, 415
Lemma di Schanuel, 155
Lemma di Schur, 118
Lemma di Yoneda, 39
Lemma di Zassenhaus, 106
Lemma di Zorn, 2
Limite diretto, 70
  di Ω-algebre, 72
Limite induttivo, *Vedi* Limite diretto
Limite inverso, 72
  di Ω-algebre, 73
Limite proiettivo, *Vedi* Limite inverso
Localizzazione
  di moduli, 397–400
  di anelli, 393–397

M

Macaulay, F. S., 388
Mackey, G., 299, 300, 301
Mac Lane, S., 530
Magnus, W., 90
Malcev, A. I., 375
Manin, J., 523
Maschke, H., 313
Matrice jacobiana, 538
McCoy, N. H., 390, 393
McCrimmon, K., 196
McKenna, K., 662
M-gruppo, 311
Modulo, 12
  artiniano, 101
  completamente riducibile, 119, 208
  su un dominio di Dedekind, 643–649
  con differenziazione, 332
  divisibile, 158
  fedele, 174
  piatto, 153–155
  libero, 43
  graduato, 384
  indecomponibile, 111
  indotto, 288
  iniettivo, 156–164
  irriducibile, 117, 205, 208–209
  noetheriano, 101
  proiettivo, 148–155
  fortemente indecomponibile, 112
Modulo artiniano, 101
Modulo completamente riducibile, 117–122
Modulo fedele, 174
Modulo fortemente indecomponibile, 112, 114
Modulo graduato, 384
Modulo indotto, 288, 299
Modulo iniettivo, 156–164
Modulo libero, 43
Modulo noetheriano, 103
Modulo piatto, 153–155
  caratterizzazione mediante Tor, 354
Modulo proiettivo, 148–155
  caratterizzazione mediante Ext, 348
  rango, 414–419
Molien, T., 184
Molteplicità di una componente irriducibile di una

rappresentazione, 260
Monomorfismo, 15
in **Grp** e in R-**mod**, 16
in **Ring**, 17
Monomorfismo essenziale, 161
Morfismo, 9
epico, 15
monico, 15
nullo, 328
Morita, K., 9
Motzkin, T., 674
Mumford, D., 523

N

Nilradicale, 391
caratterizzazione (teorema di Krull), 392
Noether, E., 184, 327, 388, 422, 436, 472
Norma spinoriale, 240
Notazione di Łukasiewicz, 55
Nucleo, 62, 271, 329
Nucleo di Frobenius, 320
Nullstellensatz di Hilbert, 429, 564–565, 583, 584
Numeri cardinali, 5
addizione, 3
aritmetica, 3–4
moltiplicazione, 4
Numeri duali, 147, 531
Numero di intrecciamento, 296
Numero ordinale, 5
Numero p-adico, 74, 568

O

Oggetto iniziale, 36
Oggetto quoziente, 18
Oggetto terminale, 36
Oggetto universale, 42
Ojanguren, M. e Sridharan, M. R., 544
Ω-algebra, 53–58
Ω-algebra libera, 78–80
Ω-algebre sottodirettamente irriducibili, 69
Omologia
funtore, 333
gruppo, 362
modulo, 333
Omomorfismo contraente, 357
Omomorfismo di connessione, 336
Omomorfismo di Ω-algebre, 60
teorema fondamentale, 62
Omomorfismo d'ordine, 574
Omomorfismo graduato, 384
Omomorfismo incrociato, 360
principale, 361
Omotopia, 337–339
Ordine archimedeo, 654
Ordine lessicografico, 555
Ordine parziale, 54
Ostwald, W., 324
Otobe, Y., 600

P

p-algebra di Lie, 531
Parola ridotta, 87
p-estensione abeliana, 509–514
p-estensioni cicliche, 513
Pfister, A., 651, 663
Piattezza della localizzazione, 399
Pic, 183, 419–420, 648
Polinomio di Eisenstein, 596
Polinomio di Hilbert (di un modulo graduato), 443–448
Polinomio normico, 670
Pontrjagin, L., 600
Posto, 579
Primi non ramificati, 640
Primo ramificato, 640, 641
Primo teorema di isomorfismo (per Ω-algebre), 63
Procesi, C., 662, 663
Prodotto
in una categoria, 33
n-ario, 54
nullario, 55
in una Ω-algebra, 54–55
Prodotto bilanciato, 126
Prodotto diretto (interno), 116
Prodotto incrociato, 475
Prodotto libero, 85
di gruppi, 85
Prodotto ridotto, 87
Prodotto semidiretto, 367
Prodotto sottodiretto di Ω-algebre, 66–70
Prodotto tensoriale
di algebre, 143
di campi, 44 (nell'indice originale), 544
di moduli, 125–133
di forme quadratiche, 644 (nell'indice originale), 664
di rappresentazioni, 249
Progeneratore, 167, 175
Proiezioni determinate da una decomposizione diretta di moduli, 111
Proprietà di scambio, 116

Q

Quillen, D., 152

R

Rabin, M., 77
Radicale di Jacobson di un anello, 192–197
caratterizzazioni, 196
di un anello artiniano, 202
Radicale (di Jacobson) di un anello, 192–197, 392
di un anello artiniano, 202
nilradicale, 392

Rango, 414, 418
Rappresentazione di un anello
  completamente riducibile, 187
  fedele, 186
  irriducibile, 186
  regolare, 191
Rappresentazione di un gruppo, 247
  assolutamente irriducibile, 263
  completamente riducibile, 253
  coniugata, 255
  contragrediente, 251
  disgiunta, 302
  equivalenza, 251
  quoziente, 252
  indotta, 288
  irriducibile, 253
  costituenti irriducibili, 255
  matriciale, 248
  per permutazioni, 248
  prodotta, 299
  regolare, 248
  similitudine, 248
  sottorappresentazione, 252
  prodotto tensoriale, 249
  unità, 251
Rappresentazione fedele, 191
Rappresentazione indotta, 288
Rappresentazione prodotta, 299
Rappresentazione proiettiva, 256, 369
Rappresentazioni del gruppo diedrale, 261–262
Rappresentazioni disgiunte, 302
Rappresentazioni di S_n, 265–269
Reid, J. D., 495
Relazione, 54
Relazione di dipendenza, 122
Relazione di dipendenza astratta, 122–125
Relazione di equivalenza, 54
Relazioni di ortogonalità, 274, 276
Relazioni di Schur, 273
Relazioni locali-globali, 400–403
Restrizione degli scalari, 291
Reticolo, 56
  completo, 57
  delle congruenze, 66–70
Retrazione, 15
Rim, D. S., 593
Risoluzione (di un modulo), 339–341
  libera, 340
  di Koszul, 383
  proiettiva, 339
  standard di un'algebra, 371–372
  standard di $\mathbb{Z}$, 357
Risoluzione libera di $\mathbb{Z}$, 359
Risoluzione proiettiva di una successione, 343
Robinson, A., 77, 651
R-successione, 454

S

Sah, H., 630, 634
Saltman, D., 523
Sansuc, J. J., 523
Schmidt, F. K., 529, 572, 592
Schreier, O., 327, 368, 501
Schur, I., 246, 247, 327, 369
Secondo teorema di isomorfismo (per Ω-algebre), 65
Semiprimitività degli anelli di polinomi (teorema di Amitsur), 393
Separabilità, 525–530
Serie caratteristica, 109
Serie centrale discendente, 90
Serie di composizione, 108
Serie di Laurent (formali), 425, 597
Serie di Newton–Puiseux, 595
Serie di Poincaré, 445
Serie di potenze (formali), 422–424
Serie di Puiseux, 595
Serie normale, 105
Serie pienamente invariante, 109
Serie principale, 109
Serre, J. P., 152, 652
Sezione, 15
Sistema di Gödel–Bernays (GB), 6
Sistema di parametri, 454
Sistemi di fattori, 361, 476
  ed estensioni di gruppi, 364
  normalizzati, 481
Sollevamento degli idempotenti, 405, 457
Somma amalgamata, 90
Somma di Baer, 353
Somma diretta (interna), 110
  di complessi, 332
  di forme quadratiche, 665
  di rappresentazioni, 253
Sottocategoria, 11
Sottoggetto, 18
Sottogruppo caratteristico, 105
Sottogruppo pienamente invariante, 105
Sottomodulo indecomponibile, 438
Sottomodulo primario, 434
Spettro massimale, 403
Spettro primo, 403–408
Springer, T., 655
Sridharan, M. R., 544
Steinitz, E., 123, 466, 620
Stone, M. H., 403
Sturm, J. F., 650
Successione esatta, 96
  lunga, 334–337, 351 (per Ext)
  corta, 96, 334 (di complessi)
Suslin, A., 152
Swinnerton-Dyer, 523
Sylvester, J. J., 662, 663

T

Tabella di Young, 265
Tamagawa, T., 630
Tarski, A., 52
Tate, J., 283, 306
Teichmüller, O., 327
Teorema della base di Hilbert, 420–421
Teorema delle sizigie di Hilbert, 385
Teorema dell'ideale principale di Krull, 452
Teorema dell'intersezione di Krull, 442
Teorema di approssimazione, 562–564
Teorema di Blichfeldt–Brauer, 308–309
Teorema di Brauer–Suzuki, 324
Teorema di Burnside, 213, 284–286
Teorema di Castelnuovo–Zariski, 523
Teorema di Clifford (A. H.), 255, 299
Teorema di decomposizione di Lasker–Noether, 433
Teorema di discesa (*going down*), 413
Teorema di esistenza di un primo sovrastante (*lying over*), 411
Teorema di Hurwitz, 665
Teorema di Jordan–Hölder, 108
Teorema di Kolchin, 215
Teorema di Krull–Schmidt, 115
Teorema di Lüroth, 522
Teorema di Maschke, 253
Teorema di normalizzazione di Noether, 518
Teorema di Ostrowski, 571–573
Teorema di raffinamento di Schreier, 106
Teorema di reciprocità di Frobenius, 297
Teorema di salita (*going up*), 412
Teorema di Shoda, 304
Teorema di Skolem–Noether, 222
Teorema di Sturm, 655
Teorema di Taketa, 311–312
Teorema di Tarski, 650
Teorema di Tsen–Lang, 669, 672
Teorema di Wedderburn sugli anelli con divisione finiti, 225
Teorema fondamentale degli omomorfismi (di Ω-algebre), 62
Teorema principale di Wedderburn, 374
Teoremi di densità, 197–201
  per i moduli completamente riducibili, 197
  per gli anelli primitivi, 199
Teoremi di Hilbert–Serre, 445–447
Teoremi di isomorfismo (per Ω-algebre), 63, 65
Teoremi di Morita, 167–168, 178, 182
Teoremi di Wedderburn–Artin, 171–173, 203–204
  formulazione matriciale, 210
Teoria di Galois, 471–475, 486–489, 541–544
Teoria di Galois infinita, 486–489
  teorema fondamentale, 488
Teoria di Galois mediante derivazioni (per estensioni puramente inseparabili di esponente uno), 541, 542
Teoria di Lasker–Macaulay–Noether, 389
Teoria di Pfister delle forme quadratiche, 663–669
Thompson, J., 246, 285, 320
Thrall, R. M., 483
Topologia di Zariski, 403, 430–432
Topologia finita, 469
Topologia I-adica, 455–461
Tor, 353–355
Trasformazione naturale, 23–25
Trasformazione ortogonale, 237
Trasversale, 287

U

Ultrafiltro, 76
Ultraprodotti, 75–78
  di anelli con divisione, 77
  di Ω-algebre, 77
Unipotente, 215
Unirazionale, 523
Unità di un anello di polinomi (teorema di McCoy), 393
Universali, 40–45

V

Valenza, 78
Valore assoluto, 558–562
  archimedeo, 561
  di un'estensione di campi di dimensione finita, 585–588, 637
  su $F(x)$, 566
  non archimedeo, 561
  su $\mathbb{Q}$, 564–566
  banale, 559
Valore assoluto p-adico su $\mathbb{Q}$, 558
Valutazione, 578–579
  canonica, 578
  definizione, 578
  discreta, 590
  esponenziale, 576
  di rango uno, 583
van Dantzig, D., 600
van der Waerden, B. L., 87
Varietà algebrica affine, 427–433
Varietà di Ω-algebre, 81–86
  coprodotti, 84
  algebre libere, 82
  caratterizzazione interna, 92
Vettori di Witt, 501–509
  e p-estensioni abeliane, 509–514
von Neumann, J., 265

W

Weber, H., 557
Wedderburn, J. H. M., 184, 327, 485
Weil, A., 549
Weyl, H., 245

Whitehead, A. N., 52
Whitehead, J. H. C., 374
Whitney, H., 125
Witt, E., 502, 611
Wronskiano, 540

Y

Young, A., 265

Z

Zariski, O. e Samuel, P., 462, 618
Zassenhaus, H., 367
Zero (in una categoria), 36