

© 1997 Bollati Boringhieri editore s.r.l., Torino, corso Vittorio Emanuele 86  
I diritti di memorizzazione elettronica, di riproduzione e di adattamento totale  
o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche)  
sono riservati

L'editore potrà concedere a pagamento l'autorizzazione a riprodurre una porzione  
non superiore a un decimo del presente volume. Le richieste di riproduzione vanno  
inoltrate all'Associazione Italiana per i Diritti di Riproduzione delle Opere a Stampa  
(AIDROS), via delle Erbe 2, 20121 Milano, tel. 02/86463091, fax 02/89010863

Stampato in Italia dalla Stampatre di Torino  
ISBN 88-339-5586-9

Titolo originale *Algebra*

© 1991 New Jersey by Prentice-Hall, Inc. a Simon & Schuster Company Engle-  
wood Cliffs

Traduzione di Paolo Maroscia

## Indice

<i>Prefazione</i>	<i>IX</i>
<i>Nota per il docente</i>	<i>XI</i>
<i>Ringraziamenti</i>	<i>XV</i>
<b>1 Operazioni tra matrici</b>	<i>I</i>
1 Le operazioni fondamentali, 1	
2 Riduzione per righe, 10	
3 Determinanti, 21	
4 Matrici di permutazione, 29	
5 La regola di Cramer, 33	
Esercizi, 36	
<b>2 Gruppi</b>	<i>45</i>
1 Definizione di gruppo, 45	
2 Sottogruppi, 52	
3 Isomorfismi, 57	
4 Omomorfismi, 60	
5 Relazioni di equivalenza e partizioni, 62	
6 Classi laterali, 67	
7 Restrizione di un omomorfismo a un sottogruppo, 70	
8 Prodotti di gruppi, 72	
9 Aritmetica modulare, 75	
10 Gruppi quoziante, 78	
Esercizi, 82	
<b>3 Spazi vettoriali</b>	<i>94</i>
1 Spazi vettoriali reali, 94	
2 Campi astratti, 98	
3 Basi e dimensione, 104	
4 Calcoli con le basi, 113	
5 Spazi di dimensione infinita, 119	
6 Somme dirette, 122	
Esercizi, 124	

**4 Applicazioni lineari**

- 1 La formula della dimensione, 131
- 2 La matrice di un'applicazione lineare, 134
- 3 Operazioni lineari e autovettori, 138
- 4 Il polinomio caratteristico, 143
- 5 Matrici ortogonali e rotazioni, 148
- 6 Diagonalizzazione, 155
- 7 Sistemi di equazioni differenziali, 159
- 8 L'esponenziale di una matrice, 165
- Esercizi, 172

**5 Simmetria**

- 1 Simmetria delle figure piane, 185
- 2 Il gruppo dei movimenti del piano, 187
- 3 Gruppi finiti di movimenti, 193
- 4 Gruppi discreti di movimenti, 198
- 5 Simmetria astratta: azioni di un gruppo, 208
- 6 L'azione sulle classi laterali, 212
- 7 La formula delle classi, 214
- 8 Rappresentazioni mediante permutazioni, 216
- 9 Sottogruppi finiti del gruppo delle rotazioni, 218
- Esercizi, 223

**6 Ulteriori proprietà dei gruppi**

- 1 Le azioni di un gruppo su se stesso, 234
- 2 L'equazione delle classi del gruppo icosaedrale, 238
- 3 Azioni sui sottoinsiemi, 241
- 4 I teoremi di Sylow, 243
- 5 I gruppi di ordine 12, 248
- 6 Calcoli nel gruppo simmetrico, 250
- 7 Il gruppo libero, 258
- 8 Generatori e relazioni, 261
- 9 L'algoritmo di Todd-Coxeter, 265
- Esercizi, 272

**7 Forme bilineari**

- 1 Definizione di forma bilineare, 282
- 2 Forme simmetriche: ortogonalità, 288
- 3 La geometria associata a una forma positiva, 294
- 4 Forme hermitiane, 296
- 5 Il teorema spettrale, 300
- 6 Coniche e quadriche, 303
- 7 Il teorema spettrale per operatori normali, 307
- 8 Forme antisimmetriche, 309
- 9 Sommario dei risultati, in notazione matriciale, 310
- Esercizi, 312

**8 Gruppi lineari**

- 1 I gruppi lineari classici, 321
- 2 Il gruppo unitario speciale  $SU_2$ , 323
- 3 La rappresentazione ortogonale di  $SU_2$ , 328
- 4 Il gruppo lineare speciale  $SL_2(\mathbb{R})$ , 334
- 5 Sottogruppi a un parametro, 336
- 6 L'algebra di Lie, 340
- 7 Traslazione in un gruppo, 347
- 8 Gruppi semplici, 351
- Esercizi, 356

**9 Rappresentazioni di gruppi**

- 1 Definizione di rappresentazione di un gruppo, 365
- 2 Forme  $G$ -invarianti e rappresentazioni unitarie, 368
- 3 Gruppi compatti, 371
- 4 Sottospazi  $G$ -invarianti e rappresentazioni irriducibili, 373
- 5 Caratteri, 376
- 6 Le rappresentazioni mediante permutazioni e la rappresentazione regolare, 382
- 7 Le rappresentazioni del gruppo icosaedrale, 384
- 8 Rappresentazioni di dimensione uno, 386
- 9 Lemma di Schur, e dimostrazione delle relazioni di ortogonalità, 387
- 10 Rappresentazioni del gruppo  $SU_2$ , 392
- Esercizi, 398

**10 Anelli**

- 1 Definizione di anello, 410
- 2 Costruzione formale degli interi e dei polinomi, 413
- 3 Omomorfismi e ideali, 419
- 4 Anelli quoziante e relazioni in un anello, 426
- 5 Aggiunzione di elementi, 431
- 6 Domini di integrità e campi di frazioni, 437
- 7 Ideali massimali, 439
- 8 Geometria algebrica, 442
- Esercizi, 449

**11 Fattorizzazione**

- 1 Fattorizzazione di interi e polinomi, 461
- 2 Domini a fattorizzazione unica, domini a ideali principali, domini euclidei, 464
- 3 Il lemma di Gauss, 472
- 4 Fattorizzazione esplicita dei polinomi, 476
- 5 Primi nell'anello degli interi di Gauss, 480
- 6 Interi algebrici, 484
- 7 Fattorizzazione nei campi quadratici immaginari, 490
- 8 Fattorizzazione degli ideali, 495
- 9 La relazione tra gli ideali primi di  $R$  e i numeri primi, 502
- 10 Classi di ideali nei campi quadratici immaginari, 503
- 11 Classi quadratici reali, 512
- 12 Alcune equazioni diofantee, 516
- Esercizi, 520



**12 Moduli**

- 1 Definizione di modulo, 532
- 2 Matrici, moduli liberi, basi, 534
- 3 Il principio di permanenza delle identità, 538
- 4 Diagonalizzazione delle matrici intere, 540
- 5 Generatori e relazioni per i moduli, 547
- 6 Il teorema di struttura per i gruppi cebeliani, 556
- 7 Applicazione agli operatori lineari, 561
- 8 Moduli liberi su anelli di polinomi, 568
- Esercizi, 569

**13 Campi**

- 1 Esempi di campi, 580
- 2 Elementi algebrici e trascendenti, 581
- 3 Grado di un'estensione di campi, 585
- 4 Costruzioni con riga e compasso, 589
- 5 Aggiunzione simbolica di radici, 596
- 6 Campi finiti, 599
- 7 Campi di funzioni, 606
- 8 Estensioni trascendenti, 617
- 9 Campi algebricamente chiusi, 619
- Esercizi, 623

**14 Teoria di Galois**

- 1 Il teorema fondamentale della teoria di Galois, 630
- 2 Equazioni di terzo grado, 636
- 3 Funzioni simmetriche, 641
- 4 Elementi primitivi, 647
- 5 Dimostrazione del teorema fondamentale, 651
- 6 Equazioni di quarto grado, 655
- 7 Estensioni di Kummer, 662
- 8 Estensioni ciclotomiche, 664
- 9 Equazioni di quinto grado, 668
- Esercizi, 673

**Appendice Nozioni di base**

- 1 Teoria degli insiemi, 686
- 2 Tecniche di dimostrazione, 691
- 3 Topologia, 696
- 4 Il teorema delle funzioni implicite, 700
- Esercizi, 702

**Notazioni****Bibliografia**

Per quanto possano essere importanti i concetti generali e le proposizioni che ci ha regalato – in algebra forse più che in ogni altro campo – la passione laboriosa di oggi per l'assiomatizzazione e la generalizzazione, sono convinto, ciò nondimeno, che base e nucleo della matematica siano, in tutta la loro complessità, i problemi speciali, e che superarne le difficoltà richieda alla fin fine il maggior lavoro.

Hermann Weyl

*La stesura di questo libro è iniziata circa vent'anni fa, sotto forma di appunti integrativi per i miei corsi di algebra. Volevo trattare alcuni argomenti concreti, quali la simmetria, i gruppi lineari e i campi di numeri quadratici, più dettagliatamente rispetto a quanto sviluppato nel testo, e spostare l'accento, in teoria dei gruppi, dai gruppi di permutazioni ai gruppi di matrici. I reticolati, un altro argomento ricorrente, comparvero spontaneamente. La mia speranza era che il materiale concreto avrebbe interessato gli studenti e reso più comprensibili le astrazioni: in breve, che essi avrebbero fatto maggiori progressi apprendendo entrambe le cose nello stesso tempo. Ciò ha funzionato abbastanza bene. Mi ci è voluto un po' di tempo per decidere ciò che volevo mettere nel libro, ma ho distribuito un po' alla volta vari appunti e alla fine ho cominciato a insegnare servandomi solo di essi, senza altri testi. Ne è nato un libro che è alquanto diverso, credo, da quelli esistenti. Ho incontrato però molte difficoltà nell'adattare le varie parti, e pertanto non consiglierei ad altri di partire in questo modo.*

*La novità principale del libro consiste nell'importanza assegnata agli argomenti speciali. Essi tendevano ad espandersi ad ogni nuova stesura del testo, perché avevo osservato che, se la matematica concreta veniva posta a confronto con i concetti astratti, spesso gli studenti desideravano saperne di più. Di conseguenza, gli argomenti concreti sopra menzionati sono diventati le parti più importanti del libro, in cui non mancano peraltro cenni su argomenti inconsueti, quali l'algoritmo di Todd-Coxeter e la semplicità del gruppo  $PSL_2$ .*

*Nel scrivere il libro, ho cercato di rispettare i principi seguenti:*

1. Anteporre alle definizioni astratte alcuni esempi significativi.
2. Introdurre tecniche generali solo se strettamente necessario.
3. Trattare solo argomenti importanti per la cultura media di un matematico.

*Anche se questi principi possono sembrare scontati, ho trovato utile il fatto di esplicitarli, se non altro perché: "Fa' come ti è stato insegnato" non è tra essi. Questi principi, naturalmente, sono stati occasionalmente violati.*

# Capitolo 1

## Operazioni tra matrici

Si dà innanzitutto il nome di grandezza a tutto ciò che è capace di accrescimento o rimpicciolimento, o a cui si può aggiungere, o da cui si può togliere, ancora qualcosa.

Leonhard Euler

Le matrici svolgono un ruolo centrale in questo libro: esse costituiscono una parte importante della teoria e molti esempi concreti sono basati su di esse. Pertanto è indispensabile che lo studente acquisti un po' di scioltezza nel calcolo matriciale. Poiché le matrici pervadono molti settori della matematica, le tecniche di cui qui avremo bisogno saranno certamente utili in altri casi.

I concetti per i quali occorrerà fare un po' di pratica sono quelli di *moltiplicazione tra matrici* e di *determinante*.

### 1 Le operazioni fondamentali

Siano  $m, n$  interi positivi. Una matrice  $m \times n$  è una collezione di  $mn$  numeri disposti in una tabella rettangolare:

$$(1.1) \quad \begin{matrix} & n \text{ colonne} \\ m \text{ righe} & \left[ \begin{matrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{m1} & \dots & a_{mn} \end{matrix} \right] \end{matrix}$$

Per esempio,  $\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}$  è una matrice  $2 \times 3$ .

I numeri che compaiono in una matrice sono chiamati gli *elementi della matrice* e sono denotati con  $a_{ij}$ , dove  $i, j$  sono indici (interi) con  $1 \leq i \leq m$  e  $1 \leq j \leq n$ . Gli indici  $i, j$  vengono chiamati, rispettivamente, *indice di riga* e *indice di colonna*. Così  $a_{ij}$  è l'elemento che compare nella  $i$ -esima riga e nella  $j$ -esima colonna della

matrice:

$$j \\ \left[ \begin{array}{ccc} & \dots & \dots \dots \\ i & \dots & a_{ij} & \dots \dots \\ & \vdots & & \end{array} \right].$$

Nell'esempio sopra riportato,  $a_{11} = 2$ ,  $a_{13} = 0$  e  $a_{23} = 5$ .

Denoteremo di solito una matrice con  $A$  oppure con  $(a_{ij})$ .

Una matrice  $1 \times n$  prende il nome di *vettore riga* di dimensione  $n$ . Se  $m = 1$ , l'indice  $i$  viene omesso e un vettore riga si scrive nella forma:

$$(1.2) \quad A = [a_1 \ \dots \ a_n] \quad \text{oppure} \quad A = (a_1, \dots, a_n),$$

dove le virgole sono facoltative. Analogamente, una matrice  $m \times 1$  prende il nome di *vettore colonna* di dimensione  $m$ :

$$(1.3) \quad B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

Una matrice  $1 \times 1$  [ $a$ ] contiene un solo numero e pertanto non distingueremo una matrice siffatta dal suo elemento.

(1.4) L'*addizione* tra matrici è l'addizione tra vettori:

$$(a_{ij}) + (b_{ij}) = (s_{ij}),$$

dove  $s_{ij} = a_{ij} + b_{ij}$  per ogni  $i, j$ . Così

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 3 \\ 4 & -3 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 & 3 \\ 5 & 0 & 6 \end{bmatrix}.$$

La somma di due matrici  $A, B$  è definita soltanto se esse sono entrambe dello stesso tipo, ossia se sono matrici  $m \times n$  con gli stessi  $m, n$ , rispettivamente.

(1.5) La *moltiplicazione scalare* di una matrice per un numero si definisce come per i vettori. Il risultato della moltiplicazione di un numero  $c$  per una matrice  $(a_{ij})$  è un'altra matrice:

$$c(a_{ij}) = (b_{ij}),$$

dove  $b_{ij} = ca_{ij}$  per ogni  $i, j$ . Così

$$2 \begin{bmatrix} 0 & 1 \\ 2 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 4 & 6 \\ 4 & 2 \end{bmatrix}.$$

I numeri saranno chiamati anche *scalari*.

Più complicata è la nozione di *moltiplicazione tra matrici*. Il primo caso da imparare è quello del prodotto  $AB$  di un vettore riga  $A$  (1.2) per un vettore colonna  $B$  (1.3), il quale è definito se entrambi hanno la stessa dimensione, ossia  $m = n$ . In tal caso il prodotto  $AB$  è la matrice  $1 \times 1$ , ossia lo scalare:

$$(1.6) \quad a_1 b_1 + a_2 b_2 + \dots + a_m b_m.$$

(Questo prodotto è chiamato spesso il "prodotto scalare" dei due vettori.) Così

$$[3 \ 1 \ 2] \begin{bmatrix} 1 \\ -1 \\ 4 \end{bmatrix} = 3 \cdot 1 + 1 \cdot (-1) + 2 \cdot 4 = 10.$$

L'utilità di questa definizione diventa chiara, se consideriamo  $A$  e  $B$  come vettori che rappresentano quantità contrassegnate da indici. Per esempio, consideriamo una barra di cioccolato farcita contenente  $m$  ingredienti. Denotiamo con  $a_i$  il numero di grammi dell'ingrediente  $i$ -esimo per barra e con  $b_i$  il costo dell'ingrediente  $i$ -esimo al grammo. Allora il prodotto di matrici  $AB = c$  fornisce il costo di una tavoletta:

$$(\text{grammi/barra}) \cdot (\text{costo/grammo}) = (\text{costo/barra}).$$

D'altra parte, il fatto di considerare ciò come il prodotto di una riga per una colonna è una scelta arbitraria.

In generale, il prodotto di due matrici  $A$  e  $B$  è definito se il numero delle colonne di  $A$  è uguale al numero delle righe di  $B$ , ossia se  $A$  è una matrice  $\ell \times m$  e  $B$  è una matrice  $m \times n$ . In tal caso, il prodotto è una matrice  $\ell \times n$ . In simboli,  $(\ell \times m) \cdot (m \times n) = (\ell \times n)$ . Gli elementi della matrice prodotto si calcolano moltiplicando tutte le righe di  $A$  per tutte le colonne di  $B$ , usando la regola (1.6) sopra descritta. Così, se denotiamo il prodotto  $AB$  con  $P$ , si ha:

$$(1.7) \quad p_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \dots + a_{im} b_{mj}.$$

Esso è il prodotto della  $i$ -esima riga di  $A$  per la  $j$ -esima colonna di  $B$ .

$$i \begin{bmatrix} a_{i1} & \cdots & a_{im} \end{bmatrix} \cdot \begin{bmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{bmatrix} = \begin{bmatrix} \cdots & p_{ij} & \cdots \end{bmatrix}.$$

Per esempio,

$$(1.8) \quad \begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Questa definizione di moltiplicazione tra matrici fornisce di fatto uno strumento di calcolo molto appropriato.

Ritornando all'esempio precedente, supponiamo di avere  $\ell$  barre di cioccolato. Allora possiamo formare una matrice  $A$  la cui riga  $i$ -esima misura gli ingredienti della barra  $i$ -esima. Se vogliamo calcolare, anno per anno, i costi delle barre riferiti a  $n$  anni assegnati, possiamo formare una matrice  $B$  la cui colonna  $j$ -esima misura il costo degli ingredienti nell'anno  $j$ -esimo. La matrice prodotto  $AB = P$  fornisce i costi delle barre:  $p_{ij}$  = costo della barra  $i$ -esima nell'anno  $j$ -esimo.

La notazione matriciale fu introdotta nel secolo XIX per rappresentare in forma concisa un sistema di equazioni lineari. Il sistema di equazioni

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n &= b_2 \\ \vdots &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

può essere scritto, con la notazione matriciale, nella forma

$$(1.9) \quad AX = B,$$

dove  $A$  denota la matrice dei coefficienti  $(a_{ij})$ ,  $X$  e  $B$  sono vettori colonna e  $AX$  è la matrice prodotto

$$\begin{bmatrix} A \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

Così l'equazione matriciale

$$\begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

rappresenta il seguente sistema di due equazioni in tre incognite:

$$-x_2 + 2x_3 = 2$$

$$3x_1 + 4x_2 - 6x_3 = 1$$

La relazione (1.8) fornisce una soluzione:  $x_1 = 1$ ,  $x_2 = 4$ ,  $x_3 = 3$ .

La formula (1.7) che definisce la matrice prodotto può essere scritta anche in una delle due forme abbreviate:

$$p_{ij} = \sum_{k=1}^m a_{ik}b_{kj} = \sum_k a_{ik}b_{kj}.$$

Le notazioni principali di cui disponiamo per trattare insiemi di numeri sono la notazione di somma  $\sum$  sopra usata e la notazione matriciale. La notazione  $\sum$  è in effetti più versatile, ma, dato che la notazione matriciale è molto più compatta, useremo questa quando sarà possibile. Uno dei problemi che affronteremo nei capitoli successivi sarà quello di tradurre strutture matematiche complicate in notazione matriciale allo scopo di lavorare comodamente con esse.

Le operazioni tra matrici soddisfano a varie *identità*, quali la *proprietà distributiva*

$$(1.10) \quad A(B+B') = AB+AB', \quad (A+A')B = AB+A'B$$

e la *proprietà associativa*

$$(1.11) \quad (AB)C = A(BC).$$

Tali leggi valgono ogni volta che le matrici in questione hanno una forma opportuna, in modo tale che i prodotti siano definiti. Per esempio, per la proprietà associativa, le matrici  $A, B, C$  dovrebbero essere, rispettivamente, di tipo  $\ell \times m$ ,  $m \times n$ ,  $n \times p$ , con  $\ell, m, n, p$  interi. Poiché i due prodotti (1.11) sono uguali, le parentesi non sono necessarie, e pertanto li denoteremo con  $ABC$ . Il triplo prodotto  $ABC$  è allora una matrice  $\ell \times p$ . Per esempio, i due modi di calcolare il prodotto

$$ABC = \begin{bmatrix} 1 \\ 2 \end{bmatrix} [1 \ 0 \ 1] \begin{bmatrix} 2 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

sono

$$(AB)C = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 6 & 2 \end{bmatrix} \quad \text{e}$$

$$A(BC) = \begin{bmatrix} 1 \\ 2 \end{bmatrix} [2 \ 1] = \begin{bmatrix} 3 & 1 \\ 6 & 2 \end{bmatrix}.$$

La moltiplicazione per uno scalare è compatibile con la moltiplicazione tra matrici, nel senso che:

$$(1.12) \quad c(AB) = (cA)B = A(cB).$$

Le dimostrazioni di tali identità sono semplici e poco interessanti.

Invece la proprietà commutativa non vale per la moltiplicazione tra matrici, ossia in generale si ha:

$$(1.13) \quad AB \neq BA.$$

Infatti, se  $A$  è una matrice  $\ell \times m$  e  $B$  è una matrice  $m \times \ell$ , cosicché  $AB$  e  $BA$  sono entrambe definite, allora  $AB$  è una matrice  $\ell \times \ell$  mentre  $BA$  è una matrice  $m \times m$ . Tuttavia, anche nel caso in cui entrambe le matrici sono quadrate, diciamo di tipo  $m \times m$ , i due prodotti, in generale, sono diversi tra loro. Per esempio,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \text{mentre} \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Poiché la moltiplicazione tra matrici non è commutativa, occorre molta attenzione nello studio delle equazioni matriciali. Possiamo moltiplicare ambo i membri di un'equazione  $B = C$  a sinistra per una matrice  $A$  e concludere che  $AB = AC$ , perché i prodotti siano definiti. Allo stesso modo, se i prodotti sono definiti, possiamo concludere che  $BA = CA$ . Tuttavia non possiamo dedurre da  $B = C$  che  $AB = CA$ !

Una matrice avente tutti gli elementi uguali a zero è detta *matrice nulla* e denotata con  $0$ , qualunque sia la sua dimensione. Talvolta è preferibile usare la notazione  $0_{m \times n}$ .

Gli elementi  $a_{ii}$  di una matrice  $A$  sono chiamati gli *elementi diagonali* di  $A$  e una matrice  $A$  è detta *matrice diagonale* se i suoi (eventuali) elementi non nulli sono elementi diagonali, ossia, se  $a_{ij} = 0$  per ogni  $i \neq j$ .

La matrice diagonale  $n \times n$  i cui elementi diagonali sono tutti uguali a 1:

$$(1.14) \quad I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{bmatrix},$$

è chiamata la matrice *identica*  $n \times n$ . Essa si comporta come il numero 1 nella moltiplicazione: se  $A$  è una matrice  $m \times n$ , allora

$$I_m A = A \quad \text{e} \quad A I_n = A.$$

Vi sono alcune descrizioni abbreviate per la matrice  $I_n$ :

$$I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

Spesso per indicare che un'intera regione in una matrice è costituita da zeri, la si lascia vuota oppure si scrive in essa un solo 0.

Useremo il simbolo  $*$  per indicare un elemento generico di una matrice. Così

$$\begin{bmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{bmatrix}$$

indica una matrice quadrata i cui elementi al di sotto della diagonale sono nulli, mentre gli altri possono essere qualunque. Una matrice siffatta è detta matrice *triangolare superiore*.

Sia  $A$  una matrice quadrata  $n \times n$ . Se esiste una matrice  $B$  tale che

$$(1.15) \quad AB = I_n \quad \text{e} \quad BA = I_n,$$

allora  $B$  è un'inversa di  $A$  e si denota con  $A^{-1}$ :

$$(1.16) \quad A^{-1}A = I_n = AA^{-1}.$$

Se  $A$  possiede un'inversa, allora  $A$  è una matrice *invertibile*. Per esempio, la matrice  $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$  è invertibile. La sua inversa è  $A^{-1} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$ , come si vede calcolando i prodotti  $AA^{-1}$  e  $A^{-1}A$ . Altri due esempi sono:

$$\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \\ & \frac{1}{2} \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix}.$$

Vedremo in seguito che  $A$  è invertibile se esiste una matrice  $B$  tale che valga l'una o l'altra delle due relazioni  $AB = I_n$ ,  $BA = I_n$  e che allora  $B$  è l'inversa di  $A$  [cfr. oltre, (2.23)]. Tuttavia, poiché la moltiplicazione tra matrici non è commutativa, tale proprietà non è ovvia. Essa non vale per matrici che non siano quadrate.

Per esempio, sia  $A = [1 \ 2]$  e  $B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ . Allora  $AB = [1] = I_1$ , ma  $BA = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \neq I_2$ .

D'altra parte, un'inversa, se esiste, è unica. In altre parole, può esistere soltanto un'inversa. Siano infatti  $B, B'$  due matrici soddisfacenti alle relazioni (1.15) rispetto a una stessa matrice  $A$ . In realtà, occorre sapere soltanto che  $AB = I_n$  ( $B$  è un'inversa destra) e che  $B'A = I_n$  ( $B'$  è un'inversa sinistra). Per la legge associativa, si ha:  $B'(AB) = (B'A)B$ . Pertanto

$$(1.17) \quad B' = B'I = B'(AB) = (B'A)B = IB = B,$$

dunque  $B' = B$ . ■

(1.18) PROPOSIZIONE *Siano  $A, B$  matrici  $n \times n$ . Se esse sono entrambe invertibili, anche il loro prodotto  $AB$  è invertibile e si ha*

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Più in generale, se  $A_1, \dots, A_m$  sono matrici invertibili, anche la matrice prodotto  $A_1 \cdots A_m$  è invertibile e la sua inversa è  $A_m^{-1} \cdots A_1^{-1}$ .

(Così l'inversa di  $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix}$  è

$$\begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & -\frac{1}{2} \\ & \frac{1}{2} \end{bmatrix}.)$$

*Dimostrazione.* Supponiamo che  $A, B$  siano invertibili. Allora verifichiamo che  $B^{-1}A^{-1}$  è l'inversa di  $AB$ :

$$ABB^{-1}A^{-1} = AIA^{-1} = AA^{-1} = I,$$

e allo stesso modo

$$B^{-1}A^{-1}AB = \dots = I.$$

L'ultima parte dell'enunciato si dimostra per induzione su  $m$  [cfr. app. (2.3)]. Per  $m = 1$ , l'enunciato afferma che, se  $A_1$  è invertibile, allora  $A_1^{-1}$  è l'inversa di  $A_1$ , che è ovvio. Supponiamo poi che l'enunciato sia vero per  $m = k$  e verifichiamolo per  $m = k + 1$ . Siano allora  $A_1, \dots, A_{k+1}$  matrici  $n \times n$  invertibili e denotiamo con  $P$  il prodotto  $A_1 \cdots A_k$  delle prime  $k$  matrici. Per l'ipotesi induttiva,  $P$  è invertibile e la sua inversa è  $A_k^{-1} \cdots A_1^{-1}$ . D'altra parte,  $A_{k+1}$  è invertibile. Pertanto, per quanto dimostrato sopra per due matrici invertibili, la matrice prodotto

$$PA_{k+1} = A_1 \cdots A_k A_{k+1}$$

è invertibile e la sua inversa è

$$A_{k+1}^{-1}P^{-1} = A_{k+1}^{-1}A_k^{-1} \cdots A_1^{-1}.$$

Dunque l'enunciato è vero per  $m = k + 1$ , il che completa la dimostrazione per induzione. ■

Vedremo che la maggior parte delle matrici quadrate sono invertibili, anche se ciò non è chiaro dalla definizione di moltiplicazione tra matrici. Tuttavia calcolare esplicitamente l'inversa di una matrice non è un problema semplice, se la matrice è grande.

L'insieme di tutte le matrici  $n \times n$  invertibili è detto *gruppo lineare generale* di dimensione  $n$  e si denota con  $GL_n$ . I gruppi lineari generali saranno tra gli esempi più importanti quando studieremo la nozione fondamentale di gruppo nel prossimo capitolo.

Talvolta la moltiplicazione tra matrici può essere semplificata con qualche artificio. Uno è la *moltiplicazione per blocchi*. Siano  $M, M'$  matrici  $m \times n$  e  $n \times p$  e sia  $r$  un intero minore di  $n$ . Possiamo scomporre le due matrici in blocchi nel modo seguente:

$$M = [A \mid B] \quad \text{e} \quad M' = \begin{bmatrix} A' \\ B' \end{bmatrix},$$

dove  $A$  ha  $r$  colonne e  $A'$  ha  $r$  righe. Allora la matrice prodotto  $MM'$  può essere calcolata come segue:

$$(1.19) \quad MM' = AA' + BB'.$$

Tale scomposizione del prodotto segue direttamente dalla definizione di moltiplicazione e può facilitare i calcoli. Per esempio:

$$\left[ \begin{array}{cc|cc} 1 & 0 & 5 \\ 0 & 1 & 7 \end{array} \right] \left[ \begin{array}{cc} 2 & 3 \\ 4 & 8 \\ \hline 0 & 0 \end{array} \right] = \left[ \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right] \left[ \begin{array}{cc} 2 & 3 \\ 4 & 8 \end{array} \right] + \left[ \begin{array}{c} 5 \\ 7 \end{array} \right] \left[ \begin{array}{cc} 0 & 0 \end{array} \right] = \left[ \begin{array}{cc} 2 & 3 \\ 4 & 8 \end{array} \right].$$

Si noti che la formula (1.19) è formalmente identica alla regola (1.6) per moltiplicare un vettore riga per un vettore colonna.

Possiamo moltiplicare anche matrici divise in più blocchi. Per i nostri scopi, una scomposizione in quattro blocchi sarà la più utile. In tal caso la regola per la moltiplicazione per blocchi è proprio quella definita per la moltiplicazione tra matrici  $2 \times 2$ . Poniamo  $r + s = n$  e  $k + \ell = m$ . Supponiamo di scomporre una matrice  $M$   $m \times n$  e una matrice  $M'$   $n \times p$  in sottomatrici

$$M = \left[ \begin{array}{c|c} A & B \\ \hline C & D \end{array} \right], \quad M' = \left[ \begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array} \right],$$

dove il numero delle colonne di  $A$  è uguale al numero delle righe di  $A'$ . Allora la regola per la moltiplicazione per blocchi è:

$$(1.20) \quad \left[ \begin{array}{c|c} A & B \\ \hline C & D \end{array} \right] \left[ \begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array} \right] = \left[ \begin{array}{c|c} AA' + BC' & AB' + BD' \\ \hline CA' + DC' & CB' + DD' \end{array} \right].$$

Per esempio,

$$\left[ \begin{array}{c|c} 1 & 0 \\ \hline 0 & 1 \end{array} \right] \left[ \begin{array}{c|c} 2 & 3 \\ \hline 4 & 1 \\ \hline 0 & 1 \end{array} \right] = \left[ \begin{array}{c|c} 2 & 8 \\ \hline 4 & 8 \\ \hline 0 & 1 \end{array} \right].$$

In questo prodotto, il blocco in alto a sinistra è  $[1 \ 0][2 \ 3] + [5][0 \ 1] = [2 \ 8]$ , e così via.

Anche questa regola può essere verificata direttamente a partire dalla definizione di moltiplicazione tra matrici. In generale, la moltiplicazione per blocchi può essere usata ogni volta che due matrici sono scomposte in sottomatrici in modo tale che i prodotti che occorre considerare siano definiti.

Oltre a facilitare i calcoli, la moltiplicazione per blocchi è uno strumento utile per dimostrare proprietà relative alle matrici, per induzione.

## 2 Riduzione per righe

Sia  $A = (a_{ij})$  una matrice  $m \times n$  e consideriamo una matrice variabile  $n \times p$ , diciamo  $X = (x_{ij})$ . Allora l'equazione matriciale

$$(2.1) \quad Y = AX$$

definisce la matrice  $m \times p$   $Y = (y_{ij})$  come funzione di  $X$ . Tale operazione è detta *moltiplicazione a sinistra* per  $A$ :

$$(2.2) \quad y_{ij} = a_{i1}x_{1j} + \cdots + a_{in}x_{nj}.$$

Si noti che nella formula (2.2) l'elemento  $y_{ij}$  dipende soltanto da  $x_{1j}, \dots, x_{nj}$ , ossia dalla  $j$ -esima colonna di  $X$  e dalla  $i$ -esima riga della matrice  $A$ . Dunque  $A$  opera separatamente su ciascuna colonna di  $X$  e possiamo capire il modo in cui  $A$  agisce, considerando la sua azione su un vettore colonna  $X$ :

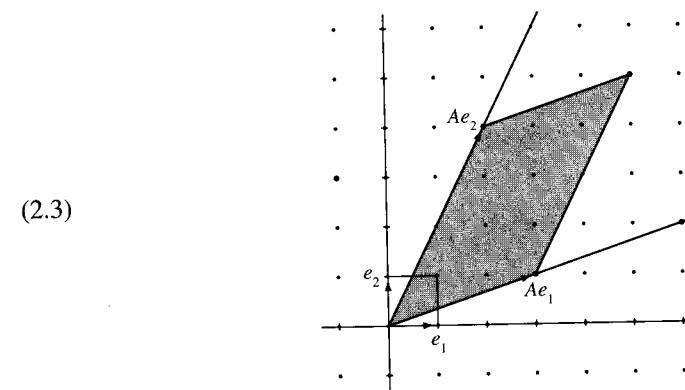
$$\boxed{A} \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}.$$

La moltiplicazione a sinistra per  $A$  sui vettori colonna può essere interpretata come una funzione dallo spazio dei vettori colonna  $X$  di dimensione  $n$  nello spazio dei vettori colonna  $Y$  di dimensione  $m$ , oppure come una collezione di  $m$  funzioni di  $n$  variabili:

$$y_i = a_{i1}x_1 + \cdots + a_{in}x_n \quad (i = 1, \dots, m).$$

Essa è detta *trasformazione lineare*, poiché le funzioni sono lineari e omogenee. (Una funzione *lineare* di un insieme di variabili  $u_1, \dots, u_k$  è una funzione della forma  $a_1u_1 + \cdots + a_ku_k + c$ , dove  $a_1, \dots, a_k, c$  sono scalari. Una funzione siffatta si dice *lineare omogenea* se il termine costante  $c$  è zero.)

Una rappresentazione grafica dell'azione della matrice  $2 \times 2 \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$  è riportata qui sotto. Essa manda il piano in se stesso:



(2.3)

Ritornando all'azione di  $A$  su una matrice  $X$  di tipo  $n \times p$ , possiamo interpretare il fatto che  $A$  agisce allo stesso modo su ciascuna colonna di  $X$  nel modo seguente. Denotiamo con  $Y_i$  la  $i$ -esima riga di  $Y$ , considerata come un vettore riga:

$$Y = \begin{bmatrix} \cdots & Y_1 & \cdots \\ \cdots & Y_2 & \cdots \\ \vdots & & \vdots \\ \cdots & Y_n & \cdots \end{bmatrix}.$$

Usando la notazione vettoriale, possiamo calcolare  $Y_i$  mediante le righe  $X_j$  di  $X$ :

$$(2.4) \quad Y_i = a_{i1}X_1 + \cdots + a_{in}X_n.$$

Si tratta precisamente di una riformulazione di (2.2) e di un altro esempio di moltiplicazione per blocchi. Per esempio, l'ultima riga del prodotto

$$\begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 4 & 2 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & -4 \end{bmatrix}$$

può essere calcolata come

$$3[1 \ 0] + 4[4 \ 2] - 6[3 \ 2] = [1 \ -4].$$

Se  $A$  è una matrice quadrata, si parla spesso della moltiplicazione a sinistra per  $A$  come di una *operazione sulle righe*.

Le matrici più semplici diverse dalla matrice nulla sono le *unità matriciali*, che denotiamo con  $e_{ij}$ :

$$(2.5) \quad e_{ij} = i \begin{bmatrix} & & j \\ & \ddots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{bmatrix}.$$

Tale matrice  $e_{ij}$  ha tutti gli elementi nulli tranne l'elemento di indici  $i, j$  che è uguale a 1. (Anche se di solito le matrici vengono denotate con lettere maiuscole, tuttavia per le unità matriciali si usano per tradizione le lettere minuscole.) Le unità matriciali sono utili poiché ogni matrice  $A = (a_{ij})$  può essere scritta come una somma del tipo:

$$A = a_{11}e_{11} + a_{12}e_{12} + \cdots + a_{nn}e_{nn} = \sum_{i,j} a_{ij}e_{ij}.$$

Gli indici  $i, j$  sotto il simbolo  $\sum$  indicano che la somma è estesa a tutti i valori di  $i$  e a tutti i valori di  $j$ . Per esempio:

$$\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 3 & \\ & 2 \end{bmatrix} + \begin{bmatrix} & 2 \\ 1 & \end{bmatrix} + \begin{bmatrix} & \\ 1 & \end{bmatrix} + \begin{bmatrix} & \\ & 4 \end{bmatrix} = 3e_{11} + 2e_{12} + 1e_{21} + 4e_{22}.$$

Una somma siffatta è chiamata *combinazione lineare* delle matrici  $e_{ij}$ .

Le unità matriciali sono utili per lo studio dell'addizione di matrici e della moltiplicazione per uno scalare. Tuttavia, nel caso della moltiplicazione tra matrici, sono più utili alcune matrici quadrate chiamate *matrici elementari*. Ve ne sono di tre tipi

$$(2.6i) \quad \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & a & \\ & & & 1 \end{bmatrix} \quad \text{oppure} \quad \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & a & \\ & & & 1 \end{bmatrix} = I + ae_{ij} \quad (i \neq j).$$

Una matrice siffatta ha tutti gli elementi diagonali uguali a 1 e un solo elemento diverso da zero al di fuori della diagonale.

$$(2.6ii) \quad \begin{bmatrix} 1 & & & \\ & 0 & & 1 \\ & & \ddots & \\ 1 & & & 0 \end{bmatrix} = I + e_{ij} + e_{ji} - e_{ii} - e_{jj}.$$

In questo caso, gli elementi diagonali  $a_{ii}$  e  $a_{jj}$  di  $I$  sono uguali a zero, mentre gli elementi  $a_{ij}$  e  $a_{ji}$  sono uguali a 1. (La formula precedente, espressa mediante le unità matriciali, è piuttosto brutta e pertanto sarà poco usata.)

$$(2.6iii) \quad \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & c & \\ & & & 1 \end{bmatrix} = I + (c-1)e_{ii}, \quad (c \neq 0).$$

In questo caso, un solo elemento diagonale della matrice identica è sostituito da un numero  $c$  diverso da zero.

Le matrici elementari  $2 \times 2$  sono

$$(i) \quad \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \quad (ii) \quad \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}; \quad (iii) \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} c & 1 \\ 1 & c \end{bmatrix};$$

dove, come sopra,  $a$  è arbitrario e  $c$  è un qualunque numero diverso da zero.

Le matrici elementari  $E$  agiscono su una matrice  $X$  nel modo seguente:

(2.7) Per ottenere la matrice  $EX$ , occorre:

**Tipo (i):** Sostituire la  $i$ -esima riga  $X_i$  con  $X_i + aX_j$ , oppure aggiungere  $a \cdot X_j$  alla riga  $X_i$ ;

**Tipo (ii):** Scambiare tra loro le righe  $X_i$  e  $X_j$ ;

**Tipo (iii):** Moltiplicare la riga  $X_i$  per uno scalare non nullo  $c$ .

Queste operazioni sono chiamate *operazioni elementari sulle righe*. Dunque la moltiplicazione per una matrice elementare è un'operazione elementare sulle righe. Tali regole di moltiplicazione vanno verificate con cura.

(2.8) **LEMMA** Le matrici elementari sono invertibili e le loro inverse sono anch'esse matrici elementari.

La dimostrazione è semplicemente un calcolo. L'inversa di una matrice elementare è la matrice corrispondente all'operazione inversa sulle righe. Se  $E = I + ae_{ij}$  è del tipo (i), allora  $E^{-1} = I - ae_{ij}$  (basta "sottrarre  $aX_j$  dalla riga  $X_i$ "). Se  $E$  è del tipo (ii), allora  $E^{-1} = E$ . Infine, se  $E$  è del tipo (iii), allora  $E^{-1}$  è dello stesso tipo, con  $c^{-1}$  nella stessa posizione occupata da  $c$  in  $E$  (basta "moltiplicare la riga  $X_i$  per  $c^{-1}$ "). ■

Studiamo ora l'effetto di operazioni elementari sulle righe (2.7) su una matrice  $A$ , al fine di ottenere una matrice più semplice  $A'$ :

$$A \xrightarrow{\text{successione di operazioni}} \cdots \xrightarrow{} A'.$$

Poiché ogni operazione elementare sulle righe è ottenuta mediante la moltiplicazione per una matrice elementare, possiamo esprimere il risultato di una successione di operazioni siffatte mediante il prodotto per una successione  $E_1, \dots, E_k$  di matrici elementari:

$$(2.9) \quad A' = E_k \cdots E_2 E_1 A.$$

Tale procedimento è chiamato *riduzione per righe* oppure *eliminazione di Gauss*. Per esempio, possiamo semplificare la matrice

$$(2.10) \quad M = \begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{bmatrix}$$

con operazioni elementari del primo tipo per eliminare quanti più elementi possibile:

$$\begin{array}{c} \left[ \begin{array}{ccccc} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{array} \right] \xrightarrow{} \left[ \begin{array}{ccccc} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 1 & 2 & 8 & 4 & 12 \end{array} \right] \xrightarrow{} \left[ \begin{array}{ccccc} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 0 & 2 & 6 & 3 & 7 \end{array} \right] \xrightarrow{} \\ \xrightarrow{} \left[ \begin{array}{ccccc} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 3 \end{array} \right] \xrightarrow{} \left[ \begin{array}{ccccc} 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 3 \end{array} \right]. \end{array}$$

La riduzione per righe è un metodo utile per risolvere i sistemi di equazioni lineari. Sia dato un sistema di  $m$  equazioni lineari in  $n$  incognite, diciamo  $AX = B$  come in (1.9), essendo  $A$  una matrice  $m \times n$ ,  $X$  un vettore colonna costituito da incognite e  $B$  un vettore colonna assegnato. Per risolvere tale sistema, consideriamo la matrice a blocchi  $m \times (n+1)$

$$(2.11) \quad M = [A|B] = \left[ \begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_n \end{array} \right],$$

ed effettuiamo operazioni sulle righe per semplificare  $M$ . Si noti che  $EM = [EA|EB]$ . Sia

$$M' = [A'|B']$$

il risultato di successive operazioni sulle righe. L'osservazione fondamentale è la seguente:

(2.12) PROPOSIZIONE *Le soluzioni del sistema  $A'X = B'$  coincidono con le soluzioni del sistema  $AX = B$ .*

*Dimostrazione.* Poiché  $M'$  è ottenuta mediante una successione di operazioni elementari sulle righe, si ha:

$$M' = E_r \cdots E_1 M.$$

Poniamo  $P = E_r \cdots E_1$ . Tale matrice è invertibile, in virtù del lemma (2.8) e della proposizione (1.18). Inoltre,

$$M' = [A' \mid B'] = [PA \mid PB].$$

Ora, se  $X$  è una soluzione del sistema di partenza  $AX = B$ , si ha:  $PAX = PB$ , ossia  $A'X = B'$ . Dunque  $X$  è anche una soluzione del nuovo sistema. Viceversa, se  $A'X = B'$ , allora  $AX = P^{-1}A'X = P^{-1}B' = B$ , sicché  $X$  è anche una soluzione del sistema  $AX = B$ . ■

Per esempio, consideriamo il sistema:

$$(2.13) \quad \begin{array}{rcl} x_1 + 2x_3 + x_4 & = & 5 \\ x_1 + x_2 + 5x_3 + 2x_4 & = & 7 \\ x_1 + 2x_2 + 8x_3 + 4x_4 & = & 12 \end{array} .$$

La sua matrice completa è la matrice  $M$  considerata sopra (2.10); quindi la riduzione per righe di tale matrice mostra che il sistema di equazioni assegnato è equivalente al sistema:

$$\begin{array}{rcl} x_1 + 2x_3 & = & 2 \\ x_2 + 3x_3 & = & -1 \\ x_4 & = & 3 \end{array} .$$

Possiamo ricavare immediatamente le soluzioni di questo sistema: basta scegliere un valore arbitrario per  $x_3$  e poi risolvere il sistema nelle variabili  $x_1, x_2$  e  $x_4$ . La soluzione generale del sistema (2.13) può essere scritta pertanto nella forma

$$x_3 = c_3, \quad x_1 = 2 - 2c_3, \quad x_2 = -1 - 3c_3, \quad x_4 = 3,$$

dove  $c_3$  è un numero arbitrario.

Ritorniamo ora alla riduzione per righe di una matrice arbitraria. Non è difficile vedere che, mediante una successione di operazioni sulle righe, ogni matrice  $A$  può essere ridotta ad una matrice della forma:

$$(2.14) \quad A = \boxed{\begin{array}{cccccc} 1 & *...* & 0 & *...* & 0 & *...* & 0 \\ 1 & *...* & 0 & *...* & 0 & & \\ 1 & *...* & 0 & *...* & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \end{array}},$$

dove  $*$  denota un numero qualsiasi e lo spazio vuoto è costituito da zeri. Essa è chiamata una *matrice a scala per righe*. Per esempio

$$\begin{bmatrix} 1 & 6 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

è una matrice a scala per righe. Tale risulta la forma finale della riduzione della matrice (2.10). La definizione di matrice a scala per righe, o più semplicemente di matrice a scala, è la seguente:

- (2.15) (a) Il primo elemento non nullo in ciascuna riga è 1. Tale elemento è chiamato pivot.  
 (b) Il primo elemento non nullo della  $(i+1)$ -esima riga si trova alla destra del primo elemento non nullo della  $i$ -esima riga.  
 (c) Gli elementi al di sopra di un pivot sono nulli.

Per effettuare una riduzione per righe, occorre svolgere le seguenti operazioni: Trovare la prima colonna che contiene un elemento non nullo (se ciò non è possibile, allora  $A = 0$  e  $0$  è una matrice a scala per righe); scambiare le righe usando un'operazione elementare del tipo (ii), portando un elemento non nullo nella prima riga; normalizzare tale elemento trasformandolo in 1, usando un'operazione del tipo (iii); eliminare gli altri elementi nella sua colonna mediante una successione di operazioni del tipo (i). Il risultato finale sarà una matrice avente

la forma a blocchi:

$$\left[ \begin{array}{ccc|ccccc} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & * & \dots & * \end{array} \right],$$

che possiamo scrivere come  $\left[ \begin{array}{c|cc} & 1 & B \\ \hline & D \end{array} \right] = A'$ .

A questo punto si può operare su  $D$  (che è più piccola di  $A$ ) così come si è fatto su  $A$ , e andare avanti così. Formalmente, stiamo applicando il principio di induzione completa [cfr. app. (2.6)] sul numero di righe della matrice. Per ipotesi induttiva possiamo supporre che ogni matrice avente meno righe di  $A$  sia riducibile alla forma a scala per righe; quindi, in particolare, la matrice  $D$  può essere ridotta ad una tale matrice, diciamo  $D''$ . Le operazioni sulle righe che portano  $D$  in  $D''$  non alterano gli altri blocchi che costituiscono  $A'$ . Quindi  $A'$  può essere ridotta alla matrice

$$\left[ \begin{array}{c|cc} & 1 & B \\ \hline & D'' \end{array} \right] = A''$$

che soddisfa le proprietà 2.15(a) e (b). Osserviamo ora che gli elementi di  $B$  al di sopra dei pivot di  $D''$  possono essere eliminati, e concludiamo la riduzione di  $A$  alla forma a scala per righe. ■

Si può dimostrare che la matrice a scala per righe ottenuta a partire da una matrice assegnata  $A$  mediante riduzione per righe è unica, ossia non dipende dalla particolare sequenza di operazioni. Tuttavia, questo fatto non è molto importante, sicché ne ometteremo la dimostrazione.

Se  $A'$  è ridotta alla forma a scala per righe, possiamo risolvere un sistema di equazioni  $A'X = B'$  immediatamente. Per esempio, supponiamo che

$$[A' | B'] = \left[ \begin{array}{cccc|c} 1 & 6 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right].$$

Il sistema  $A'X = B'$  non ammette soluzioni, poiché la terza equazione è  $0 = 1$ . D'altra parte,

$$[A' | B'] = \left[ \begin{array}{cccc|c} 1 & 6 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

ammette soluzioni. Scegliendo arbitrariamente  $x_2, x_4$ , possiamo risolvere la prima equazione nell'incognita  $x_1$  e la seconda nell'incognita  $x_3$ . Questo è il procedimento che abbiamo usato per risolvere il sistema (2.13).

La regola generale è data dalla:

(2.16) PROPOSIZIONE *Sia  $M' = [A' \mid B']$  una matrice a scala per righe. Allora il sistema di equazioni  $A'X = B'$  ammette soluzioni se e soltanto se l'ultima colonna  $B'$  non contiene pivot. In tal caso, può essere assegnato un valore arbitrario all'incognita  $x_i$ , se la colonna  $i$ -esima non contiene pivot.* ■

È chiaro che ogni sistema lineare omogeneo  $AX = 0$  ammette la soluzione banale  $X = 0$ . Tuttavia, considerando ancora la forma a scala per righe, possiamo concludere che, se vi sono più incognite che equazioni, allora il sistema omogeneo  $AX = 0$  ammette una soluzione non banale:

(2.17) COROLLARIO *Ogni sistema  $AX = 0$  di  $m$  equazioni lineari omogenee in  $n$  incognite, con  $m < n$ , ammette una soluzione  $X$  in cui almeno un elemento  $x_i$  è diverso da zero.*

Infatti, sia  $A'X = 0$  il sistema associato alla matrice a scala per righe  $A'$  e sia  $r$  il numero dei pivot di  $A'$ , sicché  $r \leq m$ . Allora, dalla proposizione (2.16) segue che possiamo assegnare valori arbitrari a  $n - r$  incognite  $x_i$ . ■

Utilizzeremo ora la riduzione per righe per caratterizzare le matrici quadrate invertibili.

(2.18) PROPOSIZIONE *Sia  $A$  una matrice quadrata. Le seguenti condizioni sono tra loro equivalenti:*

- $A$  può essere ridotta alla matrice identica mediante una successione di operazioni elementari sulle righe.*
- $A$  è un prodotto di matrici elementari.*
- $A$  è invertibile.*
- Il sistema di equazioni lineari omogenee  $AX = 0$  ammette soltanto la soluzione banale  $X = 0$ .*

*Dimostrazione.* Procederemo dimostrando le implicazioni  $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a)$ . Per far vedere che (a) implica (b), supponiamo che  $A$  sia riducibile alla matrice identica mediante operazioni sulle righe:  $E_k \cdots E_1 A = I$ . Moltiplicando

ambo i membri di questa equazione a sinistra per  $E_1^{-1} \cdots E_k^{-1}$ , si ottiene  $A = E_1^{-1} \cdots E_k^{-1}$ . Poiché l'inversa di una matrice elementare è una matrice elementare, ciò prova che  $A$  è un prodotto di matrici elementari. Inoltre, poiché un prodotto di matrici elementari è invertibile, (b) implica (c). Se  $A$  è invertibile, possiamo moltiplicare ambo i membri dell'equazione matriciale  $AX = 0$  per  $A^{-1}$  e ottenere così  $X = 0$ . Dunque il sistema di equazioni omogenee  $AX = 0$  ammette soltanto la soluzione banale. Ciò prova che (c) implica (d).

Per dimostrare l'ultima implicazione, ossia  $(d) \Rightarrow (a)$ , consideriamo una matrice quadrata a scala per righe  $M$ . Notiamo la seguente dicotomia:

(2.19) *Sia  $M$  una matrice quadrata a scala per righe. Allora, o  $M$  è la matrice identica, oppure la sua ultima riga è nulla.*

Ciò si vede facilmente (cfr. (2.15)).

Supponiamo che la proprietà (a) non valga per una data matrice  $A$ . Allora  $A$  può essere ridotta, mediante operazioni sulle righe, ad una matrice  $A'$  avente l'ultima riga nulla. In tal caso, il sistema lineare  $A'X = 0$  contiene al più  $n - 1$  equazioni non banali e pertanto, in virtù del corollario (2.17), ammette una soluzione non banale. Poiché il sistema  $AX = 0$  è equivalente al sistema  $A'X = 0$ , anch'esso ammette una soluzione non banale. Ne segue che, se (a) non vale, neppure (d) vale; dunque (d) implica (a). Ciò completa la dimostrazione della proposizione (2.18). ■

(2.20) COROLLARIO *Se una matrice quadrata  $A$  contiene una riga nulla,  $A$  non è invertibile.* ■

La riduzione per righe fornisce un metodo per calcolare l'inversa di una matrice invertibile  $A$ . In pratica, si riduce  $A$  all'identità mediante operazioni sulle righe:

$$E_k \cdots E_1 A = I,$$

come sopra; moltiplicando poi ambo i membri di tale equazione a destra per  $A^{-1}$ , si ha:

$$E_k \cdots E_1 I = A^{-1}.$$

Possiamo enunciare pertanto il risultato seguente:

(2.21) COROLLARIO *Sia  $A$  una matrice invertibile. Per calcolare la sua inversa  $A^{-1}$ , basta effettuare operazioni elementari sulle righe  $E_1, \dots, E_k$  su  $A$ , riducendola all'identità. La stessa successione di operazioni, applicata a  $I$ , fornisce  $A^{-1}$ .* ■

## (2.22) Esempio

Cerchiamo l'inversa della matrice

$$A = \begin{bmatrix} 5 & 4 \\ 6 & 5 \end{bmatrix}.$$

Per calcolarla, formiamo la matrice a blocchi  $2 \times 4$

$$[A|I] = \left[ \begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 6 & 5 & 0 & 1 \end{array} \right].$$

Effettuiamo operazioni sulle righe per ridurre  $A$  all'identità, considerando sempre il blocco a destra, così da ottenere alla fine  $A^{-1}$  a destra, in virtù del corollario (2.21).

$$\begin{aligned} [A|I] &= \left[ \begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 6 & 5 & 0 & 1 \end{array} \right] && \text{Sottrarre (riga 1) da (riga 2)} \\ \xrightarrow{\quad} & \left[ \begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 1 & 1 & -1 & 1 \end{array} \right] && \text{Sottrarre } 4 \cdot (\text{riga 2}) \text{ da (riga 1)} \\ \xrightarrow{\quad} & \left[ \begin{array}{cc|cc} 1 & 0 & 5 & -4 \\ 1 & 1 & -1 & 1 \end{array} \right] && \text{Sottrarre (riga 1) da (riga 2)} \\ \xrightarrow{\quad} & \left[ \begin{array}{cc|cc} 1 & 0 & 5 & -4 \\ 0 & 1 & -6 & 5 \end{array} \right] && = [I|A^{-1}]. \end{aligned}$$

Dunque

$$A^{-1} = \begin{bmatrix} 5 & -4 \\ -6 & 5 \end{bmatrix}.$$

(2.23) PROPOSIZIONE *Sia  $A$  una matrice quadrata, dotata di un'inversa sinistra  $B$  ( $BA = I$ ), oppure di un'inversa destra ( $AB = I$ ). Allora  $A$  è invertibile e  $B$  è la sua inversa.*

*Dimostrazione.* Supponiamo che  $AB = I$ . Effettuiamo la riduzione per righe su  $A$ . In base a (2.19), esistono matrici elementari  $E_1, \dots, E_k$  tali che  $A' = E_k \dots E_1 A$  è la matrice identica oppure ha l'ultima riga nulla. Allora  $A'B = E_k \dots E_1$ , la quale è una matrice invertibile. Quindi l'ultima riga di  $A'B$  non è nulla e, di conseguenza, tale risulta anche l'ultima riga di  $A'$ . Dunque  $A' = I$ . Per la (2.18),  $A$  è invertibile, e le equazioni  $I = E_k \dots E_1 A$  e  $AB = I$  mostrano che  $A^{-1} = E_k \dots E_1 = B$  (cfr. (1.17)). Vediamo ora il caso  $BA = I$ . Scambiando  $A$  e  $B$  nell'argomentazione

precedente si conclude che  $B$  è invertibile e  $A$  è la sua inversa. Dunque anche  $A$  è invertibile. ■

Per la maggior parte di questa trattazione, avremmo potuto considerare le colonne piuttosto che le righe. Abbiamo scelto di lavorare con le righe per applicare i risultati ai sistemi di equazioni lineari; altrimenti avremmo potuto anche usare le colonne. L'operazione che scambia tra loro righe e colonne è la *trasposizione* di matrici. La *trasposta* di una matrice  $m \times n$   $A$  è la matrice  $n \times m$   $A^t = (b_{ij})$ , dove

$$b_{ij} = a_{ji}.$$

Per esempio,

$$\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}^t = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \quad \text{e} \quad [1 \ 2 \ 3]^t = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

Le regole di calcolo per la matrice trasposta sono date in:

- (2.24) (a)  $(A + B)^t = A^t + B^t$ .  
 (b)  $(cA)^t = cA^t$ .  
 (c)  $(AB)^t = B^t A^t$  (!)  
 (d)  $(A^t)^t = A$ .

Usando le formule (2.24c, d), possiamo dedurre le proprietà della *moltiplicazione a destra*,  $XP$ , dalle corrispondenti proprietà per la moltiplicazione a sinistra.

Le matrici elementari (2.6) agiscono mediante moltiplicazione a destra come le seguenti *operazioni elementari sulle colonne*:

- (2.25) (a) Sommare  $a \cdot$  (colonna  $i$ ) alla (colonna  $j$ ).  
 (b) Scambiare tra loro la (colonna  $i$ ) e la (colonna  $j$ ).  
 (c) Moltiplicare la (colonna  $i$ ) per  $c \neq 0$ .

### 3 Determinanti

Ad ogni matrice quadrata  $A$  è associato un numero chiamato il suo *determinante*. In questo paragrafo definiremo il determinante e dimostreremo alcune sue proprietà. Il determinante di una matrice  $A$  sarà denotato con  $\det A$ .

Il determinante di una matrice  $1 \times 1$  è proprio il suo unico elemento:

$$(3.1) \quad \det[a] = a,$$

e il determinante di una matrice  $2 \times 2$  è dato dalla formula:

$$(3.2) \quad \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc.$$

Se consideriamo una matrice  $2 \times 2$   $A$  come un operatore sullo spazio  $\mathbb{R}^2$  dei vettori reali di dimensione 2, come si è visto nel paragrafo 2, allora il determinante di  $A$  può essere interpretato geometricamente. Il suo valore assoluto è l'area del parallelogramma costituito dall'immagine di un quadrato di lato 1 mediante l'operatore. Per esempio, l'area della regione tratteggiata della figura 2.3 è 10. Il determinante è positivo o negativo a seconda che l'orientazione del quadrato è preservata o meno dalla trasformazione. Inoltre,  $\det A = 0$  se e soltanto se il parallelogramma degenera in un segmento, e ciò accade se e soltanto se le due colonne di  $A$  sono proporzionali tra loro.

L'insieme di tutte le matrici  $n \times n$  forma uno spazio di dimensione  $n^2$ , che denotiamo con  $\mathbb{R}^{n \times n}$ . Considereremo il determinante di tali matrici come una funzione dallo spazio  $\mathbb{R}^{n \times n}$  allo spazio dei numeri reali:

$$\det : \mathbb{R}^{n \times n} \longrightarrow \mathbb{R}.$$

Ciò significa che  $\det$  è una funzione degli  $n^2$  elementi della matrice. Esiste una funzione siffatta per ciascun intero positivo  $n$ . Purtroppo vi sono molte formule per il determinante e tutte sono complicate quando  $n$  è grande. Il determinante è importante poiché ha proprietà molto buone ed eleganti, anche se non vi è alcuna formula semplice per esso. Non soltanto le formule sono complicate, ma talvolta non è facile dimostrare direttamente che due di esse definiscono la stessa funzione. Pertanto useremo la seguente strategia: scegliamo una formula sostanzialmente a caso e la prendiamo come definizione del determinante. Così facendo, consideriamo una funzione particolare. Dimostriamo che la funzione scelta possiede alcune proprietà molto speciali. Inoltre, dimostriamo che la funzione scelta è l'unica funzione avente tali proprietà. A questo punto, per verificare che qualche altra formula definisce lo stesso determinante, occorre verificare soltanto che la funzione definita da tale formula possiede queste stesse proprietà. In realtà, ciò risulta di solito relativamente facile.

Il determinante di una matrice  $n \times n$  può essere calcolato per mezzo di certi determinanti  $(n-1) \times (n-1)$ , mediante un procedimento chiamato *sviluppo per minori*. Tale sviluppo permette di dare una definizione ricorsiva della funzione determinante. Sia  $A$  una matrice  $n \times n$  e denotiamo con  $A_{ij}$  la matrice  $(n-1) \times (n-1)$  ottenuta cancellando la  $i$ -esima riga e la  $j$ -esima colonna di  $A$ :

$$(3.3) \quad \boxed{\begin{array}{|ccc|} \hline & & j \\ i & \diagup & \diagdown \\ & \end{array}} = A_{ij}.$$

Per esempio, se

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 2 & 1 & 2 \\ 0 & 5 & 1 \end{bmatrix}, \text{ allora } A_{21} = \begin{bmatrix} 0 & 3 \\ 5 & 1 \end{bmatrix}.$$

Lo sviluppo per minori rispetto alla prima colonna è dato dalla formula:

$$(3.4) \quad \det A = a_{11} \det A_{11} - a_{21} \det A_{21} + \cdots + (-1)^{n+1} a_{n1} \det A_{n1},$$

con i segni alternati. Prendiamo questa formula, insieme con la (3.1), come una *definizione del determinante* ricorsiva. Si noti che la formula è in accordo con la (3.2) per le matrici  $2 \times 2$ .

Il determinante della matrice  $A$  considerata sopra è:

$$\det A = 1 \cdot \det \begin{bmatrix} 1 & 2 \\ 5 & 1 \end{bmatrix} - 2 \cdot \det \begin{bmatrix} 0 & 3 \\ 5 & 1 \end{bmatrix} + 0 \cdot \det \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}.$$

I tre determinanti  $2 \times 2$  a secondo membro possono essere ancora calcolati mediante uno sviluppo per minori e usando la (3.1), oppure la (3.2), così da ottenere:

$$\det A = 1 \cdot (-9) - 2 \cdot (-15) + 0 \cdot (-3) = 21.$$

Vi sono altre formule per il determinante, comprendenti sviluppi per minori rispetto ad altre colonne e rispetto alle righe, che ricaveremo tra breve [cfr. (4.11, 5.1, 5.2)].

È importante, sia per il calcolo effettivo che per considerazioni teoriche, conoscere alcune delle tante proprietà dei determinanti. La maggior parte di esse può essere verificata mediante calcoli diretti e induzione su  $n$ , utilizzando lo sviluppo

per minori (3.4). Ne elencheremo alcune senza dare dimostrazioni formali. Per poter interpretare tali proprietà per funzioni diverse dal determinante, denoteremo per il momento il determinante con il simbolo  $d$ .

$$(3.5) \quad d(I) = 1.$$

(3.6) *La funzione  $d(A)$  è lineare rispetto alle righe della matrice.*

Intendiamo con ciò il fatto seguente: denotiamo con  $R_i$  il vettore riga dato dall' $i$ -esima riga della matrice  $A$ , sicché  $A$  può essere scritta simbolicamente nella forma

$$A = \begin{bmatrix} \cdots & R_1 & \cdots \\ \vdots & & \vdots \\ \cdots & R_n & \cdots \end{bmatrix};$$

per definizione, la *linearità* rispetto all' $i$ -esima riga significa che, se  $R$  e  $S$  sono vettori riga, allora

$$d \begin{bmatrix} \vdots \\ \cdots & R + S & \cdots \\ \vdots \end{bmatrix} = d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \vdots \end{bmatrix} + d \begin{bmatrix} \vdots \\ \cdots & S & \cdots \\ \vdots \end{bmatrix},$$

e

$$d \begin{bmatrix} \vdots \\ \cdots & cR & \cdots \\ \vdots \end{bmatrix} = c \cdot d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \vdots \end{bmatrix},$$

dove le altre righe delle matrici che compaiono in tali relazioni restano inalterate dappertutto. Per esempio,

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 3+5 & 4+6 & 2+3 \\ 2 & -1 & 0 \end{bmatrix} = \det \begin{bmatrix} 1 & 2 & 4 \\ 3 & 4 & 2 \\ 2 & -1 & 0 \end{bmatrix} + \det \begin{bmatrix} 1 & 2 & 4 \\ 5 & 6 & 3 \\ 2 & -1 & 0 \end{bmatrix},$$

e

$$\det \begin{bmatrix} 1 & 2 & 4 \\ 2 \cdot 5 & 2 \cdot 6 & 2 \cdot 3 \\ 2 & -1 & 0 \end{bmatrix} = 2 \cdot \det \begin{bmatrix} 1 & 2 & 4 \\ 5 & 6 & 3 \\ 2 & -1 & 0 \end{bmatrix}.$$

La linearità permette di operare su *una riga alla volta*, mentre le altre righe restano fisse.

Un'altra proprietà è la seguente:

(3.7) *Se due righe adiacenti di una matrice  $A$  sono uguali, allora  $d(A) = 0$ .*

Dimostriamo questo fatto per induzione su  $n$ . Supponiamo che le righe di indici  $j$  e  $j+1$  siano uguali. Allora le matrici  $A_{ij}$  definite da (3.3) hanno anch'esse due righe uguali, tranne che per  $i = j$  oppure  $i = j+1$ . Ora, se  $A_{ij}$  ha due righe uguali, il suo determinante è zero, per induzione. Pertanto soltanto due termini della somma (3.4) sono al più diversi da zero, e

$$d(A) = \pm a_{j1} d(A_{j1}) \mp a_{j+1,1} d(A_{j+1,1}).$$

Inoltre, poiché le righe  $R_j$  e  $R_{j+1}$  sono uguali, ne segue che  $A_{j1} = A_{j+1,1}$  e che  $a_{j1} = a_{j+1,1}$ . Poiché i segni sono alternati, i due termini nel secondo membro si cancellano a vicenda e il determinante è zero.

Le proprietà (3.5-3.7) caratterizzano in modo unico i determinanti [cfr. (3.14)] e noi ricaveremo ulteriori relazioni a partire da esse senza tornare alla definizione (3.4).

(3.8) *Se si aggiunge un multiplo di una riga a una riga adiacente, il determinante non cambia.*

Infatti, da (3.6) e (3.7) segue che:

$$\begin{aligned} d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & S + cR & \cdots \\ \vdots \end{bmatrix} &= d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & S & \cdots \\ \vdots \end{bmatrix} + c \cdot d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & R & \cdots \\ \vdots \end{bmatrix} = \\ &= d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & S & \cdots \\ \vdots \end{bmatrix}. \end{aligned}$$

La stessa argomentazione vale nel caso in cui  $S$  è al di sopra di  $R$ .

(3.9) *Se si scambiano tra loro due righe adiacenti, il determinante viene moltiplicato per  $-1$ .*

Basta applicare più volte (3.8):

$$\begin{aligned} d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & S & \cdots \\ \vdots \end{bmatrix} &= d \begin{bmatrix} \vdots \\ \cdots & R & \cdots \\ \cdots & -(S-R) & \cdots \\ \vdots \end{bmatrix} = d \begin{bmatrix} \vdots \\ \cdots & -R + (S-R) & \cdots \\ \cdots & -(S-R) & \cdots \\ \vdots \end{bmatrix} = \\ &= \end{aligned}$$

$$= d \begin{bmatrix} \vdots \\ S \\ -(S-R) \\ \vdots \end{bmatrix} = d \begin{bmatrix} \vdots \\ S \\ -(-R) \\ \vdots \end{bmatrix} = -d \begin{bmatrix} \vdots \\ S \\ R \\ \vdots \end{bmatrix}.$$

(3.7') Se due righe di una matrice  $A$  sono uguali, allora  $d(A) = 0$ .

Infatti, scambiando righe adiacenti più volte, si ottiene una matrice  $A'$  avente due righe adiacenti uguali. In base a (3.7), si ha:  $d(A') = 0$ , e da (3.9) segue che  $d(A) = \pm d(A')$ .

Utilizzando (3.7'), le dimostrazioni di (3.8) e (3.9) forniscono i seguenti risultati:

(3.8') Aggiungendo un multiplo di una riga a un'altra riga, il determinante non cambia.

(3.9') Scambiando tra loro due righe, il determinante viene moltiplicato per  $-1$ .

Inoltre, da (3.6) discende il risultato seguente:

(3.10) Se una riga di  $A$  è nulla, allora  $d(A) = 0$ .

Infatti, se una riga è nulla, allora la matrice  $A$  non cambia moltiplicando tale riga per 0. Ma allora, in base a (3.6),  $d(A)$  viene moltiplicato per 0. Dunque  $d(A) = 0 \cdot d(A) = 0$ .

Le regole (3.8'), (3.9') e (3.6) descrivono l'effetto sul determinante di un'operazione elementare sulle righe (2.7), sicché esse possono essere riscritte in termini di matrici elementari. Esse si enunciano dicendo che  $d(EA) = d(A)$ , se  $E$  è una matrice elementare del primo tipo, che  $d(EA) = -d(A)$ , se  $E$  è del secondo tipo, e [cfr. (3.6)] che  $d(EA) = c \cdot d(A)$ , se  $E$  è del terzo tipo. Applichiamo ora tali regole per calcolare  $d(E)$ , essendo  $E$  una matrice elementare. Poniamo  $A = I$ . Allora, poiché  $d(I) = 1$ , le regole determinano  $d(EI) = d(E)$ :

(3.11) Il determinante di una matrice elementare è:

- (i) Primo tipo (aggiungere un multiplo di una riga a un'altra):  $d(E) = 1$ , in virtù di (3.8').
- (ii) Secondo tipo (scambio di righe):  $d(E) = -1$ , in virtù di (3.9').
- (iii) Terzo tipo (moltiplicare una riga per una costante non nulla):  $d(E) = c$ , in virtù di (3.6).

Inoltre, se utilizziamo ancora le regole (3.8'), (3.9') e (3.6), applicandole a una matrice arbitraria  $A$  e usando i valori per  $d(E)$  che abbiamo appena determinato, otteniamo il seguente risultato:

(3.12) Sia  $E$  una matrice elementare e sia  $A$  una matrice arbitraria. Allora si ha:

$$d(EA) = d(E) \cdot d(A).$$

Ricordiamo che, in base a (2.19), ogni matrice quadrata  $A$  può essere ridotta, mediante operazioni elementari sulle righe, a una matrice  $A'$ , la quale o è l'identità  $I$  oppure ha l'ultima riga nulla:

$$A' = E_k \cdots E_1 A.$$

Sappiamo da (3.5) e (3.10) che si ha, rispettivamente:  $d(A') = 1$  oppure  $d(A') = 0$ . Utilizzando (3.12) e l'induzione, si ottiene:

$$(3.13) \quad d(A') = d(E_k) \cdots d(E_1) d(A).$$

D'altra parte, conosciamo  $d(E_i)$ , in virtù di (3.11), e pertanto possiamo utilizzare questa formula per calcolare  $d(A)$ .

(3.14) TEOREMA (Definizione assiomatica del determinante) La funzione determinante (3.4) è l'unica funzione che soddisfa alle proprietà (3.5-3.7).

*Dimostrazione.* Abbiamo usato soltanto tali proprietà per giungere alle equazioni (3.11) e (3.13), ed esse determinano  $d(A)$ . Poiché lo sviluppo per minori (3.4) soddisfa (3.5-3.7), esso coincide con (3.13). ■

Ritorniamo ora alla notazione usuale  $\det A$  per il determinante di una matrice.

(3.15) COROLLARIO Una matrice quadrata  $A$  è invertibile se e soltanto se  $\det A \neq 0$ .

Infatti, ciò segue dalle formule (3.11), (3.13) e (2.18). Da (3.11) segue che  $\det E_i \neq 0$  per ogni  $i$ . Pertanto, se  $A'$  è come in (3.13), allora  $\det A' \neq 0$  se e soltanto se  $\det A' \neq 0$ , e ciò accade se e soltanto se  $A' = I$ . In base a (2.18),  $A' = I$  se e soltanto se  $A$  è invertibile. ■

Siamo in grado ora di dimostrare una delle proprietà più importanti della funzione determinante: la sua compatibilità con la moltiplicazione tra matrici.

(3.16) TEOREMA Siano  $A, B$  due matrici  $n \times n$  arbitrarie. Allora si ha

$$\det(AB) = (\det A) \cdot (\det B).$$

*Dimostrazione.* Notiamo che, se  $A$  è una matrice elementare, questa formula coincide con (3.12).

*Caso 1:*  $A$  è invertibile. In base a (2.18b),  $A$  è un prodotto di matrici elementari:  $A = E_1 \cdots E_k$ . Utilizzando (3.12) e l'induzione, si ha:  $\det A = (\det E_1) \cdots (\det E_k)$  e

$$\det(AB) = \det(E_1 \cdots E_k B) = (\det E_1) \cdots (\det E_k) (\det B) = (\det A) (\det B).$$

*Caso 2:*  $A$  non è invertibile. Allora, in virtù di (3.15), si ha:  $\det A = 0$ ; pertanto, per dimostrare il teorema in questo caso, basta far vedere che  $\det(AB) = 0$ . In base a (2.18),  $A$  può essere ridotta a una matrice  $A' = E_k \cdots E_1 A$  avente l'ultima riga nulla. Allora anche l'ultima riga di  $A'B$  è nulla; pertanto si ha:

$$0 = \det(A'B) = \det(E_k \cdots E_1 AB) = (\det E_k) \cdots (\det E_1) (\det AB).$$

Poiché  $\det E_i \neq 0$ , ne segue che  $\det(AB) = 0$ . ■

(3.17) COROLLARIO Se  $A$  è invertibile, si ha:

$$\det(A^{-1}) = \frac{1}{\det A}.$$

*Dimostrazione.* Basta osservare che  $(\det A)(\det A^{-1}) = \det I = 1$ . ■

*Osservazione.* Si potrebbe pensare, in modo naturale, di cercare di definire il determinante di una matrice utilizzando le regole (3.11) e (3.16). Tali regole determinano certamente  $\det A$  per ogni matrice invertibile  $A$ , poiché possiamo scrivere una matrice siffatta come un prodotto di matrici elementari. Tuttavia c'è un problema: vi sono molti modi di scrivere una matrice assegnata come un prodotto di matrici elementari e non è affatto chiaro che due prodotti diversi avrebbero lo stesso determinante. In realtà, non è per niente facile sviluppare questa idea fino in fondo.

La dimostrazione della proposizione seguente è un buon esercizio.

(3.18) PROPOSIZIONE Denotiamo con  $A^t$  la trasposta di  $A$ . Allora si ha

$$\det A = \det A^t. ■$$

(3.19) COROLLARIO Le proprietà (3.6-3.10) continuano a valere, se la parola riga è sostituita ovunque dalla parola colonna. ■

#### 4 Matrici di permutazione

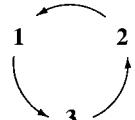
Un'applicazione biiettiva  $p$  di un insieme  $S$  in sé è una *permutazione* dell'insieme:

$$(4.1) \quad p : S \longrightarrow S.$$

Per esempio,

$$(4.2) \quad \begin{aligned} 1 &\mapsto 3 \\ 2 &\mapsto 1 \\ 3 &\mapsto 2 \end{aligned}$$

è una permutazione dell'insieme  $\{1, 2, 3\}$ . Essa è una permutazione *ciclica*, poiché opera nel modo seguente:



Vi sono parecchi modi di denotare le permutazioni. In questo paragrafo useremo la notazione funzionale, cosicché  $p(x)$  denota il valore della permutazione  $p$  sull'elemento  $x$ . Così, se  $p$  è la permutazione data in (4.2), allora

$$p(1) = 3, \quad p(2) = 1, \quad p(3) = 2.$$

Una *matrice di permutazione*  $P$  è una matrice con la seguente proprietà: l'operazione di moltiplicazione a sinistra per  $P$  è una permutazione delle righe di una matrice. Le matrici elementari del secondo tipo (2.6ii) costituiscono gli esempi più semplici. Esse corrispondono alle permutazioni chiamate *trasposizioni*, le quali scambiano tra loro due righe di una matrice, lasciando fisse le altre. Inoltre,

$$(4.3) \quad P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

è una matrice di permutazione. Essa agisce su un vettore colonna  $X = (x, y, z)^t$  nel modo seguente:

$$PX = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} y \\ z \\ x \end{bmatrix}.$$

L'elemento nella prima posizione viene mandato nella terza posizione, e così via, sicché  $P$  permuta le righe secondo la permutazione ciclica  $p$  data in (4.2).

C'è un solo punto che può creare confusione e che rende necessario precisare con cura le notazioni usate. Quando permutiamo gli *elementi* di un vettore  $(x_1, \dots, x_n)^t$  secondo una permutazione  $p$ , gli *indici* vengono permutati in senso opposto. Per esempio, moltiplicando il vettore colonna  $X = (x_1, x_2, x_3)^t$  per la matrice data in (4.3), si ottiene:

$$(4.4) \quad PX = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix}.$$

Gli indici in (4.4) sono permutati da

$$1 \mapsto 2 \mapsto 3 \mapsto 1,$$

che è l'inversa della permutazione  $p$ . Dunque vi sono due modi di associare una permutazione a una matrice di permutazione  $P$ : la permutazione  $p$  che descrive il modo in cui  $P$  permuta gli elementi e la permutazione inversa che descrive l'effetto sugli indici. Dobbiamo effettuare una scelta, sicché diremo che la permutazione associata a  $P$  è quella che descrive la sua azione sugli elementi di un vettore colonna. Allora gli indici vengono permutati in senso opposto, ossia:

$$(4.5) \quad PX = \begin{bmatrix} x_{p^{-1}(1)} \\ \vdots \\ x_{p^{-1}(n)} \end{bmatrix}.$$

La moltiplicazione per  $P$  ha l'effetto corrispondente sulle righe di una matrice  $n \times r A$ .

La matrice di permutazione  $P$  può essere espressa comodamente mediante le unità matriciali (2.5) oppure mediante certi vettori colonna chiamati *base canonica* e denotati con  $e_i$ . Il vettore  $e_i$  ha tutti gli elementi nulli tranne un 1 nella posizione  $i$ -esima, sicché tali vettori sono le unità matriciali per una matrice  $n \times 1$ .

(4.6) PROPOSIZIONE *Sia  $P$  la matrice di permutazione associata a una permutazione  $p$ .*

- (a) *La  $j$ -esima colonna di  $P$  è il vettore colonna  $e_{p(j)}$ .*
- (b)  *$P$  è una somma di  $n$  unità matriciali:*

$$P = e_{p(1)1} + \dots + e_{p(n)n} = \sum_j e_{p(j)j}. \blacksquare$$

Una matrice di permutazione  $P$  ha sempre un unico 1 in ciascuna riga e in ciascuna colonna, mentre gli altri suoi elementi sono tutti nulli. Viceversa, ogni matrice siffatta è una matrice di permutazione.

#### (4.7) PROPOSIZIONE

- (a) *Siano  $p, q$  due permutazioni, con matrici di permutazione associate  $P, Q$ . Allora la matrice associata alla permutazione  $pq$  è il prodotto  $PQ$ .*
- (b) *Una matrice di permutazione  $P$  è invertibile e la sua inversa coincide con la trasposta:  $P^{-1} = P^t$ .*

*Dimostrazione.* Denotiamo con  $pq$  la composizione delle due permutazioni:

$$(4.8) \quad pq(i) = p(q(i)).$$

Poiché  $P$  agisce permutando le righe secondo  $p$  e  $Q$  agisce permutando le righe secondo  $q$ , la proprietà associativa della moltiplicazione tra matrici assicura che  $PQ$  permuta le righe secondo  $pq$ :

$$(PQ)X = P(QX).$$

Dunque  $PQ$  è la matrice di permutazione associata a  $pq$ . Ciò dimostra (a). La dimostrazione di (b) è lasciata come esercizio. ■

Si vede facilmente, utilizzando la regola (3.9), che il determinante di una matrice di permutazione è uguale a  $\pm 1$ . Tale determinante prende il nome di *segno della permutazione*:

$$(4.9) \quad \text{sign } p = \det P = \pm 1.$$

La permutazione (4.2) ha segno  $+1$ , mentre qualsiasi trasposizione ha segno  $-1$  [cfr. (3.11ii)]. Una permutazione  $p$  si dice *pari* o *dispari* a seconda che il suo segno è  $+1$  oppure  $-1$ .

Riprendiamo ora lo studio di una matrice  $n \times n A$  arbitraria e utilizziamo la linearità del determinante (3.6) per sviluppare  $\det A$ . Cominciamo a lavorare sulla *prima riga*. Applicando (3.6), otteniamo:

$$\det A = \det \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ \hline \cdots & R_2 & \cdots & \cdots \\ \vdots & & \vdots & \\ \hline R_n & & R_n & \end{bmatrix} + \det \begin{bmatrix} 0 & a_{12} & 0 & \dots & 0 \\ \hline \cdots & R_2 & \cdots & \vdots & \\ \vdots & & \vdots & & \\ \hline R_n & & R_n & & \end{bmatrix} + \dots + \det \begin{bmatrix} 0 & \dots & 0 & a_{1n} \\ \hline \cdots & R_2 & \cdots & \vdots \\ \vdots & & \vdots & \\ \hline R_n & & R_n & \end{bmatrix}.$$

Continuiamo a sviluppare ciascuno di tali determinanti lungo la seconda riga, e così via. Alla fine del procedimento,  $\det A$  risulta espresso mediante una somma

di molti termini, ciascuno dei quali è il determinante di una matrice  $M$  avente uno e un solo elemento in ciascuna riga:

$$M = \begin{bmatrix} & a_{1?} \\ a_{2?} & \\ & \ddots \\ & & a_{n?} \end{bmatrix}.$$

Molti di tali determinanti sono nulli, poiché un'intera colonna può essere nulla. In particolare, il determinante di una matrice  $2 \times 2$  è la somma di quattro termini:

$$\begin{aligned} \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \det \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} + \det \begin{bmatrix} 0 & b \\ c & d \end{bmatrix} = \\ &= \det \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} + \det \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} + \det \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \det \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix}. \end{aligned}$$

Ma il primo e il quarto termine sono nulli; pertanto

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \det \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} + \det \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix}.$$

Infatti, le matrici  $M$  prive di colonne nulle hanno necessariamente un solo elemento  $a_{ij}$  in ciascuna riga e in ciascuna colonna. Esse somigliano alle matrici di permutazione  $P$ , con l'unica differenza che i valori uguali a 1 in  $P$  sono sostituiti dagli elementi di  $A$ :

$$(4.10) \quad P = \sum_j e_{p(j)j}, \quad M = \sum_j a_{p(j)j} e_{p(j)j}.$$

Dalla linearità del determinante [cfr. (3.6)], segue che:

$$\begin{aligned} \det M &= (a_{p(1)1} \cdots a_{p(n)n})(\det P) = \\ &= (\text{sign } p)(a_{p(1)1} \cdots a_{p(n)n}). \end{aligned}$$

Vi è un solo termine di questo tipo per ciascuna permutazione  $p$ . Ciò porta alla formula:

$$(4.11) \quad \det A = \sum_{\text{perm}_p} (\text{sign } p) a_{p(1)1} \cdots a_{p(n)n},$$

dove la somma è estesa a tutte le permutazioni dell'insieme  $\{1, \dots, n\}$ . Tale formula può essere riscritta, in modo un po' più elegante, nella forma trasposta:

$$(4.12) \quad \det A = \sum_{\text{perm}_p} (\text{sign } p) a_{1p(1)} \cdots a_{np(n)}.$$

## 5 | La regola di Cramer

Essa prende il nome di *sviluppo completo* del determinante.

Per esempio, lo sviluppo completo del determinante di una matrice  $3 \times 3$  ha 6 termini:

$$(4.13) \quad \det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \\ = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Lo sviluppo completo del determinante è più importante dal punto di vista teorico che da quello pratico, poiché per il calcolo effettivo intervengono troppi termini, se  $n$  non è piccolo. La sua importanza teorica proviene dal fatto che i determinanti sono espressi come *polinomi* nelle  $n^2$  variabili  $a_{ij}$  date dagli elementi della matrice, con coefficienti  $\pm 1$ . Ciò ha conseguenze importanti. Supponiamo, ad esempio, che ciascun elemento  $a_{ij}$  della matrice sia una funzione derivabile di una variabile:  $a_{ij} = a_{ij}(t)$ . Allora anche  $\det A$  risulta una funzione derivabile di  $t$ , poiché somme e prodotti di funzioni derivabili sono funzioni derivabili.

## 5 La regola di Cramer

La denominazione di *regola di Cramer* si riferisce a un gruppo di formule che forniscono soluzioni di sistemi di equazioni lineari espresse mediante determinanti. Per ottenere queste formule, occorre utilizzare lo sviluppo per minori rispetto alle colonne diverse dalla prima e rispetto alle righe.

(5.1) *Sviluppo per minori rispetto alla  $j$ -esima colonna:*

$$\det A = (-1)^{j+1} a_{1j} \det A_{1j} + (-1)^{j+2} a_{2j} \det A_{2j} + \cdots + (-1)^{j+n} a_{nj} \det A_{nj}.$$

(5.2) *Sviluppo per minori rispetto alla  $i$ -esima riga:*

$$\det A = (-1)^{i+1} a_{i1} \det A_{i1} + (-1)^{i+2} a_{i2} \det A_{i2} + \cdots + (-1)^{i+n} a_{in} \det A_{in}.$$

In tali formule  $A_{ij}$  è la matrice (3.3). I coefficienti  $(-1)^{i+j}$  forniscono segni alternati a seconda della posizione  $(i, j)$  nella matrice. (Si tratta di una notazione tradizionale, anche se forse non è davvero utile.) I segni possono essere evidenziati dalla figura seguente:

$$(5.3) \quad \begin{bmatrix} + & - & + & - & \cdots \\ - & + & & & \\ + & - & . & & \\ \vdots & & . & . & \end{bmatrix}.$$

Per dimostrare (5.1), si può procedere in uno dei due modi seguenti:

- Verificare direttamente le proprietà (3.5-3.7) per (5.1) e applicare il teorema (3.14), oppure
- Scambiare la  $j$ -esima colonna con la prima colonna e applicare (3.9') e (3.19).

Omettiamo tali verifiche. Una volta dimostrato (5.1), da esso si può dedurre (5.2) trasponendo la matrice e applicando (3.18).

(5.4) DEFINIZIONE Sia  $A$  una matrice  $n \times n$ , e sia  $\alpha_{ij} = (-1)^{i+j} \det A_{ij}$ , dove  $A_{ij}$  è la matrice ottenuta da  $A$  cancellando la  $i$ -esima riga e la  $j$ -esima colonna, come in (3.3). Allora l'aggiunta di  $A$  è la matrice  $\text{adj } A$  il cui elemento di posto  $(i, j)$  è  $(\text{adj})_{ij} = \alpha_{ij}$ , cioè

$$(\text{adj } A) = (\alpha_{ij})^t.$$

Così, ad esempio,

$$(5.5) \quad \text{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

e

$$(5.6) \quad \text{adj} \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 1 & -2 \\ -2 & 0 & 1 \\ -3 & -1 & 2 \end{bmatrix}^t = \begin{bmatrix} 4 & -2 & -3 \\ 1 & 0 & -1 \\ -2 & 1 & 2 \end{bmatrix}.$$

Siamo ora in grado di dimostrare la formula chiamata *regola di Cramer*.

(5.7) TEOREMA Poniamo  $\delta = \det A$ . Allora:

$$(\text{adj } A) \cdot A = \delta I \quad e \quad A \cdot (\text{adj } A) = \delta I.$$

(Si noti che, in tali relazioni,

$$\delta I = \begin{bmatrix} \delta & & \\ & \ddots & \\ & & \delta \end{bmatrix}.)$$

(5.8) COROLLARIO Supponiamo che il determinante  $\delta$  di  $A$  sia diverso da zero. Allora:

$$A^{-1} = \frac{1}{\delta} (\text{adj } A).$$

Per esempio, l'inversa della matrice  $2 \times 2 \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  è:

$$\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Il determinante della matrice  $3 \times 3$  la cui aggiunta è calcolata in (5.6) risulta uguale a 1; quindi, per tale matrice si ha:  $A^{-1} = \text{adj } A$ .

La dimostrazione del teorema (5.7) è facile. L'elemento di posto  $(i, j)$  della matrice  $(\text{adj } A) \cdot A$  è

$$(5.9) \quad (\text{adj})_{i1}a_{1j} + \cdots + (\text{adj})_{in}a_{nj} = \alpha_{1i}a_{1j} + \cdots + \alpha_{ni}a_{nj}.$$

Se  $i = j$ , si riottiene la formula (5.1) per  $\delta$ , come richiesto. Supponiamo  $i \neq j$ . Consideriamo la matrice  $B$  ottenuta a partire dalla matrice  $A$ , sostituendo l' $i$ -esima colonna con la  $j$ -esima colonna. In tal modo, la  $j$ -esima colonna compare due volte nella matrice  $B$ . Allora (5.9) è lo sviluppo per minori relativo a  $B$  rispetto alla sua  $i$ -esima colonna. Ma  $\det B = 0$ , in base a (3.7') e (3.19). Ne segue che (5.9) è zero, come richiesto. In modo simile si dimostra la seconda relazione del teorema (5.7). ■

La formula (5.8) può essere usata per scrivere la soluzione di un sistema di equazioni lineari  $AX = B$ , dove  $A$  è una matrice  $n \times n$  tale che  $\det A \neq 0$ . Moltiplicando ambo i membri per  $A^{-1}$ , si ottiene:

$$(5.10) \quad X = A^{-1}B = \frac{1}{\delta} (\text{adj } A)B,$$

dove  $\delta = \det A$ . Il prodotto a destra può essere sviluppato in modo da ottenere la formula:

$$(5.11) \quad x_j = \frac{1}{\delta} (b_1 \alpha_{1j} + \cdots + b_n \alpha_{nj}),$$

dove  $\alpha_{ij} = \pm \det A_{ij}$  come sopra.

Si noti che il termine principale ( $b_1\alpha_{1j} + \dots + b_n\alpha_{nj}$ ) a destra nella (5.11) somiglia allo sviluppo del determinante per minori rispetto alla  $j$ -esima colonna, tranne il fatto che  $b_i$  ha sostituito  $a_{ij}$ . Possiamo utilizzare questa osservazione per ottenere un'altra espressione per la soluzione del sistema di equazioni. Formiamo una nuova matrice  $M_j$  a partire da  $A$ , sostituendo la  $j$ -esima colonna di  $A$  con il vettore colonna  $B$ . Lo sviluppo per minori rispetto alla  $j$ -esima colonna mostra che

$$\det M_j = (b_1\alpha_{1j} + \dots + b_n\alpha_{nj}).$$

Ciò fornisce la formula ingegnosa:

$$(5.12) \quad x_j = \frac{\det M_j}{\det A}.$$

Per qualche ragione si è diffusa dappertutto l'abitudine di scrivere la soluzione del sistema di equazioni  $AX = B$  in questa forma ed è tale forma che spesso viene chiamata *regola di Cramer*. Tuttavia, tale espressione non semplifica i calcoli. La cosa più importante da ricordare è l'espressione (5.8) dell'inversa di una matrice mediante la sua aggiunta; le altre formule discendono da questa espressione.

Al pari dello sviluppo completo del determinante (4.12), le formule (5.8-5.12) hanno un'importanza sia teorica che pratica, poiché gli oggetti richiesti  $A^{-1}$  e  $X$  sono espressi in modo esplicito come quozienti di polinomi nelle variabili  $\{a_{ij}, b_i\}$ , a coefficienti interi. Se, per esempio,  $a_{ij}$  e  $b_i$  sono tutte funzioni continue di  $t$ , tali risultano le soluzioni  $x_i$ .

Lo sviluppo di un determinante è paragonabile a un miscuglio di liquidi apparentemente omogenei ma che, avendo punti di ebollizione diversi, possono essere separati con il metodo della distillazione frazionata.

James Joseph Sylvester

### Esercizi

#### 1 Le operazioni fondamentali

1. Quali sono gli elementi  $a_{21}$  e  $a_{23}$  della matrice  $\begin{bmatrix} 1 & 2 & 5 \\ 2 & 7 & 8 \\ 0 & 9 & 4 \end{bmatrix}$ ?

2. Calcolare i prodotti  $AB$  e  $BA$ , essendo  $A$  e  $B$  le matrici seguenti:

(a)  $A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix}$ ,  $B = \begin{bmatrix} -8 & -4 \\ 9 & 5 \\ -3 & -2 \end{bmatrix}$ ;

### Esercizi

(b)  $A = \begin{bmatrix} 1 & 4 \\ 1 & 2 \end{bmatrix}$ ,  $B = \begin{bmatrix} 6 & -4 \\ -3 & 2 \end{bmatrix}$ ;

(c)  $A = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$ ,  $B = [1 \ 2 \ 1]$ .

3. Sia  $A = (a_1, \dots, a_n)$  un vettore riga e sia  $B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$  un vettore colonna. Calcolare i prodotti  $AB$  e  $BA$ .

4. Verificare la proprietà associativa per il seguente prodotto di matrici:

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}.$$

Si noti che questo è un esercizio che si controlla automaticamente. Occorre effettuare correttamente le moltiplicazioni, altrimenti il risultato non torna. Questo esercizio può essere usato come modello, se è necessario acquistare maggior pratica nella moltiplicazione tra matrici.

5. Calcolare il prodotto  $\begin{bmatrix} 1 & a \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ & 1 \end{bmatrix}$ .

6. Calcolare la matrice  $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^n$ .

7. Trovare una formula per  $\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^n$ , e dimostrarla per induzione.

8. Calcolare i seguenti prodotti di matrici mediante la moltiplicazione per blocchi:

$$\begin{array}{c|cc} 1 & 1 & 1 & 5 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \begin{array}{c|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 3 \end{array}, \begin{array}{c|cc} 0 & 1 & 2 \\ \hline 0 & 1 & 0 \\ 3 & 0 & 1 \end{array} \begin{array}{c|cc} 1 & 2 & 3 \\ 4 & 2 & 3 \\ 5 & 0 & 4 \end{array}.$$

9. Dimostrare la regola (1.20) relativa alla moltiplicazione per blocchi.

10. Siano  $A, B$  due matrici quadrate  $n \times n$ .

- (a) Quand'è che  $(A+B)(A-B) = A^2 - B^2$ ?

- (b) Sviluppare  $(A+B)^3$ .

11. Sia  $D$  la matrice diagonale:

$$\begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix},$$

e sia  $A = (a_{ij})$  una matrice  $n \times n$  arbitraria.

- (a) Calcolare i prodotti  $DA$  e  $AD$ .
- (b) Calcolare il prodotto di due matrici diagonali.
- (c) Quand'è che una matrice diagonale è invertibile?

12. Una matrice  $n \times n$  si dice *triangolare superiore*, se  $a_{ij} = 0$  per  $i > j$ . Dimostrare che il prodotto di due matrici triangolari superiori è una matrice triangolare superiore.

13. In ciascuno dei casi seguenti, determinare tutte le matrici  $2 \times 2$  reali che commutano con la matrice assegnata:

$$(a) \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad (b) \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad (c) \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}, \quad (d) \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \quad (e) \begin{bmatrix} 2 & 3 \\ 0 & 6 \end{bmatrix}.$$

14. Dimostrare le proprietà  $0 + A = A$ ,  $0A = 0$  e  $A0 = 0$  delle matrici nulle.

15. Provare che una matrice che ha una riga di zeri non è invertibile.

16. Una matrice quadrata  $A$  si dice *nilpotente*, se  $A^k = 0$  per qualche intero  $k > 0$ . Dimostrare che, se  $A$  è nilpotente, allora  $I + A$  è invertibile.

17. (a) Trovare infinite matrici  $B$  tali che  $BA = I_2$ , essendo:

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \\ 2 & 5 \end{bmatrix}.$$

- (b) Dimostrare che non esiste nessuna matrice  $C$  tale che  $AC = I_3$ .

18. Scrivere in dettaglio la dimostrazione della proposizione (1.18), utilizzando la proprietà associativa per sviluppare il prodotto  $(AB)(B^{-1}A^{-1})$ .

19. La *traccia* di una matrice quadrata è la somma dei suoi elementi diagonali:

$$\text{tr } A = a_{11} + a_{22} + \dots + a_{nn}.$$

- (a) Dimostrare che  $\text{tr}(A + B) = \text{tr } A + \text{tr } B$  e che  $\text{tr } AB = \text{tr } BA$ .

- (b) Dimostrare che, se  $B$  è invertibile, allora  $\text{tr } A = \text{tr } BAB^{-1}$ .

20. Dimostrare che l'equazione  $AB - BA = I$  non ammette soluzioni nell'insieme delle matrici  $n \times n$  a elementi reali.

## 2 Riduzione per righe

1. (a) Per la riduzione della matrice  $M$  data nel testo in (2.10), determinare le matrici elementari corrispondenti a ciascuna operazione.  
(b) Calcolare il prodotto  $P$  di tali matrici elementari e verificare che  $PM$  è davvero il risultato finale.
2. Determinare tutte le soluzioni del sistema di equazioni  $AX = B$ , dove

$$A = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 3 & 0 & 0 & 4 \\ 1 & -4 & -2 & -2 \end{bmatrix}$$

e  $B$  è una delle matrici seguenti:

$$(a) \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad (b) \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad (c) \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}.$$

3. Trovare tutte le soluzioni dell'equazione:  $x_1 + x_2 + 2x_3 - x_4 = 3$ .

4. Determinare le matrici elementari usate nella riduzione per righe nell'esempio (2.22) e verificare che il loro prodotto è  $A^{-1}$ .

5. Trovare le inverse delle seguenti matrici:

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}.$$

6. Abbozzare un disegno che mostri l'effetto della moltiplicazione mediante la matrice

$$A = \begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix}$$

sul piano  $\mathbb{R}^2$ .

7. Quanto può essere semplificata una matrice, utilizzando sia le operazioni sulle righe che le operazioni sulle colonne?

8. (a) Calcolare il prodotto di matrici  $e_{ij}e_{k\ell}$ .

- (b) Scrivere la matrice identica come somma di unità matriciali.

- (c) Sia  $A$  una matrice  $n \times n$  arbitraria. Calcolare  $e_{ii}Ae_{jj}$ .

- (d) Calcolare  $e_{ij}A$  e  $Ae_{ij}$ .

9. Dimostrare le regole (2.7) per le operazioni definite dalle matrici elementari.

10. Sia  $A$  una matrice quadrata. Dimostrare che esiste un insieme di matrici elementari  $E_1, \dots, E_k$  tali che  $E_k \cdots E_1 A$  è l'identità oppure ha l'ultima riga nulla.

11. Dimostrare che ogni matrice  $2 \times 2$  invertibile è esprimibile come un prodotto di al più quattro matrici elementari.

12. Dimostrare che, se un prodotto  $AB$  di matrici  $n \times n$  è invertibile, allora i fattori  $A, B$  sono matrici invertibili.

- 13.** Una matrice  $A$  si dice *simmetrica*, se  $A = A^t$ . Dimostrare che, data una matrice arbitraria, la matrice  $AA^t$  è simmetrica e inoltre che, se  $A$  è una matrice quadrata allora  $A + A^t$  è simmetrica.

**14.** (a) Dimostrare che  $(AB)^t = B^tA^t$  e che  $A^{tt} = A$ .  
(b) Dimostrare che, se  $A$  è invertibile, allora  $(A^{-1})^t = (A^t)^{-1}$ .

**15.** Provare che l'inversa di una matrice simmetrica invertibile è anch'essa simmetrica.

**16.** Siano  $A$  e  $B$  matrici  $n \times n$  simmetriche. Dimostrare che il prodotto  $AB$  è una matrice simmetrica se e soltanto se  $AB = BA$ .

**17.** Sia  $A$  una matrice  $n \times n$ . Dimostrare che l'operatore "moltiplicazione a sinistra per  $A$ " determina  $A$  nel senso che, se  $AX = BX$  per ogni vettore colonna  $X$ , allora  $A = B$ .

**18.** Si consideri un sistema di equazioni lineari arbitrario  $AX = B$ , con  $A$  e  $B$  matrici a elementi reali.  
(a) Dimostrare che, se il sistema di equazioni  $AX = B$  possiede più di una soluzione, allora ne possiede infinite.  
(b) Dimostrare che, se esiste una soluzione nell'insieme dei numeri complessi, allora esiste anche una soluzione reale.

**\*19.** Provare che la forma ridotta a scala per righe, ottenuta mediante riduzione per righe di una matrice  $A$  è determinata univocamente da  $A$ .

### 3 Determinanti

1. Calcolare i determinanti delle seguenti matrici

(a)  $\begin{bmatrix} 1 & i \\ 2-i & 3 \end{bmatrix}$  (b)  $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  (c)  $\begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$  (d)  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 8 & 6 & 3 & 0 \\ 0 & 9 & 7 & 4 \end{bmatrix}$

(e) 
$$\begin{bmatrix} 1 & 4 & 1 & 3 \\ 2 & 3 & 5 & 0 \\ 4 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}$$

- ## 2. Dimostrare che

$$\det \begin{bmatrix} 1 & 2 & 5 & 6 \\ 3 & 1 & 7 & 7 \\ 0 & 0 & 2 & 3 \\ 4 & 2 & 1 & 5 \end{bmatrix} = -\det \begin{bmatrix} 2 & 1 & 5 & 1 \\ 1 & 3 & 7 & 0 \\ 0 & 0 & 2 & 1 \\ 2 & 4 & 1 & 4 \end{bmatrix}$$

3. Verificare la regola:  $\det(AB) = (\det A)(\det B)$  per le matrici  $A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$ ,  $B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ .

## Esercizi

$= \begin{bmatrix} 1 & 1 \\ 5 & -2 \end{bmatrix}$ . Si noti che questo è un esercizio che si controlla automaticamente. Esso può essere usato come modello per acquistare pratica nel calcolo dei determinanti.

4. Calcolare il determinante delle seguenti matrici  $n \times n$ , procedendo per induzione su  $n$ :

- ## 5. Calcolare

$$\det \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & & \\ 3 & 3 & 3 & & \\ \vdots & & \ddots & & \\ \vdots & & & & \ddots \\ n & \cdots & \cdots & & n \end{bmatrix}$$

- \*6. Calcolare**

$$\det \begin{bmatrix} 2 & 1 \\ 1 & 2 & 1 \\ & 1 & 2 & 1 \\ & 1 & 2 & 1 \\ & 1 & 2 & 1 \\ & & 1 & 2 \end{bmatrix}$$

7. Dimostrare che il determinante è una funzione lineare rispetto alle righe di una matrice, come affermato in (3.6).

8. Sia  $A$  una matrice  $n \times n$ . Quanto vale  $\det(-A)$ ?

9. Dimostrare che  $\det A^t = \det A$

- 10.** Ricavare la formula

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$$

dalle proprietà (3.5, 3.6, 3.7, 3.9)

11. Siano  $A$  e  $B$  matrici quadrate. Dimostrare che  $\det(AB) = \det(BA)$ .

12. Provare che  $\det \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = (\det A)(\det D)$ , se  $A$  e  $D$  sono blocchi quadrati.

\*13. Sia data una matrice  $2n \times 2n$  nella forma  $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ , dove ciascun blocco è una matrice  $n \times n$ . Supponiamo che  $A$  sia invertibile e che  $AC = CA$ . Dimostrare che  $\det M = \det(AD - CB)$ . Dare un esempio che mostri che tale formula non vale necessariamente nel caso in cui  $AC \neq CA$ .

#### 4 Matrici di permutazione

1. Si consideri la permutazione  $p$  definita da:

$$1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 2.$$

- (a) Trovare la matrice di permutazione  $P$  associata a  $p$ .
  - (b) Scrivere  $p$  come un prodotto di trasposizioni e calcolare il prodotto di matrici corrispondente.
  - (c) Calcolare il segno di  $p$ .
  - 2. Dimostrare che ogni matrice di permutazione è un prodotto di trasposizioni.
  - 3. Dimostrare che ogni matrice avente un solo 1 in ciascuna riga e un solo 1 in ciascuna colonna, e tutti gli altri elementi nulli, è una matrice di permutazione.
  - 4. Sia  $p$  una permutazione. Dimostrare che  $\text{sign } p = \text{sign } p^{-1}$ .
  - 5. Dimostrare che la trasposta di una matrice di permutazione  $P$  è la sua inversa.
  - 6. Qual è la matrice di permutazione associata alla permutazione  $\mathbf{i} \mapsto \mathbf{n} - \mathbf{i} \quad \forall i = 1, \dots, n$ ?
  - 7. (a) Lo sviluppo completo del determinante di una matrice  $3 \times 3$  è costituito da 6 tripli prodotti di elementi della matrice, accompagnati dal segno. Scrivere esplicitamente tali prodotti.  
(b) Calcolare il determinante delle seguenti matrici utilizzando lo sviluppo completo e controllare i risultati con un altro metodo:
- $$\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$
8. Dimostrare che lo sviluppo completo (4.12) definisce il determinante, verificando le proprietà (3.5-3.7).
9. Provare che le formule (4.11) e (4.12) definiscono lo stesso numero.

#### 5 La regola di Cramer

1. Sia  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  una matrice con determinante 1. Qual è la matrice  $A^{-1}$ ?

2. (Autoverifica) Calcolare le aggiunte delle matrici:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

e verificare il teorema (5.7) per esse.

3. Sia  $A$  una matrice  $n \times n$  invertibile con elementi interi  $a_{ij}$ . Dimostrare che  $A^{-1}$  ha elementi interi se e soltanto se  $\det A = \pm 1$ .

4. Provare che lo sviluppo per minori rispetto a una riga di una matrice definisce la funzione determinante.

#### Esercizi vari

1. Scrivere la matrice  $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$  come un prodotto di matrici elementari, usando il minor numero possibile di fattori. Dimostrare che un'espressione siffatta è la più corta possibile.

2. Trovare una rappresentazione dei numeri complessi mediante matrici  $2 \times 2$  reali, che sia compatibile con l'addizione e la moltiplicazione. Cominciare col trovare una soluzione espressiva dell'equazione matriciale  $A^2 = -I$ .

#### 3. (Determinante di Vandermonde)

(a) Dimostrare che:

$$\det \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} = (b-a)(c-a)(c-b).$$

(b) Dimostrare una formula analoga per le matrici  $n \times n$ , usando operazioni sulle righe per semplificare la prima colonna in modo efficiente.

\*4. Consideriamo un sistema generico  $AX = B$  di  $m$  equazioni lineari in  $n$  incognite. Se la matrice dei coefficienti  $A$  ha un'inversa sinistra  $A'$ , ossia una matrice tale che  $A'A = I$ , allora possiamo cercare di risolvere il sistema nel modo seguente:

$$AX = B$$

$$A'AX = A'B$$

$$X = A'B.$$

Tuttavia, se andiamo a verificare che  $X = A'B$  è la soluzione del sistema, ci troviamo in difficoltà:

$$X = A'B$$

$$AX = AA'B$$

$$AX \stackrel{?}{=} B.$$

Apparentemente occorre richiedere che  $A'$  sia un'inversa destra di  $A$ , ossia che  $AA' = I$ , e ciò non fa parte delle ipotesi iniziali. Provare a spiegare tale difficoltà. (Suggerimento: studiare qualche esempio.)

5. **(a)** Sia  $A$  una matrice  $2 \times 2$  reale e siano  $A_1, A_2$  le righe di  $A$ . Sia  $P$  il parallelogramma i cui vertici sono  $0, A_1, A_2, A_1 + A_2$ . Dimostrare che l'area di  $P$  è il valore assoluto del determinante di  $A$ , confrontando l'effetto di un'operazione elementare sulle righe rispettivamente sull'area e su  $\det A$ .
- \*(b)** Provare un risultato analogo per le matrici  $n \times n$ .
- \*6. Le matrici invertibili, per la maggior parte, possono essere scritte come un prodotto  $A = LU$  di una matrice triangolare inferiore  $L$  e di una matrice triangolare superiore  $U$ , con la proprietà ulteriore che tutti gli elementi diagonali di  $U$  sono uguali a 1.
  - (a)** Dimostrare l'unicità, ossia, dimostrare che vi è al più un unico modo di scrivere  $A$  come un prodotto siffatto.
  - (b)** Spiegare come calcolare  $L$  e  $U$ , data la matrice  $A$ .
  - (c)** Dimostrare che ogni matrice invertibile può esser scritta come un prodotto  $LPU$ , dove  $L, U$  sono come sopra e  $P$  è una matrice di permutazione.
7. Si consideri un sistema di  $n$  equazioni lineari in  $n$  incognite:  $AX = B$ , con  $A$  e  $B$  a elementi interi. Dimostrare la verità o la falsità delle seguenti affermazioni:
  - (a)** Il sistema ha una soluzione razionale, se  $\det A \neq 0$ .
  - (b)** Se il sistema ha una soluzione razionale, ha anche una soluzione intera.
- \*8. Siano  $A, B$  matrici  $m \times n$  e  $n \times m$  rispettivamente. Dimostrare che  $I_m - AB$  è invertibile, se e soltanto se,  $I_n - BA$  è invertibile.

## Capitolo 2

### Gruppi

Poche nozioni, in matematica, sono più primitive della legge di composizione.

Nicolas Bourbaki

#### 1 Definizione di gruppo

In questo capitolo studieremo uno dei concetti algebrici più importanti, quello di **gruppo**. Un gruppo è un insieme nel quale è definita una legge di composizione tale che ogni elemento abbia un inverso. La definizione precisa è data più avanti, in (1.10). Per esempio, l'insieme dei numeri reali non nulli costituisce un gruppo  $\mathbb{R}^*$  rispetto alla moltiplicazione e l'insieme di tutti i numeri reali costituisce un gruppo  $\mathbb{R}$  rispetto all'addizione. L'insieme delle matrici  $n \times n$  invertibili, chiamato **gruppo lineare generale**, è un esempio di gruppo, molto importante, in cui la legge di composizione è la moltiplicazione tra matrici. Nel seguito, vedremo molti altri esempi di gruppi.

Per **legge di composizione** in un insieme  $S$  si intende una regola che associa a ogni coppia di elementi  $a, b$  di  $S$  un altro elemento, diciamo  $p$ , di  $S$ . I modelli fondamentali per tale nozione sono l'addizione e la moltiplicazione di numeri reali. Da un punto di vista formale, una legge di composizione è una funzione di due variabili su  $S$ , a valori in  $S$ , ossia è un'applicazione

$$S \times S \rightarrow S$$

$$(a, b) \mapsto p.$$

Qui  $S \times S$  denota, come sempre, l'insieme di tutte le coppie ordinate  $(a, b)$  di elementi di  $S$ .

La notazione funzionale  $p = f(a, b)$  non è molto comoda per le leggi di composizione. Per indicare l'elemento ottenuto applicando la legge a una coppia  $(a, b)$ , si preferisce ricorrere a una notazione simile a quelle usate per la moltiplicazione o l'addizione:

$$p = ab, \quad a \times b, \quad a \circ b, \quad a + b, \quad \text{e così via.}$$

dove la scelta dipende dalla particolare legge in questione. L'elemento  $p$  prende il nome di *prodotto* o *somma* di  $a$  e  $b$ , a seconda della notazione scelta.

Il primo esempio (uno dei due più importanti) di legge di composizione è la moltiplicazione tra matrici nell'insieme  $S$  delle matrici  $n \times n$ .

Useremo più frequentemente la notazione moltiplicativa  $ab$ ; d'altra parte, tutto ciò che dimostreremo con la notazione moltiplicativa può essere riscritto usando un'altra notazione, come l'addizione. Le conclusioni resteranno comunque valide.

È importante notare che il simbolo  $ab$  indica un certo elemento di  $S$ . Precisamente, si tratta dell'elemento ottenuto applicando la legge di composizione assegnata agli elementi chiamati  $a$  e  $b$ . Così, se la legge è la moltiplicazione tra matrici e se  $a = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}$  e  $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ , allora  $ab$  denota la matrice  $\begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$ . Una volta calcolato il prodotto, è impossibile da esso risalire agli elementi  $a, b$ .

Consideriamo una legge di composizione scritta con notazione moltiplicativa, nella forma  $ab$ . Diremo che essa è *associativa* se, per ogni  $a, b, c$  in  $S$ , vale la relazione

$$(1.1) \quad (ab)c = a(bc) \text{ (proprietà associativa)}$$

e che è *commutativa* se, per ogni  $a, b$  in  $S$  vale la relazione

$$(1.2) \quad ab = ba \text{ (proprietà commutativa).}$$

La moltiplicazione tra matrici è un esempio di legge associativa ma non commutativa.

Quando parleremo di gruppi in generale, useremo la notazione moltiplicativa. Di solito si riserva la notazione additiva  $a + b$  per le leggi di composizione commutative, ossia quando  $a + b = b + a$  per ogni  $a, b$ . La notazione moltiplicativa non ha implicazioni di sorta circa la commutatività.

Con la notazione additiva, la proprietà associativa è  $(a + b) + c = a + (b + c)$ , e con quella funzionale è

$$f(f(a, b), c) = f(a, f(b, c)).$$

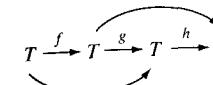
Questa formula, decisamente poco elegante, mostra che la notazione funzionale non è adatta per i calcoli algebrici.

La proprietà associativa è di gran lunga più importante della proprietà commutativa; uno dei motivi è il fatto che la composizione di funzioni (il secondo esempio di legge di composizione) è associativa. Sia  $T$  un insieme, e siano  $g, f$  funzioni (o applicazioni) da  $T$  a  $T$ . Denotiamo con  $g \circ f$  l'applicazione composta  $t \mapsto g(f(t))$ . La regola

$$(g, f) \mapsto g \circ f$$

è una legge di composizione nell'insieme  $S = \text{Appl}(T, T)$  di tutte le applicazioni  $T \rightarrow T$ .

La composizione di applicazioni, così come la moltiplicazione tra matrici, è una legge associativa. Infatti, se  $f, g, h$  sono tre applicazioni di  $T$  in sé, allora  $(h \circ g) \circ f = h \circ (g \circ f)$ :



Ciò è evidente, poiché entrambe le applicazioni composte mandano  $t$  in  $h(g(f(t)))$ .

L'esempio più semplice è quello di un insieme  $T$  formato da due elementi  $\{a, b\}$ . Allora esistono quattro applicazioni  $T \rightarrow T$ :

$i$ : l'applicazione *identica*, definita da  $i(a) = a, i(b) = b$ ;

$\tau$ : la *trasposizione*, definita da:  $\tau(a) = b, \tau(b) = a$ ;

$\alpha$ : l'applicazione costante  $\alpha(a) = \alpha(b) = a$ ;

$\beta$ : l'applicazione costante  $\beta(a) = \beta(b) = b$ .

La legge di composizione in  $S$  può essere descritta esplicitamente mediante una *tabella di moltiplicazione*:

	$i$	$\tau$	$\alpha$	$\beta$
$i$	$i$	$\tau$	$\alpha$	$\beta$
$\tau$	$\tau$	$i$	$\beta$	$\alpha$
$\alpha$	$\alpha$	$\alpha$	$\alpha$	$\alpha$
$\beta$	$\beta$	$\beta$	$\beta$	$\beta$

la quale va letta nel modo seguente:

	...	$v$	...
:		:	
$u$	...	$u \circ v$	
:			

Così  $\tau \circ \alpha = \beta$ , mentre  $\alpha \circ \tau = \alpha$ . La composizione di applicazioni non è quindi commutativa.

Ritornando allo studio di una legge generale di composizione, supponiamo di voler definire il prodotto di una successione finita di  $n$  elementi di un insieme:

$$a_1 a_2 \cdots a_n = ?$$

Possiamo farlo in vari modi, quando sia data la legge che ci dice come moltiplicare due elementi. Per esempio, potremmo dapprima trovare il prodotto  $a_1 a_2$ , poi mol-

tiplicare questo elemento per  $a_3$ , e così via:

$$((a_1 a_2) a_3) a_4 \dots$$

Per  $n = 4$ , vi sono altri quattro modi di combinare gli stessi elementi;  $(a_1 a_2)(a_3 a_4)$  è uno di essi. Si può dimostrare per induzione che, se la legge è *associativa*, tutti i prodotti così ottenuti sono uguali. Ciò permette di parlare del prodotto di una successione finita arbitraria di elementi.

**(1.4) PROPOSIZIONE** *Supponiamo che in un insieme  $S$  sia data una legge di composizione associativa. Allora vi è un unico modo di definire, per ogni intero  $n$ , un prodotto di  $n$  elementi  $a_1, \dots, a_n$  di  $S$  (lo denotiamo provvisoriamente con  $[a_1 \dots a_n]$ ) con le seguenti proprietà:*

- (i) *il prodotto  $[a_1]$  di un solo elemento è l'elemento stesso;*
- (ii) *il prodotto  $[a_1 a_2]$  di due elementi è dato dalla legge di composizione;*
- (iii) *per ogni intero  $i$  compreso tra 1 e  $n$ , si ha:*

$$[a_1 \dots a_n] = [a_1 \dots a_i][a_{i+1} \dots a_n].$$

Il secondo membro dell'equazione (iii) sta a indicare che prima si calcolano i prodotti  $[a_1 \dots a_i]$  e  $[a_{i+1} \dots a_n]$  poi si moltiplicano i risultati con la legge di composizione assegnata.

*Dimostrazione.* Procediamo per induzione su  $n$ . Il prodotto è definito da (i) e (ii) per  $n \leq 2$  e soddisfa (iii) per  $n = 2$ . Supponiamo ora di saper definire il prodotto di  $r$  elementi con  $r \leq n - 1$ , e che tale prodotto sia l'unico che soddisfi (iii). Definiamo allora il prodotto di  $n$  elementi mediante la regola:

$$[a_1 \dots a_n] = [a_1 \dots a_{n-1}][a_n],$$

dove i termini a destra sono quelli già definiti. Se esiste un prodotto che soddisfa (iii), allora tale formula fornisce il prodotto poiché essa dà (iii) per  $i = n - 1$ . Dunque, se esiste, il prodotto è unico. Dobbiamo ora verificare (iii) per  $i < n - 1$ :

$$\begin{aligned} (\text{definizione}) \quad [a_1 \dots a_n] &= [a_1 \dots a_{n-1}][a_n] = \\ (\text{ipotesi induttiva}) \quad &= ([a_1 \dots a_i][a_{i+1} \dots a_{n-1}])[a_n] = \\ (\text{proprietà associativa}) \quad &= [a_1 \dots a_i]([a_{i+1} \dots a_{n-1}][a_n]) = \\ (\text{ipotesi induttiva}) \quad &= [a_1 \dots a_i][a_{i+1} \dots a_n] \end{aligned}$$

Ciò completa la dimostrazione. D'ora in poi eliminiamo le parentesi e denoteremo il prodotto con  $a_1 \dots a_n$ . ■

Un'identità o *elemento neutro* per una legge di composizione è un elemento  $e$  di  $S$  avente la seguente proprietà:

$$(1.5) \quad ea = a \quad \text{e} \quad ae = a, \quad \text{per ogni } a \in S.$$

Non può esservi più di un elemento neutro. Infatti, se  $e$ ,  $e'$  fossero due elementi siffatti, allora  $ee' = e'$  (essendo  $e$  un'identità) e inoltre  $ee' = e$  (essendo  $e'$  un'identità). Dunque  $e = e'$ .

Entrambe le leggi di composizione citate, la moltiplicazione di matrici  $n \times n$  e la composizione di applicazioni  $T \rightarrow T$ , ammettono una identità: nel primo caso è la matrice  $I_n$  [cap. 1 (1.14)], nel secondo l'applicazione identica  $i$  definita poc'anzi.

Spesso l'identità si denota con 1, se la legge di composizione è scritta con notazione moltiplicativa, oppure con 0, se è scritta con notazione additiva. Tali elementi non devono essere collegati necessariamente con i numeri 1 e 0, anche se hanno in comune con essi la proprietà di essere identità per le rispettive leggi di composizione.

Supponiamo di avere una legge di composizione che ammette un'identità che indichiamo con il simbolo 1. Un elemento  $a \in S$  si dice *invertibile* se esiste un elemento  $b \in S$  tale che

$$ab = 1 \quad \text{e} \quad ba = 1.$$

Come per la moltiplicazione tra matrici [cap. 1 (1.17)], dalla proprietà associativa segue che l'inverso di un elemento, se esiste, è unico. Esso si denota con  $a^{-1}$ :

$$aa^{-1} = a^{-1}a = 1.$$

Gli inversi si moltiplicano tra loro nell'ordine opposto:

$$(1.6) \quad (ab)^{-1} = b^{-1}a^{-1}.$$

La dimostrazione è uguale a quella svolta per le matrici [cap. 1 (1.18)].

Con una legge di composizione associativa si può usare la notazione esponenziale

$$\begin{aligned} (1.7) \quad a^n &= \underbrace{a \cdots a}_{n \text{ volte}} & (n \geq 1) \\ a^0 &= 1 & (\text{se esiste l'identità}) \\ a^{-n} &= \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ volte}} & (\text{se } a \text{ è invertibile}). \end{aligned}$$

Nel qual caso valgono le solite regole per il calcolo delle potenze:

$$(1.8) \quad a^{r+s} = a^r a^s \quad \text{e} \quad (a^r)^s = a^{rs}.$$

Non è opportuno invece introdurre la notazione frazionaria

$$(1.9) \quad \frac{b}{a},$$

a meno che la legge di composizione non sia commutativa, poiché non è chiaro se la frazione indichi  $ba^{-1}$  oppure  $a^{-1}b$ , e d'altra parte questi due elementi possono essere diversi.

Se per la legge di composizione si usa la notazione additiva, l'inverso di un elemento  $a$  si indica con  $-a$  e la notazione  $a^n$  è sostituita da  $na = a + \dots + a$  ( $n$  volte), come per l'addizione di numeri reali.

(1.10) DEFINIZIONE *Un gruppo è un insieme  $G$  con una legge di composizione associativa, dotato di identità e tale che ogni suo elemento ha un inverso.*

Il gruppo e l'insieme dei suoi elementi si denotano di solito con lo stesso simbolo.

Un *gruppo abeliano* è un gruppo la cui legge di composizione è commutativa. Per i gruppi abeliani si usa spesso la notazione additiva. Semplici esempi di gruppi abeliani sono:

- $\mathbb{Z}$ : i numeri interi, rispetto all'addizione;
- $\mathbb{R}$ : i numeri reali, rispetto all'addizione;
- $\mathbb{R}^*$ : i numeri reali non nulli, rispetto alla moltiplicazione;
- $\mathbb{C}, \mathbb{C}^*$ : i gruppi analoghi, ove  $\mathbb{R}$  è sostituito dall'insieme  $\mathbb{C}$  dei numeri complessi.

Dimostriamo ora una importante proprietà dei gruppi:

(1.12) PROPOSIZIONE (Legge di cancellazione) *Siano  $a, b, c$  elementi di un gruppo  $G$ . Se  $ab = ac$ , allora  $b = c$ . Se  $ba = ca$ , allora  $b = c$ .*

*Dimostrazione.* Moltiplicando ambo i membri della relazione  $ab = ac$  a sinistra per  $a^{-1}$ , si ha  $b = a^{-1}ab = a^{-1}ac = c$ . ■

La moltiplicazione per  $a^{-1}$  nella dimostrazione precedente non è un artificio, ma è un fatto essenziale. Se un elemento  $a$  non è invertibile, la legge di cancellazione non vale necessariamente. Per esempio,  $0 \cdot 1 = 0 \cdot 2$ , oppure

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}.$$

I due esempi fondamentali di gruppi si ottengono a partire dagli esempi di leggi di composizione che abbiamo considerato, ossia, la moltiplicazione tra matrici e la composizione di applicazioni, lasciando fuori gli elementi che non sono invertibili. Come abbiamo osservato nel capitolo 1, il *gruppo lineare generale*  $n \times n$  è il gruppo delle matrici  $n \times n$  invertibili. Esso si denota con

$$(1.13) \quad GL_n = \{\text{matrici } n \times n \text{ } A, \text{ con } \det A \neq 0\}.$$

Per indicare che stiamo lavorando con matrici reali o con matrici complesse scriveremo rispettivamente

$$GL_n(\mathbb{R}) \text{ oppure } GL_n(\mathbb{C}).$$

Nell'insieme di applicazioni  $S = \text{Appl}(T, T)$ , un'applicazione  $f : T \rightarrow T$  ha un'inversa se e soltanto se è biettiva. Un'applicazione biettiva è chiamata anche *permutazione* di  $T$ . L'insieme delle permutazioni costituisce un gruppo. Nell'esempio (1.3), gli elementi invertibili sono  $i$  e  $\tau$  ed essi formano un gruppo con due elementi. Questi due elementi sono le permutazioni dell'insieme  $\{a, b\}$ .

Il gruppo delle permutazioni dell'insieme di  $n$  elementi  $\{1, 2, \dots, n\}$  è detto *gruppo simmetrico* e si denota con  $S_n$ :

$$(1.14) \quad S_n = \text{gruppo delle permutazioni di } \{1, \dots, n\}.$$

Poiché vi sono  $n!$  permutazioni di un insieme di  $n$  elementi,  $S_n$  ha  $n!$  elementi. (Si dice che l'*ordine* del gruppo è  $n!$ ) Il gruppo  $S_2$ , ad esempio, è formato dai due elementi  $i$  e  $\tau$ , dove  $i$  è la permutazione identica e  $\tau$  è la trasposizione che scambia tra loro 1 e 2 come in (1.3). La legge del gruppo, ossia la composizione di applicazioni, è descritta dal fatto che  $i$  è l'identità e dalla relazione  $\tau\tau = \tau^2 = i$ .

La struttura di  $S_n$  diventa molto complicata al crescere di  $n$ , ma possiamo analizzare il caso  $n = 3$  abbastanza facilmente. Il gruppo simmetrico  $S_3$  contiene sei elementi e costituisce un esempio importante, poiché è il più piccolo gruppo la cui legge di composizione non è commutativa. Per descrivere questo gruppo, scegliamo due permutazioni particolari  $x, y$ , mediante le quali si possano scrivere tutte le altre. Prendiamo come  $x$  la permutazione ciclica degli indici, rappresentata dalla matrice (4.3) del capitolo 1:

$$(1.15) \quad x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Come  $y$ , prendiamo la trasposizione che scambia 1 e 2, lasciando fisso 3:

$$(1.16) \quad y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Le sei permutazioni di  $\{1, 2, 3\}$  sono

$$(1.17) \quad \{1, x, x^2, y, xy, x^2y\} = \{x^i y^j \mid 0 \leq i \leq 2, 0 \leq j \leq 1\},$$

dove 1 denota la permutazione identica. Ciò può essere verificato calcolando i prodotti.

Le regole

$$(1.18) \quad x^3 = 1, \quad y^2 = 1, \quad yx = x^2y$$

possono essere verificate direttamente. Esse sono sufficienti per effettuare i calcoli nel gruppo  $S_3$ . Applicando più volte le (1.18) un qualsiasi prodotto degli elementi  $x, y$  e dei loro inversi, ad esempio  $x^{-1}y^3x^2y$ , può essere ridotto nella forma  $x^i y^j$ , con  $0 \leq i \leq 2$  e  $0 \leq j \leq 1$ . A tale scopo, spostiamo tutti i termini contenenti  $y$  a destra utilizzando l'ultima relazione e portiamo poi gli esponenti negli intervalli di variabilità indicati utilizzando le prime due relazioni:

$$x^{-1}y^3x^2y = x^2yx^2y = x^2(yx)xy = x^2x^2yxy = \dots = x^6y^2 = 1.$$

Con le (1.18), si può scrivere una tabella di moltiplicazione completa per  $S_3$ . Per questo motivo tali regole vengono chiamate *relazioni che definiscono* il gruppo, nozione che studieremo formalmente nel capitolo 6.

Si noti che in  $S_3$  non vale la proprietà commutativa, poiché  $yx \neq xy$ .

## 2 Sottogruppi

Un motivo per cui il gruppo lineare generale e il gruppo simmetrico sono così importanti è che molti altri gruppi sono contenuti in essi come sottogruppi. Un sottoinsieme  $H$  di un gruppo  $G$  è un *sottogruppo* se ha le seguenti proprietà:

- (a) *Chiusura:* Se  $a \in H$  e  $b \in H$ , allora  $ab \in H$ .
- (2.1) (b) *Identità:*  $1 \in H$ .
- (c) *Inversi:* Se  $a \in H$ , allora  $a^{-1} \in H$ .

La (a) dice che la legge di composizione  $G$  può essere usata per definire, in  $H$ , una *legge di composizione indotta*. La seconda e la terza condizione, (b), (c), dicono che rispetto a tale legge indotta  $H$  è un gruppo. Si noti che (2.1) raggruppa tutte le proprietà che definiscono un gruppo, tranne la proprietà associativa. Non è necessario menzionare tale proprietà, poiché essa si trasmette automaticamente da  $G$  a  $H$ .

Ogni gruppo ha due sottogruppi banali: l'intero gruppo e il sottogruppo  $\{1\}$  costituito soltanto dall'identità. Ogni altro sottogruppo è un *sottogruppo proprio*.

### (2.2) Esempi

- (a) L'insieme  $T$  delle matrici  $2 \times 2$  triangolari superiori invertibili

$$\begin{bmatrix} a & b \\ & d \end{bmatrix} \quad (a, d \neq 0)$$

è un sottogruppo del gruppo lineare generale  $GL_2(\mathbb{R})$ .

- (b) L'insieme dei numeri complessi con valore assoluto 1, ossia, l'insieme dei punti sulla circonferenza unitaria nel piano complesso, è un sottogruppo di  $\mathbb{C}^*$ .

Come esempio ulteriore, determiniamo i sottogruppi del gruppo additivo  $\mathbb{Z}$  degli interi. Denotiamo con  $b\mathbb{Z}$  il sottoinsieme di  $\mathbb{Z}$  costituito da tutti i multipli di un intero  $b$  assegnato:

$$(2.3) \quad b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = bk \text{ per qualche } k \in \mathbb{Z}\}.$$

- (2.4) PROPOSIZIONE *Per ogni intero  $b$ , il sottoinsieme  $b\mathbb{Z}$  è un sottogruppo di  $\mathbb{Z}$ . Inoltre, ogni sottogruppo  $H$  di  $\mathbb{Z}$  è del tipo  $H = b\mathbb{Z}$  per qualche intero  $b$ .*

*Dimostrazione.* Lasciamo come esercizio la verifica che  $b\mathbb{Z}$  è un sottogruppo e dimostriamo che ogni sottogruppo di  $\mathbb{Z}$  è di questa forma. Sia  $H$  un sottogruppo di  $\mathbb{Z}$ . Ricordiamo che la legge di composizione in  $\mathbb{Z}$  è l'addizione, l'identità è 0, e l'inverso di un elemento  $a$  è  $-a$ . Pertanto le proprietà del sottogruppo prendono la forma seguente:

- (i) se  $a \in H$  e  $b \in H$ , allora  $a + b \in H$ ;
- (ii)  $0 \in H$ ;
- (iii) se  $a \in H$ , allora  $-a \in H$ .

Da (ii) segue che  $0 \in H$ . Se 0 è l'unico elemento di  $H$ , allora  $H = 0\mathbb{Z}$  e non c'è più nulla da dimostrare. Altrimenti, esistono interi positivi in  $H$ . Infatti, sia  $a \in H$  un elemento non nullo arbitrario. Se  $a$  è negativo,  $-a$  è positivo e l'assioma (iii) assicura che  $-a$  appartiene a  $H$ . Sia  $b$  il più piccolo intero positivo in  $H$ , e facciamo vedere che  $H = b\mathbb{Z}$ .

Dimostriamo innanzitutto che  $b\mathbb{Z} \subset H$ , ossia che  $bk \in H$  per ogni intero  $k$ . Se  $k$  è un intero positivo, allora  $bk = b + b + \dots + b$  ( $k$  termini). Tale elemento appartiene a  $H$ , in base all'assioma (i) e all'induzione. Ciò accade anche per  $b(-k) = -bk$ , in base all'assioma (iii). Infine l'assioma (ii) assicura che  $b0 = 0 \in H$ .

Proviamo poi che  $H \subset b\mathbb{Z}$ , ossia che ogni elemento  $n \in H$  è un multiplo intero di  $b$ . Usiamo la divisione con resto per scrivere  $n = bq + r$ , dove  $q, r$  sono interi e il resto  $r$  è soggetto alle limitazioni:  $0 \leq r < b$ . Allora  $n$  e  $bq$  sono entrambi in  $H$ , e gli assiomi (iii) e (i) provano che anche  $r = n - bq$  appartiene a  $H$ . Ora, poiché  $b$  è il più piccolo intero positivo in  $H$  e inoltre  $0 \leq r < b$ , si ha necessariamente:  $r = 0$ , da cui:  $n = bq \in b\mathbb{Z}$ , come richiesto. ■

Gli elementi del sottogruppo  $b\mathbb{Z}$  possono essere descritti come gli interi che sono divisibili per  $b$ . Questa descrizione conduce a una notevole applicazione della proposizione (2.4) ai sottogruppi che sono generati da *due* interi  $a, b$ . Supponiamo che  $a$  e  $b$  siano non entrambi nulli. L'insieme

$$(2.5) \quad a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ar + bs, \text{ con } r, s \text{ interi}\}$$

è un sottogruppo di  $\mathbb{Z}$  che viene detto *generato* da  $a$  e  $b$ , perché è il più piccolo sottogruppo che contiene entrambi gli elementi. La proposizione (2.4) assicura che tale sottogruppo ha la forma  $d\mathbb{Z}$  per qualche intero  $d$ , sicché esso è l'insieme di tutti gli interi che sono divisibili per  $d$ . Il generatore  $d$  è chiamato il *massimo comune divisore* di  $a$  e  $b$ , essendo tale denominazione giustificata dal risultato seguente:

(2.6) PROPOSIZIONE *Siano  $a, b$  interi non entrambi nulli, e sia  $d$  l'intero positivo che genera il sottogruppo  $a\mathbb{Z} + b\mathbb{Z}$ . Allora:*

- (a)  *$d$  può essere scritto nella forma  $d = ar + bs$ , essendo  $r, s$  interi opportuni.*
- (b)  *$d$  divide  $a$  e  $b$ .*
- (c) *Se un intero  $e$  divide  $a$  e  $b$ , divide anche  $d$ .*

*Dimostrazione.* La prima affermazione (a) rienuncia semplicemente il fatto che  $d$  è contenuto in  $a\mathbb{Z} + b\mathbb{Z}$ . Inoltre, poiché  $a$  e  $b$  appartengono al sottogruppo  $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ , è chiaro che  $d$  divide  $a$  e  $b$ . Infine, se  $e$  è un intero che divide  $a$  e  $b$ , allora  $a$  e  $b$  appartengono a  $e\mathbb{Z}$  e pertanto qualsiasi intero della forma  $n = ar + bs$  appartiene a  $e\mathbb{Z}$ . Per ipotesi,  $d$  ha questa forma; dunque  $e$  divide  $d$ . ■

Dati due interi  $a, b$ , un modo per trovare il loro massimo comune divisore è quello di fattorizzare ciascuno di essi in un prodotto di numeri primi e raccogliere poi i fattori comuni. Così il massimo comune divisore di  $36 = 2 \cdot 2 \cdot 3 \cdot 3$  e  $60 = 2 \cdot 2 \cdot 3 \cdot 5$  è  $12 = 2 \cdot 2 \cdot 3$ . Le proprietà (2.6 ii, iii) sono facili da verificare. Tuttavia, senza la proposizione (2.4), il fatto che il numero intero determinato in questo modo è della forma  $ar + bs$  non sarebbe affatto chiaro. (Nell'esempio precedente,  $12 = 36 \cdot 2 - 60 \cdot 1$ ). Discuteremo le applicazioni di questo fatto all'aritmetica nel capitolo 11.

Passiamo ora a un esempio astratto importante di sottogruppo: il *sottogruppo ciclico* generato da un elemento arbitrario  $x$  di un gruppo  $G$ . Usiamo qui la notazione moltiplicativa. Il sottogruppo ciclico  $H$  generato da  $x$  è l'insieme di tutte le potenze di  $x$ :

$$(2.7) \quad H = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}.$$

Esso è un sottogruppo di  $G$ , e precisamente il più piccolo sottogruppo contenente  $x$ . Tuttavia, per interpretare correttamente (2.7), occorre ricordare che  $x^n$  denota un ben determinato elemento di  $G$  e può ben accadere che vi siano ripetizioni nella lista. Per esempio, se  $x = 1$ , allora tutti gli elementi nella lista sono uguali a 1. Si presentano a priori due casi possibili: o le potenze di  $x$  sono elementi tutti distinti, oppure no. Nel primo caso,  $H$  è un gruppo *ciclico infinito*.

Supponiamo di trovarci nel secondo caso, sicché due potenze sono uguali, diciamo  $x^n = x^m$ , con  $n > m$ . Allora, in base alla legge di cancellazione (1.12), si ha:  $x^{n-m} = 1$  e pertanto esiste una potenza di  $x$  con esponente non nullo che è uguale a 1.

(2.8) LEMMA *L'insieme  $S$  degli interi  $n$  tali che  $x^n = 1$  è un sottogruppo di  $\mathbb{Z}$ .*

*Dimostrazione.* Se  $x^m = 1$  e  $x^n = 1$ , allora  $x^{m+n} = x^m \cdot x^n = 1$ . Ciò prova che, se  $m, n \in S$ , allora  $m + n \in S$ . Dunque l'assioma (i) di un sottogruppo è verificato. Vale inoltre l'assioma (ii), poiché  $x^0 = 1$ . Infine, se  $x^n = 1$ , allora  $x^{-n} = x^n x^{-n} = x^0 = 1$ . Quindi, se  $n \in S$ , allora  $-n \in S$ . ■

Dal lemma (2.8) e dalla proposizione (2.4) segue che  $S = m\mathbb{Z}$ , dove  $m$  è il più piccolo intero positivo tale che  $x^m = 1$ . Gli  $m$  elementi  $1, x, \dots, x^{m-1}$  sono tutti distinti. (Se  $x^i = x^j$  con  $0 \leq i < j < m$ , allora  $x^{j-i} = 1$ . Ma  $j - i < m$ ; dunque ciò è impossibile.) Inoltre, una potenza arbitraria  $x^n$  è uguale a uno di essi: utilizzando la divisione con resto, si può scrivere  $n = mq + r$ , con  $0 \leq r < m$ , sicché  $x^n = (x^m)^q x^r = x^r$ . Dunque  $H$  è costituito dai seguenti  $m$  elementi:

$$(2.9) \quad H = \{1, x, \dots, x^{m-1}\}, \text{ essendo le potenze tutte distinte e } x^m = 1.$$

Un gruppo siffatto è chiamato *gruppo ciclico di ordine  $m$* .

L'*ordine* di un gruppo  $G$  è il numero dei suoi elementi. Lo indicheremo spesso con  $|G|$ :

$$(2.10) \quad |G| = \text{numero degli elementi di } G.$$

Naturalmente, l'ordine può essere infinito.

Si dice che un *elemento* di un gruppo ha *ordine  $m$*  (eventualmente infinito) se il sottogruppo ciclico da esso generato ha ordine  $m$ . Ciò significa che  $m$  è il più

piccolo intero positivo tale che  $x^m = 1$ , oppure, se l'ordine è infinito, che  $x^m \neq 1$  per ogni  $m \neq 0$ .

Per esempio, la matrice  $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$  è un elemento di ordine 6 in  $GL_2(\mathbb{R})$ , sicché il sottogruppo ciclico da essa generato ha ordine 6. D'altra parte, la matrice  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  ha ordine infinito, poiché

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Più in generale, si può parlare del sottogruppo *generato da un sottoinsieme*  $U$  del gruppo  $G$ . Esso è il più piccolo sottogruppo di  $G$  contenente  $U$  ed è formato da tutti gli elementi di  $G$  che possono essere espressi come un prodotto di una successione finita di elementi di  $U$  e di loro inversi. In particolare, si dice che un sottoinsieme  $U$  di  $G$  *genera*  $G$  se ogni elemento di  $G$  è un prodotto siffatto. Per esempio, si è visto in (1.17) che l'insieme  $U = \{x, y\}$  genera il gruppo simmetrico  $S_3$ . La proposizione (2.18) del capitolo 1 dimostra che le matrici elementari generano  $GL_n$ .

Il *gruppo quadrinomio di Klein V* è l'esempio più semplice di un gruppo non ciclico. Esso comparirà in molte forme. Per esempio, può essere realizzato come il gruppo formato dalle 4 matrici

$$(2.11) \quad \begin{bmatrix} \pm 1 & & \\ & \pm 1 & \\ & & \pm 1 \end{bmatrix}.$$

Due elementi qualsiasi diversi dall'identità generano  $V$ .

Il *gruppo di quaternioni H* è un altro esempio di un piccolo sottogruppo di  $GL_2(\mathbb{C})$  che non è ciclico. Esso è formato dalle otto matrici

$$(2.12) \quad H = \{\pm 1, \pm i, \pm j, \pm k\},$$

dove

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

I due elementi  $i, j$  generano  $H$ , e valgono le formule:

$$(2.13) \quad i^2 = 1, \quad i^2 = j^2, \quad ji = i^2 j.$$

Tali prodotti determinano la tabella di moltiplicazione di  $H$ .

### 3 Isomorfismi

Siano  $G$  e  $G'$  due gruppi. Diremo che essi sono *isomorfi* se tutte le proprietà della struttura di gruppo di  $G$  valgono anche per  $G'$ , e viceversa. Per esempio, sia  $G$  l'insieme delle matrici reali della forma

$$\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}.$$

$G$  è un sottogruppo di  $GL_2(\mathbb{R})$ , e il prodotto di due matrici di questo tipo è

$$\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ & 1 \end{bmatrix}.$$

Moltiplicando le matrici, gli elementi in alto a destra si sommano tra loro, mentre gli altri elementi delle matrici restano invariati. Pertanto, lavorando con queste matrici, dobbiamo considerare soltanto gli elementi in alto a destra. Questo fatto si esprime formalmente dicendo che il gruppo  $G$  è isomorfo al gruppo additivo dei numeri reali.

Anche se non è immediatamente chiaro come precisare il concetto di isomorfismo, tuttavia viene fuori che il modo giusto è quello di collegare due gruppi mediante una *corrispondenza biunivoca* tra i loro elementi, *compatibile con le leggi di composizione*, ossia, una corrispondenza biunivoca

$$(3.1) \quad G \longleftrightarrow G'$$

avente la seguente proprietà: se  $a, b \in G$  corrispondono ad  $a', b' \in G'$ , allora il prodotto  $ab$  in  $G$  corrisponde al prodotto  $a'b'$  in  $G'$ . Quando ciò accade, tutte le proprietà della struttura di gruppo si trasmettono da un gruppo all'altro.

Per esempio, gli elementi neutri di gruppi isomorfi  $G$  e  $G'$  corrispondono l'uno all'altro. Per vedere ciò, supponiamo che l'elemento neutro  $1$  di  $G$  corrisponda a un elemento  $\epsilon'$  di  $G'$ , e dimostriamo che  $\epsilon' = 1'$ , l'elemento neutro di  $G'$ . Sia  $a'$  un elemento arbitrario di  $G'$  e sia  $a$  l'elemento corrispondente di  $G$ . Poiché, per ipotesi, prodotti corrispondono a prodotti e inoltre  $1a = a$  in  $G$ , ne segue che  $\epsilon'a' = a'$  in  $G'$ . Ciò dimostra che  $\epsilon' = 1'$ . Un altro esempio: gli ordini di elementi corrispondenti sono uguali. Infatti, se  $a \in G$  corrisponde ad  $a'$  in  $G'$ , allora, poiché la corrispondenza è compatibile con la moltiplicazione, si ha che  $a^r = 1$  se e soltanto se  $(a')^r = 1'$ .

Poiché due gruppi isomorfi hanno le stesse proprietà, spesso è comodo identificare i due gruppi, parlando in modo informale. Per esempio, il gruppo simmetrico  $S_n$  delle permutazioni di  $\{1, \dots, n\}$  è isomorfo al gruppo delle matrici di permutazione, un sottogruppo di  $GL_n(\mathbb{R})$ , e spesso si fa fatica a distinguere questi due gruppi tra loro.

Di solito, la corrispondenza (3.1) viene scritta in modo asimmetrico come una funzione o applicazione  $\varphi : G \rightarrow G'$ . Dunque un *isomorfismo*  $\varphi$  da  $G$  a  $G'$  è un'applicazione biiettiva che è compatibile con le leggi di composizione. Se esplicitiamo tale compatibilità, utilizzando la notazione funzionale per  $\varphi$ , otteniamo la condizione

$$(3.2) \quad \varphi(ab) = \varphi(a)\varphi(b),$$

per ogni scelta di  $a, b$  in  $G$ .

Il membro a sinistra di questa uguaglianza sta a indicare che dapprima si moltiplicano  $a$  e  $b$  in  $G$  e poi si applica  $\varphi$ , mentre a destra gli elementi  $\varphi(a)$  e  $\varphi(b)$ , denotati prima con  $a'$  e  $b'$ , vengono moltiplicati in  $G'$ . Potremmo anche scrivere tale condizione nella forma:

$$(ab)' = a'b'.$$

Naturalmente, la scelta di  $G$  come dominio per tale isomorfismo è del tutto arbitraria. Infatti, avremmo potuto usare ugualmente la funzione inversa  $\varphi^{-1} : G' \rightarrow G$ :

Due gruppi  $G$  e  $G'$  si dicono *isomorfi* se esiste un isomorfismo  $\varphi : G \rightarrow G'$ . Per indicare questo fatto scriveremo talvolta il simbolo  $\approx$ :

$$(3.3) \quad G \approx G'.$$

Per esempio, sia  $C = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$  un gruppo ciclico infinito. Allora l'applicazione

$$\varphi : \mathbb{Z} \rightarrow C$$

definita da  $\varphi(n) = a^n$  è un isomorfismo. Poiché la notazione è additiva nel dominio  $\mathbb{Z}$  e moltiplicativa nel codominio  $C$ , la condizione (3.2) diventa in questo caso  $\varphi(m+n) = \varphi(m)\varphi(n)$ , oppure

$$a^{m+n} = a^m a^n.$$

Vediamo un altro semplice esempio.

Siano  $G = \{1, x, x^2, \dots, x^{n-1}\}$  e  $G' = \{1, y, y^2, \dots, y^{n-1}\}$  due gruppi ciclici, generati da elementi  $x, y$  dello stesso ordine. Allora l'applicazione che manda  $x^i$  in  $y^i$  è un isomorfismo. Quindi due gruppi ciclici dello stesso ordine sono isomorfi.

Ricapitolando, due gruppi  $G$  e  $G'$  sono isomorfi se esiste un'applicazione biiettiva compatibile con le leggi di composizione  $\varphi : G \rightarrow G'$ , ossia un isomorfismo. I gruppi isomorfi a un dato gruppo  $G$  formano la cosiddetta *classe di isomorfismo* di  $G$ , e due gruppi arbitrari in una classe di isomorfismo sono isomorfi. Quando si parla di *classificazione* dei gruppi, si intende descrivere le classi di isomorfismo.

Ciò è troppo difficile da fare per tutti i gruppi, tuttavia vedremo più avanti che vi è, per esempio, una sola classe di isomorfismo di gruppi di ordine 3 [cfr. (6.13)] e che vi sono due classi di isomorfismo di gruppi di ordine 4 e cinque classi di isomorfismo di gruppi di ordine 12 [cfr. cap. 6 (5.1)].

Un fatto che può creare confusione riguardo agli isomorfismi è l'esistenza di isomorfismi di un gruppo  $G$  in sé:

$$\varphi : G \rightarrow G.$$

In questo caso, l'isomorfismo  $\varphi$  è detto *automorfismo* di  $G$ . Naturalmente, l'applicazione identica è un automorfismo, ma quasi sempre vi sono anche altri automorfismi. Per esempio, sia  $G = \{1, x, x^2\}$  un gruppo ciclico di ordine 3, in cui  $x^3 = 1$ . Allora la trasposizione che scambia tra loro  $x$  e  $x^2$  è un automorfismo di  $G$ :

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto x^2 \\ x^2 &\mapsto x. \end{aligned}$$

Ciò dipende dal fatto che  $x^2$  è un altro elemento di ordine 3 nel gruppo. Se denotiamo tale elemento con  $y$ , il sottogruppo ciclico  $\{1, y, y^2\}$  generato da  $y$  è l'intero gruppo  $G$ , poiché  $y^2 = x$ . L'automorfismo mette a confronto le due realizzazioni di  $G$  come gruppo ciclico.

L'esempio più importante di automorfismo è il coniugio. Sia  $b \in G$  un elemento fissato. Allora il *coniugio mediante  $b$*  è l'applicazione  $\varphi : G \rightarrow G$  definita da

$$(3.4) \quad \varphi(x) = bxb^{-1}.$$

Essa è un automorfismo di  $G$ , poiché, innanzitutto, è compatibile con la moltiplicazione in  $G$ :

$$\varphi(xy) = bxyb^{-1} = bx b^{-1} by b^{-1} = \varphi(x)\varphi(y),$$

e inoltre, è un'applicazione biiettiva, poiché ha un'applicazione inversa, precisamente il coniugio mediante  $b^{-1}$ . Se il gruppo è abeliano, allora il coniugio è l'applicazione identica:  $bab^{-1} = abb^{-1} = a$ . Invece, se il gruppo non è commutativo, allora esiste qualche coniugio non banale e quindi il gruppo possiede automorfismi non banali.

L'elemento  $bab^{-1}$  è chiamato il *coniugato* di  $a$  mediante  $b$  e comparirà spesso nel seguito. Due elementi  $a, a'$  di un gruppo  $G$  si dicono *coniugati*, se  $a' = bab^{-1}$  per qualche  $b \in G$ . Il coniugato di un elemento  $a$  si comporta esattamente come l'elemento  $a$ ; per esempio, esso ha lo stesso ordine nel gruppo. Ciò segue dal fatto che esso è l'immagine di  $a$  mediante un automorfismo.

Il coniugato ha un'interpretazione utile, anche se banale. Precisamente, se denotiamo  $bab^{-1}$  con  $a'$ , allora:

$$(3.5) \quad ba = a'b.$$

Dunque il coniugio mediante  $b$  può essere pensato come la trasformazione di  $a$  prodotta dallo spostamento di  $b$  da un lato all'altro di  $a$  stesso.

## 4 Omomorfismi

Siano  $G, G'$  due gruppi. Un *omomorfismo*  $\varphi : G \rightarrow G'$  è un'applicazione che soddisfa alla seguente proprietà:

$$(4.1) \quad \varphi(ab) = \varphi(a)\varphi(b), \text{ per ogni scelta di } a, b \text{ in } G.$$

Si tratta della stessa proprietà richiesta per un isomorfismo [cfr. (3.2)]. La differenza è che qui non si suppone che l'applicazione  $\varphi$  sia biiettiva.

### (4.2) Esempi

Le seguenti applicazioni sono omomorfismi:

- (a) la funzione determinante  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ ;
- (b) il segno di una permutazione  $\text{sign} : S_n \rightarrow \{+1, -1\}$  [cfr. cap. 1 (4.9)];
- (c) l'applicazione  $\varphi : \mathbb{Z} \rightarrow G$  definita da  $\varphi(n) = a^n$ , dove  $a$  è un elemento fissato in  $G$ ;
- (d) l'inclusione  $i : H \rightarrow G$  di un sottogruppo  $H$  in un gruppo  $G$ , definita da  $i(x) = x$ .

**(4.3) PROPOSIZIONE** *Un omomorfismo di gruppi  $\varphi : G \rightarrow G'$  porta l'identità nell'identità e gli inversi negli inversi. In altre parole,  $\varphi(1_G) = 1_{G'}$  e  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .*

*Dimostrazione.* Poiché  $\varphi$  è un omomorfismo e  $1 = 1 \cdot 1$ , si ha:  $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ . Cancellando  $\varphi(1)$  in entrambi i membri, in base a (1.12), si ottiene:  $1 = \varphi(1)$ . Inoltre,  $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1) = 1$  e similmente,  $\varphi(a)\varphi(a^{-1}) = 1$ . Ne segue che  $\varphi(a^{-1}) = \varphi(a)^{-1}$ . ■

Ogni omomorfismo di gruppi  $\varphi$  determina due sottogruppi notevoli: l'immagine e il nucleo. L'*immagine* di un omomorfismo  $\varphi : G \rightarrow G'$  è l'immagine dell'applicazione  $\varphi$

$$(4.4) \quad \text{im } \varphi = \{x \in G' \mid x = \varphi(a) \text{ per qualche } a \in G\},$$

ed è un sottogruppo di  $G'$ . L'immagine di  $\varphi$  si denota anche con  $\varphi(G)$ . Negli esempi (4.2a,b), l'immagine coincide con il codominio dell'applicazione; invece, nell'esempio (4.2c), l'immagine è il sottogruppo ciclico di  $G$  generato da  $a$ , e nell'esempio (4.2d), è il sottogruppo  $H$ .

Il *nucleo* di  $\varphi$  è una nozione più raffinata. Esso è l'insieme degli elementi di  $G$  che vengono trasformati nell'identità di  $G'$ :

$$(4.5) \quad \ker \varphi = \{a \in G \mid \varphi(a) = 1\},$$

che può essere descritto anche come la controimmagine  $\varphi^{-1}(1)$  dell'identità di  $G'$  [cfr. app. (1.5)]. Il nucleo è un sottogruppo di  $G$ , poiché, se  $a, b \in \ker \varphi$ , allora  $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$ , sicché  $ab \in \ker \varphi$ , e così via.

Il nucleo dell'omomorfismo "determinante" è il sottogruppo delle matrici con determinante 1. Tale sottogruppo di  $GL_n(\mathbb{R})$  è chiamato il *gruppo lineare speciale* e si denota con  $SL_n(\mathbb{R})$ :

$$(4.6) \quad SL_n(\mathbb{R}) = \{\text{matrici reali } n \times n \mid \det A = 1\}.$$

Il nucleo dell'omomorfismo "sign" nell'esempio (4.2b) precedente è chiamato il *gruppo alterno* e si denota con  $A_n$ :

$$(4.7) \quad A_n = \{\text{permutazioni pari}\};$$

è un sottogruppo di  $S_n$ . Il nucleo dell'omomorfismo (4.2d) è l'insieme degli interi  $n$  tali che  $a^n = 1$ . Abbiamo già dimostrato in precedenza che è un sottogruppo di  $\mathbb{Z}$  [cfr. (2.8)].

Oltre ad essere un sottogruppo, il nucleo di un omomorfismo possiede un'altra proprietà molto importante, cioè: se  $a \in \ker \varphi$  e  $b$  è un elemento qualsiasi di  $G$ , allora il coniugato  $bab^{-1}$  appartiene a  $\ker \varphi$ . Infatti, dire che  $a \in \ker \varphi$  significa che  $\varphi(a) = 1$ . Allora:

$$\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)1\varphi(b)^{-1} = 1,$$

dunque  $bab^{-1} \in \ker \varphi$ .

**(4.8) DEFINIZIONE** *Un sottogruppo  $N$  di un gruppo  $G$  si chiama sottogruppo normale se soddisfa alla seguente proprietà: per ogni  $a \in N$  e per ogni  $b \in G$ , il coniugato  $bab^{-1}$  appartiene a  $N$ .*

Per quanto abbiamo appena visto, si ha:

**(4.9) Il nucleo di un omomorfismo è un sottogruppo normale.**

Dunque  $SL_n(\mathbb{R})$  è un sottogruppo normale di  $GL_n(\mathbb{R})$  e  $A_n$  è un sottogruppo normale di  $S_n$ .

Ogni sottogruppo di un gruppo abeliano  $G$  è normale, poiché, essendo  $G$  abeliano, si ha  $bab^{-1} = a$ . Invece i sottogruppi di un gruppo non abeliano non sono necessariamente normali. Per esempio, il gruppo  $T$  delle matrici triangolari superiori invertibili non è un sottogruppo normale di  $GL_2(\mathbb{R})$ . Infatti, se  $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$  e  $B = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$ , allora  $BAB^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ . Ebbene  $A \in T$  e  $B \in GL_2(\mathbb{R})$ , ma  $BAB^{-1} \notin T$ .

Il *centro* di un gruppo  $G$ , denotato talvolta con  $Z$  o con  $Z(G)$ , è l'insieme degli elementi che commutano con ogni elemento di  $G$ :

$$(4.10) \quad Z = \{z \in G \mid zx = xz \text{ per ogni } x \in G\}.$$

Il centro di un qualunque gruppo  $G$  è un sottogruppo normale di  $G$ . Per esempio, si può dimostrare che il centro di  $GL_n(\mathbb{R})$  è il gruppo delle *matrici scalari*, ossia, delle matrici della forma  $cI$ .

## 5 Relazioni di equivalenza e partizioni

Un procedimento matematico fondamentale è quello di costruire, a partire da un insieme  $S$ , un nuovo insieme, identificando tra loro certi elementi di  $S$  secondo una data regola. Per esempio, possiamo dividere l'insieme degli interi in due classi: gli interi pari e gli interi dispari. Oppure possiamo considerare triangoli congruenti nel piano come oggetti geometrici equivalenti. Questo procedimento molto generale si presenta in vari modi, come ora vedremo.

Sia  $S$  un insieme. Una *partizione*  $P$  di  $S$  si definisce come una suddivisione di  $S$  in sottoinsiemi disgiunti:

$$(5.1) \quad S = \text{unione di sottoinsiemi non vuoti disgiunti.}$$

Per esempio, gli insiemi

$$\{1, 3\}, \{2, 5\}, \{4\}$$

formano una partizione dell'insieme  $\{1, 2, 3, 4, 5\}$ . I due insiemi, degli interi pari e degli interi dispari, formano una partizione dell'insieme  $Z$  di tutti gli interi.

Una *relazione di equivalenza* in  $S$  è una relazione che intercorre tra certi elementi di  $S$ . Spesso la indicheremo con  $a \sim b$  e parleremo di essa come di *equivalenza* tra  $a$  e  $b$ .

(5.2) Una relazione di equivalenza è una relazione che soddisfa alle seguenti proprietà:

(i) *transitiva*: se  $a \sim b$  e  $b \sim c$ , allora  $a \sim c$ ;

(ii) *simmetrica*: se  $a \sim b$ , allora  $b \sim a$ ;

(iii) *riflessiva*:  $a \sim a$  per ogni  $a \in S$ .

La relazione di congruenza tra triangoli è un esempio di relazione di equivalenza nell'insieme  $S$  dei triangoli del piano.

Da un punto di vista formale, una relazione in un insieme  $S$  è la stessa cosa che un sottoinsieme  $R$  dell'insieme  $S \times S$  delle coppie ordinate di elementi di  $S$ ; precisamente, il sottoinsieme  $R$  è costituito dalle coppie  $(a, b)$  tali che  $a \sim b$ . Possiamo allora riscrivere gli assiomi di una relazione di equivalenza nella forma:  
(i) se  $(a, b) \in R$  e  $(b, c) \in R$ , allora  $(a, c) \in R$ ;  
(ii) se  $(a, b) \in R$ , allora  $(b, a) \in R$ ;  
(iii)  $(a, a) \in R$  per ogni  $a$ .

Le nozioni di partizione di  $S$  e di relazione di equivalenza in  $S$  sono equivalenti dal punto di vista logico, anche se spesso, in pratica, ne viene introdotta una sola. Data una partizione  $P$  di  $S$ , possiamo definire una relazione di equivalenza  $R$  mediante la regola:  $a \sim b$ , se  $a$  e  $b$  appartengono a uno stesso sottoinsieme della partizione. Gli assiomi (5.2) sono banalmente soddisfatti. Viceversa, data una relazione di equivalenza  $R$ , possiamo definire una partizione  $P$  nel modo seguente: il sottoinsieme contenente  $a$  è l'insieme di tutti gli elementi  $b$  tali che  $a \sim b$ . Tale sottoinsieme è chiamato la *classe di equivalenza* di  $a$ , e  $S$  è così ripartito in classi di equivalenza.

Verifichiamo che le classi di equivalenza formano una partizione dell'insieme  $S$ . Denotiamo con  $C_a$  la classe di equivalenza di un elemento  $a \in S$ . Dunque  $C_a$  è costituita dagli elementi  $b$  tali che  $a \sim b$ :

$$(5.3) \quad C_a = \{b \in S \mid a \sim b\}.$$

La proprietà riflessiva afferma che  $a \in C_a$ . Quindi le classi  $C_a$  sono non vuote e inoltre, data l'arbitrarietà di  $a$ , esse ricoprono  $S$ . Per concludere che le classi di equivalenza formano una partizione, occorre verificare soltanto che sono disgiunte.

A questo punto, è facile restare un po' confusi, poiché, se  $a \sim b$ , allora per definizione  $b \in C_a$ . D'altra parte,  $b \in C_b$ . Ma ciò non prova che  $C_a$  e  $C_b$  hanno elementi in comune? Occorre ricordare però che  $C_a$  è un simbolo che denota un sottoinsieme di  $S$  definito in un certo modo. La partizione è costituita dai sottoinsiemi, non dalle notazioni. È vero che  $C_a$  e  $C_b$  hanno l'elemento  $b$  in comune, ma non c'è nulla di strano, poiché si tratta di due notazioni per uno stesso insieme. Dimostriamo allora il risultato seguente:

(5.4) Supponiamo che  $C_a$  e  $C_b$  abbiano un elemento  $d$  in comune. Allora  $C_a = C_b$ .

Dimostriamo innanzitutto che, se  $a \sim b$ , allora  $C_a = C_b$ . Sia  $x$  un elemento arbitrario di  $C_b$ . Allora  $b \sim x$ . Poiché  $a \sim b$ , dalla proprietà transitiva segue che  $a \sim x$ , dunque  $x \in C_a$ . Pertanto  $C_b \subset C_a$ . L'inclusione opposta si ottiene

scambiando i ruoli di  $a$  e  $b$ . Per dimostrare (5.4), supponiamo di avere  $d \in C_a$ ,  $d \in C_b$ ; ne segue che  $a \sim d$  e  $b \sim d$ . Allora, per quanto visto sopra, si ha  $C_a = C_d = C_b$ , come richiesto. ■

Supponiamo che sia data in un insieme  $S$  una relazione di equivalenza (oppure una partizione). Allora possiamo costruire un nuovo insieme  $\bar{S}$  i cui elementi sono le classi di equivalenza (o i sottoinsiemi della partizione). Per semplificare le notazioni, la classe di equivalenza di  $a$  (o il sottoinsieme della partizione che contiene  $a$ ) si denota spesso con  $\bar{a}$ . Dunque  $\bar{a}$  è un elemento di  $\bar{S}$ .

Si noti che esiste un'applicazione suriettiva naturale

$$(5.5) \quad S \rightarrow \bar{S}, \text{ la quale manda } a \text{ in } \bar{a}.$$

Nell'esempio precedente della partizione di  $S = \mathbb{Z}$ , l'insieme  $\bar{S}$  contiene i due elementi  $(Pari)$ ,  $(Dispari)$ , dove il simbolo  $(Pari)$  rappresenta l'insieme degli interi pari e  $(Dispari)$  l'insieme degli interi dispari. In particolare,  $\bar{0} = \bar{2} = \bar{4}$  e così via. Possiamo dunque denotare l'insieme  $(Pari)$  con uno qualsiasi di questi simboli. L'applicazione

$$(5.6) \quad \mathbb{Z} \rightarrow \{(Pari), (Dispari)\}$$

è definita in modo ovvio.

Ci sono due modi di pensare a tale costruzione. Possiamo immaginare di ammucchiare gli elementi di  $S$  in pile separate, una per ciascun sottoinsieme della partizione, e poi riguardare le pile come elementi di un nuovo insieme  $\bar{S}$ . L'applicazione  $S \rightarrow \bar{S}$  associa a ciascun elemento la sua pila. Oppure, possiamo pensare di cambiare il significato di uguaglianza tra elementi di  $S$ , interpretando  $a \sim b$  come  $a = b$  in  $\bar{S}$ . Seguendo questo approccio, gli elementi nei due insiemi  $S$  e  $\bar{S}$  si corrispondono, ma in  $\bar{S}$  molti di essi sono uguali tra loro. Questo è il modo in cui vengono studiati a scuola i triangoli congruenti. La notazione con la barra (5.5) si adatta bene a questa immagine intuitiva. Possiamo lavorare con gli stessi simboli usati in  $S$ , ma con la barra sopra per ricordare la nuova regola:

$$(5.7) \quad \bar{a} = \bar{b} \text{ significa } a \sim b.$$

Questa notazione spesso è molto comoda.

Un inconveniente della notazione con la barra è che molti simboli diversi rappresentano uno stesso elemento di  $\bar{S}$ . Talvolta questo inconveniente può essere superato scegliendo una volta per tutte un elemento particolare, ossia un *rappresentante* in ciascuna classe di equivalenza. Per esempio, di solito si rappresenta  $(Pari)$  con  $\bar{0}$  e  $(Dispari)$  con  $\bar{1}$ :

$$(5.8) \quad \{(Pari), (Dispari)\} = \{\bar{0}, \bar{1}\}.$$

Anche se l'immagine delle pile è più immediata, il secondo modo di vedere  $\bar{S}$  è spesso il migliore, poiché le operazioni sulle pile sono difficili da visualizzare, mentre la notazione con la barra si adatta bene ai calcoli algebrici.

Una qualunque applicazione tra insiemi  $\varphi : S \rightarrow T$  definisce una relazione di equivalenza nel dominio  $S$ , precisamente la relazione data dalla regola:  $a \sim b$ , se  $\varphi(a) = \varphi(b)$ . Essa prende il nome di *relazione di equivalenza definita dall'applicazione*. La partizione corrispondente è costituita dalle controimmagini non vuote degli elementi di  $T$ . Per definizione, la *controimmagine* di un elemento  $t \in T$  è il sottoinsieme di  $S$  costituito da tutti gli elementi  $s$  tali che  $\varphi(s) = t$ . Si denota simbolicamente nel modo seguente:

$$(5.9) \quad \varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}.$$

Dunque  $\varphi^{-1}(t)$  è un sottoinsieme del dominio  $S$ , determinato dall'elemento  $t \in T$ . (Si noti che si tratta di una notazione puramente simbolica, poiché, in generale,  $\varphi^{-1}$  non è un'applicazione.) Le controimmagini vengono chiamate anche le *fibre* dell'applicazione  $\varphi$ . Le fibre  $\varphi^{-1}(t)$  che sono *non vuote*, ossia tali che  $t$  appartiene all'immagine di  $\varphi$ , formano una partizione di  $S$ . In questo caso, l'insieme  $\bar{S}$  delle classi di equivalenza, che è l'insieme delle fibre non vuote, ha un'altra realizzazione, mediante l'immagine  $\text{im } \varphi$  dell'applicazione. Precisamente, vi è un'applicazione biiettiva

$$(5.10) \quad \bar{\varphi} : \bar{S} \rightarrow \text{im } \varphi,$$

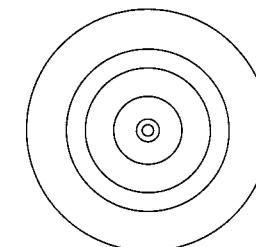
definita mandando un elemento  $\bar{s}$  di  $\bar{S}$  in  $\varphi(s)$ .

Ritorniamo ora allo studio degli omomorfismi tra gruppi. Sia  $\varphi : G \rightarrow G'$  un omomorfismo; analizziamo la relazione di equivalenza in  $G$  associata all'applicazione  $\varphi$  oppure, in modo equivalente, le fibre dell'omomorfismo. Tale relazione si denota di solito con  $\equiv$ , anziché con  $\sim$ , e prende il nome di *congruenza*:

$$(5.11) \quad a \equiv b, \text{ se } \varphi(a) = \varphi(b).$$

Per esempio, sia  $\varphi : \mathbb{C}^* \rightarrow \mathbb{R}^*$  l'omomorfismo "valore assoluto" definito da  $\varphi(a) = |a|$ . La relazione di equivalenza indotta è la seguente:  $a \equiv b$ , se  $|a| = |b|$ . Le fibre di tale applicazione sono le circonferenze concentriche intorno all'origine. Esse sono in corrispondenza biunivoca con gli elementi di  $\text{im } \varphi$ , l'insieme dei numeri reali positivi.

(5.12)



Fibre dell'applicazione "valore assoluto"  $\mathbb{C}^* \rightarrow \mathbb{R}^*$ .

La relazione (5.11) può essere riscritta in più modi, il più importante dei quali, per i nostri scopi, è il seguente:

(5.13) PROPOSIZIONE *Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi con nucleo  $N$ , e siano  $a, b$  elementi di  $G$ . Allora  $\varphi(a) = \varphi(b)$  se e solo se  $b = an$  per qualche elemento  $n \in N$ , ossia,  $a^{-1}b \in N$ .*

*Dimostrazione.* Supponiamo che  $\varphi(a) = \varphi(b)$ . Allora  $\varphi(a)^{-1}\varphi(b) = 1$ , e poiché  $\varphi$  è un omomorfismo, possiamo utilizzare (4.1) e (4.3) per riscrivere tale uguaglianza nella forma:  $\varphi(a^{-1}b) = 1$ . Ora, per definizione, il nucleo  $N$  è l'insieme di tutti gli elementi  $x \in G$  tali che  $\varphi(x) = 1$ . Dunque  $a^{-1}b \in N$ , ossia,  $a^{-1}b = n$  per qualche  $n \in N$ . Ne segue che  $b = an$ , come richiesto. Viceversa, se  $b = an$ , con  $n \in N$ , allora  $\varphi(b) = \varphi(a)\varphi(n) = \varphi(a)1 = \varphi(a)$ . ■

L'insieme degli elementi della forma  $an$  si denota con  $aN$  e si chiama una *classe laterale* di  $N$  in  $G$ :

$$(5.14) \quad aN = \{g \in G \mid g = an \text{ per qualche } n \in N\}.$$

Dunque la classe laterale  $aN$  è l'insieme di tutti gli elementi  $b$  del gruppo che sono congruenti ad  $a$ . La relazione di congruenza  $a \equiv b$  ripartisce il gruppo  $G$  in *classi di congruenza*: le classi laterali  $aN$ . Esse sono le fibre dell'applicazione  $\varphi$ . In particolare, le circonferenze intorno all'origine raffigurate in (5.12) sono le classi laterali dell'omomorfismo “valore assoluto”.

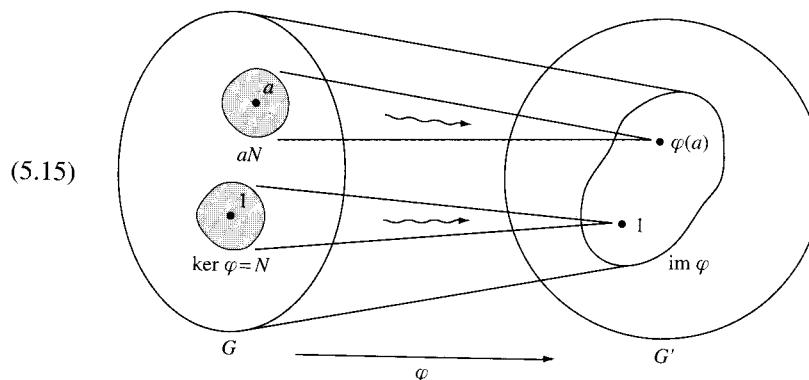


Diagramma schematico di un omomorfismo di gruppi.

Un caso importante da considerare è quello in cui il nucleo è il sottogruppo banale. In tal caso, la proposizione (5.13) si rieuncia nella forma seguente:

(5.16) COROLLARIO *Un omomorfismo di gruppi  $\varphi : G \rightarrow G'$  è iniettivo se e solo se il suo nucleo è il sottogruppo banale  $\{1\}$ .* ■

Tale risultato fornisce un modo per stabilire che un omomorfismo è un isomorfismo. Infatti, basta verificare che  $\ker \varphi = \{1\}$ , che implica  $\varphi$  iniettivo, e inoltre che  $\text{im } \varphi = G'$ , ossia che  $\varphi$  è suriettivo.

## 6 Classi laterali

È possibile definire le classi laterali per un qualunque sottogruppo  $H$  di un gruppo  $G$ , e non soltanto per il nucleo di un omomorfismo. Una *classe laterale sinistra* è un sottoinsieme della forma:

$$(6.1) \quad aH = \{ah \mid h \in H\}.$$

Si noti che il sottogruppo  $H$  è esso stesso una classe laterale, poiché  $H = 1H$ .

Le classi laterali sono classi di equivalenza rispetto alla relazione di *congruenza*:

$$(6.2) \quad a \equiv b, \text{ se } b = ah, \text{ per qualche } h \in H.$$

Verifichiamo che la congruenza è una relazione di equivalenza. (*Transitività*).

Supponiamo che  $a \equiv b$  e  $b \equiv c$ . Ciò significa che  $b = ah$  e  $c = bh'$ , con  $h, h' \in H$ .

Pertanto  $c = ahh'$ . Poiché  $H$  è un sottogruppo,  $hh' \in H$ , e quindi  $a \equiv c$ . (*Simmetria*).

Supponiamo che  $a \equiv b$ , sicché  $b = ah$ . Allora  $a = bh^{-1}$  e  $h^{-1} \in H$ , da cui segue che  $b \equiv a$ . (*Riflessività*).  $a = a1$  e  $1 \in H$ , sicché  $a \equiv a$ . Si noti che abbiamo utilizzato tutte le proprietà che definiscono un sottogruppo.

Poiché le classi di equivalenza formano una partizione, si ottiene il seguente risultato:

(6.3) COROLLARIO *Le classi laterali sinistre di un sottogruppo costituiscono una partizione del gruppo.* ■

(6.4) OSSERVAZIONE. La notazione  $aH$  definisce un sottoinsieme ben determinato di  $G$ . Così come accade per una relazione di equivalenza arbitraria, notazioni diverse possono rappresentare lo stesso sottoinsieme. Infatti, sappiamo che  $aH$  è l'unica classe laterale contenente  $a$ , e pertanto

$$(6.5) \quad aH = bH \text{ se e solo se } a \equiv b.$$

Il corollario è solo una riformulazione del risultato (5.4):

(6.6) *Se  $aH$  e  $bH$  hanno un elemento in comune, allora sono uguali.*

Per esempio, sia  $G$  il gruppo simmetrico  $S_3$ , con la descrizione data in (1.18):  $G = \{1, x, x^2, y, xy, x^2y\}$ . L'elemento  $xy$  ha ordine 2 e pertanto genera un sottogruppo ciclico  $H = \{1, xy\}$  di ordine 2. Le classi laterali sinistre di  $H$  in  $G$

sono i tre insiemi:

$$(6.7) \quad \{1, xy\} = H = xyH, \quad \{x, x^2y\} = xH = x^2yH, \quad \{x^2, y\} = x^2H = yH.$$

Si noti che essi formano una partizione del gruppo.

Il numero delle classi laterali sinistre di un sottogruppo è chiamato *indice* di  $H$  in  $G$  e si denota con

$$(6.8) \quad [G : H].$$

Quindi nel nostro esempio l'indice è 3. Naturalmente, se  $G$  contiene infiniti elementi, anche l'indice può essere infinito.

Osserviamo che esiste un'applicazione biiettiva dal sottogruppo  $H$  alla classe laterale  $aH$ , la quale manda  $h \mapsto ah$ . (Verificare che si tratta di un'applicazione biiettiva!) Pertanto:

$$(6.9) \quad \text{Ogni classe laterale } aH \text{ ha lo stesso numero di elementi di } H.$$

Poiché  $G$  è l'unione delle classi laterali di  $H$  e poiché tali classi sono disgiunte tra loro, si ottiene la formula notevole, detta anche "formula delle classi":

$$(6.10) \quad |G| = |H| \cdot [G : H],$$

dove  $|G|$  denota l'ordine del gruppo [cfr. (2.10)] e l'uguaglianza continua a valere in modo ovvio se alcuni termini sono infiniti. Applicando questa formula all'esempio (6.7), si ha  $6 = 2 \cdot 3$ .

Il fatto che i due termini a destra nell'equazione (6.10) devono dividere il termine a sinistra ha molte importanti conseguenze. Enunciamo formalmente una di esse:

(6.11) COROLLARIO (Teorema di Lagrange) *Sia  $G$  un gruppo finito e sia  $H$  un sottogruppo di  $G$ . Allora l'ordine di  $H$  divide l'ordine di  $G$ . ■*

Nel paragrafo 2 abbiamo definito l'ordine di un elemento  $a \in G$  come l'ordine del sottogruppo ciclico generato da  $a$ . Pertanto, dal teorema di Lagrange segue che

$$(6.12) \quad \text{L'ordine di un elemento divide l'ordine del gruppo.}$$

Tale fatto ha una conseguenza notevole:

(6.13) COROLLARIO *Supponiamo che un gruppo  $G$  abbia  $p$  elementi e che  $p$  sia un numero primo. Allora, se  $a \in G$  è un qualunque elemento diverso dall'identità,  $G$  è il gruppo ciclico  $\{1, a, \dots, a^{p-1}\}$  generato da  $a$ .*

**Infatti**, essendo  $a \neq 1$ , l'ordine di  $a$  è maggiore di 1 e inoltre divide  $|G| = p$ . Dunque esso è uguale a  $p$ . Poiché  $G$  ha ordine  $p$ , risulta:  $\{1, a, \dots, a^{p-1}\} = G$ . ■

In tal modo abbiamo classificato tutti i gruppi di ordine primo  $p$ . Essi formano un'unica classe di isomorfismo: la classe di un gruppo ciclico di ordine  $p$ .

La formula (6.10) può essere applicata anche quando si ha un omomorfismo. Infatti, sia  $\varphi : G \rightarrow G'$  un omomorfismo. Come si è visto in (5.13), le classi laterali sinistre di  $\ker \varphi$  sono le fibre dell'applicazione  $\varphi$ . Poiché esse sono in corrispondenza biunivoca con gli elementi dell'immagine, si ha:

$$(6.14) \quad [G : \ker \varphi] = |\text{im } \varphi|.$$

Dunque dalla formula (6.10) discende il risultato seguente:

(6.15) COROLLARIO *Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi finiti. Allora:*

$$|G| = |\ker \varphi| \cdot |\text{im } \varphi|.$$

Dunque  $|\ker \varphi|$  divide  $|G|$  e  $|\text{im } \varphi|$  divide sia  $|G|$  che  $|G'|$ .

**Dimostrazione.** La formula si ottiene combinando (6.10) e (6.14), ed implica che  $|\ker \varphi|$  e  $|\text{im } \varphi|$  dividono  $|G|$ . Poiché  $\text{im } \varphi$  è un sottogruppo di  $G'$ ,  $|\text{im } \varphi|$  divide anche  $|G'|$ . ■

Ritorniamo per un momento alla definizione di classe laterale. Abbiamo definito le classi laterali sinistre  $aH$ . Ebbene, possiamo definire anche le classi laterali destre di un sottogruppo  $H$  e ripetere per esse le considerazioni fatte in precedenza per le classi laterali sinistre. Le *classi laterali destre* di un sottogruppo  $H$  sono gli insiemi

$$(6.16) \quad Ha = \{ha \mid h \in H\},$$

che sono classi di equivalenza rispetto alla relazione (*congruenza a destra*):

$$a \equiv b, \text{ se } b = ha, \text{ per qualche } h \in H.$$

Le classi laterali destre non coincidono necessariamente con classi laterali sinistre. Per esempio, le classi laterali destre del sottogruppo  $\{1, xy\}$  di  $S_3$  sono

$$(6.17) \quad \{1, xy\} = H = Hxy, \quad \{x, y\} = Hx = Hy, \quad \{x^2, x^2y\} = Hx^2 = Hx^2y.$$

Tale partizione di  $S_3$  è diversa dalla partizione (6.7) in classi laterali sinistre.

Tuttavia, se  $N$  è un sottogruppo normale, allora le classi laterali destre e le classi laterali sinistre coincidono.

(6.18) PROPOSIZIONE *Un sottogruppo  $H$  di un gruppo  $G$  è normale se e soltanto se ogni classe laterale sinistra è anche una classe laterale destra. Se  $H$  è normale, allora  $aH = Ha$  per ogni  $a \in G$ .*

*Dimostrazione.* Supponiamo che  $H$  sia normale. Allora, per ogni  $h \in H$  e per ogni  $a \in G$ , si ha

$$ah = (aha^{-1})a.$$

Poiché  $H$  è un sottogruppo normale, l'elemento coniugato  $k = aha^{-1}$  sta in  $H$ . Dunque l'elemento  $ah = ka$  sta in  $aH$  e anche in  $Ha$ . Ciò prova che  $aH \subset Ha$ . Analogamente,  $aH \supset Ha$  e quindi le due classi laterali sono uguali. Viceversa, supponiamo che  $H$  non sia normale. Allora esistono elementi  $h \in H$  e  $a \in G$  tali che  $aha^{-1} \notin H$ . Allora  $ah$  appartiene alla classe laterale sinistra  $aH$ , ma non alla classe laterale destra  $Ha$ . Altrimenti, se si avesse:  $ah = h'a$  per qualche  $h' \in H$ , allora risulterebbe:  $aha^{-1} = h' \in H$ , contro le ipotesi. D'altra parte,  $aH$  e  $Ha$  hanno un elemento in comune, precisamente l'elemento  $a$ . Quindi  $aH$  non può essere contenuta in nessun'altra classe laterale destra. Ciò prova che la partizione in classi laterali sinistre è diversa dalla partizione in classi laterali destre. ■

## 7 Restrizione di un omomorfismo a un sottogruppo

Per cercare di capire la struttura di un gruppo complicato, è naturale studiare prima la struttura di alcuni suoi sottogruppi meno complicati. Se si dovesse scegliere il metodo di studio più importante in teoria dei gruppi, sarebbe questo. Per esempio, il gruppo lineare generale  $GL_2$  è molto più complicato del gruppo delle matrici triangolari superiori invertibili. Noi siamo in grado di risolvere praticamente qualunque problema riguardante le matrici triangolari superiori, e del resto, moltiplicando matrici triangolari superiori e inferiori, otteniamo quasi tutte le matrici di  $GL_2$ . Naturalmente il punto centrale è riuscire a ricavare informazioni su tutto il gruppo a partire dai suoi sottogruppi, ma purtroppo non esiste una regola generale su come fare questo. Comunque, ogniqualvolta si studia una nuova costruzione in teoria di gruppi, bisognerebbe studiare i suoi effetti sui sottogruppi. Ecco cosa si intende per *restrizione a un sottogruppo*. In questo paragrafo faremo questo per quanto riguarda sottogruppi e omomorfismi.

Sia  $H$  un sottogruppo di un gruppo  $G$ . Consideriamo dapprima il caso in cui sia dato un secondo sottogruppo  $K$ . La restrizione di  $K$  a  $H$  è l'intersezione  $K \cap H$ .

La proposizione seguente è un semplice esercizio.

(7.1) PROPOSIZIONE *L'intersezione  $K \cap H$  di due sottogruppi è un sottogruppo di  $H$ . Se  $K$  è un sottogruppo normale di  $G$ , allora  $K \cap H$  è un sottogruppo normale di  $H$ . ■*

In generale, non c'è molto altro da dire in proposito; tuttavia, se  $G$  è un gruppo finito, possiamo applicare la formula (6.10), in particolare il teorema di Lagrange, per ottenere informazioni relative all'intersezione. Infatti,  $K \cap H$  è un sottogruppo di  $H$  e anche un sottogruppo di  $K$ , quindi il suo ordine divide entrambi gli ordini  $|H|$  e  $|K|$ . Se  $|H|$  e  $|K|$  non hanno fattori comuni, possiamo concludere che  $K \cap H = \{1\}$ .

Supponiamo ora che sia dato un omomorfismo  $\varphi : G \rightarrow G'$  e che  $H$  sia un sottogruppo di  $G$  come sopra. Allora possiamo *restringere*  $\varphi$  a  $H$ , ottenendo un omomorfismo

$$(7.2) \quad \varphi|_H : H \rightarrow G'.$$

Ciò significa che prendiamo la stessa applicazione  $\varphi$ , ma restringiamo il suo dominio a  $H$ . In altre parole,  $\varphi|_H(h) = \varphi(h)$ , per ogni  $h \in H$ . La restrizione è un omomorfismo poiché tale è  $\varphi$ .

Il nucleo di  $\varphi|_H$  è l'intersezione di  $\ker \varphi$  con  $H$ :

$$(7.3) \quad \ker \varphi|_H = (\ker \varphi) \cap H.$$

Questo è ovvio dalla definizione di nucleo:  $\varphi(h) = 1$  se e soltanto se  $h \in \ker \varphi$ .

Di nuovo, la formula (6.10) può aiutare a descrivere tale restrizione. Infatti, l'immagine di  $\varphi|_H$  è  $\varphi(H)$ . In base al corollario (6.15),  $|\varphi(H)|$  divide sia  $|H|$  che  $|G'|$ . Pertanto, se  $|H|$  e  $|G'|$  non hanno fattori comuni, si ha:  $\varphi(H) = \{1\}$ . Allora possiamo concludere che  $H \subset \ker \varphi$ .

Per esempio, il segno di una permutazione è descritto dall'omomorfismo (4.2b):  $S_n \rightarrow \{+1, -1\}$ . Il codominio di tale omomorfismo ha ordine 2 e il suo nucleo è il gruppo alterno. Se un sottogruppo  $H$  di  $S_n$  ha ordine dispari, allora la restrizione di tale omomorfismo a  $H$  è banale, e ciò significa che  $H$  è contenuto nel gruppo alterno, ossia  $H$  è costituito da permutazioni pari. Ciò accade, ad esempio, se  $H$  è il sottogruppo ciclico generato da una permutazione  $p$  il cui ordine nel gruppo sia dispari. Ne segue che ogni permutazione di ordine dispari è una permutazione pari. Invece, non si può concludere nulla per le permutazioni di ordine pari: esse possono essere dispari o pari.

Dati un omomorfismo  $\varphi : G \rightarrow G'$  e un sottogruppo  $H'$  di  $G'$ , possiamo anche *restringere*  $\varphi$  a  $H'$ . Ma per questo, dobbiamo rimpicciolire opportunamente il dominio di  $\varphi$ . Il modo più naturale è prendere l'intera controimmagine di  $H'$ , riducendo  $G$  il meno possibile:

(7.4) PROPOSIZIONE Sia  $\varphi : G \rightarrow G'$  un omomorfismo e sia  $H'$  un sottogruppo di  $G'$ . Denotiamo con  $\tilde{H}$  la controimmagine di  $H'$

$$\tilde{H} = \varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}.$$

Allora:

- (a)  $\tilde{H}$  è un sottogruppo di  $G$ .
- (b) Se  $H'$  è un sottogruppo normale di  $G'$ , allora  $\tilde{H}$  è un sottogruppo normale di  $G$ .
- (c)  $\tilde{H}$  contiene  $\ker \varphi$ .
- (d) La restrizione di  $\varphi$  a  $\tilde{H}$  definisce un omomorfismo  $\tilde{H} \rightarrow H'$ , il cui nucleo è  $\ker \varphi$ .

Per esempio, consideriamo l'omomorfismo determinante  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ . L'insieme  $P$  dei numeri reali positivi è un sottogruppo di  $\mathbb{R}^*$ , e la sua controimmagine è l'insieme delle matrici  $n \times n$  invertibili con determinante positivo, il quale è un sottogruppo normale di  $GL_n(\mathbb{R})$ .

*Dimostrazione.* La dimostrazione si riduce a un semplice esercizio, ma occorre tener presente che  $\varphi^{-1}$  non è un'applicazione. Per definizione,  $\tilde{H}$  è l'insieme degli elementi  $x \in G$  tali che  $\varphi(x) \in H'$ . Verifichiamo innanzitutto che  $\tilde{H}$  è un sottogruppo di  $G$ . (*Chiusura*). Supponiamo che  $x, y \in \tilde{H}$ ; dunque  $\varphi(x)$  e  $\varphi(y)$  stanno in  $H'$ , ed essendo  $H'$  un sottogruppo, anche  $\varphi(x)\varphi(y) \in H'$ . Poiché  $\varphi$  è un omomorfismo, si ha:  $\varphi(x)\varphi(y) = \varphi(xy) \in H'$  e quindi  $xy \in \tilde{H}$ . (*Identità*).  $1 \in \tilde{H}$  poiché  $\varphi(1) = 1 \in H'$ . (*Inversi*). Supponiamo che  $x \in \tilde{H}$ , cioè  $\varphi(x) \in H'$ ; allora  $\varphi(x)^{-1} \in H'$ , essendo  $H'$  un sottogruppo. Poiché  $\varphi$  è un omomorfismo, si ha:  $\varphi(x)^{-1} = \varphi(x^{-1})$  e quindi  $x^{-1} \in \tilde{H}$ .

Supponiamo che  $H'$  sia un sottogruppo normale, e sia  $x \in \tilde{H}$  e  $g \in G$ . Allora  $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1}$  e  $\varphi(x) \in H'$ . Pertanto  $\varphi(gxg^{-1}) \in H'$  e quindi  $gxg^{-1} \in \tilde{H}$ . Inoltre,  $\tilde{H}$  contiene  $\ker \varphi$ , poiché, se  $x \in \ker \varphi$ , allora  $\varphi(x) = 1$ , e  $1 \in H'$ . Dunque  $x \in \varphi^{-1}(H')$ . A questo punto la (d) dovrebbe essere chiara. ■

## 8 Prodotti di gruppi

Siano  $G, G'$  due gruppi. L'insieme prodotto  $G \times G'$  può essere dotato di una struttura di gruppo mediante la moltiplicazione componenti per componente. Ossia, definiamo la moltiplicazione tra coppie ordinate mediante la regola:

$$(8.1) \quad (a, a'), (b, b') \mapsto (ab, a'b'),$$

con  $a, b \in G$  e  $a', b' \in G'$ . La coppia  $(1, 1)$  è un'identità, e  $(a, a')^{-1} = (a^{-1}, a'^{-1})$ . La proprietà associativa in  $G \times G'$  segue dal fatto che essa vale in  $G$  e in  $G'$ . Il gruppo così ottenuto è chiamato il *prodotto* di  $G$  e  $G'$  e si denota con  $G \times G'$ . Il suo ordine è il prodotto degli ordini di  $G$  e  $G'$ .

Il gruppo prodotto è collegato ai due fattori  $G, G'$  in un modo semplice, che può essere riassunto mediante alcuni omomorfismi:

$$(8.2) \quad \begin{array}{ccc} G & & G \\ \searrow i & & \nearrow p \\ & G \times G' & \\ \nearrow i' & & \searrow p' \\ G' & & G' \end{array}$$

definiti da

$$\begin{aligned} i(x) &= (x, 1), & i'(x') &= (1, x'), \\ p(x, x') &= x, & p'(x, x') &= x'. \end{aligned}$$

Le applicazioni  $i, i'$  sono iniettive e identificano  $G, G'$  con i sottogruppi  $G \times 1, 1 \times G'$  di  $G \times G'$ . Le applicazioni  $p, p'$  sono suriettive,  $\ker p = 1 \times G'$  e  $\ker p' = G \times 1$ . Tali applicazioni  $p, p'$  vengono chiamate *proiezioni*. Inoltre,  $G \times 1$  e  $1 \times G'$  sono sottogruppi *normali* di  $G \times G'$ , essendo nuclei di omomorfismi.

(8.3) PROPOSIZIONE (Proprietà delle applicazioni relative ai prodotti) Sia  $H$  un gruppo. Gli omomorfismi  $\Phi : H \rightarrow G \times G'$  sono in corrispondenza biunivoca con le coppie ordinate di omomorfismi  $(\varphi, \varphi')$ :

$$\varphi : H \rightarrow G, \quad \varphi' : H \rightarrow G'.$$

Il nucleo di  $\Phi$  è l'intersezione  $(\ker \varphi) \cap (\ker \varphi')$ .

*Dimostrazione.* Data una coppia ordinata  $(\varphi, \varphi')$  di omomorfismi, definiamo l'omomorfismo corrispondente

$$\Phi : H \rightarrow G \times G'$$

mediante la regola:  $\Phi(h) = (\varphi(h), \varphi'(h))$ . Si vede facilmente che tale applicazione è un omomorfismo. Viceversa, dato  $\Phi$ , otteniamo  $\varphi$  e  $\varphi'$  mediante la composizione con le proiezioni cioè:

$$\varphi = p \Phi, \quad \varphi' = p' \Phi.$$

È ovvio che  $\Phi(h) = (1, 1)$  se e soltanto se  $\varphi(h) = 1$  e  $\varphi'(h) = 1$ ; quindi  $\ker \Phi = (\ker \varphi) \cap (\ker \varphi')$ . ■

È chiaro che sarebbe bello poter esprimere un gruppo assegnato  $G$  come un prodotto, ossia trovare due gruppi  $H$  e  $H'$  tali che  $G$  sia isomorfo al prodotto  $H \times H'$ . Infatti i gruppi  $H$ ,  $H'$  sarebbero più piccoli e pertanto più semplici e inoltre, la relazione tra  $H \times H'$  e i suoi fattori si comprende facilmente. Purtroppo, è molto raro che un gruppo assegnato sia un prodotto, ma a volte succede.

Per esempio, è abbastanza sorprendente che un gruppo ciclico di ordine 6 possa essere decomposto: un gruppo ciclico  $C_6$  di ordine 6 è isomorfo al prodotto  $C_2 \times C_3$  di due gruppi ciclici di ordini 2 e 3. Ciò si può dimostrare usando la proprietà delle applicazioni relative ai prodotti appena discussa. Scriviamo:  $C_6 = \{1, x, x^2, \dots, x^5\}$ ,  $C_2 = \{1, y\}$ ,  $C_3 = \{1, z, z^2\}$ . L'applicazione

$$\varphi : C_6 \rightarrow C_2 \times C_3$$

definita da  $\varphi(x^i) = (y^i, z^i)$  è un omomorfismo, e il suo nucleo è l'insieme degli elementi  $x^i$  tali che  $y^i = 1$  e  $z^i = 1$ . Ora  $y^i = 1$  se e solo se  $i$  è divisibile per 2, mentre  $z^i = 1$  se e solo se  $i$  è divisibile per 3. Non esiste alcun intero compreso tra 1 e 5 che sia divisibile per 2 e per 3; allora  $\ker \varphi = \{1\}$ , e  $\varphi$  è iniettivo. Poiché entrambi i gruppi hanno ordine 6,  $\varphi$  è un'applicazione biettiva e quindi è un isomorfismo. ■

La stessa argomentazione vale per un gruppo *ciclico* di ordine  $rs$ , ogni volta che i due interi  $r$  e  $s$  sono primi tra loro.

(8.4) PROPOSIZIONE *Siano  $r, s$  interi primi tra loro. Un gruppo ciclico di ordine  $rs$  è isomorfo al prodotto di un gruppo ciclico di ordine  $r$  e un gruppo ciclico di ordine  $s$ .* ■

D'altra parte, un gruppo ciclico di ordine 4 *non* è isomorfo al prodotto di due gruppi ciclici di ordine 2. Infatti, si vede facilmente che ogni elemento di  $C_2 \times C_2$  ha ordine 1 o 2, mentre un gruppo ciclico di ordine 4 contiene due elementi di ordine 4. Inoltre, la proposizione non dice nulla a proposito di un gruppo che non è ciclico.

Siano  $A$  e  $B$  sottoinsiemi di un gruppo  $G$ . Denotiamo allora l'insieme dei prodotti di elementi di  $A$  e di  $B$  con

$$(8.5) \quad AB = \{x \in G \mid x = ab \text{ per qualche } a \in A \text{ e } b \in B\}.$$

La proposizione seguente caratterizza i gruppi prodotto.

(8.6) PROPOSIZIONE *Siano  $H$  e  $K$  sottogruppi di un gruppo  $G$ .*

(a) *Se  $H \cap K = \{1\}$ , l'applicazione prodotto  $p : H \times K \rightarrow G$  definita da:  $p(h, k) = hk$  è iniettiva. La sua immagine è il sottoinsieme  $HK$ .*

- (b) *Se  $H$  o  $K$  è un sottogruppo normale di  $G$ , allora gli insiemi prodotto  $HK$  e  $KH$  sono uguali e, inoltre,  $HK$  è un sottogruppo di  $G$ .*
- (c) *Se  $H$  e  $K$  sono sottogruppi normali,  $H \cap K = \{1\}$  e  $HK = G$ , allora  $G$  è isomorfo al gruppo prodotto  $H \times K$ .*

**Dimostrazione.** (a) Siano  $(h_1, k_1), (h_2, k_2)$  elementi di  $H \times K$  tali che  $h_1k_1 = h_2k_2$ . Moltiplicando ambo i membri a sinistra per  $h_1^{-1}$  e a destra per  $k_2^{-1}$ , si ottiene  $k_1k_2^{-1} = h_1^{-1}h_2$ . Poiché  $H \cap K = \{1\}$ , si ha  $k_1k_2^{-1} = h_1^{-1}h_2 = 1$ , da cui  $h_1 = h_2$  e  $k_1 = k_2$ . Quindi  $p$  è iniettiva.

(b) Supponiamo che  $H$  sia un sottogruppo normale di  $G$  e consideriamo due elementi  $h \in H$  e  $k \in K$ . Osserviamo che  $kh = (khk^{-1})k$ . Poiché  $H$  è normale,  $khk^{-1} \in H$ . Pertanto  $kh \in HK$ , e ciò dimostra che  $HK \subset KH$ . L'inclusione opposta si dimostra allo stesso modo. A questo punto si prova facilmente che  $HK$  è un sottogruppo. Per la chiusura rispetto alla moltiplicazione, basta osservare che in un prodotto  $(hk)(h'k') = h(kh')k'$ , il termine centrale  $kh'$  sta in  $HK = KH$ , diciamo  $kh' = h''k''$ , sicché  $hk'h'k' = (hh'')(k''k') \in HK$ . È chiaro poi che  $1 = 1 \cdot 1 \in HK$ . Vale infine la chiusura rispetto agli inversi:  $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ . Dunque  $HK$  è un sottogruppo. La dimostrazione è del tutto analoga nel caso in cui  $K$  è normale.

(c) Supponiamo che  $H$  e  $K$  siano normali e che  $H \cap K = \{1\}$ . Consideriamo il prodotto  $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$ . Poiché  $K$  è un sottogruppo normale, il termine a sinistra sta in  $K$ . Poiché  $H$  è normale, il termine a destra sta in  $H$ . Dunque tale prodotto sta nell'intersezione  $H \cap K$ , ossia  $hkh^{-1}k^{-1} = 1$ . Pertanto  $hk = kh$ . A questo punto, il fatto che  $p$  è un omomorfismo segue direttamente. Infatti, nel gruppo  $H \times K$  la moltiplicazione è definita da:  $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$ , e tale elemento corrisponde a  $h_1h_2k_1k_2$  in  $G$ , mentre in  $G$  il prodotto di  $h_1k_1$  e  $h_2k_2$  è dato da  $h_1k_1h_2k_2$ . Poiché  $h_2k_1 = k_1h_2$ , i prodotti sono uguali. Per concludere, basta osservare che, dal punto (a) precedente, segue che  $p$  è iniettivo, mentre l'ipotesi che  $HK = G$  mostra che  $p$  è suriettivo. ■

È importante osservare che l'applicazione prodotto  $p : H \times K \rightarrow G$  non è un omomorfismo di gruppi, a meno che i due sottogruppi non commutino tra loro.

## 9 Aritmetica modulare

In questo paragrafo studieremo la nozione, introdotta da Gauss, di congruenza tra interi, che è uno dei concetti più importanti in teoria dei numeri. Supporremo sempre di lavorare con un intero positivo  $n$  fissato arbitrariamente.

Due interi  $a, b$  si dicono *congrui modulo n*, e si scrive

$$(9.1) \quad a \equiv b \pmod{n},$$

se  $n$  divide  $b - a$ , ossia, se  $b = a + nk$  per qualche intero  $k$ . È facile verificare che la congruenza modulo  $n$  è una relazione di equivalenza. Dunque possiamo considerare le classi di equivalenza, chiamate *classi di congruenza modulo n* o *classi resto modulo n*, definite da tale relazione, come si è visto nel paragrafo 5. La classe di congruenza di un intero  $a$  si indica con il simbolo  $\bar{a}$ . Essa è l'insieme degli interi

$$(9.2) \quad \bar{a} = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}.$$

Se  $a$  e  $b$  sono interi, l'equazione  $\bar{a} = \bar{b}$  significa che  $n$  divide  $b - a$ .

La classe di congruenza di 0 è il sottogruppo

$$\bar{0} = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}$$

del gruppo additivo  $\mathbb{Z}$  costituito da tutti i multipli di  $n$ . Le altre classi di congruenza sono le classi laterali di questo sottogruppo. Purtroppo, si presenta qui un piccolo problema di notazioni, poiché la notazione  $n\mathbb{Z}$  somiglia a quella usata per le classi laterali. Invece  $n\mathbb{Z}$  non è una classe laterale, ma è un sottogruppo di  $\mathbb{Z}$ . La notazione per una classe laterale di un sottogruppo  $H$  analoga a (6.1), ma espressa con la notazione additiva per la legge di composizione, è:

$$a + H = \{a + h \mid h \in H\}.$$

Per evitare di scrivere una classe laterale come  $a + n\mathbb{Z}$ , denotiamo il sottogruppo  $n\mathbb{Z}$  con  $H$ . Allora le classi laterali di  $H$  sono gli insiemi

$$(9.3) \quad a + H = \{a + nk \mid k \in \mathbb{Z}\}.$$

Esse sono le classi di congruenza  $\bar{a} = a + H$ .

Gli  $n$  interi  $0, 1, \dots, n-1$  formano un insieme naturale di elementi rappresentativi per le classi di congruenza:

(9.4) PROPOSIZIONE *Esistono n classi di congruenza modulo n, precisamente:*

$$\bar{0}, \bar{1}, \dots, \bar{n-1}.$$

Ossia, l'indice  $[\mathbb{Z} : n\mathbb{Z}]$  del sottogruppo  $n\mathbb{Z}$  in  $\mathbb{Z}$  è  $n$ .

*Dimostrazione.* Sia  $a$  un numero intero. Allora, utilizzando la divisione con resto, possiamo scrivere:

$$a = nq + r,$$

dove  $q, r$  sono interi e il resto  $r$  varia nell'intervallo  $0 \leq r < n$ . Allora  $a$  è congruo al resto:  $a \equiv r \pmod{n}$ . Dunque  $\bar{a} = \bar{r}$ . Ciò prova che  $\bar{a}$  è una delle classi di congruenza elencate nella proposizione. D'altra parte, se  $a$  e  $b$  sono due interi distinti minori di  $n$ , diciamo  $a < b$ , allora  $b - a$  è minore di  $n$  e diverso da zero, sicché  $n$  non divide  $b - a$ . Dunque  $a \not\equiv b \pmod{n}$ , ossia  $\bar{a} \neq \bar{b}$ . Pertanto le  $n$  classi  $\bar{0}, \bar{1}, \dots, \bar{n-1}$  sono tutte distinte. ■

La proprietà più importante delle classi di congruenza è che l'addizione e la moltiplicazione tra numeri interi conservano la congruenza modulo  $n$  e pertanto tali leggi possono essere usate per definire l'addizione e la moltiplicazione tra classi di congruenza. Ciò si esprime dicendo che l'insieme delle classi di congruenza forma un *anello*. Studieremo gli anelli nel capitolo 10.

Siano  $\bar{a}$  e  $\bar{b}$  classi di congruenza rappresentate da interi  $a$  e  $b$ . La loro *somma* è definita come la classe di congruenza di  $a+b$ , e il loro *prodotto* è definito come la classe di  $ab$ . In altre parole, definiamo:

$$(9.5) \quad \bar{a} + \bar{b} = \overline{a+b} \quad \text{e} \quad \bar{a}\bar{b} = \overline{ab}.$$

Questa definizione richiede qualche giustificazione, poiché la stessa classe di congruenza  $\bar{a}$  può essere rappresentata da molti interi diversi. Un qualsiasi intero  $a'$  congruo ad  $a$  modulo  $n$  rappresenta la stessa classe. Così, sarebbe bene se fosse vero che, se  $a' \equiv a$  e  $b' \equiv b$ , allora  $a' + b' \equiv a + b$  e  $a'b' \equiv ab$ . Fortunatamente è proprio così.

(9.6) LEMMA *Se  $a' \equiv a$  e  $b' \equiv b$  (modulo n), allora  $a' + b' \equiv a + b$  (modulo n) e  $a'b' \equiv ab$  (modulo n).*

*Dimostrazione.* Supponiamo che  $a' \equiv a$  e  $b' \equiv b$ , cioè  $a' = a + nr$  e  $b' = b + ns$ , con  $r, s$  interi opportuni. Allora  $a' + b' = a + b + n(r+s)$ , quindi  $a' + b' \equiv a + b$ . Analogamente,  $a'b' = (a + nr)(b + ns) = ab + n(as + rb + nrs)$ , da cui segue che  $a'b' \equiv ab$ , come richiesto. ■

Le proprietà associativa, commutativa e distributiva valgono per le leggi di composizione (9.5), poiché valgono per l'addizione e la moltiplicazione tra numeri interi. Per esempio, la verifica formale della legge distributiva è la seguente:

$$(\text{definizione di } + \text{ e } \times \text{ per classi di congruenza}) \quad \bar{a}(\bar{b} + \bar{c}) = \overline{a(b+c)} = \overline{ab+ac} =$$

$$(\text{proprietà distributiva degli interi}) \quad = \overline{ab+ac} =$$

$$(\text{definizione di } + \text{ e } \times \text{ per classi di congruenza}). \quad = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{ab} + \overline{ac} = \overline{ab+ac} =$$

L'insieme delle classi di congruenza modulo  $n$  si denota di solito con

$$(9.7) \quad \mathbb{Z}/n\mathbb{Z}.$$

Le addizioni, le sottrazioni e le moltiplicazioni in  $\mathbb{Z}/n\mathbb{Z}$  possono essere effettuate esplicitamente lavorando con gli interi e prendendo i resti nella divisione per  $n$ . Questo è il significato delle formule (9.5). Esse dicono che l'applicazione

$$(9.8) \quad \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

che manda un intero  $a$  nella sua classe di congruenza  $\bar{a}$  è compatibile con l'addizione e la moltiplicazione. Pertanto i calcoli possono essere fatti sugli interi e riportati in  $\mathbb{Z}/n\mathbb{Z}$  alla fine. Tuttavia, tale procedimento non è efficiente, poiché i calcoli sono più semplici se i numeri si mantengono piccoli. Ebbene, noi possiamo tenerli piccoli calcolando il resto dopo che un po' di calcoli sono stati effettuati. Così, se  $n = 13$ , sicché

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{12}\},$$

allora

$$(\bar{7} + \bar{9})(\bar{11} + \bar{6})$$

può essere calcolato, osservando che  $\bar{7} + \bar{9} = \bar{3}$ ,  $\bar{11} + \bar{6} = \bar{4}$ ,  $\bar{3} \cdot \bar{4} = \bar{12}$ .

Le barre sopra i numeri appesantiscono le notazioni, sicché spesso vengono omesse. L'unica cosa da ricordare è la regola seguente:

$$(9.9) \quad \text{Dire: } a = b \text{ in } \mathbb{Z}/n\mathbb{Z} \text{ significa: } a \equiv b \text{ (modulo } n).$$

## 10 Gruppi quoziante

Abbiamo visto nell'ultimo paragrafo che le classi di congruenza degli interi modulo  $n$  sono le classi laterali del sottogruppo  $n\mathbb{Z}$  di  $\mathbb{Z}$ . Pertanto, l'addizione tra classi di congruenza fornisce una legge di composizione nell'insieme delle classi laterali. In questo paragrafo dimostreremo che è possibile definire una legge di composizione tra le classi laterali di un sottogruppo normale  $N$  di un qualsiasi gruppo  $G$ . Faremo vedere inoltre in che modo l'insieme delle classi laterali risulta essere un gruppo, chiamato *gruppo quoziante*.

L'addizione tra angoli è un esempio familiare di costruzione del quoziante. Ogni numero reale rappresenta un angolo, e due numeri reali rappresentano uno stesso angolo se differiscono per un multiplo intero di  $2\pi$ . Ciò è ben noto. Il punto centrale dell'esempio è che l'addizione tra angoli è definita mediante l'addizione tra numeri reali. Il gruppo degli angoli è un gruppo quoziante, in cui  $G = \mathbb{R}$  e  $N$  è il sottogruppo dei multipli interi di  $2\pi$ .

Richiamiamo ora una notazione introdotta nel paragrafo 8. Se  $A$  e  $B$  sono sottoinsiemi di un gruppo  $G$ , allora

$$AB = \{ab \mid a \in A, b \in B\}.$$

Chiameremo tale sottoinsieme il *prodotto* dei due sottoinsiemi  $A$  e  $B$ , anche se, in altri contesti, lo stesso termine indica l'insieme  $A \times B$ .

(10.1) LEMMA Sia  $N$  un sottogruppo normale di un gruppo  $G$ . Allora il prodotto di due classi laterali  $aN$ ,  $bN$  è ancora una classe laterale, precisamente:

$$(aN)(bN) = abN.$$

*Dimostrazione.* Osserviamo che  $Nb = bN$ , in base a (6.18) e inoltre  $NN = N$ , essendo  $N$  un sottogruppo. A questo punto, con un po' di passaggi formali, si dimostra il lemma:

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN. \blacksquare$$

Il lemma (10.1) permette di definire la moltiplicazione tra due classi laterali  $C_1, C_2$  mediante la regola seguente:  $C_1C_2$  è l'insieme prodotto. Per calcolare la classe laterale prodotto, basta scegliere arbitrariamente due elementi  $a \in C_1$  e  $b \in C_2$ , così che  $C_1 = aN$  e  $C_2 = bN$ . Allora  $C_1C_2 = abN$  è la classe laterale contenente  $ab$ . Questo è il modo in cui l'addizione tra classi di congruenza è stata definita nell'ultimo paragrafo.

Per esempio, consideriamo le classi laterali della circonferenza unitaria  $N$  in  $G = \mathbb{C}^*$ . Come abbiamo visto nel paragrafo 5, tali classi laterali sono le circonferenze concentriche

$$C_r = \{z \mid |z| = r\}.$$

La formula (10.1) afferma in questo caso che, se  $|\alpha| = r$  e  $|\beta| = s$ , allora  $|\alpha\beta| = rs$ :

$$C_r C_s = C_{rs}.$$

L'ipotesi che  $N$  sia un sottogruppo normale di  $G$  è essenziale per la validità della formula (10.1). Infatti, se  $H$  non è un sottogruppo normale di  $G$ , allora esisteranno classi laterali sinistre  $C_1, C_2$  di  $H$  in  $G$ , il cui prodotto non è contenuto in una classe laterale sinistra. Infatti, dire che  $H$  non è normale significa che esistono elementi  $h \in H$  e  $a \in G$  tali che  $aha^{-1} \notin H$ . Allora l'insieme

$$(10.2) \quad (aH)(a^{-1}H)$$

non è contenuto in nessuna classe laterale sinistra. Esso contiene l'elemento  $aha^{-1}h^{-1} = 1$ , che appartiene a  $H$ , quindi, se l'insieme (10.2) fosse contenuto in

una classe laterale, questa dovrebbe essere necessariamente la classe  $H = 1H$ . Ma l'insieme (10.2) contiene anche l'elemento  $aha^{-1}1$ , che non appartiene a  $H$ . ■

L'insieme delle classi laterali di un sottogruppo normale  $N$  di un gruppo  $G$  si denota di solito con il simbolo

$$(10.3) \quad G/N = \text{insieme delle classi laterali di } N \text{ in } G.$$

Ciò è in accordo con la notazione  $\mathbb{Z}/n\mathbb{Z}$  introdotta nel paragrafo 9. Un'altra notazione che useremo frequentemente per l'insieme delle classi laterali è la notazione con la barra:

$$G/N = \overline{G} \quad \text{e} \quad aN = \overline{a},$$

sicché  $\overline{a}$  denota la classe laterale contenente  $a$ . Tale notazione è quella naturale quando si vuol considerare l'applicazione

$$(10.4) \quad \pi : G \rightarrow \overline{G} = G/N \text{ che manda } a \text{ in } \overline{a} = aN.$$

(10.5) **TEOREMA** *Rispetto alla legge di composizione definita sopra,  $\overline{G} = G/N$  è un gruppo, l'applicazione  $\pi$  definita in (10.4) è un omomorfismo e il suo nucleo è  $N$ .*

L'ordine di  $G/N$  è l'indice  $[G : N]$  di  $N$  in  $G$ .

(10.6) **COROLLARIO** *Ogni sottogruppo normale di un gruppo  $G$  è il nucleo di un omomorfismo. ■*

Questo corollario permette di utilizzare tutto ciò che conosciamo sugli omomorfismi per comprendere meglio i sottogruppi normali.

*Dimostrazione del teorema (10.5).* Osserviamo innanzitutto che  $\pi$  è compatibile con le leggi di composizione: infatti, dato che la moltiplicazione tra classi laterali è definita mediante la moltiplicazione tra elementi, si ha:  $\pi(a)\pi(b) = \pi(ab)$ . Inoltre, gli elementi di  $G$  aventi la stessa immagine dell'identità 1 sono quelli appartenenti a  $N$ :  $1 = 1N = N$ . Infine gli assiomi di gruppo sono verificati in  $\overline{G}$ , in virtù del seguente lemma:

(10.7) **LEMMA** *Sia  $G$  un gruppo e sia  $S$  un insieme dotato di una legge di composizione. Sia  $\varphi : G \rightarrow S$  un'applicazione suriettiva tale che  $\varphi(a)\varphi(b) = \varphi(ab)$  per ogni scelta di  $a, b$  in  $G$ . Allora  $S$  è un gruppo.*

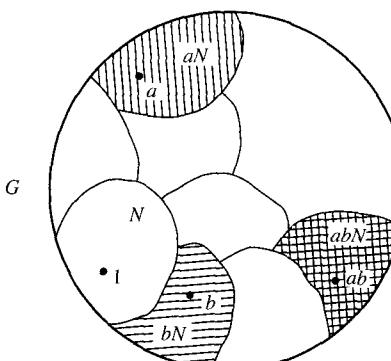
*Dimostrazione.* In realtà, qualsiasi proprietà riguardante la moltiplicazione che vale in  $G$  può essere trasportata a  $S$ . Vediamo ad esempio la dimostrazione della

proprietà associativa. Dati  $s_1, s_2, s_3 \in S$ , sappiamo che  $s_i = \varphi(a_i)$  per qualche  $a_i \in G$ , poiché  $\varphi$  è suriettiva. Allora:

$$\begin{aligned} (s_1s_2)s_3 &= (\varphi(a_1)\varphi(a_2))\varphi(a_3) = \varphi(a_1a_2)\varphi(a_3) = \varphi(a_1a_2a_3) = \\ &= \varphi(a_1)\varphi(a_2a_3) = \varphi(a_1)(\varphi(a_2)\varphi(a_3)) = s_1(s_2s_3). \end{aligned}$$

La verifica degli altri assiomi di gruppo è lasciata come esercizio. ■

(10.8)



Rappresentazione schematica della moltiplicazione tra classi laterali.

Per esempio, sia  $G = \mathbb{R}^*$  il gruppo moltiplicativo dei numeri reali non nulli e sia  $P$  il sottogruppo dei numeri reali positivi. Vi sono due classi laterali, precisamente  $P$  e  $-P = \{\text{numeri reali negativi}\}$ , e  $\overline{G} = G/P$  è il gruppo formato da due elementi. La regola di moltiplicazione è quella ben nota:  $(Neg)(Neg) = (Pos)$ , e così via.

La costruzione del gruppo quoziante è collegata ad un omomorfismo generale di gruppi  $\varphi : G \rightarrow G'$  nel modo seguente:

(10.9) **TEOREMA (Primo teorema di isomorfismo)** *Sia  $\varphi : G \rightarrow G'$  un omomorfismo suriettivo di gruppi e sia  $N = \ker \varphi$ . Allora  $G/N$  è isomorfo a  $G'$  mediante l'applicazione  $\bar{\varphi}$  che manda la classe laterale  $\overline{a} = aN$  in  $\varphi(a)$ :*

$$\bar{\varphi}(\overline{a}) = \varphi(a),$$

come nella figura seguente:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & \swarrow \bar{\varphi} & \\ G/\ker \varphi & & \end{array}$$

Questo è il metodo fondamentale per identificare i gruppi quoziante. Per esempio, l'applicazione "valore assoluto"  $\mathbb{C}^* \rightarrow \mathbb{R}^*$  manda i numeri complessi non nulli

nei numeri reali positivi, e il suo nucleo è la circonferenza unitaria  $U$ . Pertanto il gruppo quoziante  $\mathbb{C}^*/U$  è isomorfo al gruppo moltiplicativo dei numeri reali positivi. Analogamente, l'applicazione "determinante" è un omomorfismo suriettivo  $GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ , il cui nucleo è il gruppo lineare speciale  $SL_n(\mathbb{R})$ . Pertanto il gruppo quoziante  $GL_n(\mathbb{R})/SL_n(\mathbb{R})$  è isomorfo a  $\mathbb{R}^*$ .

*Dimostrazione.* In base alla proposizione (5.13), le fibre non vuote di  $\varphi$  sono le classi laterali  $aN$ . Dunque possiamo considerare  $\overline{G}$  in due modi: o come l'insieme delle classi laterali oppure come l'insieme delle fibre non vuote di  $\varphi$ . Pertanto l'applicazione cercata è quella definita in (5.10) per un'applicazione tra insiemi. Essa manda biettivamente  $\overline{G}$  sull'immagine di  $\varphi$ , la quale coincide con  $G'$ , poiché  $\varphi$  è suriettivo. Per costruzione, essa è compatibile con la moltiplicazione:  $\overline{\varphi}(ab) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a)\overline{\varphi}(b)$ . ■

Vi sono molte specie diverse di grandezze che a malapena si possono descrivere; nascono allora le diverse branche della matematica, ciascuna dedicata a un tipo particolare di grandezza.

Leonhard Euler

## Esercizi

### 1 Definizione di gruppo

1. (a) Verificare le relazioni (1.17) e (1.18) mediante calcoli esplicativi.
- (b) Costruire una tabella di moltiplicazione per  $S_3$ .
2. (a) Dimostrare che  $GL_n(\mathbb{R})$  è un gruppo.
- (b) Dimostrare che  $S_n$  è un gruppo.
3. Sia  $S$  un insieme dotato di una legge di composizione associativa e di un'identità. Dimostrare che il sottoinsieme di  $S$  costituito dagli elementi invertibili è un gruppo.
4. Data in un gruppo l'equazione  $xyz^{-1}w = 1$ , ricavare  $y$ .
5. Supponiamo che in un gruppo  $G$  valga l'equazione  $xyz = 1$ . Segue da ciò che  $yzx = 1$ , oppure che  $yxz = 1$ ?
6. Scrivere tutti i modi possibili per formare un prodotto di quattro elementi  $a, b, c, d$  nell'ordine assegnato.
7. Sia  $S$  un insieme qualsiasi. Dimostrare che la legge di composizione definita da  $ab = a$  è associativa.
8. Dare un esempio di matrici  $2 \times 2$  tali che  $A^{-1}B \neq BA^{-1}$ .
9. Dimostrare che, se  $ab = a$  in un gruppo, allora  $b = 1$  e, se  $ab = 1$ , allora  $b = a^{-1}$ .
10. Siano  $a, b$  elementi di un gruppo  $G$ . Dimostrare che l'equazione  $ax = b$  possiede una e una sola soluzione in  $G$ .
11. Sia  $G$  un gruppo, con notazione moltiplicativa. Definiamo il *gruppo opposto*  $G^0$  con la seguente legge di composizione  $a \circ b$ : l'insieme sostegno è ancora  $G$ , ma la legge di composizione è l'opposta, ossia, definita da  $a \circ b = ba$ . Dimostrare che tale legge definisce un gruppo.

### 2 Sottogruppi

1. Determinare esplicitamente gli elementi del gruppo ciclico generato dalla matrice  $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ .
2. Siano  $a, b$  elementi di un gruppo  $G$ . Supponiamo che  $a$  abbia ordine 5 e che  $a^3b = ba^3$ . Dimostrare che  $ab = ba$ .
3. Quali dei seguenti insiemi sono sottogruppi?
  - (a)  $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ .
  - (b)  $\{1, -1\} \subset \mathbb{R}^*$ .
  - (c) L'insieme degli interi positivi in  $\mathbb{Z}$ .
  - (d) L'insieme dei reali positivi in  $\mathbb{R}^*$ .
  - (e) L'insieme di tutte le matrici  $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ , con  $a \neq 0$ , in  $GL_2(\mathbb{R})$ .
4. Dimostrare che un sottoinsieme non vuoto  $H$  di un gruppo  $G$  è un sottogruppo se per ogni scelta di  $x, y$  in  $H$  anche l'elemento  $xy^{-1}$  sta in  $H$ .
5. Una radice  $n$ -esima dell'unità è un numero complesso  $z$  tale che  $z^n = 1$ . Dimostrare che le radici  $n$ -esime dell'unità formano un sottogruppo ciclico di  $\mathbb{C}^*$  di ordine  $n$ .
6. (a) Trovare generatori e relazioni analoghe alle (2.13) per il gruppo quadrinomio di Klein.  
 (b) Trovare tutti i sottogruppi del gruppo quadrinomio di Klein.
7. Siano  $a$  e  $b$  interi.
  - (a) Dimostrare che il sottoinsieme  $a\mathbb{Z} + b\mathbb{Z}$  è un sottogruppo di  $\mathbb{Z}$ .
  - (b) Dimostrare che  $a$  e  $b+7a$  generano il sottogruppo  $a\mathbb{Z} + b\mathbb{Z}$ .
8. Costruire una tabella di moltiplicazione per il gruppo di quaternioni  $H$ .
9. Sia  $H$  il sottogruppo generato da due elementi  $a, b$  di un gruppo  $G$ . Dimostrare che se  $ab = ba$ , allora  $H$  è un gruppo abeliano.
10. (a) Supponiamo che un elemento  $x$  di un gruppo abbia ordine  $rs$ . Determinare l'ordine di  $x^r$ .  
 (b) Supponendo che un elemento  $x$  abbia ordine  $n$ , con  $n$  arbitrario, qual è l'ordine di  $x^r$ ?
11. Dimostrare che in un gruppo gli ordini di  $ab$  e di  $ba$  sono uguali.
12. Descrivere tutti i gruppi  $G$  che non contengono sottogruppi propri.
13. Dimostrare che ogni sottogruppo di un gruppo ciclico è ciclico.
14. Sia  $G$  un gruppo ciclico di ordine  $n$  e sia  $r$  un intero che divide  $n$ . Dimostrare che  $G$  contiene uno ed un solo sottogruppo di ordine  $r$ .

15. (a) Nella definizione di sottogruppo, si richiede che l'identità di  $H$  sia l'identità di  $G$ . Si potrebbe richiedere soltanto che  $H$  abbia un'identità, non necessariamente uguale all'identità di  $G$ . Dimostrare che, se  $H$  possiede un'identità, allora essa è l'identità di  $G$ , per cui tale definizione risulterebbe equivalente a quella data.
- (b) Dimostrare la proprietà analoga per gli inversi.
16. (a) Sia  $G$  un gruppo ciclico di ordine 6. Quanti sono i generatori di  $G$ ?
- (b) Rispondere alla stessa domanda per i gruppi ciclici di ordine 5, 8 e 10.
- (c) Quanti elementi di un gruppo ciclico di ordine  $n$  sono generatori del gruppo?
17. Dimostrare che un gruppo in cui ogni elemento diverso dall'identità ha ordine 2 è abeliano.
18. In base alla proposizione (2.18) del capitolo 1, le matrici elementari generano il gruppo  $GL_n(\mathbb{R})$ .
- (a) Dimostrare che le matrici elementari del primo e del terzo tipo sono sufficienti per generare il gruppo.
- (b) Il *gruppo lineare speciale*  $SL_n(\mathbb{R})$  è l'insieme delle matrici  $n \times n$  reali con determinante 1. Dimostrare che  $SL_n(\mathbb{R})$  è un sottogruppo di  $GL_n(\mathbb{R})$ .
- \*(c) Utilizzare la riduzione per righe per dimostrare che le matrici elementari del primo tipo generano  $SL_n(\mathbb{R})$ . Esaminare per primo il caso delle matrici  $2 \times 2$ .
19. Determinare il numero degli elementi di ordine 2 nel gruppo simmetrico  $S_4$ .
20. (a) Siano  $a, b$  elementi di un gruppo abeliano, rispettivamente di ordine  $m, n$ . Cosa si può dire per l'ordine del loro prodotto  $ab$ ?
- \*(b) Mostrare con un esempio che il prodotto di elementi di ordine finito in un gruppo non abeliano non ha necessariamente ordine finito.
21. Dimostrare che l'insieme degli elementi di ordine finito in un gruppo abeliano è un sottogruppo.
22. Dimostrare che il massimo comune divisore di  $a$  e  $b$ , definito nel paragrafo 2, può essere ottenuto fattorizzando  $a$  e  $b$  in prodotti di numeri primi e raccogliendo i fattori comuni.

### 3 Isomorfismi

1. Dimostrare che il gruppo additivo  $\mathbb{R}$  dei numeri reali è isomorfo al gruppo moltiplicativo  $P$  dei reali positivi.
2. Dimostrare che i prodotti  $ab$  e  $ba$  sono elementi coniugati in un gruppo.
3. Siano  $a, b$  elementi di un gruppo  $G$  e poniamo  $a' = bab^{-1}$ . Dimostrare che  $a = a'$  se e solo se  $a$  e  $b$  commutano tra loro.
4. (a) Posto  $b' = aba^{-1}$ , dimostrare che  $b'^n = ab^n a^{-1}$ .
- (b) Dimostrare che, se  $aba^{-1} = b^2$ , allora  $a^3 ba^{-3} = b^8$ .
5. Sia  $\varphi : G \rightarrow G'$  un isomorfismo di gruppi. Dimostrare che anche l'applicazione inversa  $\varphi^{-1}$  è un isomorfismo.

6. Sia  $\varphi : G \rightarrow G'$  un isomorfismo di gruppi; presi due elementi  $x, y \in G$ , poniamo:  $x' = \varphi(x)$  e  $y' = \varphi(y)$ .
- (a) Dimostrare che gli ordini di  $x$  e di  $x'$  sono uguali.
- (b) Dimostrare che, se  $xyx = yxy$ , allora  $x'y'x' = y'x'y'$ .
- (c) Dimostrare che  $\varphi(x^{-1}) = x'^{-1}$ .
7. Dimostrare che le matrici  $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$  sono elementi coniugati nel gruppo  $GL_2(\mathbb{R})$ , ma che esse non sono elementi coniugati nel gruppo  $SL_2(\mathbb{R})$ .
8. Dimostrare che le matrici  $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ & 2 \end{bmatrix}$  sono elementi coniugati in  $GL_2(\mathbb{R})$ .
9. Trovare un isomorfismo da un gruppo  $G$  al suo gruppo opposto  $G^0$  (cfr. § 1, esercizio 11).
10. Dimostrare che l'applicazione  $A \mapsto (A^t)^{-1}$  è un automorfismo di  $GL_n(\mathbb{R})$ .
11. Provare che l'insieme  $\text{Aut } G$  degli automorfismi di un gruppo  $G$  costituisce un gruppo rispetto alla legge di composizione data dalla composizione di applicazioni.
12. Sia  $G$  un gruppo e sia  $\varphi : G \rightarrow G$  l'applicazione definita da  $\varphi(x) = x^{-1}$ .
- (a) Dimostrare che  $\varphi$  è biettiva.
- (b) Dimostrare che  $\varphi$  è un automorfismo se e soltanto se  $G$  è abeliano.
13. (a) Sia  $G$  un gruppo di ordine 4. Dimostrare che ogni elemento di  $G$  ha ordine 1, 2, o 4.
- (b) Classificare i gruppi di ordine 4 considerando i due casi seguenti:
- (i)  $G$  contiene un elemento di ordine 4.
- (ii) Ogni elemento di  $G$  ha ordine  $< 4$ .
14. Determinare il gruppo degli automorfismi dei seguenti gruppi: (a)  $\mathbb{Z}$ , (b) un gruppo ciclico di ordine 10, (c)  $S_3$ .
15. Dimostrare che le funzioni  $f = 1/x$ ,  $g = (x - 1)/x$  generano un gruppo di funzioni, rispetto alla legge di composizione data dalla composizione di funzioni, il quale è isomorfo al gruppo simmetrico  $S_3$ .
16. Dare un esempio di due gruppi isomorfi tali che tra di essi esista più di un isomorfismo.

### 4 Omomorfismi

1. Sia  $G$  un gruppo, con la legge di composizione denotata con  $x \# y$ . Sia  $H$  un gruppo con legge di composizione  $u \circ v$ . Qual è la condizione affinché un'applicazione  $\varphi : G \rightarrow H$  sia un omomorfismo?
2. Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi. Dimostrare che, presi comunque  $k$  elementi  $a_1, \dots, a_k$  in  $G$ , si ha:  $\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$ .

3. Dimostrare che il nucleo e l'immagine di un omomorfismo sono sottogruppi.
4. Descrivere tutti gli omomorfismi  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$  e determinare quali tra di essi sono iniettivi, quali suriettivi e quali isomorfismi.
5. Sia  $G$  un gruppo abeliano. Provare che l'applicazione "potenza  $n$ -esima"  $\varphi : G \rightarrow G$  definita da  $\varphi(x) = x^n$  è un omomorfismo.
6. Sia  $f : \mathbb{R} \rightarrow \mathbb{C}^*$  l'applicazione definita da  $f(x) = e^{ix}$ . Dimostrare che  $f$  è un omomorfismo e determinarne il nucleo e l'immagine.
7. Dimostrare che l'applicazione "valore assoluto"  $|\cdot| : \mathbb{C}^* \rightarrow \mathbb{R}^*$  che manda  $\alpha$  in  $|\alpha|$  è un omomorfismo, e determinarne il nucleo e l'immagine.
8. (a) Trovare tutti i sottogruppi di  $S_3$  e determinare quali tra di essi sono normali.  
 (b) Trovare tutti i sottogruppi del gruppo dei quaternioni e determinare quali tra di essi sono normali.
9. (a) Dimostrare che la composizione  $\varphi \circ \psi$  di due omomorfismi  $\varphi, \psi$  è un omomorfismo.  
 (b) Descrivere il nucleo di  $\varphi \circ \psi$ .
10. Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi. Dimostrare che  $\varphi(x) = \varphi(y)$  se e soltanto se  $xy^{-1} \in \ker \varphi$ .
11. Siano  $G, H$  gruppi ciclici generati, rispettivamente, da elementi  $x, y$ . Determinare la condizione sugli ordini  $m, n$  di  $x$  e  $y$  affinché l'applicazione che manda  $x^i$  in  $y^i$  sia un omomorfismo di gruppi.
12. Dimostrare che le matrici  $n \times n$   $M$  aventi la forma a blocchi  $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ , con  $A \in GL_r(\mathbb{R})$  e  $D \in GL_{n-r}(\mathbb{R})$ , formano un sottogruppo  $P$  di  $GL_n(\mathbb{R})$  e che l'applicazione  $P \rightarrow GL_r(\mathbb{R})$  che manda  $M$  in  $A$  è un omomorfismo. Qual è il suo nucleo?
13. (a) Sia  $H$  un sottogruppo di  $G$  e sia  $g \in G$ . Il sottogruppo coniugato  $gHg^{-1}$  è per definizione l'insieme di tutti i coniugati  $ghg^{-1}$ , con  $h \in H$ . Dimostrare che  $gHg^{-1}$  è un sottogruppo di  $G$ .  
 (b) Provare che un sottogruppo  $H$  di un gruppo  $G$  è normale se e solo se  $gHg^{-1} = H$ , per ogni  $g \in G$ .
14. Sia  $N$  un sottogruppo normale di  $G$ . Dimostrare che, se  $g \in G$  e  $n \in N$ , si ha:  $g^{-1}ng \in N$ .
15. Siano  $\varphi$  e  $\psi$  due omomorfismi da un gruppo  $G$  a un altro gruppo  $G'$ , e sia  $H \subset G$  il sottoinsieme  $\{x \in G \mid \varphi(x) = \psi(x)\}$ . È vero che  $H$  è un sottogruppo di  $G$ ?
16. Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi e sia  $x \in G$  un elemento di ordine  $r$ . Cosa si può dire sull'ordine di  $\varphi(x)$ ?
17. Dimostrare che il centro di un gruppo è un sottogruppo normale.
18. Provare che il centro di  $GL_n(\mathbb{R})$  è il sottogruppo  $Z = \{cI \mid c \in \mathbb{R}, c \neq 0\}$ .
19. Dimostrare che, se un gruppo contiene un solo elemento di ordine 2, allora tale elemento appartiene al centro del gruppo.

20. Si consideri l'insieme  $U$  delle matrici  $3 \times 3$  reali della forma

$$\begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}.$$

- (a) Dimostrare che  $U$  è un sottogruppo di  $SL_3(\mathbb{R})$ .
  - (b) È vero che  $U$  è normale?
  - (c) Determinare il centro di  $U$ .
  21. Dimostrare, mediante un esempio esplicito, che  $GL_2(\mathbb{R})$  non è un sottogruppo normale di  $GL_2(\mathbb{C})$ .
  22. Sia  $\varphi : G \rightarrow G'$  un omomorfismo suriettivo di gruppi. Dimostrare che:
    - (a) Se  $G$  è ciclico, anche  $G'$  è ciclico.
    - (b) Se  $G$  è abeliano, anche  $G'$  è abeliano.
  23. Sia  $\varphi : G \rightarrow G'$  un omomorfismo suriettivo, e sia  $N$  un sottogruppo normale di  $G$ . Dimostrare che  $\varphi(N)$  è un sottogruppo normale di  $G'$ .
- ### 5 Relazioni di equivalenza e partizioni
1. Dimostrare che le fibre non vuote di un'applicazione formano una partizione del dominio.
  2. Sia  $S$  un insieme di gruppi. Dimostrare che la relazione:  $G \sim H$  se  $G$  è isomorfo a  $H$  è una relazione di equivalenza in  $S$ .
  3. Determinare il numero delle relazioni di equivalenza in un insieme di cinque elementi.
  4. È vero che l'intersezione  $R \cap R'$  di due relazioni di equivalenza  $R, R' \subset S \times S$  è una relazione di equivalenza? Cosa si può dire per l'unione?
  5. Sia  $H$  un sottogruppo di un gruppo  $G$ . Dimostrare che la relazione definita dalla regola:  $a \sim b$  se  $b^{-1}a \in H$  è una relazione di equivalenza in  $G$ .
  6. (a) Dimostrare che la relazione "x coniugato a y" in un gruppo  $G$  è una relazione di equivalenza in  $G$ .  
 (b) Descrivere gli elementi  $a$  la cui classe di equivalenza rispetto alla relazione definita in (a) è costituita soltanto dall'elemento  $a$ .
  7. Sia  $R$  una relazione nell'insieme  $\mathbb{R}$  dei numeri reali. Allora possiamo considerare  $R$  come un sottoinsieme del piano  $(x, y)$ . Illustrare il significato geometrico delle proprietà riflessiva e simmetrica.
  8. Per ciascuno dei seguenti sottoinsiemi  $R$  del piano  $(x, y)$ , determinare quali degli assiomi (5.2) sono soddisfatti e stabilire se  $R$  è o no una relazione di equivalenza nell'insieme  $\mathbb{R}$  dei numeri reali:
    - (a)  $R = \{(s, s) \mid s \in \mathbb{R}\}$ ;
    - (b)  $R = \text{insieme vuoto}$ ;

- (c)  $R = \{(x, y) \mid y = 0\}$ ;  
 (d)  $R = \{(x, y) \mid xy + 1 = 0\}$ ;  
 (e)  $R = \{(x, y) \mid x^2y - xy^2 - x + y = 0\}$ ;  
 (f)  $R = \{(x, y) \mid x^2 - xy + 2x - 2y = 0\}$ .

9. Descrivere la più piccola relazione di equivalenza nell'insieme dei numeri reali che contiene la retta  $x - y = 1$  nel piano  $(x, y)$ , e abbozzarne un disegno.  
 10. Disegnare le fibre dell'applicazione dal piano  $(x, z)$  all'asse  $y$ , definita da:  $y = zx$ .  
 11. Definire, a partire dalle operazioni sugli interi, l'addizione e la moltiplicazione nell'insieme (5.8).  
 12. Dimostrare che le classi laterali (5.14) sono le fibre dell'applicazione  $\varphi$ .

### 6 Classi laterali

1. Determinare l'indice  $[Z : nZ]$ .  
 2. Dimostrare direttamente che classi laterali distinte non hanno elementi in comune.  
 3. Dimostrare che ogni gruppo il cui ordine è una potenza di un numero primo  $p$  contiene un elemento di ordine  $p$ .  
 4. Mostrare con un esempio che le classi laterali sinistre e le classi laterali destre di  $GL_2(\mathbb{R})$  in  $GL_2(\mathbb{C})$  non sono sempre uguali.  
 5. Siano  $H, K$  sottogruppi di un gruppo  $G$ , rispettivamente di ordine 3, 5. Provare che  $H \cap K = \{1\}$ .  
 6. Dimostrare nei dettagli il corollario (6.15).  
 7. (a) Sia  $G$  un gruppo abeliano finito di ordine dispari. Dimostrare che l'applicazione  $\varphi : G \rightarrow G$  definita da:  $\varphi(x) = x^2$  è un automorfismo di  $G$ .  
 (b) Generalizzare il risultato enunciato in (a).  
 8. Sia  $W$  il sottogruppo additivo di  $\mathbb{R}^m$  costituito dalle soluzioni di un sistema di equazioni lineari omogenee  $AX = 0$ . Dimostrare che le soluzioni di un sistema non omogeneo  $AX = B$  formano una classe laterale di  $W$ .  
 9. Sia  $H$  un sottogruppo di un gruppo  $G$ . Dimostrare che il numero delle classi laterali sinistre è uguale al numero delle classi laterali destre (a) se  $G$  è finito e (b) in generale.  
 10. (a) Dimostrare che ogni sottogruppo di indice 2 è normale.  
 (b) Dare un esempio di un sottogruppo di indice 3 che non è normale.  
 11. Classificare i gruppi di ordine 6 analizzando i tre casi seguenti:  
 (a)  $G$  contiene un elemento di ordine 6.  
 (b)  $G$  contiene un elemento di ordine 3, ma non contiene nessun elemento di ordine 6.  
 (c) Tutti gli elementi di  $G$  hanno ordine 1 o 2.

12. Siano  $G, H$  i seguenti sottogruppi di  $GL_2(\mathbb{R})$ :

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \right\}, \quad H = \left\{ \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \mid x > 0 \right\}.$$

Un elemento di  $G$  può essere rappresentato con un punto nel piano  $(x, y)$ . Disegnare le partizioni del piano in classi laterali sinistre e in classi laterali destre di  $H$ .

### 7 La restrizione di un omomorfismo a un sottogruppo

1. Siano  $G$  e  $G'$  gruppi finiti i cui ordini siano primi tra loro. Dimostrare che l'unico omomorfismo  $\varphi : G \rightarrow G'$  è quello banale:  $\varphi(x) = 1$  per ogni  $x$ .  
 2. Dare un esempio di una permutazione di ordine pari che sia dispari e un esempio di una che sia pari.  
 3. (a) Siano  $H$  e  $K$  sottogruppi di un gruppo  $G$ . Dimostrare che l'intersezione  $xH \cap yK$  di due classi laterali di  $H$  e  $K$  o è vuota oppure è una classe laterale del sottogruppo  $H \cap K$ .  
 (b) Provare che se  $H$  e  $K$  hanno indice finito in  $G$  allora anche  $H \cap K$  ha indice finito.  
 4. Dimostrare la proposizione (7.1).  
 5. Siano  $H, N$  sottogruppi di un gruppo  $G$ , con  $N$  normale. Dimostrare che  $HN = NH$  e che tale insieme è un sottogruppo.  
 6. Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi con nucleo  $K$ , e sia  $H$  un altro sottogruppo di  $G$ . Descrivere  $\varphi^{-1}(\varphi(H))$  mediante  $H$  e  $K$ .  
 7. Dimostrare che un gruppo di ordine 30 può avere al più 7 sottogruppi di ordine 5.  
 \*8. Dimostrare il teorema di corrispondenza: Sia  $\varphi : G \rightarrow G'$  un omomorfismo suriettivo di gruppi con nucleo  $N$ . L'insieme dei sottogruppi  $H'$  di  $G'$  è in corrispondenza biunivoca con l'insieme dei sottogruppi  $H$  di  $G$  che contengono  $N$ , essendo tale corrispondenza definita dalle applicazioni  $H \mapsto \varphi(H)$  e  $H' \mapsto \varphi^{-1}(H')$ . Inoltre, sottogruppi normali di  $G$  corrispondono a sottogruppi normali di  $G'$ .  
 9. Siano  $G$  e  $G'$  gruppi ciclici di ordine 12 e 6, generati, rispettivamente, da elementi  $x, y$  e sia  $\varphi : G \rightarrow G'$  l'applicazione definita da  $\varphi(x^i) = y^i$ . Descrivere esplicitamente la corrispondenza biunivoca definita nell'esercizio precedente.

### 8 Prodotti di gruppi

1. Siano  $G, G'$  due gruppi. Qual è l'ordine del gruppo prodotto  $G \times G'$ ?  
 2. È vero che il gruppo simmetrico  $S_3$  è un prodotto diretto di gruppi non banali?  
 3. Dimostrare che un gruppo ciclico finito di ordine  $rs$  è isomorfo al prodotto di due gruppi ciclici di ordine  $r$  e  $s$  se e soltanto se  $r$  e  $s$  sono primi tra loro.  
 4. In ciascuno dei casi seguenti, stabilire se  $G$  è o no isomorfo al prodotto di  $H$  e  $K$ .  
 (a)  $G = \mathbb{R}^*$ ,  $H = \{1, -1\}$ ,  $K = \{\text{numeri reali positivi}\}$ .

- (b)  $G = \{\text{matrici } 2 \times 2 \text{ triangolari superiori invertibili}\}$ ,  $H = \{\text{matrici diagonali invertibili}\}$ ,  $K = \{\text{matrici triangolari superiori con elementi diagonali uguali a } 1\}$ .
- (c)  $G = \mathbb{C}^*$ ,  $H = \{\text{circonferenza unitaria}\}$ ,  $K = \{\text{reali positivi}\}$ .
5. Dimostrare che il prodotto di due gruppi ciclici infiniti non è un gruppo ciclico infinito.
6. Provare che il centro del prodotto di due gruppi è il prodotto dei loro centri.
7. (a) Siano  $H, K$  sottogruppi di un gruppo  $G$ . Dimostrare che l'insieme dei prodotti  $HK = \{hk \mid h \in H, k \in K\}$  è un sottogruppo se e soltanto se  $HK = KH$ .
- (b) Dare un esempio di un gruppo  $G$  con due sottogruppi  $H, K$  tali che  $HK$  non sia un sottogruppo.
8. Sia  $G$  un gruppo contenente sottogruppi normali di ordine 3 e 5, rispettivamente. Dimostrare che  $G$  contiene un elemento di ordine 15.
9. Sia  $G$  un gruppo finito il cui ordine sia un prodotto di due interi:  $n = ab$ . Siano  $H, K$  sottogruppi di  $G$  di ordine  $a$  e  $b$ , rispettivamente. Supponiamo che  $H \cap K = \{1\}$ . Dimostrare che  $HK = G$ . È vero che  $G$  è isomorfo al gruppo prodotto  $H \times K$ ?
10. Dati due gruppi  $G$  e  $G'$ , sia  $x \in G$  un elemento di ordine  $m$  e  $y \in G'$  un elemento di ordine  $n$ . Qual è l'ordine di  $(x, y)$  in  $G \times G'$ ?
11. Sia  $H$  un sottogruppo di un gruppo  $G$  e sia  $\varphi : G \rightarrow H$  un omomorfismo la cui restrizione a  $H$  è l'applicazione identica:  $\varphi(h) = h$  se  $h \in H$ . Poniamo  $N = \ker \varphi$ .
- (a) Dimostrare che, se  $G$  è abeliano, allora  $G$  è isomorfo al gruppo prodotto  $H \times N$ .
- (b) Trovare un'applicazione biiettiva  $\varphi : G \rightarrow H \times N$  senza l'ipotesi che  $G$  sia abeliano, ma mostrare con un esempio che  $\varphi$  non è necessariamente un isomorfismo.

### 9 Aritmetica modulare

1. Calcolare  $(7+14)(3-16)$  modulo 17.
2. (a) Dimostrare che il quadrato  $a^2$  di un intero  $a$  è congruo a 0 oppure a 1 modulo 4.  
 (b) Quali sono i valori possibili di  $a^2$  modulo 8?
3. (a) Dimostrare che 2 non possiede un inverso modulo 6.  
 (b) Determinare tutti gli interi  $n$  tali che 2 possiede un inverso modulo  $n$ .
4. Dimostrare che ogni intero  $a$  è congruo alla somma delle sue cifre modulo 9.
5. Risolvere la congruenza  $2x \equiv 5$  (a) modulo 9 e (b) modulo 6.
6. Determinare gli interi  $n$  per i quali le congruenze  $x+y \equiv 2$ ,  $2x-3y \equiv 3$  (modulo  $n$ ) ammettono una soluzione.
7. Dimostrare la proprietà associativa e la proprietà commutativa per la moltiplicazione in  $\mathbb{Z}/n\mathbb{Z}$ .

8. Utilizzare la proposizione (2.6) per dimostrare il *teorema cinese dei resti*: Siano  $m, n, a, b$  interi e supponiamo che il massimo comune divisore di  $m$  e  $n$  sia 1. Allora esiste un intero  $x$  tale che  $x \equiv a$  (modulo  $m$ ) e  $x \equiv b$  (modulo  $n$ ).

### 10 Gruppi quoziante

1. Sia  $G$  il gruppo delle matrici reali  $2 \times 2$  triangolari superiori invertibili. Stabilire se le seguenti condizioni descrivono sottogruppi normali  $H$  di  $G$ . In caso affermativo, utilizzare il primo teorema di isomorfismo per identificare il gruppo quoziante  $G/H$ .
- (a)  $a_{11} = 1$ ; (b)  $a_{12} = 0$ ; (c)  $a_{11} = a_{22}$ ; (d)  $a_{11} = a_{22} = 1$ .
2. Scrivere per esteso la dimostrazione del lemma (10.1) in termini di elementi.
3. Sia  $P$  una partizione di un gruppo  $G$  con la proprietà che per ogni coppia di elementi  $A, B$  della partizione, l'insieme prodotto  $AB$  è contenuto interamente in un altro elemento  $C$  della partizione. Sia  $N$  l'elemento di  $P$  che contiene 1. Dimostrare che  $N$  è un sottogruppo normale di  $G$  e che  $P$  è l'insieme delle sue classi laterali.
4. (a) Si consideri la descrizione (1.17) del gruppo simmetrico  $S_3$ . Sia  $H$  il sottogruppo  $\{1, y\}$ . Calcolare gli insiemi prodotto  $(1H)(xH)$  e  $(1H)(x^2H)$ , e verificare che essi non sono classi laterali.  
 (b) Dimostrare che un gruppo ciclico di ordine 6 ha due generatori che soddisfano alle regole:  $x^3 = 1$ ,  $y^2 = 1$ ,  $yx = xy$ .  
 (c) Ripetere i calcoli indicati in (a), sostituendo le relazioni (1.18) con le relazioni date nella parte (b) precedente. Spiegare i risultati.
5. Descrivere il gruppo quoziante  $\mathbb{R}^*/P$ , dove  $P$  denota il sottogruppo dei numeri reali positivi.
6. Sia  $H = \{1, -1, i, -i\}$  il sottogruppo di  $G = \mathbb{C}^*$  delle radici quarte dell'unità. Descrivere esplicitamente le classi laterali di  $H$  in  $G$  e dimostrare che  $G/H$  è isomorfo a  $G$ .
7. Determinare tutti i sottogruppi normali  $N$  del gruppo dei quaternioni  $H$  e descrivere i quozienti  $H/N$ .
8. Dimostrare che il sottoinsieme  $H$  di  $G = GL_n(\mathbb{R})$  delle matrici con determinante positivo costituisce un sottogruppo normale e descrivere il gruppo quoziante  $G/H$ .
9. Provare che il sottoinsieme  $G \times 1$  del gruppo prodotto  $G \times G'$  è un sottogruppo normale isomorfo a  $G$  e che  $(G \times G')/(G \times 1)$  è isomorfo a  $G'$ .
10. Descrivere i gruppi quoziante  $\mathbb{C}^*/P$  e  $\mathbb{C}^*/U$ , dove  $U$  è il sottogruppo dei numeri complessi di modulo 1 e  $P$  denota il sottogruppo dei reali positivi.
11. Dimostrare che i gruppi  $\mathbb{R}/\mathbb{Z}$  e  $\mathbb{R}/2\pi\mathbb{Z}$  sono isomorfi.

### Esercizi vari

1. Quanto vale il prodotto di tutte le radici  $m$ -esime dell'unità in  $\mathbb{C}$ ?  
 2. Calcolare il gruppo degli automorfismi del gruppo dei quaternioni.  
 3. Dimostrare che un gruppo di ordine pari contiene un elemento di ordine 2.

4. Siano  $K \subset H \subset G$  sottogruppi di un gruppo finito  $G$ . Dimostrare la formula:  $[G : K] = [G : H][H : K]$ .

\*5. Un *semigruppo*  $S$  è un insieme con una legge di composizione associativa e un'identità. Tuttavia, non si richiede che gli elementi abbiano un inverso, sicché la legge di cancellazione non vale necessariamente. Il semigruppo  $S$  si dice generato da un elemento  $s$ , se l'insieme  $\{1, s, s^2, \dots\}$  delle potenze non negative di  $s$  è l'intero insieme  $S$ . Per esempio, le relazioni  $s^2 = 1$  e  $s^2 = s$  descrivono due strutture distinte di semigruppo sull'insieme  $\{1, s\}$ . Definire la nozione di isomorfismo tra semigruppi e descrivere tutte le classi di isomorfismo dei semigruppi generati da un elemento.

6. Sia  $S$  un semigruppo con un numero finito di elementi che soddisfi alla legge di cancellazione (1.12). Dimostrare che  $S$  è un gruppo.

\*7. Siano  $a = (a_1, \dots, a_k)$  e  $b = (b_1, \dots, b_k)$  punti nello spazio  $k$ -dimensionale  $\mathbb{R}^k$ . Un *cammino*, o *arco*, da  $a$  a  $b$  è una funzione continua nell'intervallo  $[0, 1]$  a valori in  $\mathbb{R}^k$ , ossia una funzione  $f : [0, 1] \rightarrow \mathbb{R}^k$ , la quale manda  $t$  in  $f(t) = (x_1(t), \dots, x_k(t))$ , tale che  $f(0) = a$  e  $f(1) = b$ . Se  $S$  è un sottoinsieme di  $\mathbb{R}^k$  e se  $a, b \in S$ , definiamo  $a \sim b$ , se  $a$  e  $b$  possono essere congiunti mediante un cammino contenuto interamente in  $S$ .

(a) Dimostrare che la relazione  $\sim$  è una relazione di equivalenza in  $S$ . Occorre verificare attentamente che i cammini che si costruiscono sono contenuti in  $S$ .

(b) Un sottoinsieme  $S$  di  $\mathbb{R}^k$  si dice *connesso per archi*, se  $a \sim b$  per ogni coppia di punti  $a, b \in S$ . Dimostrare che ogni sottoinsieme  $S$  ammette una partizione in sottoinsiemi connessi per archi con la proprietà che due punti appartenenti a sottoinsiemi distinti non possono essere congiunti mediante un cammino contenuto in  $S$ .

(c) Quali dei seguenti sottoinsiemi di  $\mathbb{R}^2$  sono connessi per archi?

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\};$$

$$\{(x, y) \in \mathbb{R}^2 \mid xy = 0\};$$

$$\{(x, y) \in \mathbb{R}^2 \mid xy = 1\}.$$

\*8. L'insieme delle matrici  $n \times n$  può essere identificato con lo spazio  $\mathbb{R}^{n \times n}$ . Sia  $G$  un sottogruppo di  $GL_n(\mathbb{R})$ . Provare che:

(a) Se  $A, B, C, D \in G$  e se esistono cammini in  $G$  da  $A$  a  $B$  e da  $C$  a  $D$ , allora esiste un cammino in  $G$  da  $AC$  a  $BD$ .

(b) L'insieme delle matrici che possono essere congiunte all'identità  $I$  costituisce un sottogruppo normale di  $G$  (chiamato la *componente connessa* di  $G$ ).

\*9. (a) Utilizzando il fatto che  $SL_n(\mathbb{R})$  è generato dalle matrici elementari del primo tipo (cfr. § 2, esercizio 18), provare che tale gruppo è connesso per archi.

(b) Dimostrare che  $GL_n(\mathbb{R})$  è l'unione di due sottoinsiemi connessi per archi, e descrivere tali sottoinsiemi.

10. Siano  $H, K$  sottogruppi di un gruppo  $G$ , e sia  $g \in G$ . L'insieme

$$HgK = \{x \in G \mid x = hgk \text{ per qualche } h \in H, k \in K\}$$

è chiamato una *classe laterale doppia*.

(a) Provare che le classi laterali doppie formano una partizione di  $G$ .

(b) È vero che tutte le classi laterali doppie hanno lo stesso ordine?

11. Sia  $H$  un sottogruppo di un gruppo  $G$ . Dimostrare che le classi laterali doppie  $HgH$  sono le classi laterali sinistre  $gH$  se  $H$  è normale, ma che, se  $H$  non è normale, allora esiste una classe laterale doppia che contiene propriamente una classe laterale sinistra.

\*12. Dimostrare che le classi laterali doppie in  $GL_n(\mathbb{R})$  dei sottogruppi  $H = \{\text{matrici triangolari inferiori}\}$  e  $K = \{\text{matrici triangolari superiori}\}$  sono gli insiemi  $HPK$ , dove  $P$  è una matrice di permutazione.

## Capitolo 3

### Spazi vettoriali

#### (1.2) Esempio

I sottospazi  $W$  dello spazio  $\mathbb{R}^2$  sono di tre tipi:

- (i) il vettore nullo:  $W = \{0\}$ ;
- (ii) i vettori giacenti su una retta  $L$  passante per l'origine;
- (iii) l'intero spazio:  $W = \mathbb{R}^2$ .

Ciò si può vedere dalla regola del parallelogramma per l'addizione tra vettori. Se  $W$  contiene due vettori  $w_1, w_2$  non giacenti su una stessa retta, allora ogni vettore  $v$  può essere ottenuto a partire da essi come una "combinazione lineare":

$$c_1w_1 + c_2w_2,$$

dove  $c_1, c_2$  sono scalari. In questo caso dunque,  $W = \mathbb{R}^2$ . Se  $W$  non contiene due vettori così, allora ci troviamo nel caso (i) o nel caso (ii). ■

Iniziare sempre con gli esempi più semplici.  
David Hilbert

#### 1 Spazi vettoriali reali

Il modello fondamentale per gli spazi vettoriali è lo spazio dei vettori riga o colonna  $n$ -dimensionali:

$\mathbb{R}^n$ : insieme dei vettori riga  $v = (a_1, \dots, a_n)$ , oppure

$$\text{insieme dei vettori colonna } v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Sebbene i vettori riga occupino meno spazio nella scrittura, la definizione di moltiplicazione tra matrici fa sì che l'uso dei vettori colonna sia più conveniente. Pertanto lavoreremo soprattutto con i vettori colonna. Per risparmiare spazio, scriveremo talvolta un vettore colonna nella forma  $(a_1, \dots, a_n)^t$ .

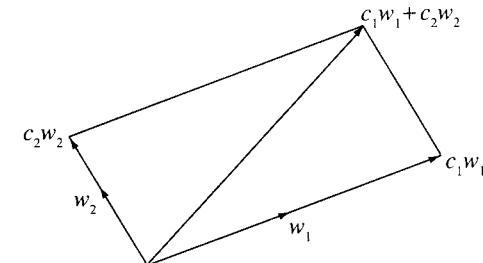
Per ora studieremo soltanto due operazioni:

$$\text{addizione tra vettori: } \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

(1.1)

$$\text{moltiplicazione per uno scalare: } c \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}.$$

Con tali operazioni,  $\mathbb{R}^n$  diventa uno *spazio vettoriale*. Prima di passare alla definizione formale di spazio vettoriale, consideriamo altri esempi di sottoinsiemi non vuoti di  $\mathbb{R}^n$ , chiusi rispetto alle operazioni (1.1). Un tale sottoinsieme è chiamato un *sottospazio*.



Allo stesso modo, si può dimostrare che i sottospazi di  $\mathbb{R}^3$  sono di quattro tipi:

- (i) il vettore nullo;
- (ii) i vettori giacenti su una retta passante per l'origine;
- (iii) i vettori giacenti in un piano passante per l'origine;
- (iv) l'intero spazio  $\mathbb{R}^3$ .

Questa classificazione dei sottospazi di  $\mathbb{R}^2$  e  $\mathbb{R}^3$  risulterà chiara nel paragrafo 4, mediante il concetto di *dimensione*.

I sistemi di equazioni lineari omogenee forniscono molti esempi. L'insieme delle soluzioni di un tale sistema è sempre un sottospazio. Infatti, se scriviamo il sistema con la notazione matriciale nella forma  $AX = 0$ , dove  $A$  è una matrice  $m \times n$  e  $X$  è un vettore colonna, allora è chiaro che:

- (a)  $AX = 0$  e  $AY = 0$  implicano:  $A(X + Y) = 0$ . In altre parole, se  $X$  e  $Y$  sono soluzioni, anche  $X + Y$  è una soluzione.
- (b)  $AX = 0$  implica  $AcX = 0$ . Ossia, se  $X$  è una soluzione, anche  $cX$  è una soluzione.

Per esempio, sia  $W$  l'insieme delle soluzioni dell'equazione:

$$(1.3) \quad 2x_1 - x_2 - 2x_3 = 0, \text{ ossia } AX = 0,$$

dove  $A = [2 \quad -1 \quad -2]$ . Tale spazio è l'insieme dei vettori giacenti nel piano passante per l'origine e ortogonale ad  $A$ . Ogni soluzione è una combinazione lineare  $c_1 w_1 + c_2 w_2$  di due soluzioni particolari  $w_1, w_2$ . La maggior parte delle coppie di soluzioni, per esempio

$$(1.4) \quad w_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix},$$

generano lo spazio delle soluzioni in questo modo. Dunque ogni soluzione ha la forma:

$$(1.5) \quad c_1 w_1 + c_2 w_2 = \begin{bmatrix} c_1 + c_2 \\ 2c_2 \\ c_1 \end{bmatrix},$$

dove  $c_1, c_2$  sono costanti arbitrarie. Un'altra scelta delle soluzioni particolari  $w_1, w_2$  darebbe luogo a una descrizione diversa, ma equivalente, dello spazio di tutte le soluzioni.

(1.6) DEFINIZIONE *Uno spazio vettoriale reale è un insieme  $V$  dotato di due leggi di composizione:*

(a) Addizione:  $V \times V \rightarrow V$ , scritta  $v, w \mapsto v + w$ .

(b) Moltiplicazione per uno scalare:  $\mathbb{R} \times V \rightarrow V$ , scritta  $c, v \mapsto cv$ .

Queste leggi di composizione devono soddisfare ai seguenti assiomi:

(i)  *$V$  è un gruppo abeliano rispetto all'addizione.*

(ii) *La moltiplicazione per uno scalare è associativa rispetto alla moltiplicazione tra numeri reali:*

$$(ab)v = a(bv).$$

(iii) *La moltiplicazione per il numero reale 1 è l'identità:*

$$1v = v.$$

(iv) *Valgono due leggi distributive:*

$$(a+b)v = av + bv$$

$$a(v+w) = av + aw.$$

Naturalmente, si suppone che tali assiomi valgano per ogni scelta di  $a, b$  in  $\mathbb{R}$  e per ogni scelta di  $v, w$  in  $V$ .

L'identità rispetto all'addizione in  $V$  si denota con 0, oppure con  $0_V$ , se vi è il pericolo di confondere il vettore nullo con il numero zero.

Si noti che la moltiplicazione per uno scalare associa ad ogni coppia, costituita da un numero reale  $c$  e da un vettore  $v$ , un altro vettore  $cv$ . Una regola di questo tipo è chiamata *legge di composizione esterna* sullo spazio vettoriale.

La moltiplicazione tra due vettori non fa parte della struttura di spazio vettoriale, sebbene vari prodotti, quale il prodotto scalare di vettori in  $\mathbb{R}^3$ , possono essere definiti. Tali prodotti non hanno un carattere del tutto intrinseco; essi dipendono dalla scelta delle coordinate. Pertanto essi sono considerati come una struttura aggiuntiva sullo spazio vettoriale.

L'assioma (ii) va letto con attenzione. L'espressione a sinistra va calcolata moltiplicando  $a$  e  $b$  come numeri reali e successivamente, moltiplicando lo scalare  $ab$  per  $v$ , così da ottenere un vettore. Invece, a destra, le operazioni indicate sono entrambe moltiplicazioni per uno scalare.

Le due leggi di composizione sono collegate tra loro dalle leggi distributive, di importanza fondamentale. Si noti che, nella prima legge distributiva, il simbolo + a sinistra indica l'addizione tra numeri reali, mentre a destra indica l'addizione tra vettori.

(1.7) PROPOSIZIONE *In uno spazio vettoriale  $V$  valgono le seguenti identità:*

- (a)  $0_{\mathbb{R}}v = 0_V$ , per ogni  $v \in V$ ,
- (b)  $c0_V = 0_V$ , per ogni  $c \in \mathbb{R}$ ,
- (c)  $(-1)v = -v$ , per ogni  $v \in V$ .

*Dimostrazione.* Per provare (a), utilizziamo la legge distributiva per scrivere:

$$0v + 0v = (0+0)v = 0v = 0v + 0.$$

Cancellando  $0v$  nella prima e nell'ultima espressione, si ottiene:  $0v = 0$ . Occorre procedere con attenzione, distinguendo il simbolo 0 riferito al numero zero dal simbolo 0 riferito al vettore nullo.

Allo stesso modo si ha:  $c0 + c0 = c(0 + 0) = c0$ , da cui:  $c0 = 0$ . Infine,

$$v + (-1)v = 1v + (-1)v = (1 + (-1))v = 0v = 0.$$

Pertanto  $(-1)v$  è l'opposto di  $v$ . ■

### (1.8) Esempi

- (a) Un sottospazio di  $\mathbb{R}^n$  è uno spazio vettoriale, con le leggi di composizione indotte da quelle definite su  $\mathbb{R}^n$ .
- (b) Sia  $V = \mathbb{C}$  l'insieme dei numeri complessi. Tralasciamo la moltiplicazione tra numeri complessi e consideriamo soltanto l'addizione  $\alpha + \beta$  e la moltiplicazione  $c\alpha$  di un numero complesso  $\alpha$  per un numero reale  $c$ . Con tali operazioni,  $\mathbb{C}$  risulta uno spazio vettoriale reale.
- (c) L'insieme dei polinomi a coefficienti reali  $p(x) = a_nx^n + \dots + a_0$  è uno spazio vettoriale, rispetto alle operazioni di addizione tra polinomi e di moltiplicazione di un polinomio per uno scalare.
- (d) Sia  $V$  l'insieme delle funzioni a valori reali continue nell'intervallo  $[0, 1]$ . Consideriamo soltanto le operazioni di addizione tra funzioni  $f + g$  e di moltiplicazione di una funzione per un numero reale  $cf$ . Con tali operazioni,  $V$  risulta uno spazio vettoriale reale.

Si noti che ciascuno degli esempi precedenti ha una struttura più ricca di quella di spazio vettoriale da noi considerata. Ciò è tipico in matematica. Infatti, qualsiasi esempio particolare possiede delle proprietà caratteristiche che lo distinguono dagli altri, ma questo non è un inconveniente della definizione. Al contrario, la potenza dell'approccio astratto sta nel fatto che le conseguenze degli assiomi generali possono essere applicate a molti esempi differenti.

## 2 Campi astratti

In algebra lineare conviene trattare simultaneamente il caso reale e il caso complesso. Ciò si può fare elencando le proprietà degli "scalari" che sono necessarie dal punto di vista assiomatico, pervenendo così alla nozione di *campo*.

Un tempo si usava parlare soltanto di sottocampi di  $\mathbb{C}$ . Un *sottocampo* di  $\mathbb{C}$  è un qualsiasi sottoinsieme di  $\mathbb{C}$  chiuso rispetto alle quattro operazioni (addizione, sottrazione, moltiplicazione e divisione) e contenente 1. In altre parole,  $F$  è un sottocampo di  $\mathbb{C}$ , se valgono le seguenti proprietà:

- (2.1) (a) Se  $a, b \in F$ , allora  $a + b \in F$ .
- (b) Se  $a \in F$ , allora  $-a \in F$ .

- (c) Se  $a, b \in F$ , allora  $ab \in F$ .
- (d) Se  $a \in F$  e  $a \neq 0$ , allora  $a^{-1} \in F$ .
- (e)  $1 \in F$ .

Si noti che è possibile utilizzare gli assiomi (a), (b), (e) per concludere che  $1 - 1 = 0$  è un elemento di  $F$ . Dunque  $F$  è un sottoinsieme che è un sottogruppo di  $\mathbb{C}$  rispetto all'addizione e tale che  $F - \{0\} = F^*$  è un sottogruppo di  $\mathbb{C}^*$  rispetto alla moltiplicazione. Viceversa, ogni sottoinsieme siffatto è un sottocampo di  $\mathbb{C}$ . Ecco alcuni esempi di sottocampi di  $\mathbb{C}$ :

### (2.2) Esempi

- (a)  $F = \mathbb{R}$ , il campo dei numeri reali.
- (b)  $F = \mathbb{Q}$ , il campo dei numeri razionali (= frazioni di interi).
- (c)  $F = \mathbb{Q}[\sqrt{2}]$ , il campo di tutti i numeri complessi della forma  $a + b\sqrt{2}$ , con  $a, b \in \mathbb{Q}$ .

È un buon esercizio verificare gli assiomi (2.1) per l'ultimo esempio.

Oggi, si usa introdurre la nozione di campo in modo astratto. Si tratta di una nozione più difficile da afferrare rispetto a quella di sottocampo di  $\mathbb{C}$ , ma essa comprende nuove classi importanti di campi, inclusi i campi finiti.

**(2.3) DEFINIZIONE** *Un campo  $F$  è un insieme dotato di due leggi di composizione:*

$$\begin{array}{ccc} F \times F & \xrightarrow{+} & F \\ a, b & \longmapsto a + b & \end{array} \quad \text{e} \quad \begin{array}{ccc} F \times F & \xrightarrow{*} & F \\ a, b & \longmapsto ab & \end{array}$$

*chiamate addizione e moltiplicazione, e soddisfacenti ai seguenti assiomi:*

- (i)  *$F$  risulta un gruppo abeliano rispetto all'addizione. Il suo elemento neutro si denota con 0.*
- (ii) *La moltiplicazione è associativa e commutativa e, rispetto ad essa,  $F^* = F - \{0\}$  risulta un gruppo. Il suo elemento neutro si denota con 1.*
- (iii) *Proprietà distributiva:  $(a + b)c = ac + bc$ , per ogni  $a, b, c \in F$ .*

I primi due assiomi descrivono, separatamente, le proprietà delle due leggi di composizione: l'addizione e la moltiplicazione. Il terzo assioma, ossia la proprietà distributiva, è quello che collega l'addizione con la moltiplicazione. Esso ha un ruolo cruciale, poiché se le due leggi non fossero collegate tra loro, potremmo studiare ciascuna di esse separatamente. Come è noto, i numeri reali soddisfano a tali assiomi, tuttavia per capire che essi sono tutto ciò che serve per le operazioni aritmetiche, occorre un po' di pratica.

È possibile considerare matrici  $A$  i cui elementi  $a_{ij}$  appartengono a un campo arbitrario  $F$ . La trattazione sviluppata nel capitolo 1 può essere ripetuta senza cambiamenti, ed è opportuno tornare indietro a rivedere tale argomento, alla luce di quanto ora osservato.

Gli esempi più semplici di campi, a parte i sottocampi del campo dei numeri complessi, sono certi campi finiti chiamati campi primi, che ora passiamo a descrivere. Abbiamo visto (cap. 2, §9) che l'insieme  $\mathbb{Z}/n\mathbb{Z}$  delle classi di congruenza modulo  $n$  è dotato di leggi di addizione e moltiplicazione che derivano dall'addizione e dalla moltiplicazione tra numeri interi. Ora tutti gli assiomi di un campo valgono per gli interi, tranne l'esistenza degli inversi nell'assioma (2.3ii). Gli interi non sono chiusi rispetto alla divisione. Inoltre, come è stato già osservato, tali assiomi si trasportano all'addizione e alla moltiplicazione tra classi di congruenza. Tuttavia non vi è motivo di supporre che, per le classi di congruenza, esistano gli inversi rispetto alla moltiplicazione, e infatti ciò non è vero. Per esempio, la classe di 2, modulo 6, non possiede un inverso. Pertanto è sorprendente il fatto che, se  $p$  è un numero primo, tutte le classi di congruenza non nulle modulo  $p$  hanno gli inversi, e quindi l'insieme  $\mathbb{Z}/p\mathbb{Z}$  risulta un campo. Tale campo è chiamato *campo primo* e si denota di solito con  $\mathbb{F}_p$ :

$$(2.4) \quad \mathbb{F}_p = \{\bar{0}, \bar{1}, \dots, \bar{p-1}\} = \mathbb{Z}/p\mathbb{Z}.$$

(2.5) TEOREMA Sia  $p$  un numero primo. Ogni elemento non nullo  $\bar{a} \in \mathbb{F}_p$  possiede un inverso rispetto alla moltiplicazione, e quindi  $\mathbb{F}_p$  è un campo con  $p$  elementi.

Il teorema può essere enunciato anche nella forma seguente:

(2.6) Sia  $p$  un primo e sia  $a$  un qualsiasi intero non divisibile per  $p$ . Allora esiste un intero  $b$  tale che  $ab \equiv 1$  (modulo  $p$ ).

Infatti  $ab \equiv 1$  (modulo  $p$ ) equivale a  $\bar{a}\bar{b} = \bar{a}\bar{b} = \bar{1}$ , cioè  $\bar{b}$  è l'inverso di  $\bar{a}$ .

Per esempio, sia  $p = 13$  e  $\bar{a} = \bar{6}$ . Allora  $(\bar{a})^{-1} = \bar{11}$ , poiché

$$6 \cdot 11 = 66 \equiv 1 \pmod{13}.$$

Non è facile, in generale, trovare l'inversa di una classe di congruenza  $\bar{a}$  (modulo  $p$ ), tuttavia si può fare per tentativi, se  $p$  è piccolo. Un modo sistematico di procedere è quello di calcolare le potenze di  $\bar{a}$ . Poiché ogni classe di congruenza non nulla ha un'inversa, l'insieme di tutte le classi non nulle risulta un gruppo finito di ordine  $p - 1$ , denotato di solito con  $\mathbb{F}_p^*$ . Pertanto ogni elemento  $\bar{a}$  ha un ordine finito che divide  $p - 1$ . Così, ad esempio, se  $p = 13$  e  $\bar{a} = \bar{3}$ , si ottiene:  $\bar{a}^2 = \bar{9}$  e  $\bar{a}^3 = \bar{27} = \bar{1}$ , il che prova che  $\bar{a}$  ha ordine 3. Qui siamo stati fortunati:

$(\bar{a})^{-1} = \bar{a}^2 = \bar{9}$ . D'altra parte, se avessimo utilizzato questo metodo con  $\bar{a} = \bar{6}$ , avremmo trovato che  $\bar{6}$  ha ordine 12. In tal caso, i calcoli sarebbero stati laboriosi.

**Dimostrazione del teorema** (2.5). Sia  $\bar{a} \in \mathbb{F}_p$  un elemento non nullo arbitrario e utilizziamo il metodo appena esposto per dimostrare che  $\bar{a}$  possiede un inverso. Consideriamo le potenze  $1, \bar{a}, \bar{a}^2, \bar{a}^3, \dots$ . Poiché tali potenze sono infinite e d'altra parte  $\mathbb{F}_p$  ha soltanto un numero finito di elementi, esistono necessariamente due potenze uguali, diciamo  $\bar{a}^m = \bar{a}^n$ , con  $m < n$ . A questo punto, basterebbe cancellare  $\bar{a}^m$  per ottenere:  $\bar{1} = \bar{a}^{n-m}$ . Una volta giustificata tale cancellazione, avremo dimostrato che  $\bar{a}^{n-m-1}$  è l'inverso di  $\bar{a}$ . Ciò completerà la dimostrazione.

Ecco la legge di cancellazione di cui abbiamo bisogno:

(2.7) LEMMA (Legge di cancellazione) Siano  $\bar{a}, \bar{c}, \bar{d}$  elementi di  $\mathbb{F}_p$ , con  $\bar{a} \neq \bar{0}$ . Se  $\bar{a}\bar{c} = \bar{a}\bar{d}$ , allora  $\bar{c} = \bar{d}$ .

**Dimostrazione.** Posto:  $\bar{b} = \bar{c} - \bar{d}$ , il lemma si può enunciare dicendo che, se  $\bar{a}\bar{b} = \bar{0}$  e  $\bar{a} \neq \bar{0}$ , allora  $\bar{b} = \bar{0}$ . Per provare ciò, rappresentiamo le classi di congruenza  $\bar{a}, \bar{b}$  mediante gli interi  $a, b$ . Allora ciò che occorre dimostrare è il fatto seguente, abbastanza chiaro intuitivamente:

(2.8) LEMMA Sia  $p$  un numero primo e siano  $a, b$  interi. Se  $p$  divide il prodotto  $ab$ , allora  $p$  divide  $a$  oppure  $p$  divide  $b$ .

**Dimostrazione.** Supponiamo che  $p$  non divida  $a$ , ma divida  $ab$ ; dobbiamo provare che  $p$  divide  $b$ . Poiché  $p$  è primo, 1 e  $p$  sono gli unici interi positivi che lo dividono. Poiché  $p$  non divide  $a$ , l'unico divisore comune di  $p$  e  $a$  è 1. Pertanto 1 è il loro massimo comune divisore. Dalla proposizione (2.6) del capitolo 2 segue che esistono interi  $r, s$  tali che  $1 = rp + sa$ , da cui, moltiplicando ambo i membri per  $b$ , si ottiene:  $b = rpb + sab$ . Ora, entrambi i termini che compaiono a destra in tale uguaglianza sono divisibili per  $p$ , e quindi anche il termine a sinistra  $b$  è divisibile per  $p$ , da cui la tesi. ■

Come con le congruenze, nel campo  $\mathbb{F}_p$  si possono fare i calcoli lavorando con gli interi, fatta eccezione per la divisione, che negli interi non si può effettuare. Questa difficoltà spesso può essere risolta, ponendo tutto su un denominatore comune in modo tale che la divisione richiesta è lasciata fino alla fine. Per esempio, supponiamo di cercare nel campo  $\mathbb{F}_p$  le soluzioni di un sistema di  $n$  equazioni lineari in  $n$  incognite. Rappresentiamo il sistema di equazioni mediante un sistema a coefficienti interi, scegliendo rappresentanti per le classi resto in modo opportuno. Il sistema sarà quindi della forma:  $AX = B$ , dove  $A$  è una matrice  $n \times n$  ad elementi interi e  $B$  è un vettore colonna ad elementi interi. Per risolvere il sistema in  $\mathbb{F}_p$ , cerchiamo di invertire la matrice  $A$  modulo  $p$ . La regola di Cramer:  $(\text{adj } A)A = \delta I$ , dove  $\delta = \det A$ , è una formula valida negli

interi [cap. 1 (5.7)], e pertanto essa vale anche in  $\mathbb{F}_p$ , quando si sostituiscono gli elementi della matrice con le loro classi di congruenza. Se la classe resto di  $b$  è diversa da zero, allora possiamo invertire la matrice  $A$  in  $\mathbb{F}_p$ , e la sua inversa è  $\delta^{-1}(\text{adj } A)$ .

(2.9) COROLLARIO Sia  $AX = B$  un sistema di  $n$  equazioni lineari in  $n$  incognite, dove gli elementi di  $A, B$  appartengono a  $\mathbb{F}_p$ . Se  $\det A \neq 0$  in  $\mathbb{F}_p$ , il sistema ha un'unica soluzione in  $\mathbb{F}_p$ . ■

Per esempio, consideriamo il sistema di equazioni lineari  $AX = B$ , dove

$$A = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 3 \\ -1 \end{bmatrix}.$$

Dato che i coefficienti sono interi, definiscono un sistema di equazioni in  $\mathbb{F}_p$  per ogni primo  $p$ . Il determinante di  $A$  è 42; quindi il sistema ha un'unica soluzione in  $\mathbb{F}_p$  per ogni primo  $p$  diverso da 2, 3 e 7. Così, se  $p = 13$ , eseguendo i calcoli (modulo 13), otteniamo  $\det A = 3$ . Abbiamo già visto che  $3^{-1} = 9$  in  $\mathbb{F}_{13}$ . Dunque possiamo usare la regola di Cramer per calcolare:

$$A^{-1} = \begin{bmatrix} 2 & -1 \\ 8 & 7 \end{bmatrix} \quad \text{e} \quad X = A^{-1}B = \begin{bmatrix} 7 \\ 4 \end{bmatrix}, \text{ in } \mathbb{F}_{13}.$$

Il sistema non ha soluzioni né in  $\mathbb{F}_2$  né in  $\mathbb{F}_3$ . Ha soluzioni in  $\mathbb{F}_7$ , sebbene in tale campo risulti  $\det A = 0$ .

Osserviamo, per inciso, che le matrici invertibili a elementi nel campo  $\mathbb{F}_p$  forniscono nuovi esempi di gruppi finiti, ossia, i gruppi lineari generali su campi finiti:

$$GL_n(\mathbb{F}_p) = \{\text{matrici invertibili } n \times n \text{ a elementi in } \mathbb{F}_p\}.$$

Il più piccolo di essi è il gruppo  $GL_2(\mathbb{F}_2)$  delle matrici invertibili  $2 \times 2$  a elementi in  $\mathbb{F}_2$ , il quale è costituito dalle sei matrici:

$$(2.10) \quad GL_2(\mathbb{F}_2) = \left\{ \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

Vi è una proprietà dei campi finiti  $F = \mathbb{F}_p$  che li distingue dai sottocampi di  $\mathbb{C}$  e che interessa talvolta i calcoli. Si tratta del fatto che sommando 1 con se stesso un certo numero di volte (precisamente  $p$  volte) si ottiene 0. Si dice che un campo  $F$  ha caratteristica  $p$ , se  $1 + \dots + 1$  ( $p$  volte) = 0 in  $F$ , e se inoltre  $p$  è il più piccolo intero positivo con tale proprietà. In altre parole, la caratteristica di  $F$  è l'ordine di 1, quale elemento del gruppo additivo  $F$ , purché l'ordine sia finito

(cap. 2, § 2). Nel caso in cui l'ordine è infinito, ossia  $1 + \dots + 1$  non è mai 0 in  $F$ , si dice, paradossalmente, che il campo ha *caratteristica zero*. Pertanto i sottocampi di  $\mathbb{C}$  hanno caratteristica zero, mentre il campo primo  $\mathbb{F}_p$  ha caratteristica  $p$ . Si può dimostrare che la caratteristica di qualsiasi campo  $F$  o è zero oppure è un numero primo.

Ora, sia  $F$  un campo arbitrario. Uno spazio vettoriale su un campo  $F$  si definisce come in (1.6), sostituendo  $\mathbb{R}$  con  $F$ .

(2.11) DEFINIZIONE Uno spazio vettoriale  $V$  su un campo  $F$  è un insieme dotato di due leggi di composizione:

(a) **addizione:**  $V \times V \rightarrow V$ , scritta

$$v, w \mapsto v + w,$$

(b) **moltiplicazione per uno scalare:**  $F \times V \rightarrow V$ , scritta

$$c, v \mapsto cv,$$

che soddisfa i seguenti assiomi:

- (i)  $V$  è un gruppo commutativo rispetto all'addizione.
- (ii) La moltiplicazione per uno scalare è associativa con la moltiplicazione in  $F$ .
- (iii) L'elemento 1 agisce come l'identità:  $1v = v$ , per ogni  $v \in V$ .
- (iv) Valgono due leggi distributive:

$$(a+b)v = av + bv \quad \text{e} \quad a(v+w) = av + aw,$$

per ogni  $a, b \in F$  e  $v, w \in V$ .

Tutto il contenuto del paragrafo 1 può essere rienunciato sostituendo il campo  $\mathbb{R}$  con  $F$ . Ad esempio, lo spazio  $F^n$  dei vettori riga  $(a_1, \dots, a_n)$ , con  $a_i \in F$ , è uno spazio vettoriale su  $F$ , e così via.

È importante notare che la definizione di spazio vettoriale include implicitamente la scelta di un campo  $F$ . Gli elementi di questo campo  $F$  sono chiamati spesso *scalari*. Di solito, manterremo fisso questo campo. Naturalmente, se  $V$  è uno spazio vettoriale complesso, ossia uno spazio vettoriale su  $\mathbb{C}$ , e se  $F$  è un sottocampo arbitrario di  $\mathbb{C}$ , allora  $V$  risulta anche, in modo naturale, uno spazio vettoriale su  $F$ , poiché  $cv$  è definito per ogni  $c \in F$ . Tuttavia la struttura di spazio vettoriale viene cambiata, quando restringiamo gli scalari da  $\mathbb{C}$  a  $F$ .

Due concetti importanti analoghi ai sottogruppi e agli isomorfismi di gruppi sono quelli di sottospazio e di isomorfismo di spazi vettoriali. Abbiamo già definito i sottospazi di uno spazio vettoriale complesso, e la definizione è la stessa per un

campo qualsiasi. Un *sottospazio*  $W$  di uno spazio vettoriale  $V$  (su un campo  $F$ ) è un sottoinsieme di  $V$  con le seguenti proprietà:

- (2.12) (a) Se  $w, w' \in W$ , allora  $w + w' \in W$ .
- (b) Se  $w \in W$  e  $c \in F$ , allora  $cw \in W$ .
- (c)  $0 \in W$ .

Un sottospazio  $W$  è chiamato sottospazio *proprio* di  $V$ , se esso è diverso dall'intero spazio  $V$  e dal sottospazio nullo  $\{0\}$ .

Si vede facilmente che un sottospazio è precisamente un sottoinsieme sul quale le leggi di composizione inducono la struttura di spazio vettoriale.

Come si è visto nel paragrafo 1, lo spazio di tutte le soluzioni di un sistema di  $m$  equazioni lineari in  $n$  incognite

$$AX = 0$$

a coefficienti in  $F$ , è un esempio di un sottospazio dello spazio  $F^n$ .

(2.13) DEFINIZIONE Un isomorfismo  $\varphi$  da uno spazio vettoriale  $V$  a uno spazio vettoriale  $V'$ , entrambi sullo stesso campo  $F$ , è un'applicazione biiettiva  $\varphi : V \rightarrow V'$  compatibile con le leggi di composizione, ossia, un'applicazione biiettiva tale che:

- (a)  $\varphi(v + v') = \varphi(v) + \varphi(v')$  e (b)  $\varphi(cv) = c\varphi(v)$ ,

per ogni  $v, v' \in V$  e per ogni  $c \in F$ .

#### (2.14) Esempi

- (a) Lo spazio  $F^n$  dei vettori riga  $n$ -dimensionali è isomorfo allo spazio dei vettori colonna  $n$ -dimensionali.
- (b) Consideriamo l'insieme dei numeri complessi  $\mathbb{C}$  come uno spazio vettoriale reale, come in (1.8b). Allora l'applicazione  $\varphi : \mathbb{R}^2 \rightarrow \mathbb{C}$  che manda  $(a, b)$  in  $a + bi$  è un isomorfismo.

### 3 Basi e dimensione

In questo paragrafo studieremo le nozioni che derivano dall'uso delle due operazioni (addizione e moltiplicazione per uno scalare) in uno spazio vettoriale astratto. I nuovi concetti sono: *sottospazio generato*, *indipendenza lineare* e *base*.

Conviene lavorare qui con insiemi *ordinati* di vettori. L'ordinamento sarà trascurabile quasi sempre, ma risulterà essenziale nei calcoli espliciti. Finora abbiamo

indicato gli insiemi non ordinati con parentesi graffe, quindi, per distinguerli, useremo per gli insiemi ordinati le parentesi tonde. Così l'insieme ordinato  $(a, b)$  è diverso dall'insieme ordinato  $(b, a)$ , mentre gli insiemi  $\{a, b\}$  e  $\{b, a\}$  sono uguali. Inoltre in un insieme ordinato ci possono essere ripetizioni; per esempio,  $(a, a, b)$  è diverso da  $(a, b)$ , mentre per gli insiemi non ordinati  $\{a, a, b\}$  e  $\{a, b\}$  indicano lo stesso insieme.

Sia  $V$  uno spazio vettoriale su un campo  $F$  e sia  $(v_1, \dots, v_n)$  un insieme ordinato di elementi di  $V$ . Una *combinazione lineare* di  $(v_1, \dots, v_n)$  è un qualsiasi vettore della forma:

$$(3.1) \quad w = c_1 v_1 + c_2 v_2 + \dots + c_n v_n, \text{ con } c_i \in F.$$

Per esempio, supponiamo che l'insieme ordinato sia costituito dai due vettori di  $\mathbb{R}^3$  considerati in (1.4):  $v_1 = (1, 0, 1)^t$  e  $v_2 = (1, 2, 0)^t$ . Allora una combinazione lineare avrà la forma (1.5):

$$(c_1 + c_2, 2c_2, c_1)^t.$$

Il vettore  $(3, 4, 1)^t = v_1 + 2v_2$  è una combinazione lineare di questo tipo.

Una soluzione  $x$  di un sistema di equazioni lineari scritto nella forma matriciale:  $AX = B$  [cap. 1 (1.9)] permette di esprimere il vettore colonna  $B$  come una combinazione lineare delle colonne della matrice  $A$ . I coefficienti sono gli elementi del vettore  $X$ .

Una combinazione lineare di un singolo vettore  $(v)$  è un multiplo  $cv$  di  $v$ .

L'insieme di tutti i vettori  $w$  che sono combinazioni lineari di  $(v_1, \dots, v_n)$  costituisce un sottospazio  $W$  di  $V$ , chiamato il sottospazio *generato* da  $(v_1, \dots, v_n)$ . Infatti, se  $w = c_1 v_1 + \dots + c_n v_n$  e  $w' = c'_1 v_1 + \dots + c'_n v_n$  sono elementi di  $W$ , allora tale risulta anche

$$w + w' = (c_1 + c'_1) v_1 + \dots + (c_n + c'_n) v_n,$$

e inoltre, se  $a \in F$ , allora  $aw = (ac_1) v_1 + \dots + (ac_n) v_n$  appartiene a  $W$ . Pertanto  $w + w'$  e  $aw$  appartengono a  $W$ . Infine,  $0 = 0v_1 + \dots + 0v_n \in W$ . Ciò prova che le condizioni (2.12) sono verificate.

Il sottospazio generato da un insieme finito  $S$  sarà denotato spesso con  $\text{Span } S$ . È chiaro che  $\text{Span } S$  è il più piccolo sottospazio di  $V$  che contiene  $S$ . Si noti che l'ordine, qui, è irrilevante, infatti il sottospazio generato da  $S$  è lo stesso, qualunque sia l'ordinamento di  $S$ .

È possibile definire anche il sottospazio generato da un insieme infinito di vettori, come vedremo nel paragrafo 5. In questo paragrafo, supponiamo che gli insiemi in questione siano *finiti*.

(3.2) PROPOSIZIONE Sia  $S$  un insieme di vettori di  $V$ , e sia  $W$  un sottospazio di  $V$ . Se  $S \subset W$ , allora  $\text{Span } S \subset W$ .

Ciò è ovvio, poiché  $W$  è chiuso rispetto all'addizione e alla moltiplicazione per uno scalare. Se  $S \subset W$ , qualsiasi combinazione lineare di vettori di  $S$  appartiene ancora a  $W$ . ■

Una relazione lineare tra i vettori  $v_1, \dots, v_n$  è una qualsiasi relazione della forma:

$$(3.3) \quad c_1v_1 + c_2v_2 + \dots + c_nv_n = 0,$$

dove i coefficienti  $c_i$  appartengono a  $F$ . Un insieme ordinato di vettori  $(v_1, \dots, v_n)$  si dice *linearmente indipendente*, se non esiste nessuna relazione lineare tra i vettori dell'insieme, tranne la relazione banale in cui tutti i coefficienti  $c_i$  sono nulli. È utile enunciare tale condizione in positivo:

(3.4) Sia  $(v_1, \dots, v_n)$  un insieme linearmente indipendente. Allora dall'equazione:  $c_1v_1 + \dots + c_nv_n = 0$ , si può concludere che  $c_i = 0$ , per ogni  $i = 1, \dots, n$ .

Viceversa, se vale (3.4), allora i vettori sono linearmente indipendenti.

I vettori (1.4) sono linearmente indipendenti.

Si noti che un insieme linearmente indipendente  $S$  non può contenere elementi ripetuti. Infatti, se due vettori  $v_i, v_j$  di  $S$  sono uguali, allora

$$v_i - v_j = 0$$

è una relazione lineare della forma (3.3), essendo gli altri coefficienti tutti nulli. Inoltre, nessun vettore  $v_i$  di una famiglia linearmente indipendente può essere nullo, poiché altrimenti si avrebbe la relazione lineare:  $v_i = 0$ .

Un insieme di vettori che non è linearmente indipendente si dice *linearmente dipendente*.

Se  $V$  è lo spazio  $F^m$  e se i vettori  $(v_1, \dots, v_n)$  sono dati esplicitamente, si può stabilire l'indipendenza lineare risolvendo un sistema di equazioni lineari omogenee. Infatti, dire che una combinazione lineare  $x_1v_1 + \dots + x_nv_n$  è nulla significa che ogni coordinata di  $x_1v_1 + \dots + x_nv_n$  è zero, e ciò dà luogo a  $m$  equazioni nelle  $n$  incognite  $x_i$ . Per esempio, consideriamo l'insieme dei tre vettori:

$$(3.5) \quad v_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

Indichiamo con  $A$  la matrice avente come colonne tali vettori:

$$(3.6) \quad A = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}.$$

Una combinazione lineare generica di tali vettori avrà la forma:  $x_1v_1 + x_2v_2 + x_3v_3$ . Portando i coefficienti a destra, possiamo scrivere questa combinazione lineare nella forma:  $AX$ , dove  $X = (x_1, x_2, x_3)^t$ . Poiché  $\det A = 1$ , l'equazione  $AX = 0$  possiede soltanto la soluzione banale, e ciò dimostra che  $(v_1, v_2, v_3)$  è un insieme linearmente indipendente. D'altra parte, se aggiungiamo a questo insieme un quarto vettore arbitrario  $v_4$ , otteniamo un insieme linearmente dipendente, poiché ogni sistema di tre equazioni omogenee in quattro incognite possiede una soluzione non banale [cap. 1 (2.17)].

Vediamo ora alcune proprietà elementari relative all'indipendenza lineare.

### (3.7) PROPOSIZIONE

- (a) Un insieme ottenuto riordinando un insieme linearmente indipendente è linearmente indipendente.
- (b) Se  $v_1 \in V$  è un vettore non nullo, l'insieme  $(v_1)$  è linearmente indipendente.
- (c) Un insieme  $(v_1, v_2)$  di due vettori è linearmente dipendente se e solo se  $v_1 = 0$  oppure  $v_2$  è un multiplo di  $v_1$ .

Verifichiamo la terza asserzione. Supponiamo che  $(v_1, v_2)$  sia linearmente dipendente, e che si abbia una relazione della forma  $c_1v_1 + c_2v_2 = 0$ , con  $c_1, c_2$  non entrambi nulli. Se  $c_2 \neq 0$ , possiamo risolvere rispetto a  $v_2$ , ottenendo:

$$v_2 = \frac{-c_1}{c_2} v_1.$$

In questo caso,  $v_2$  è un multiplo di  $v_1$ . Se  $c_2 = 0$ , allora  $c_1 \neq 0$  e la relazione prova che  $v_1 = 0$ . Viceversa, se  $v_2 = cv_1$ , la relazione  $cv_1 - v_2 = 0$  prova che l'insieme  $(v_1, v_2)$  è linearmente dipendente, e se  $v_1 = 0$ , allora la relazione  $v_1 + 0v_2 = 0$  dimostra la stessa cosa. ■

Un insieme di vettori  $(v_1, \dots, v_n)$  che è linearmente indipendente e che inoltre genera  $V$  si chiama una *base*. Per esempio, i vettori (1.4) formano una base per lo spazio delle soluzioni dell'equazione lineare (1.3). Useremo spesso un simbolo del tipo **B** per denotare una base.

Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base. Allora, poiché **B** genera  $V$ , ogni vettore  $w \in V$  può essere scritto come una combinazione lineare della forma (3.1):  $w = c_1v_1 + c_2v_2 + \dots + c_nv_n$ , con  $c_i \in F$ . Poiché **B** è linearmente indipendente, tale espressione è unica.

(3.8) PROPOSIZIONE L'insieme  $\mathbf{B} = (v_1, \dots, v_n)$  è una base se e solo se ogni vettore  $w \in V$  può essere scritto in modo unico nella forma (3.1).

*Dimostrazione.* Supponiamo che  $\mathbf{B}$  sia una base e che  $w$  sia scritto come una combinazione lineare in due modi, ad esempio  $w = c_1 v_1 + \dots + c_n v_n$  e  $w = c'_1 v_1 + \dots + c'_n v_n$ . Allora si ha:

$$0 = w - w = (c_1 - c'_1)v_1 + \dots + (c_n - c'_n)v_n.$$

Ne segue, in virtù di (3.4), che  $c_1 - c'_1 = 0, \dots, c_n - c'_n = 0$ , sicché le due combinazioni lineari coincidono. D'altra parte, la definizione di indipendenza lineare per  $\mathbf{B}$  può essere rientrata dicendo che il vettore nullo ha un'unica espressione come combinazione lineare. Ciò dimostra il viceversa. ■

### (3.9) Esempio

Sia  $V = F^n$  lo spazio dei vettori colonna e denotiamo con  $e_i$  il vettore colonna con 1 nella posizione  $i$ -esima e zero altrove. Gli  $n$  vettori  $e_i$  formano una base per  $F^n$ , chiamata la *base canonica*, già introdotta in precedenza (cap. 1, §4). Essa sarà denotata con  $\mathbf{E}$ . Ogni vettore  $X = (x_1, \dots, x_n)^t$  si scrive in modo unico come una combinazione lineare di  $\mathbf{E} = (e_1, \dots, e_n)$ :

$$X = x_1 e_1 + \dots + x_n e_n.$$

L'insieme (3.5) è un'altra base di  $\mathbb{R}^3$ .

Passiamo ora a discutere i risultati più importanti (3.15-3.17) che collegano tra loro le nozioni di sottospazio generato da un insieme, indipendenza lineare e base.

(3.10) PROPOSIZIONE Sia  $L$  un sottoinsieme ordinato linearmente indipendente di  $V$  e sia  $v$  un vettore di  $V$ . Allora l'insieme ordinato  $L' = (L, v)$  ottenuto aggiungendo  $v$  a  $L$  è linearmente indipendente se e solo se  $v$  non appartiene al sottospazio generato da  $L$ .

*Dimostrazione.* Sia  $L = (v_1, \dots, v_r)$ . Allora, se  $v \in \text{Span } L$ , si ha:  $v = c_1 v_1 + \dots + c_r v_r$ , con  $c_i \in F$ . Pertanto

$$c_1 v_1 + \dots + c_r v_r + (-1)v = 0$$

è una relazione lineare tra i vettori di  $L'$ , con coefficienti non tutti nulli. Dunque  $L'$  è linearmente dipendente.

Viceversa, supponiamo che  $L'$  sia linearmente dipendente, sicché esiste almeno una relazione lineare

$$c_1 v_1 + \dots + c_r v_r + bv = 0,$$

con i coefficienti non tutti nulli. Allora risulta certamente:  $b \neq 0$ . Infatti, se fosse  $b = 0$ , l'espressione precedente si ridurrebbe a

$$c_1 v_1 + \dots + c_r v_r = 0.$$

Poiché, per ipotesi,  $L$  è linearmente indipendente, ne segue che anche i coefficienti  $c_1, \dots, c_r$  sono nulli, il che contraddice l'ipotesi iniziale. Quindi risulta  $b \neq 0$ , da cui si ottiene:

$$v = \frac{-c_1}{b} v_1 + \dots + \frac{-c_r}{b} v_r.$$

Dunque  $v \in \text{Span } L$ . ■

(3.11) PROPOSIZIONE Sia  $S$  un insieme ordinato di vettori, sia  $v$  un vettore di  $V$  e poniamo  $S' = (S, v)$ . Allora  $\text{Span } S = \text{Span } S'$  se e solo se  $v \in \text{Span } S$ .

*Dimostrazione.* Per definizione,  $v \in \text{Span } S'$ . Pertanto, se  $v \notin \text{Span } S$ , allora  $\text{Span } S \neq \text{Span } S'$ . Viceversa, se  $v \in \text{Span } S$ , allora  $S' \subset \text{Span } S$  e quindi  $\text{Span } S' \subset \text{Span } S$  (cfr. 3.2). L'inclusione opposta:  $\text{Span } S' \supset \text{Span } S$  è banale, sicché  $\text{Span } S' = \text{Span } S$ . ■

(3.12) DEFINIZIONE Uno spazio vettoriale  $V$  si dice di dimensione finita se esiste un insieme finito  $S$  che genera  $V$ .

Supporremo fino alla fine del paragrafo che lo spazio vettoriale  $V$  assegnato sia di dimensione finita.

(3.13) PROPOSIZIONE Ogni insieme finito  $S$  che genera  $V$  contiene una base. In particolare, ogni spazio vettoriale di dimensione finita possiede una base.

*Dimostrazione.* Sia  $S = (v_1, \dots, v_n)$  un insieme che genera  $V$  e supponiamo che  $S$  non sia linearmente indipendente. Allora esiste una relazione lineare:

$$c_1 v_1 + \dots + c_n v_n = 0$$

in cui almeno un coefficiente  $c_i$  è diverso da zero, sia ad esempio  $c_n \neq 0$ . Ne segue

$$v_n = \frac{-c_1}{c_n} v_1 + \dots + \frac{-c_{n-1}}{c_n} v_{n-1}.$$

Ciò prova che  $v_n \in \text{Span}(v_1, \dots, v_{n-1})$ . Ponendo  $v = v_n$  e  $S = (v_1, \dots, v_{n-1})$  in (3.11), si conclude che  $\text{Span}(v_1, \dots, v_{n-1}) = \text{Span}(v_1, \dots, v_n) = V$ . Pertanto possiamo eliminare  $v_n$  da  $S$ . Proseguendo in questo modo, otteniamo alla fine una famiglia di vettori che è linearmente indipendente e inoltre genera  $V$ , ossia una base.

**Osservazione.** Se  $V$  è lo spazio vettoriale nullo  $\{0\}$  la dimostrazione precedente non è valida. Infatti, partendo da un insieme arbitrario di vettori in  $V$  (tutti uguali a zero), e seguendo il procedimento sopra esposto, i vettori vengono eliminati uno alla volta, finché resta un solo vettore  $v_1 = 0$ , e d'altra parte  $\{0\}$  è un insieme linearmente dipendente. Come si può risolvere il problema? Naturalmente lo spazio vettoriale nullo non è particolarmente interessante. Tuttavia il problema resta e può comparire in qualsiasi momento. Dobbiamo ammettere la possibilità che uno spazio vettoriale che viene fuori nel corso di qualche calcolo, come accade ad esempio risolvendo un sistema di equazioni lineari omogenee, sia lo spazio nullo. Per evitare di dover menzionare ogni volta questo fatto, adottiamo le seguenti convenzioni:

- (3.14) (a) L'insieme vuoto è linearmente indipendente.
- (b) Lo spazio generato dall'insieme vuoto è il sottospazio nullo.

Dunque l'insieme vuoto è una base per lo spazio vettoriale nullo. Con tali convenzioni, possiamo eliminare l'ultimo vettore  $v_1 = 0$ , e salvare così la dimostrazione. ■

(3.15) PROPOSIZIONE *Sia  $V$  uno spazio vettoriale di dimensione finita. Allora ogni insieme linearmente indipendente  $L$  può essere ampliato con l'aggiunta di nuovi elementi, in modo da ottenere una base.*

**Dimostrazione.** Sia  $S$  un insieme finito che genera  $V$ . Se tutti gli elementi di  $S$  appartengono a  $\text{Span}L$ , allora  $L$  genera  $V$  (cfr. 3.2) e quindi è una base. Altrimenti, scegliamo un vettore  $v$  in  $S$ , che non appartiene a  $\text{Span}L$ . In virtù di (3.10), l'insieme  $(L, v)$  è linearmente indipendente. Proseguendo in questo modo, si ottiene una base. ■

(3.16) PROPOSIZIONE *Siano  $S, L$  sottoinsiemi finiti di  $V$ . Supponiamo che  $S$  generi  $V$  e che  $L$  sia linearmente indipendente. Allora il numero degli elementi di  $S$  è maggiore o uguale al numero degli elementi di  $L$ .*

**Dimostrazione.** Per dimostrare la tesi, scriviamo ciò che significa una relazione di dipendenza lineare su  $L$  in termini dell'insieme  $S$ , ottenendo un sistema omogeneo di  $m$  equazioni lineari in  $n$  incognite, dove  $m = |S|$  e  $n = |L|$ . Sia

$s = (v_1, \dots, v_m)$  e  $L = (w_1, \dots, w_n)$ . Scriviamo ciascun vettore  $w_j$  come una combinazione lineare di  $S$ , ciò che è possibile poiché  $S$  genera  $V$ , e sia:

$$w_j = a_{1j}v_1 + \dots + a_{mj}v_m = \sum_i a_{ij}v_i.$$

**Sia**

$$u = c_1w_1 + \dots + c_nw_n = \sum_j c_jw_j$$

una combinazione lineare. Sostituendo a  $w_j$  la sua espressione, si ottiene:

$$u = \sum_{i,j} c_j a_{ij} v_i.$$

In questa somma, il coefficiente di  $v_i$  è

$$\sum_j a_{ij}c_j.$$

Se questo coefficiente è zero per ogni  $i$ , allora  $u = 0$ . Pertanto, per trovare una relazione lineare tra i vettori di  $L$ , basta risolvere il sistema

$$\sum_j a_{ij}x_j = 0$$

di  $m$  equazioni in  $n$  incognite. Se  $m < n$ , allora tale sistema ha una soluzione non banale [cfr. cap. 1, (2.17)], e pertanto  $L$  è linearmente dipendente. ■

(3.17) PROPOSIZIONE *Due basi  $B_1, B_2$  dello spazio vettoriale  $V$  hanno lo stesso numero di elementi.*

**Dimostrazione.** Se poniamo  $B_1 = S$ ,  $B_2 = L$  in (3.16), otteniamo:  $|B_1| \geq |B_2|$ . Per simmetria, si ha:  $|B_2| \geq |B_1|$ , da cui la tesi. ■

(3.18) DEFINIZIONE *La dimensione di uno spazio vettoriale di dimensione finita  $V$  è il numero dei vettori di una sua base. La dimensione si denota con  $\dim V$ .*

(3.19) PROPOSIZIONE

- (a) *Se  $S$  genera  $V$ , allora  $|S| \geq \dim V$ , e vale l'uguaglianza soltanto se  $S$  è una base.*
- (b) *Se  $L$  è linearmente indipendente, allora  $|L| \leq \dim V$ , e vale l'uguaglianza soltanto se  $L$  è una base.*

**Dimostrazione.** Segue da (3.13) e (3.15). ■

(3.20) PROPOSIZIONE Se  $W \subset V$  è un sottospazio di uno spazio vettoriale di dimensione finita, allora  $W$  è di dimensione finita, e  $\dim W \leq \dim V$ . Inoltre, si ha  $\dim W = \dim V$  soltanto se  $W = V$ .

*Dimostrazione.* Il risultato è ovvio, una volta dimostrato che  $W$  è di dimensione finita. Infatti, se  $W < V$ , ossia  $W$  è contenuto in  $V$  ma non è uguale a  $V$ , allora una base di  $W$  non potrà generare  $V$ , tuttavia essa può essere estesa a una base di  $V$ , in virtù di (3.15). Ne segue che  $\dim W < \dim V$ .

Verifichiamo ora che  $W$  è di dimensione finita. Se un insieme linearmente indipendente assegnato  $L$  in  $W$  non genera  $W$ , esiste un vettore  $w$  di  $W$  non appartenente a  $\text{Span } L$ , e  $(L, w)$  è linearmente indipendente, in virtù della proposizione (3.10). Pertanto, possiamo partire dall'insieme vuoto e aggiungere elementi di  $W$ , utilizzando (3.10), sperando di ottenere alla fine una base di  $W$ . Ora è ovvio che, se  $L$  è un insieme linearmente indipendente in  $W$ , allora  $L$  è anche linearmente indipendente, considerato come un sottoinsieme di  $V$ . Pertanto, da (3.16) segue che  $|L| \leq n = \dim V$ . Dunque, il procedimento che consiste nell'aggiungere vettori a  $L$  termina dopo al più  $n$  passi. Quando non è più possibile applicare di nuovo (3.10),  $L$  è una base di  $W$ . Ciò prova che  $W$  è di dimensione finita, come richiesto. ■

### Osservazioni

- (a) I risultati fondamentali da ricordare sono: (3.13), (3.15) e (3.16). Gli altri risultati discendono da questi.
- (b) Gli argomenti sviluppati non sono molto profondi. Date le definizioni, è possibile che il lettore pervenga da solo alla dimostrazione del risultato principale (3.16), anche se probabilmente il primo tentativo risulterebbe un po' goffo.

Un esempio importante di spazio vettoriale si ottiene a partire da un insieme arbitrario  $S$ , considerando combinazioni lineari di elementi di  $S$  a coefficienti in  $F$ , in modo formale. Se  $S = (s_1, \dots, s_n)$  è un insieme ordinato finito i cui elementi sono a due a due distinti tra loro, allora lo spazio  $V = V(S)$  è l'insieme di tutte le espressioni della forma:

$$(3.21) \quad a_1s_1 + \dots + a_ns_n, \quad \text{con } a_i \in F.$$

L'addizione e la moltiplicazione per uno scalare vengono effettuate formalmente, supponendo che non esistano relazioni tra gli elementi  $s_i$ :

$$(3.22) \quad (a_1s_1 + \dots + a_ns_n) + (b_1s_1 + \dots + b_ns_n) = (a_1 + b_1)s_1 + \dots + (a_n + b_n)s_n$$

$$c(a_1s_1 + \dots + a_ns_n) = (ca_1)s_1 + \dots + (ca_n)s_n.$$

Tale spazio vettoriale è isomorfo a  $F^n$ , mediante la corrispondenza:

$$(3.23) \quad (a_1, \dots, a_n) \mapsto a_1s_1 + \dots + a_ns_n.$$

Pertanto gli elementi  $s_i$ , interpretati come le combinazioni lineari:

$$s_1 = 1s_1 + 0s_2 + \dots + 0s_n, \dots$$

formano una base che corrisponde alla base canonica di  $F^n$  mediante l'isomorfismo (3.23). Per questo motivo,  $V(S)$  spesso viene chiamato *lo spazio con base S*, oppure *lo spazio delle combinazioni lineari formali di S*. Se  $S$  è un insieme infinito,  $V(S)$  viene definito come lo spazio di tutte le espressioni finite (3.21), dove  $s_i \in S$  (cfr. § 5).

Poiché  $V(S)$  è isomorfo a  $F^n$  quando  $S$  contiene  $n$  elementi, non vi è alcuna necessità logica per introdurre tale spazio. Tuttavia, in molte applicazioni,  $V(S)$  possiede un'interpretazione naturale. Per esempio, se  $S$  è un insieme di ingredienti, allora un vettore  $v$  può rappresentare una ricetta. Oppure, se  $S$  è un insieme di punti nel piano, allora un vettore  $v$  dato da (3.21) può essere interpretato come un insieme di pesi nei punti di  $S$ .

### 4 Calcoli con le basi

L'utilità delle basi negli spazi vettoriali consiste nel fornire un metodo di calcolo, e in questo paragrafo ci proponiamo di imparare a usarle. Considereremo due problemi: esprimere un vettore mediante una base assegnata e mettere in relazione tra loro due basi diverse di uno stesso spazio vettoriale.

Supponiamo di avere una base  $(v_1, \dots, v_n)$  di uno spazio vettoriale  $V$ . Ciò significa che ogni vettore  $v \in V$  può essere espresso come una combinazione lineare:

$$(4.1) \quad v = x_1v_1 + \dots + x_nv_n, \quad \text{con } x_i \in F,$$

in modo unico. Gli scalari  $x_i$  sono chiamati le *coordinate* di  $v$ , e il vettore colonna

$$(4.2) \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

è chiamato il *vettore delle coordinate* di  $v$ , rispetto alla base assegnata. Ci poniamo il problema di calcolare tale vettore delle coordinate.

Il caso più semplice da esaminare è quello in cui  $V$  è lo spazio dei vettori colonna  $F^n$ . Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di  $F^n$ . Allora ciascun elemento  $v_i$  di  $\mathbf{B}$  è un vettore colonna, e pertanto la  $n$ -upla  $(v_1, \dots, v_n)$  forma una matrice  $n \times n$ . Sembra opportuno introdurre un nuovo simbolo per questa matrice, sicché la scriviamo nella forma:

$$(4.3) \quad [\mathbf{B}] = \begin{bmatrix} & & & \\ | & & & | \\ v_1 & \dots & v_n \\ | & & & | \end{bmatrix}.$$

Per esempio, se  $\mathbf{B}$  è la base

$$(4.4) \quad v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 3 \\ 5 \end{bmatrix}, \quad \text{allora } [\mathbf{B}] = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}.$$

Se  $\mathbf{E} = (e_1, \dots, e_n)$  è la base canonica, la matrice  $[\mathbf{E}]$  è la matrice identità.

Una combinazione lineare  $x_1v_1 + \dots + x_nv_n$  può essere scritta come la matrice prodotto:

$$(4.5) \quad [\mathbf{B}]X = \begin{bmatrix} | & & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1x_1 + \dots + v_nx_n,$$

dove  $X$  denota il vettore colonna  $(x_1, \dots, x_n)^t$ . Questo è un altro esempio di moltiplicazione per blocchi. L'unica novità è che la definizione di moltiplicazione tra matrici ha prodotto lo spostamento dei coefficienti scalari  $x_i$  alla destra dei vettori, ma non ha importanza.

Ora, se è dato un vettore  $Y = (y_1, \dots, y_n)^t$ , possiamo determinare il suo vettore delle coordinate rispetto alla base  $\mathbf{B}$ , risolvendo l'equazione:

$$(4.6) \quad \begin{bmatrix} | & & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad \text{ossia} \quad [\mathbf{B}]X = Y$$

rispetto al vettore delle incognite  $X$ . Ciò si fa invertendo la matrice  $[\mathbf{B}]$ .

(4.7) PROPOSIZIONE Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di  $F^n$ , e sia  $Y \in F^n$  un vettore. Allora il vettore delle coordinate di  $Y$  rispetto alla base  $\mathbf{B}$  è:

$$X = [\mathbf{B}]^{-1}Y. \blacksquare$$

Si noti che, se  $\mathbf{B}$  è la base canonica  $\mathbf{E}$ , riotteniamo  $Y$ , poiché  $[\mathbf{E}]$  è la matrice identica.

Nell'esempio (4.4), si ha:

$$[\mathbf{B}]^{-1} = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix}.$$

Pertanto il vettore delle coordinate di  $Y = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$  è  $X = \begin{bmatrix} 7 \\ -2 \end{bmatrix}$ ; ciò significa che  $Y = 7v_1 - 2v_2$ .

Naturalmente, possiamo procedere in questo modo soltanto se la matrice è invertibile. Per fortuna,  $[\mathbf{B}]$  è sempre invertibile, e in realtà può essere una matrice invertibile qualsiasi.

(4.8) PROPOSIZIONE Sia  $A$  una matrice  $n \times n$  con elementi in un campo  $F$ . Allora le colonne di  $A$  formano una base di  $F^n$  se e solo se  $A$  è invertibile.

**Dimostrazione.** Indichiamo l' $i$ -esima colonna di  $A$  con  $v_i$ . Per un qualsiasi vettore colonna  $X = (x_1, \dots, x_n)^t$ , la matrice prodotto  $AX = v_1x_1 + \dots + v_nx_n$  è una combinazione lineare dell'insieme  $(v_1, \dots, v_n)$ . Pertanto tale insieme è linearmente indipendente se e soltanto se l'unica soluzione dell'equazione  $AX = 0$  è la soluzione banale  $X = 0$ . Come è noto, ciò è vero se e soltanto se  $A$  è invertibile [cap. 1 (2.18)]. Inoltre, se  $(v_1, \dots, v_n)$  è un insieme linearmente indipendente, allora costituisce una base, poiché la dimensione di  $F^n$  è  $n$ . ■

Sia ora  $V$  uno spazio vettoriale astratto. Vogliamo usare la notazione matriciale per facilitare i calcoli con le basi, ed è a questo scopo che abbiamo scelto a suo tempo la notazione per gli insiemi ordinati di vettori:

$$(4.9) \quad (v_1, \dots, v_n).$$

Forse un insieme ordinato di questo tipo dovrebbe essere chiamato un *ipervettore*. Se i vettori in questione non sono assegnati concretamente, non potremo rappresentare tale ipervettore mediante una matrice, sicché esso verrà trattato formalmente, come se fosse un vettore. Poiché la moltiplicazione di due elementi di uno spazio vettoriale non è definita, non possiamo moltiplicare tra loro due matrici i cui elementi sono vettori. Ma nulla ci impedisce di moltiplicare l'ipervettore  $(v_1, \dots, v_m)$  per una matrice di scalari. Così una combinazione lineare di tali vettori può essere scritta come il prodotto dell'ipervettore per un vettore colonna  $X$ :

$$(4.10) \quad (v_1, \dots, v_m) \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} = v_1x_1 + \dots + v_mx_m.$$

Calcolando il prodotto otteniamo un altro vettore, dato da una combinazione lineare. I coefficienti scalari  $x_i$  compaiono alla destra dei vettori, come prima. Se denotiamo l'insieme  $(v_1, \dots, v_m)$  con  $\mathbf{B}$ , allora la notazione per tale combinazione lineare diventa molto compatta:  $\mathbf{B}X = v_1x_1 + \dots + v_mx_m$ .

Possiamo anche moltiplicare un ipervettore a destra per una matrice di scalari. Se  $A$  è una matrice  $m \times n$ , il prodotto sarà un altro ipervettore, diciamo  $(w_1, \dots, w_n)$ :

$$(4.11) \quad (v_1, \dots, v_m) \begin{bmatrix} A \end{bmatrix} = (w_1, \dots, w_n).$$

Per calcolare il prodotto, utilizziamo la regola per la moltiplicazione tra matrici:

$$(4.12) \quad w_j = v_1 a_{1j} + v_2 a_{2j} + \cdots + v_m a_{mj}.$$

Quindi ciascun vettore  $w_j$  è una combinazione lineare di  $(v_1, \dots, v_m)$ , e i coefficienti scalari di questa combinazione lineare formano le colonne della matrice  $A$ . Ecco il significato dell'equazione. Per esempio,

$$(v_1, v_2) \begin{bmatrix} 3 & 2 & 1 \\ 4 & 0 & 1 \end{bmatrix} = (3v_1 + 4v_2, 2v_1, v_1 + v_2).$$

Rienunciamo in modo formale il risultato così ottenuto:

(4.13) PROPOSIZIONE *Siano  $S = (v_1, \dots, v_m)$  e  $U = (w_1, \dots, w_n)$  insiemi ordinati di elementi di uno spazio vettoriale  $V$ . Gli elementi di  $U$  appartengono al sottospazio generato da  $S$  se e solo se esiste una matrice di scalari  $m \times n$ ,  $A$ , tale che  $(v_1, \dots, v_m)A = (w_1, \dots, w_n)$ .* ■

Consideriamo ora il problema di determinare il vettore delle coordinate  $X$  di un vettore assegnato  $v \in V$ , rispetto a una data base  $\mathbf{B} = (v_1, \dots, v_n)$ . Ossia, vogliamo scrivere esplicitamente  $v = \mathbf{B}X$ , come in (4.10). È chiaro che il problema, in questa forma, non può essere risolto, a meno che la base e il vettore non siano entrambi assegnati in qualche modo esplicito. Tuttavia possiamo utilizzare la moltiplicazione per l'ipervettore  $\mathbf{B}$ , per definire astrattamente un *isomorfismo di spazi vettoriali*:

$$(4.14) \quad \psi : F^n \rightarrow V \quad \text{che manda } X \text{ in } \mathbf{B}X,$$

dallo spazio  $F^n$  dei vettori colonna a  $V$ . Tale applicazione è biettiva, poiché ogni vettore  $v$  si scrive, in modo unico, come una combinazione lineare della forma (4.10). Più precisamente,  $\psi$  è suriettiva poiché l'insieme  $\mathbf{B}$  genera  $V$ , ed è iniettiva poiché  $\mathbf{B}$  è linearmente indipendente. Inoltre, gli assiomi di un isomorfismo dati in (2.13) si verificano facilmente. Possiamo allora utilizzare questo isomorfismo per introdurre le *coordinate* nello spazio vettoriale  $V$ .

Il vettore delle coordinate di un vettore  $v$  è  $X = \psi^{-1}(v)$ . Si noti che il simbolo  $\mathbf{B}^{-1}$  non è definito. Perciò, a meno che la base non sia assegnata più concretamente, non avremo una formula esplicita per la funzione inversa  $\psi^{-1}$ . Tuttavia l'esistenza dell'isomorfismo  $\psi$  è interessante di per sé:

(4.15) COROLLARIO *Ogni spazio vettoriale  $V$  di dimensione  $n$  è isomorfo allo spazio  $F^n$  dei vettori colonna.* ■

Conviene osservare che  $F^n$  non è isomorfo a  $F^m$ , se  $m \neq n$ , poiché  $F^n$  ha una base di  $n$  elementi, e il numero degli elementi di una base dipende soltanto

dallo spazio vettoriale e non dalla scelta della base. Dunque gli spazi vettoriali di dimensione finita  $V$  sopra un campo  $F$  sono completamente classificati, in virtù di (4.15): ogni spazio  $V$  è isomorfo a  $F^n$ , essendo  $n$  un intero univocamente determinato. Ne segue che, se studiamo gli esempi fondamentali dei vettori colonna, conosceremo tutte le proprietà di uno spazio vettoriale arbitrario di dimensione finita. In tal modo, qualsiasi problema sugli spazi vettoriali viene ricondotto nell'ambito dell'algebra ben nota dei vettori colonna, una volta fissata una base.

Passiamo ora a introdurre un metodo di calcolo molto importante: il *cambiamento di base*. In generale, è utile identificare  $V$  con lo spazio vettoriale isomorfo  $F^n$  quando viene data una base naturale, ma non quando la base assegnata si adatta male al problema in esame. In tal caso, conviene cambiare coordinate. Supponiamo allora di avere due basi di uno stesso spazio vettoriale  $V$ , diciamo  $\mathbf{B} = (v_1, \dots, v_n)$  e  $\mathbf{B}' = (v'_1, \dots, v'_n)$ . Considereremo  $\mathbf{B}$  come la *vecchia* base e  $\mathbf{B}'$  come una *nuova* base. Vi sono due problemi che vogliamo risolvere. Il primo è: come sono collegate tra loro le due basi? In secondo luogo, un vettore  $v \in V$  avrà naturalmente coordinate diverse rispetto a  $\mathbf{B}$  e a  $\mathbf{B}'$ . Perciò chiediamo: come sono collegate tra loro i due vettori delle coordinate? Queste sono le operazioni chiamate *cambiamento di base*. Saranno molto importanti nei capitoli successivi, ma è facile confondersi con tali operazioni e addirittura trovarsi in grosse difficoltà, se non si organizzano per bene le notazioni.

Cominciamo con l'osservare che, poiché la nuova base genera  $V$ , ogni vettore della vecchia base  $\mathbf{B}$  è una combinazione lineare della nuova base  $\mathbf{B}' = (v'_1, \dots, v'_n)$ . Pertanto, in base alla proposizione (4.13), esiste un'equazione della forma:

$$(4.16) \quad (v'_1, \dots, v'_n)[P] = (v_1, \dots, v_n), \quad \text{ossia } \mathbf{B}'P = \mathbf{B},$$

dove  $P$  è una matrice di scalari  $n \times n$ . Questa equazione matriciale si legge nella forma seguente:

$$(4.17) \quad v'_1 p_{1j} + v'_2 p_{2j} + \cdots + v'_n p_{nj} = v_j,$$

dove i coefficienti  $p_{ij}$  sono gli elementi di  $P$ . La matrice  $P$  è chiamata la *matrice del cambiamento di base*. La sua colonna  $j$ -esima è il vettore delle coordinate del vettore  $v_j$  della vecchia base, calcolato rispetto alla nuova base  $\mathbf{B}'$ .

Si noti che la matrice del cambiamento di base è *invertibile*. Ciò si può dimostrare nel modo seguente: scambiando i ruoli di  $\mathbf{B}$  e  $\mathbf{B}'$ , si ottiene una matrice  $P'$  tale che  $\mathbf{B}'P' = \mathbf{B}$ . Questa relazione, insieme con la (4.16), fornisce la relazione:  $\mathbf{B}'P'P = \mathbf{B}$ , ossia:

$$(v_1, \dots, v_n)[P'P] = (v_1, \dots, v_n).$$

Tale formula esprime ciascun vettore  $v_i$  come una combinazione lineare dei vettori  $(v_1, \dots, v_n)$ . Gli elementi della matrice prodotto  $P'P$  forniscono i coefficienti. Ma dato che  $\mathbf{B}$  è un insieme linearmente indipendente, vi è un *unico modo* di scrivere

$v_i$  come una combinazione lineare di  $(v_1, \dots, v_n)$ , precisamente  $v_i = v_i$  ossia  $\mathbf{B}I = \mathbf{B}$ . Pertanto  $P'P = I$ . Ciò dimostra che  $P$  è invertibile.

Sia ora  $X$  il vettore delle coordinate di  $v$ , calcolato rispetto alla vecchia base  $\mathbf{B}$ , sicché  $v = \mathbf{B}X$ . Utilizzando la relazione (4.16), si ottiene l'equazione matriciale:

$$(4.18) \quad v = \mathbf{B}X = \mathbf{B}'PX.$$

Tale equazione mostra che  $PX = X'$  è il vettore delle coordinate di  $v$  rispetto alla nuova base  $\mathbf{B}'$ .

Ricapitolando, abbiamo una sola matrice  $P$ , la matrice del cambiamento di base, con le proprietà duali:

$$(4.19) \quad \mathbf{B} = \mathbf{B}'P \quad \text{e} \quad PX = X',$$

dove  $X, X'$  denotano i vettori delle coordinate di un vettore arbitrario  $v$  rispetto alle due basi. Ciascuna di tali proprietà caratterizza  $P$ . Si noti che occorre fare attenzione alla posizione degli apici.

Possiamo calcolare esplicitamente la matrice del cambiamento di base quando  $V = F^n$  e la vecchia base è la base canonica  $\mathbf{E}$ , mentre la nuova base  $\mathbf{B}'$  è arbitraria. Le due basi determinano le matrici  $[\mathbf{E}] = I$  e  $[\mathbf{B}']$ , come in (4.3). La formula (4.19) dà l'equazione matriciale  $I = [\mathbf{B}']P$ . Pertanto la matrice del cambiamento di base è:

$$(4.20) \quad P = [\mathbf{B}']^{-1}, \quad \text{se } V = F^n \text{ e se la vecchia base è } \mathbf{E}.$$

Possiamo anche scrivere tale relazione nella forma  $[\mathbf{B}'] = P^{-1}$ . Quindi:

$$(4.21) \quad \text{Se la vecchia base è } \mathbf{E}, \text{ i vettori della nuova base sono le colonne della matrice } P^{-1}.$$

Nella discussione precedente, la matrice  $P$  era individuata dalle due basi  $\mathbf{B}$  e  $\mathbf{B}'$ . Potremmo anche ragionare in un altro modo, partendo da una sola base  $\mathbf{B}$  e da una matrice invertibile  $P \in GL_n(F)$ . Allora possiamo definire una nuova base mediante la formula (4.16), cioè:

$$(4.22) \quad \mathbf{B}' = \mathbf{B}P^{-1}.$$

I vettori  $v_i$  della vecchia base appartengono al sottospazio generato da  $\mathbf{B}'$ . poiché  $\mathbf{B} = \mathbf{B}'P$  (cfr. 4.13). Pertanto  $\mathbf{B}'$  genera  $V$  e, avendo il numero giusto di elementi,  $\mathbf{B}'$  è una base.

(4.23) COROLLARIO Sia  $\mathbf{B}$  una base di uno spazio vettoriale  $V$ . Le altre basi sono gli insiemi della forma  $\mathbf{B}' = \mathbf{B}P^{-1}$ , dove  $P \in GL_n(F)$  è una matrice invertibile.

Naturalmente, non è necessario mettere una matrice inversa nell'enunciato. Poiché  $P$  è arbitraria, tale risulta  $P^{-1}$ . Potremmo porre senz'altro  $P^{-1} = Q$  e dire che  $\mathbf{B}' = \mathbf{B}Q$ , dove  $Q \in GL_n(F)$ . ■

Come applicazione del ragionamento precedente, calcoliamo l'ordine del gruppo lineare generale  $GL_2(F)$  quando  $F$  è il campo primo  $\mathbb{F}_p$ . Per far questo, calcoliamo il numero delle basi dello spazio vettoriale  $V = F^2$ . Poiché  $V$  ha dimensione 2, ogni insieme linearmente indipendente  $(v_1, v_2)$  di due elementi è una base. Il primo vettore  $v_1$  di un insieme linearmente indipendente è diverso dal vettore nullo. Ora, poiché l'ordine di  $F$  è  $p$ ,  $V$  contiene  $p^2$  vettori, incluso il vettore nullo. Pertanto vi sono  $p^2 - 1$  scelte per il vettore  $v_1$ . Inoltre, un insieme  $(v_1, v_2)$  di due vettori, con  $v_1 \neq 0$ , è linearmente indipendente se e solo se  $v_2$  non è un multiplo di  $v_1$  (cfr. 3.7). Esistono  $p$  multipli di un vettore  $v_1 \neq 0$ . Pertanto, fissato  $v_1$ , esistono  $p^2 - p$  vettori  $v_2$  tali che  $(v_2, v_1)$  è linearmente indipendente. In tal modo, si ottengono complessivamente

$$(p^2 - 1)(p^2 - p) = p(p+1)(p-1)^2$$

basi per  $V$ .

(4.24) COROLLARIO L'ordine di  $GL_2(\mathbb{F}_p)$  è  $p(p+1)(p-1)^2$ .

Dimostrazione. La Proposizione (4.23) stabilisce una corrispondenza biunivoca tra le basi di  $F^n$  e gli elementi di  $GL_n(F)$ . ■

## 5 Spazi di dimensione infinita

Alcuni spazi vettoriali sono troppo grandi per poter essere generati da un insieme finito di vettori. Sono chiamati spazi vettoriali di dimensione infinita. Non avremo bisogno di considerare tali spazi molto spesso, ma dato che essi sono molto importanti in analisi, li esamineremo brevemente.

L'esempio più semplice di spazio di dimensione infinita è lo spazio  $\mathbb{R}^\infty$  dei vettori reali infiniti:

$$(5.1) \quad (a) = (a_1, a_2, a_3, \dots).$$

Esso può essere pensato anche come lo spazio delle successioni  $\{a_n\}$  di numeri reali. Gli esempi (1.8c,d) sono anch'essi di dimensione infinita.

Lo spazio  $\mathbb{R}^\infty$  ha molti sottospazi importanti. Ecco alcuni esempi:

### (5.2) Esempi

(a) Successioni convergenti:  $C = \{(a) \in \mathbb{R}^\infty \mid \lim_{n \rightarrow \infty} a_n \text{ esiste}\}$ .

(b) Successioni limitate:  $\ell^\infty = \{(a) \in \mathbb{R}^\infty \mid \{a_n\} \text{ è limitata}\}$ .

Una successione  $\{a_n\}$  si dice *limitata*, se esiste un *maggiorante*, ossia, un numero reale  $b$  tale che  $|a_n| \leq b$ , per ogni  $n$ .

(c) Serie assolutamente convergenti:  $\ell^1 = \left\{ (a) \in \mathbb{R}^\infty \mid \sum_1^\infty |a_n| < \infty \right\}$ .

(d) Successioni con un numero finito di termini non nulli:

$$Z = \{(a) \in \mathbb{R}^\infty \mid a_n = 0 \text{ per ogni } n, \text{ tranne al più un numero finito di indici}\}.$$

I sottospazi sopra descritti sono tutti di dimensione infinita. È un buon esercizio cercare di trovarne altri.

Supponiamo ora che  $V$  sia uno spazio vettoriale, non necessariamente di dimensione infinita. Cosa si dovrebbe intendere per sottospazio *generato* da un insieme infinito  $S$  di vettori? La difficoltà è la seguente: non sempre è possibile assegnare un vettore come il valore di una combinazione lineare infinita  $c_1v_1 + c_2v_2 + \dots$ , in modo logico. Se stiamo considerando lo spazio vettoriale dei numeri reali, ossia  $v_i \in \mathbb{R}^1$ , allora possiamo assegnare un valore, purché la serie  $c_1v_1 + c_2v_2 + \dots$  converga. La stessa cosa può essere fatta per le serie convergenti di vettori in  $\mathbb{R}^n$  o in  $\mathbb{R}^\infty$ . Tuttavia molte serie non convergono, e allora non sappiamo quale valore assegnare.

In algebra di solito si parla soltanto di combinazioni lineari di un numero finito di vettori. Pertanto, il sottospazio generato da un insieme infinito  $S$  deve essere interpretato come l'insieme di quei vettori  $v$  che sono combinazioni lineari di *un numero finito* di elementi di  $S$ :

$$(5.3) \quad v = c_1v_1 + \dots + c_rv_r, \text{ dove } v_1, \dots, v_r \in S.$$

Il numero  $r$  può essere arbitrariamente grande, al variare del vettore  $v$ :

$$(5.4) \quad \text{Span } S = \left\{ \begin{array}{l} \text{combinazioni lineari finite} \\ \text{di elementi di } S \end{array} \right\}.$$

Con questa definizione, le proposizioni (3.2) e (3.11) continuano a valere.

Per esempio, sia  $e_i = (0, \dots, 0, 1, 0, \dots)$  il vettore in  $\mathbb{R}^\infty$  avente 1 nella  $i$ -esima posizione come unica coordinata non nulla. Sia  $S = (e_1, e_2, e_3, \dots)$  l'insieme infinito di tali vettori  $e_i$ . L'insieme  $S$  non genera  $\mathbb{R}^\infty$ , poiché il vettore

$$w = (1, 1, 1, \dots)$$

non è una combinazione lineare (finita). Invece lo spazio generato da  $S$  è il sottospazio  $Z$  definito in (5.2d).

Un insieme  $S$ , finito o infinito, si dice *linearmente indipendente*, se non esiste nessuna relazione finita della forma:

$$(5.5) \quad c_1v_1 + \dots + c_rv_r = 0, \text{ con } v_1, \dots, v_r \in S,$$

tranne la relazione banale in cui  $c_1 = \dots = c_r = 0$ . Anche in questo caso, il numero  $r$  è arbitrario, ossia, la condizione deve valere per un intero  $r$  arbitrariamente grande e per vettori arbitrari  $v_1, \dots, v_r \in S$ . Per esempio, se  $w, e_i$  sono i vettori definiti in precedenza, l'insieme  $S' = (w, e_1, e_2, e_3, \dots)$  è linearmente indipendente. Con questa definizione di indipendenza lineare, la proposizione (3.10) continua a valere.

Così come accade con gli insiemi finiti, una *base*  $S$  di  $V$  è un insieme linearmente indipendente che genera  $V$ . Così  $S = (e_1, e_2, \dots)$  è una base dello spazio  $Z$ . Si può dimostrare, utilizzando l'*assioma della scelta*, che ogni spazio vettoriale  $V$  possiede una base, ma la dimostrazione non ci dice come trovarne una. Una base per  $\mathbb{R}^\infty$  sarà un insieme non numerabile di vettori e pertanto non può essere scritta in forma esplicita. Non avremo bisogno molto spesso di basi per spazi vettoriali di dimensione infinita.

Ritorniamo per un momento al caso di uno spazio vettoriale  $V$  di dimensione finita (cfr. 3.12) e chiediamoci se può esistere una base *infinita*. Nel paragrafo 3, abbiamo visto che due basi finite arbitrarie hanno lo stesso numero di elementi. Completeremo ora il quadro, dimostrando che ogni base è finita. L'unico punto che potrebbe generare confusione è risolto dalla proposizione seguente:

**(5.6) PROPOSIZIONE** *Sia  $V$  uno spazio vettoriale di dimensione finita, e sia  $S$  un insieme arbitrario che genera  $V$ . Allora  $S$  contiene un sottoinsieme finito che genera  $V$ .*

*Dimostrazione.* Per ipotesi, esiste almeno un insieme finito, diciamo  $(w_1, \dots, w_m)$ , che genera  $V$ . Ciascun vettore  $w_i$  è una combinazione lineare di un numero finito di elementi di  $S$ , poiché  $\text{Span } S = V$ . Pertanto, quando esprimiamo i vettori  $w_1, \dots, w_m$  mediante l'insieme  $S$ , abbiamo bisogno di utilizzare soltanto un numero finito di elementi di  $S$ . Tali elementi formano un sottoinsieme finito  $S' \subset S$ . Dunque,  $(w_1, \dots, w_m) \subset \text{Span } S'$ . Ora, poiché  $(w_1, \dots, w_m)$  genera  $V$ , anche  $S'$  genera  $V$ . ■

**(5.7) PROPOSIZIONE** *Sia  $V$  uno spazio vettoriale di dimensione finita.*

- (a) *Ogni insieme  $S$  che genera  $V$  contiene una base finita.*
- (b) *Ogni insieme linearmente indipendente  $L$  è finito e pertanto si estende a una base finita.*
- (c) *Ogni base è finita.*

*La dimostrazione è lasciata come esercizio. ■*

## 6 Somme dirette

Sia  $V$  uno spazio vettoriale e siano  $W_1, \dots, W_n$  sottospazi di  $V$ . Gran parte della teoria relativa all'indipendenza lineare e agli spazi generati da vettori può essere estesa ai sottospazi vettoriali, come vedremo ora.

Consideriamo i vettori  $v \in V$  che possono essere scritti come una somma:

$$(6.1) \quad v = w_1 + \dots + w_n,$$

dove  $w_i$  è un vettore in  $W_i$ . L'insieme di tutti i vettori di questa forma è chiamato la *somma* dei sottospazi oppure lo spazio da essi *generato*, e si indica con

$$(6.2) \quad W_1 + \dots + W_n = \{v \in V \mid v = w_1 + \dots + w_n, \text{ con } w_i \in W_i\}.$$

La somma è un sottospazio di  $V$ , analogo al sottospazio generato da un insieme  $\{v_1, \dots, v_n\}$  di vettori. È chiaro che esso è il più piccolo sottospazio di  $V$  che contiene  $W_1, \dots, W_n$ .

I sottospazi  $W_1, \dots, W_n$  si dicono *indipendenti*, se nessuna somma di vettori del tipo  $w_1 + \dots + w_n$ , con  $w_i \in W_i$ , è uguale al vettore nullo, tranne la somma banale in cui  $w_i = 0$  per ogni  $i$ . In altre parole, gli spazi sono indipendenti, se

$$(6.3) \quad w_1 + \dots + w_n = 0, \text{ con } w_i \in W_i \text{ implica } w_i = 0 \text{ per ogni } i.$$

Nel caso in cui lo spazio generato è l'intero spazio e i sottospazi sono indipendenti, si dice che  $V$  è la *somma diretta* di  $W_1, \dots, W_n$  e si scrive:

$$(6.4) \quad V = W_1 \oplus \dots \oplus W_n, \text{ se } V = W_1 + \dots + W_n \text{ e inoltre } W_1, \dots, W_n \text{ sono indipendenti.}$$

Ciò equivale a dire che ogni vettore  $v \in V$  può essere scritto nella forma (6.1) in modo unico.

Pertanto, se  $W_1, \dots, W_n$  sono sottospazi indipendenti di uno spazio vettoriale  $V$  e se  $U = W_1 + \dots + W_n$  è la loro somma, allora  $U$  risulta di fatto la loro somma diretta:  $U = W_1 \oplus \dots \oplus W_n$ .

La dimostrazione delle due proposizioni seguenti è lasciata come esercizio.

### (6.5) PROPOSIZIONE

(a) Un singolo sottospazio  $W_1$  è indipendente.

(b) Due sottospazi  $W_1, W_2$  sono indipendenti se e soltanto se  $W_1 \cap W_2 = \{0\}$ . ■

(6.6) PROPOSIZIONE Siano  $W_1, \dots, W_n$  sottospazi di uno spazio vettoriale di dimensione finita  $V$ , e sia  $\mathbf{B}_i$  una base di  $W_i$ .

## Somme dirette

- (a) L'insieme ordinato  $\mathbf{B}$  ottenuto scrivendo, nell'ordine, le basi  $\mathbf{B}_1, \dots, \mathbf{B}_n$  è una base di  $V$  se e solo se  $V$  è la somma diretta  $W_1 \oplus \dots \oplus W_n$ .
- (b)  $\dim(W_1 + \dots + W_n) \leq (\dim W_1) + \dots + (\dim W_n)$ , e si ha l'uguaglianza se e solo se gli spazi sono indipendenti. ■

(6.7) COROLLARIO Sia  $W$  un sottospazio di uno spazio vettoriale di dimensione finita  $V$ . Allora esiste un altro sottospazio  $W'$  tale che  $V = W \oplus W'$ .

*Dimostrazione.* Sia  $(w_1, \dots, w_d)$  una base di  $W$ . Estendiamo tale base ad una base  $(w_1, \dots, w_d; v_1, \dots, v_{n-d})$  di  $V$  [cfr. (3.15)]. Lo spazio generato da  $(v_1, \dots, v_{n-d})$  è il sottospazio  $W'$  richiesto. ■

### (6.8) Esempio

Siano  $v_1, \dots, v_n$  vettori non nulli, e sia  $W_i$  il sottospazio generato dal vettore  $v_i$ . Esso è il sottospazio di dimensione uno costituito da tutti i multipli scalari di  $v_i$ :  $W_i = \{cv_i\}$ . Allora  $W_1, \dots, W_n$  sono sottospazi indipendenti se e soltanto se  $(v_1, \dots, v_n)$  è un insieme linearmente indipendente. Ciò risulta chiaro, se confrontiamo gli enunciati (3.4) e (6.3). In realtà, l'enunciato in termini di sottospazi è più semplice, poiché i coefficienti scalari vengono assorbiti.

(6.9) PROPOSIZIONE Siano  $W_1, W_2$  sottospazi di uno spazio vettoriale  $V$  di dimensione finita. Allora

$$\dim W_1 + \dim W_2 = \dim(W_1 \cap W_2) + \dim(W_1 + W_2).$$

*Dimostrazione.* Osserviamo innanzitutto che l'intersezione di due sottospazi è ancora un sottospazio. Scegliamo una base  $(u_1, \dots, u_r)$  per lo spazio  $W_1 \cap W_2$ , dove  $r = \dim(W_1 \cap W_2)$ . Essa è un insieme linearmente indipendente ed è contenuta in  $W_1$ . Pertanto può essere estesa ad una base di  $W_1$ , diciamo:

$$(6.10) \quad (u_1, \dots, u_r; x_1, \dots, x_{m-r}),$$

dove  $m = \dim W_1$ . Similmente, essa può essere estesa ad una base di  $W_2$ , diciamo:

$$(6.11) \quad (u_1, \dots, u_r; y_1, \dots, y_{n-r}),$$

dove  $n = \dim W_2$ . Per dimostrare la proposizione, basta provare che l'insieme:

$$(6.12) \quad (u_1, \dots, u_r; x_1, \dots, x_{m-r}; y_1, \dots, y_{n-r})$$

è una base di  $W_1 + W_2$ .

Tale affermazione è composta da due parti. Innanzitutto, i vettori (6.12) generano  $W_1 + W_2$ . Infatti, ogni vettore  $v$  in  $W_1 + W_2$  è una somma:  $v = w_1 + w_2$ , con  $w_i \in W_i$ . Possiamo scrivere  $w_1$  come una combinazione lineare di (6.10), e  $w_2$  come una combinazione lineare di (6.11). Raccogliendo i termini, si ottiene che  $v$  è una combinazione lineare di (6.12).

In secondo luogo, i vettori (6.12) sono linearmente indipendenti. Infatti supponiamo che una loro combinazione lineare sia nulla, diciamo:

$$a_1 u_1 + \cdots + a_r u_r + b_1 x_1 + \cdots + b_m - r x_m - r + c_1 y_1 + \cdots + c_n - r y_n - r = 0,$$

o in forma abbreviata:  $u + x + y = 0$ . Risolviamo rispetto a  $y$ :  $y = -u - x \in W_1$ . Ma  $y \in W_2$ ; dunque  $y \in W_1 \cap W_2$  e pertanto  $y$  è una combinazione lineare, diciamo  $u'$ , di  $(u_1, \dots, u_r)$ . Allora  $-u' + y = 0$  è una relazione tra i vettori (6.11), i quali sono indipendenti. Pertanto essa è la relazione banale, e quindi  $y = 0$ . Dunque la relazione di partenza si riduce a  $u + x = 0$ . Poiché l'insieme (6.10) è una base, tale relazione è banale, ossia  $u = 0$  e  $x = 0$ . Concludendo, l'intera relazione iniziale è banale, come richiesto. ■

Non c'è bisogno che io impari quanto fa  $8+7$ : basta che ricordi  $8+8$  e tolga 1.

T. Cuyler Young jr.

### Esercizi

#### 1 Spazi vettoriali reali

- Quali dei seguenti sottoinsiemi dello spazio vettoriale delle matrici reali  $n \times n$  sono sottospazi?
  - Le matrici simmetriche ( $A = A^t$ );
  - le matrici invertibili;
  - le matrici triangolari superiori.
- Dimostrare che l'intersezione di due sottospazi è un sottospazio.
- Dimostrare la legge di cancellazione in uno spazio vettoriale: se  $cv = cw$  e  $c \neq 0$ , allora  $v = w$ .
- Provare che, se  $w$  è un elemento di un sottospazio  $W$ , allora anche  $-w$  appartiene a  $W$ .
- Dimostrare che la classificazione dei sottospazi di  $\mathbb{R}^3$  enunciata dopo (1.2) è completa.
- Dimostrare che ogni soluzione dell'equazione:  $2x_1 - x_2 - 2x_3 = 0$  ha la forma (1.5).
- Qual è la descrizione analoga a (1.5), ottenuta dalle soluzioni particolari  $u_1 = (2, 2, 1)$  e  $u_2 = (0, 2, -1)$ ?

### Esercizi

#### 2 Campi astratti

- Dimostrare che l'insieme dei numeri della forma:  $a + b\sqrt{2}$ , dove  $a, b$  sono numeri razionali, è un campo.
- Quali sottoinsiemi di  $\mathbb{C}$  sono chiusi rispetto a  $+$ ,  $-$ ,  $\times$ ,  $\div$ , ma non contengono 1?
- Sia  $F$  un sottoinsieme di  $\mathbb{C}$  tale che  $F(+)$  è un sottogruppo di  $\mathbb{C}(+)$  e  $F^*(\cdot)$  è un sottogruppo di  $\mathbb{C}^*(\cdot)$ . Dimostrare che  $F$  è un sottocampo di  $\mathbb{C}$ .
- Sia  $V = \mathbb{F}^n$  lo spazio dei vettori colonna. Dimostrare che ogni sottospazio  $W$  di  $V$  è lo spazio delle soluzioni di un sistema di equazioni lineari omogenee  $AX = 0$ .
- Dimostrare che un sottoinsieme non vuoto  $W$  di uno spazio vettoriale soddisfa alle condizioni (2.12) per un sottospazio se e solo se è chiuso rispetto all'addizione e alla moltiplicazione per uno scalare.
- Dimostrare che, nella definizione (2.3), l'assioma (ii) può essere sostituito dall'assioma seguente:  $F^*$  è un gruppo abeliano, e  $1 \neq 0$ . Cosa accade se la condizione:  $1 \neq 0$  viene omessa?
- Definire gli omomorfismi tra campi, e provare che ogni omomorfismo tra campi è iniettivo.
- Trovare l'inverso di 5 (modulo  $p$ ) per  $p = 2, 3, 7, 11, 13$ .
- Calcolare il polinomio  $(x^2+3x+1)(x^3+4x^2+2x+2)$ , dove i coefficienti sono considerati elementi dei campi (a)  $\mathbb{F}_5$  (b)  $\mathbb{F}_7$ .

10. Si consideri il sistema di equazioni lineari:  $\begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix}$ .

(a) Risolvere tale sistema in  $\mathbb{F}_p$ , per  $p = 5, 11, 17$ .

(b) Determinare il numero delle soluzioni per  $p = 7$ .

- Trovare tutti i primi  $p$  tali che la matrice:

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix}$$

sia invertibile, considerando i suoi elementi appartenenti a  $\mathbb{F}_p$ .

- Risolvere completamente i sistemi di equazioni lineari  $AX = B$ , dove:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

(a) in  $\mathbb{Q}$ ; (b) in  $\mathbb{F}_2$ ; (c) in  $\mathbb{F}_3$ ; (d) in  $\mathbb{F}_7$ .

- Sia  $p$  un numero primo. Gli elementi non nulli di  $\mathbb{F}_p$  formano un gruppo  $\mathbb{F}_p^*$  di ordine  $p-1$ . Si può dimostrare che tale gruppo è sempre ciclico. Verificare ciò per tutti i primi  $p < 20$ , determinando esplicitamente un generatore.

14. (a) Sia  $p$  un numero primo. Utilizzare il fatto che  $\mathbb{F}_p^*$  è un gruppo per dimostrare che  $a^{p-1} \equiv 1$  (modulo  $p$ ) per ogni intero  $a$  che non sia congruo a zero modulo  $p$ .  
 (b) Dimostrare il *teorema di Fermat*: Per ogni intero  $a$ , si ha:  

$$a^p \equiv a \pmod{p}$$
15. (a) Accoppiando gli elementi con i rispettivi inversi, dimostrare che il prodotto di tutti gli elementi non nulli di  $\mathbb{F}_p$  è uguale a  $-1$ .  
 (b) Sia  $p$  un numero primo. Dimostrare il *teorema di Wilson*:  

$$(p-1)! \equiv -1 \pmod{p}$$

16. Si consideri un sistema  $AX = B$  di  $n$  equazioni lineari in  $n$  incognite, con  $A$  e  $B$  ad elementi interi. È vero che, se il sistema ha una soluzione intera, allora esso ha una soluzione in  $\mathbb{F}_p$ , per ogni primo  $p$ ?

17. Dimostrare che le quattro matrici ad elementi in  $\mathbb{F}_2$ :  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$ , formano un campo.

18. La dimostrazione del lemma (2.8) contiene una dimostrazione più diretta di (2.6). Esplicitare tale dimostrazione.

### 3 Basi e Dimensione

- Trovare una base del sottospazio di  $\mathbb{R}^4$  generato dai vettori  $(1, 2, -1, 0)$ ,  $(4, 8, -4, -3)$ ,  $(0, 1, 3, 4)$ ,  $(2, 5, 1, 4)$ .
- Sia  $W \subset \mathbb{R}^4$  lo spazio delle soluzioni del sistema di equazioni lineari  $AX = 0$ , dove  $A = \begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix}$ . Trovare una base di  $W$ .
- (a) Dimostrare che un sottoinsieme di un insieme linearmente indipendente è linearmente indipendente.  
 (b) Dimostrare che ogni insieme di vettori ottenuto riordinando una base è ancora una base.
- Sia  $V$  uno spazio vettoriale di dimensione  $n$  su  $F$ , e sia  $0 \leq r \leq n$ . Dimostrare che  $V$  contiene un sottospazio di dimensione  $r$ .
- Trovare una base dello spazio delle matrici  $n \times n$  simmetriche.
- Dimostrare che una matrice quadrata  $A$  è invertibile se e solo se le sue colonne sono linearmente indipendenti.
- Sia  $V$  lo spazio vettoriale delle funzioni a valori reali continue nell'intervallo  $[0, 1]$ . Dimostrare che le funzioni  $x^3$ ,  $\sin x$ ,  $\cos x$  sono linearmente indipendenti.
- Sia  $A$  una matrice  $m \times n$ , e sia  $A'$  una matrice ottenuta da  $A$  mediante successive operazioni elementari sulle righe. Dimostrare che le righe di  $A$  e le righe di  $A'$  generano lo stesso sottospazio.

- Sia  $V$  uno spazio vettoriale complesso di dimensione  $n$ . Dimostrare che  $V$  ha dimensione  $2n$ , come spazio vettoriale reale.
- Una matrice complessa  $n \times n$  si dice *hermitiana*, se  $a_{ij} = \overline{a_{ji}}$  per ogni  $i, j$ . Dimostrare che le matrici hermitiane formano uno spazio vettoriale reale, trovare una base per tale spazio, e determinare la sua dimensione.
- Quanti elementi vi sono nello spazio vettoriale  $\mathbb{F}_p^n$ ?
- Sia  $F = \mathbb{F}_2$ . Trovare tutte le basi di  $F^2$ .
- Sia  $F = \mathbb{F}_5$ . Calcolare il numero dei sottospazi delle varie dimensioni contenuti nello spazio  $F^3$ .
- (a) Sia  $V$  uno spazio vettoriale di dimensione 3 sul campo  $\mathbb{F}_p$ . Quanti sono i sottospazi delle varie dimensioni contenuti in  $V$ ?  
 (b) Rispondere alla stessa domanda per uno spazio vettoriale di dimensione 4.
- (a) Sia  $F = \mathbb{F}_2$ . Dimostrare che il gruppo  $GL_2(F)$  è isomorfo al gruppo simmetrico  $S_3$ .  
 (b) Sia  $F = \mathbb{F}_3$ . Determinare gli ordini di  $GL_2(F)$  e di  $SL_2(F)$ .
- Sia  $W$  un sottospazio di  $V$ .
  - Dimostrare che esiste un sottospazio  $U$  di  $V$  tale che  $U + W = V$  e  $U \cap W = 0$ .
  - Dimostrare che non esiste nessun sottospazio  $U$  di  $V$  tale che  $W \cap U = 0$  e  $\dim W + \dim U > \dim V$ .
- 4 Calcoli con le basi**
  - Calcolare la matrice  $P$  del cambiamento di base in  $\mathbb{R}^2$  che collega la base canonica  $\mathbf{E}$  alla base  $\mathbf{B}' = (v_1, v_2)$ , dove  $v_1 = (1, 3)^t$ ,  $v_2 = (2, 2)^t$ .
  - Determinare la matrice del cambiamento di base, nel caso in cui la vecchia base è la base canonica  $(e_1, \dots, e_n)$  e la nuova base è  $(e_n, e_{n-1}, \dots, e_1)$ .
  - Determinare la matrice  $P$  del cambiamento di base, nel caso in cui la vecchia base è  $(e_1, e_2)$  e la nuova base è  $(e_1 + e_2, e_1 - e_2)$ .
  - Consideriamo il sistema di coordinate equilatero in  $\mathbb{R}^2$ , dato dalla base  $\mathbf{B}'$  in cui  $v_1 = e_1$  e  $v_2$  è un vettore di lunghezza unitaria che forma un angolo di  $120^\circ$  con  $v_1$ . Trovare la matrice che collega la base canonica  $\mathbf{E}$  a  $\mathbf{B}'$ .
    - Dimostrare che l'insieme  $\mathbf{B} = ((1, 2, 0)^t, (2, 1, 2)^t, (3, 1, 1)^t)$  è una base di  $\mathbb{R}^3$ .
    - Trovare il vettore delle coordinate del vettore  $v = (1, 2, 3)^t$  rispetto a tale base  $\mathbf{B}$ .
    - Sia  $\mathbf{B}' = ((0, 1, 0)^t, (1, 0, 1)^t, (2, 1, 0)^t)$ . Trovare la matrice  $P$  che collega  $\mathbf{B}$  a  $\mathbf{B}'$ .
    - Per quali primi  $p$   $\mathbf{B}$  è una base di  $\mathbb{F}_p^3$ ?
  - Siano  $\mathbf{B}$  e  $\mathbf{B}'$  due basi dello spazio vettoriale  $F^n$ . Dimostrare che la matrice del cambiamento di base è  $P = [\mathbf{B}']^{-1}[\mathbf{B}]$ .
  - Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di uno spazio vettoriale  $V$ . Dimostrare che è possibile passare da  $\mathbf{B}$  a un'altra base qualsiasi  $\mathbf{B}'$  mediante una successione finita di operazioni dei seguenti tipi:

- (i) Sostituire  $v_i$  con  $v_i + av_j$ ,  $i \neq j$ , per qualche  $a \in F$ .
  - (ii) Sostituire  $v_i$  con  $cv_i$ , per qualche  $c \neq 0$ .
  - (iii) Scambiare tra loro  $v_i$  e  $v_j$ .
8. Riscrivere la dimostrazione della proposizione (3.16), utilizzando le notazioni della proposizione (4.13).
9. Sia  $V = F^n$ . Stabilire una corrispondenza biunivoca tra l'insieme  $\mathcal{B}$  delle basi di  $V$  e  $GL_n(F)$ .
10. Sia  $F$  un campo contenente 81 elementi, e sia  $V$  uno spazio vettoriale di dimensione 3 su  $F$ . Determinare il numero dei sottospazi di  $V$  di dimensione 1.
11. Sia  $F = \mathbb{F}_p$ .
  - (a) Calcolare l'ordine di  $SL_2(F)$ .
  - (b) Calcolare il numero delle basi di  $F^n$ , e gli ordini di  $GL_n(F)$  e  $SL_n(F)$ .

12. (a) Sia  $A$  una matrice  $m \times n$ , con  $m < n$ . Dimostrare che  $A$  non possiede un'inversa a sinistra, confrontando  $A$  con la matrice quadrata  $n \times n$  ottenuta aggiungendo  $(n-m)$  righe di zeri in fondo.
- (b) Siano  $\mathbf{B} = (v_1, \dots, v_m)$  e  $\mathbf{B}' = (v'_1, \dots, v'_n)$  due basi di uno spazio vettoriale  $V$ . Dimostrare che  $m = n$ , definendo le matrici del cambiamento di base e provando che esse sono invertibili.

### 5 Spazi di dimensione infinita

1. Dimostrare che l'insieme  $(w; e_1, e_2, \dots)$  introdotto nel testo è linearmente indipendente, e descrivere lo spazio da esso generato.
2. Si consideri lo spazio delle successioni doppiamente infinite  $(a) = (\dots, a_{-1}, a_0, a_1, \dots)$ , con  $a_i \in \mathbb{R}$ . Dimostrare che tale spazio è isomorfo a  $\mathbb{R}^\infty$ .
3. Dimostrare che lo spazio  $Z$  (5.2)d è isomorfo allo spazio dei polinomi reali.
4. Descrivere altri cinque sottospazi di dimensione infinita dello spazio  $\mathbb{R}^\infty$ .
5. Per ogni intero positivo  $p$ , è possibile definire lo spazio  $\ell^p$  come lo spazio delle successioni tali che  $\sum |a_i|^p < \infty$ .
  - (a) Dimostrare che  $\ell^p$  è un sottospazio di  $\mathbb{R}^\infty$ .
  - (b) Dimostrare che  $\ell^p < \ell^{p+1}$ .
6. Sia  $V$  uno spazio vettoriale generato da un insieme numerabile di vettori. Dimostrare che ogni sottoinsieme linearmente indipendente di  $V$  è finito o numerabile.
7. Dimostrare la proposizione (5.7).

### 6 Somme dirette

1. Dimostrare che lo spazio  $\mathbb{R}^{n \times n}$  di tutte le matrici reali  $n \times n$  è la somma diretta dei sottospazi delle matrici simmetriche ( $A = A^t$ ) e delle matrici antisimmetriche ( $A = -A^t$ ).

### Esercizi

2. Sia  $W$  lo spazio delle matrici  $n \times n$  la cui traccia è zero. Trovare un sottospazio  $W'$  tale che  $\mathbb{R}^{n \times n} = W \oplus W'$ .
3. Dimostrare che la somma di sottospazi è un sottospazio.
4. Dimostrare la proposizione (6.5).
5. Dimostrare la proposizione (6.6).

### Esercizi vari

1. (a) Dimostrare che l'insieme dei simboli  $\{a + bi \mid a, b \in \mathbb{F}_3\}$  costituisce un campo con nove elementi, rispetto alle operazioni di addizione e di moltiplicazione identiche a quelle definite per i numeri complessi.
- (b) Verificare se lo stesso metodo funziona anche per  $\mathbb{F}_5$  o per  $\mathbb{F}_7$ .
- \*2. Sia  $V$  uno spazio vettoriale sopra un campo infinito  $F$ . Dimostrare che  $V$  non è l'unione di un numero finito di sottospazi propri.
- \*3. Siano  $W_1, W_2$  sottospazi di uno spazio vettoriale  $V$ . La formula:

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$$

è analoga alla formula:

$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|,$$

che vale per gli insiemi. Dati tre insiemi, si ha:

$$|S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|.$$

È vero che vale la formula corrispondente per le dimensioni di sottospazi?

4. Sia  $F$  un campo avente caratteristica diversa da 2, e sia  $x^2 + bx + c = 0$  un'equazione di secondo grado a coefficienti in  $F$ . Supponiamo che il discriminante  $b^2 - 4c$  sia un quadrato in  $F$ , ossia che esista un elemento  $\delta \in F$  tale che  $\delta^2 = b^2 - 4c$ . Dimostrare che la formula  $x = (-b + \delta)/2a$  risolve l'equazione di secondo grado in  $F$ , e che se il discriminante non è un quadrato il polinomio non ha radici in  $F$ .
5. (a) Quali sono gli ordini degli elementi  $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 2 & \\ & 1 \end{bmatrix}$  di  $GL_2(\mathbb{R})$ ?
- (b) Considerare gli elementi di tali matrici come elementi di  $\mathbb{F}_7$ , e calcolare gli ordini delle relative matrici nel gruppo  $GL_2(\mathbb{F}_7)$ .
6. Si consideri l'applicazione  $\det : F^{n \times n} \rightarrow F$ , dove  $F = \mathbb{F}_p$  è un campo finito con  $p$  elementi e  $F^{n \times n}$  è l'insieme delle matrici  $n \times n$ .
  - (a) Verificare che tale applicazione è suriettiva.
  - (b) Dimostrare che tutti i valori non nulli del determinante vengono ottenuti uno stesso numero di volte.

7. Sia  $A$  una matrice  $n \times n$ . Dimostrare che esiste un polinomio  $f(t) = a_r t^r + a_{r-1} t^{r-1} + \dots + a_1 t + a_0$  che ha  $A$  come radice, cioè:  $a_r A^r + a_{r-1} A^{r-1} + \dots + a_2 A^2 + a_1 A + a_0 I = 0$ . (Suggerimento: dimostrare che le matrici  $I, A, A^2, A^3, \dots$  sono linearmente dipendenti.)

\*8. Una curva algebrica in  $\mathbb{R}^2$  è il luogo degli zeri di un polinomio  $f(x, y)$  in due variabili. Per cammino polinomiale in  $\mathbb{R}^2$  si intende un cammino avente una parametrizzazione della forma:  $x = x(t)$ ,  $y = y(t)$ , dove  $x(t)$ ,  $y(t)$  sono polinomi in  $t$ .

- (a) Dimostrare che ogni cammino polinomiale giace su una curva algebrica reale, verificando che, per  $n$  abbastanza grande, le funzioni  $x(t)^i y(t)^j$ ,  $0 \leq i, j \leq n$ , sono linearmente dipendenti.
- (b) Determinare esplicitamente la curva algebrica che è l'immagine del cammino:  $x = t^2 + t$ ,  $y = t^3$ , e disegnarla.

## Capitolo 4 Applicazioni lineari

Quella confusione di pensiero e quegli errori di ragionamento ancora offuscano gli inizi dell'algebra, e questa è la più seria e fondata lagranza da parte delle menti rigorose e profonde.

Sir William Rowan Hamilton

### 1 La formula della dimensione

L'analogo di un omomorfismo di gruppi per gli spazi vettoriali è un'applicazione

$$T : V \rightarrow W$$

da uno spazio vettoriale su un campo  $F$  a un altro, che è compatibile con l'addizione e la moltiplicazione per uno scalare:

$$(1.1) \quad T(v_1 + v_2) = T(v_1) + T(v_2) \quad \text{e} \quad T(cv) = cT(v),$$

per ogni  $v_1, v_2, v$  in  $V$  e per ogni  $c \in F$ . Un'applicazione con queste caratteristiche viene chiamata di solito *applicazione lineare*, piuttosto che *omomorfismo*, termine peraltro ugualmente corretto. Si noti che un'applicazione lineare è compatibile con le combinazioni lineari:

$$(1.2) \quad T\left(\sum_i c_i v_i\right) = \sum_i c_i T(v_i).$$

Ciò segue, per induzione, dalla (1.1). Si noti inoltre che la prima delle condizioni (1.1) afferma che  $T$  è un omomorfismo di gruppi additivi:  $V(+)$   $\longrightarrow$   $W(+)$ .

Noi già conosciamo un notevole esempio di applicazione lineare: la moltiplicazione a sinistra per una matrice. Sia  $A$  una matrice  $m \times n$  a elementi in  $F$ , e consideriamo  $A$  come un operatore sui vettori colonna. Essa definisce un'applicazione lineare:

$$(1.3) \quad F^n \xrightarrow{\text{molt. a sin. per } A} F^m$$

$$X \longmapsto AX.$$

Infatti,  $A(X_1 + X_2) = AX_1 + AX_2$ , e  $A(cX) = cAX$ .

Vediamo ora un altro esempio. Sia  $P_n$  lo spazio vettoriale delle funzioni polinomiali reali di grado  $\leq n$ , della forma:

$$(1.4) \quad a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

La derivata  $\frac{d}{dx}$  è un'applicazione lineare da  $P_n$  a  $P_{n-1}$ .

Sia  $T : V \rightarrow W$  un'applicazione lineare. Introduciamo due sottospazi:

$$(1.5) \quad \begin{aligned} \ker T &= \text{nucleo di } T = \{v \in V \mid T(v) = 0\}, \\ \text{im } T &= \text{immagine di } T = \{w \in W \mid w = T(v) \text{ per qualche } v \in V\}. \end{aligned}$$

Come nel caso analogo degli omomorfismi di gruppi (cap. 2, §4),  $\ker T$  è un sottospazio di  $V$  e  $\text{im } T$  è un sottospazio di  $W$ .

È interessante interpretare il nucleo e l'immagine nel caso in cui  $T$  è la moltiplicazione a sinistra per una matrice  $A$ . In questo caso, il nucleo di  $T$  è l'insieme delle soluzioni dell'equazione lineare omogenea  $AX = 0$ , mentre l'immagine di  $T$  è l'insieme dei vettori  $B \in F^m$  tali che l'equazione lineare  $AX = B$  ha una soluzione.

Il risultato principale di questo paragrafo è la *formula della dimensione*, data dal teorema seguente:

(1.6) TEOREMA *Sia  $T : V \rightarrow W$  un'applicazione lineare, e supponiamo che  $V$  sia di dimensione finita. Allora*

$$\dim V = \dim(\ker T) + \dim(\text{im } T).$$

Le dimensioni di  $\text{im } T$  e  $\ker T$  sono chiamate, rispettivamente, il *rango* e la *nullità* di  $T$ . Dunque l'enunciato (1.6) può essere espresso nella forma:

$$(1.7) \quad \dim V = \text{rango} + \text{nullità}.$$

Si noti l'analogia con la formula:  $|G| = |\ker \varphi| \cdot |\text{im } \varphi|$  per gli omomorfismi di gruppi [cap. 2 (6.15)].

Il *rango* e la *nullità* di una matrice  $m \times n$   $A$  sono definiti come le dimensioni, rispettivamente, dell'immagine e del nucleo della moltiplicazione a sinistra per  $A$ . Denotiamo il rango con  $r$  e la nullità con  $k$ . Allora  $k$  è la dimensione dello spazio delle soluzioni dell'equazione  $AX = 0$ . I vettori  $B$  tali che l'equazione lineare  $AX = B$  possiede una soluzione costituiscono l'immagine, che è uno spazio di dimensione  $r$ . La somma di queste due dimensioni è  $n$ .

Sia  $B$  un vettore nell'immagine della moltiplicazione per  $A$ , sicché l'equazione  $AX = B$  possiede almeno una soluzione  $X = X_0$ . Denotiamo con  $K$  lo spazio delle soluzioni dell'equazione omogenea  $AX = 0$ , ossia il nucleo della moltiplicazione per  $A$ . Allora l'insieme delle soluzioni dell'equazione  $AX = B$  è la classe laterale

**additiva**  $X_0 + K$ . Ciò esprime in forma concisa un risultato ben noto: aggiungendo una qualsiasi soluzione dell'equazione omogenea  $AX = 0$  ad una soluzione particolare  $X_0$  dell'equazione non omogenea  $AX = B$  si ottiene un'altra soluzione dell'equazione non omogenea.

Supponiamo che  $A$  sia una matrice quadrata  $n \times n$ . Se  $\det A \neq 0$ , allora, com'è noto, il sistema di equazioni  $AX = B$  possiede una e una sola soluzione per ogni  $B$ , poiché  $A$  è invertibile. In tal caso,  $k = 0$  e  $r = n$ . D'altra parte, se  $\det A = 0$ , allora lo spazio  $K$  ha dimensione  $k > 0$ . Dalla formula della dimensione segue che  $r < n$ , ossia, che l'immagine non è l'intero spazio  $F^n$ . Ciò significa che non tutte le equazioni  $AX = B$  hanno soluzioni. Tuttavia, quelle che hanno soluzioni ne hanno più di una, poiché l'insieme delle soluzioni di  $AX = B$  è una classe laterale di  $K$ .

*Dimostrazione del teorema (1.6).* Sia  $\dim V = n$ . Allora, data una base  $(u_1, \dots, u_k)$  del sottospazio  $\ker T$ , la estendiamo a una base di  $V$  [cap. 3 (3.15)]:

$$(1.8) \quad (u_1, \dots, u_k; v_1, \dots, v_{n-k}).$$

Poniamo  $w_i = T(v_i)$ , per  $i = 1, \dots, n-k$ . Se dimostriamo che  $(w_1, \dots, w_{n-k}) = S$  è una base di  $\text{im } T$ , allora seguirà che  $\text{im } T$  ha dimensione  $n-k$ . Ciò proverà il teorema.

Dunque dobbiamo dimostrare che  $S$  genera  $\text{im } T$  e che  $S$  è un insieme linearmente indipendente. Sia  $w$  un elemento arbitrario appartenente a  $\text{im } T$ . Allora  $w = T(v)$  per qualche  $v \in V$ . Scriviamo  $v$  mediante la base (1.8):

$$v = a_1 u_1 + \cdots + a_k u_k + b_1 v_1 + \cdots + b_{n-k} v_{n-k},$$

e applichiamo  $T$ , osservando che  $T(u_i) = 0$ :

$$w = 0 + \cdots + 0 + b_1 w_1 + \cdots + b_{n-k} w_{n-k}.$$

Dunque  $w$  appartiene allo spazio generato da  $S$ , e pertanto  $S$  genera  $\text{im } T$ .

Inoltre, supponiamo che sia data una relazione lineare:

$$(1.9) \quad c_1 w_1 + \cdots + c_{n-k} w_{n-k} = 0,$$

e consideriamo la combinazione lineare  $v = c_1 v_1 + \cdots + c_{n-k} v_{n-k}$ , dove i  $v_i$  sono i vettori (1.8). Applicando  $T$  a  $v$ , si ottiene:

$$T(v) = c_1 w_1 + \cdots + c_{n-k} w_{n-k} = 0.$$

Dunque  $v \in \ker T$ . Pertanto possiamo scrivere  $v$  mediante la base  $(u_1, \dots, u_k)$  di  $\ker T$ , diciamo  $v = a_1 u_1 + \cdots + a_k u_k$ . Allora

$$(-a_1 u_1) + \cdots + (-a_k u_k) + c_1 v_1 + \cdots + c_{n-k} v_{n-k} = 0.$$

Ma, poiché (1.8) è una base, si ha  $-a_1 = 0, \dots, -a_k = 0$ , e  $c_1 = 0, \dots, c_{n-k} = 0$ . Pertanto la relazione (1.9) è necessariamente la relazione banale, e quindi  $S$  è linearmente indipendente. Ciò completa la dimostrazione. ■

## 2 La matrice di un'applicazione lineare

Non è difficile dimostrare che ogni applicazione lineare  $T : F^n \rightarrow F^m$  è la moltiplicazione a sinistra per una matrice  $m \times n$ . A tal fine, consideriamo le immagini  $T(e_j)$  dei vettori  $e_j$  della base canonica di  $F^n$ . Indichiamo gli elementi di tali vettori nel modo seguente:

$$(2.1) \quad T(e_j) = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix},$$

e formiamo la matrice  $m \times n$   $A = (a_{ij})$  avente come colonne questi vettori. Possiamo scrivere un vettore arbitrario  $X = (x_1, \dots, x_n)^t$  di  $F^n$  nella forma  $X = e_1x_1 + \dots + e_nx_n$ , mettendo gli scalari a destra. Allora:

$$T(X) = \sum_j T(e_j)x_j = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} x_1 + \dots + \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} x_n = AX.$$

Per esempio, l'applicazione lineare  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  tale che:

$$T(e_1) = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \quad \text{e} \quad T(e_2) = \begin{bmatrix} -1 \\ 0 \end{bmatrix},$$

è la moltiplicazione a sinistra per la matrice:

$$A = \begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix}.$$

Se  $X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = e_1x_1 + e_2x_2$ , allora

$$T(X) = \begin{bmatrix} 1 \\ 2 \end{bmatrix} x_1 + \begin{bmatrix} -1 \\ 0 \end{bmatrix} x_2 = \begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 - x_2 \\ 2x_1 \end{bmatrix}.$$

Utilizzando la notazione introdotta nel capitolo 3 (§ 4), possiamo fare un calcolo simile con un'applicazione lineare arbitraria  $T : V \rightarrow W$ , una volta assegnate le basi dei due spazi. Siano  $\mathbf{B} = (v_1, \dots, v_n)$  e  $\mathbf{C} = (w_1, \dots, w_m)$  basi di  $V$

e  $W$ , rispettivamente, e utilizziamo la notazione abbreviata  $T(\mathbf{B})$  per denotare l'ipervettore:

$$T(\mathbf{B}) = (T(v_1), \dots, T(v_n)).$$

Dato che gli elementi di tale ipervettore appartengono a  $W$  e  $\mathbf{C}$  è una base di  $W$ , esiste una matrice  $m \times n$ ,  $A$ , tale che

$$(2.2) \quad T(\mathbf{B}) = \mathbf{C}A, \quad \text{ossia} \quad (T(v_1), \dots, T(v_n)) = (w_1, \dots, w_m) \begin{bmatrix} A \\ \vdots \\ A \end{bmatrix}$$

[cap. 3 (4.13)]. Ricordiamo che ciò significa che, per ogni  $j$ ,

$$(2.3) \quad T(v_j) = \sum_i w_i a_{ij} = w_1 a_{1j} + \dots + w_m a_{mj}.$$

Quindi  $A$  è la matrice la cui  $j$ -esima colonna è il vettore delle coordinate di  $T(v_j)$ . Tale matrice  $m \times n$   $A = (a_{ij})$  è chiamata la *matrice di  $T$  rispetto alle basi  $\mathbf{B}, \mathbf{C}$* . Scegliendo basi diverse, si ottengono matrici diverse.

Nel caso in cui  $V = F^n$ ,  $W = F^m$ , e le due basi sono quelle canoniche,  $A$  è la matrice costruita a partire da (2.1).

La matrice di un'applicazione lineare può essere usata per calcolare le coordinate del vettore immagine  $T(v)$  mediante le coordinate di  $v$ . Per fare ciò, scriviamo  $v$  mediante la base, diciamo:

$$v = \mathbf{B}X = v_1x_1 + \dots + v_nx_n.$$

Allora:

$$T(v) = T(v_1)x_1 + \dots + T(v_n)x_n = T(\mathbf{B})X = \mathbf{C}AX.$$

Pertanto il vettore delle coordinate di  $T(v)$  è:

$$Y = AX,$$

infatti  $T(v) = CY$ . Ricapitolando, la matrice  $A$  dell'applicazione lineare possiede due proprietà duali:

$$(2.4) \quad T(\mathbf{B}) = \mathbf{C}A \quad \text{e} \quad Y = AX.$$

La relazione tra  $T$  e  $A$  può essere spiegata tramite gli isomorfismi  $\psi : F^n \rightarrow V$  e  $\psi' : F^m \rightarrow W$  determinati dalle due basi [cap. 3 (4.14)]. Se utilizziamo  $\psi$  e  $\psi'$  per identificare  $V$  e  $W$  con  $F^n$  e  $F^m$ , allora  $T$  corrisponde alla moltiplicazione

a sinistra per  $A$ :

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ \psi \uparrow & & \uparrow \psi' \\ F^n & \xrightarrow{\text{molt. per } A} & F^m \end{array} \quad \begin{array}{c} \mathbf{B}X \longleftarrow \mathbf{CAX} \\ X \longleftarrow AX. \end{array}$$

Percorrendo il diagramma nelle due direzioni, si ottiene lo stesso risultato:  $T \circ \psi = \psi' \circ A$ .

Dunque ogni applicazione lineare tra spazi vettoriali di dimensione finita  $V$  e  $W$  può essere identificata con la moltiplicazione per una matrice, una volta scelte le basi per i due spazi. Ma se studiamo i cambiamenti di base in  $V$  e  $W$ , possiamo fare di meglio. Chiediamoci come cambia la matrice  $A$  quando scegliamo altre basi per  $V$  e  $W$ . Siano  $\mathbf{B}' = (v'_1, \dots, v'_n)$ ,  $\mathbf{C}' = (w'_1, \dots, w'_m)$  nuove basi per tali spazi. Possiamo collegare la nuova base  $\mathbf{B}'$  alla vecchia base  $\mathbf{B}$  mediante una matrice  $P \in GL_n(F)$  [cfr. cap. 3 (4.19)]. Analogamente,  $\mathbf{C}'$  è collegata a  $\mathbf{C}$  mediante una matrice  $Q \in GL_m(F)$ . Tali matrici hanno le seguenti proprietà:

$$(2.6) \quad PX = X' \quad \text{e} \quad QY = Y'.$$

Qui  $X$  e  $X'$  denotano i vettori delle coordinate di un vettore  $v \in V$  rispetto alle basi  $\mathbf{B}$  e  $\mathbf{B}'$ , mentre  $Y$  e  $Y'$  denotano i vettori delle coordinate di un vettore  $w \in W$  rispetto a  $\mathbf{C}$  e  $\mathbf{C}'$ .

Denotiamo con  $A'$  la matrice di  $T$  rispetto alle nuove basi, definita come sopra [cfr. (2.4)], così che  $A'X' = Y'$ . Allora  $QAP^{-1}X' = QAX = QY = Y'$ . Pertanto:

$$(2.7) \quad A' = QAP^{-1}.$$

Si noti che  $P$  e  $Q$  sono matrici invertibili  $n \times n$  e  $m \times m$  arbitrarie [cap. 3 (4.23)]. Otteniamo così la seguente descrizione delle matrici di un'applicazione lineare assegnata:

(2.8) PROPOSIZIONE *Sia  $A$  la matrice di un'applicazione lineare  $T$  rispetto a due basi  $\mathbf{B}, \mathbf{C}$ . Le matrici  $A'$  che rappresentano  $T$  rispetto ad altre basi sono quelle della forma:*

$$A' = QAP^{-1},$$

dove  $Q \in GL_m(F)$  e  $P \in GL_n(F)$  sono matrici invertibili arbitrarie. ■

Ora, data un'applicazione lineare  $T : V \rightarrow W$ , è naturale cercare basi  $\mathbf{B}, \mathbf{C}$  di  $V$  e  $W$  tali che la matrice di  $T$  risulti particolarmente semplice. In effetti la matrice può essere semplificata notevolmente.

### (2.9) PROPOSIZIONE

(a) (Spazi vettoriali) *Sia  $T : V \rightarrow W$  un'applicazione lineare. È possibile scegliere basi  $\mathbf{B}, \mathbf{C}$  in modo tale che la matrice di  $T$  abbia la forma:*

$$(2.10) \quad A = \begin{pmatrix} I_r & \\ & 0 \end{pmatrix},$$

dove  $I_r$  è la matrice identica  $r \times r$ , e  $r = \text{rank } T$ .

(b) (Matrici) *Data una matrice  $m \times n$   $A$ , esistono due matrici  $Q \in GL_m(F)$  e  $P \in GL_n(F)$  tali che  $QAP^{-1}$  ha la forma (2.10).*

Dalla discussione precedente segue che questi due enunciati sono tra loro equivalenti. Per ottenere (a) da (b), scegliamo due basi arbitrarie  $\mathbf{B}, \mathbf{C}$ , e sia  $A$  la matrice di  $T$  rispetto a tali basi. Applicando (b), possiamo trovare  $P, Q$  tali che  $QAP^{-1}$  abbia la forma richiesta. Siano  $\mathbf{B}' = BP^{-1}$  e  $\mathbf{C}' = CQ^{-1}$  le nuove basi [cfr. cap. 3 (4.22)]. Allora la matrice di  $T$  rispetto alle basi  $\mathbf{B}', \mathbf{C}'$  è  $QAP^{-1}$ , così queste nuove basi sono quelle richieste. Viceversa, per ottenere (b) da (a), interpretiamo una matrice  $A$  arbitraria come la matrice dell'applicazione lineare "moltiplicazione a sinistra per  $A$ ", rispetto alle basi canoniche. Allora (a) e (2.7) garantiscono l'esistenza di  $P, Q$  tali che  $QAP^{-1}$  abbia la forma richiesta.

Si noti che possiamo interpretare  $QAP^{-1}$  come la matrice ottenuta da  $A$  mediante una successione di operazioni sulle righe e sulle colonne. Infatti, se scriviamo  $P$  e  $Q$  come prodotti di matrici elementari  $P = E_p \cdots E_1$  e  $Q = E'_q \cdots E'_1$  [cap. 1 (2.18)], allora  $QAP^{-1} = E'_q \cdots E'_1 A E_1^{-1} \cdots E_p^{-1}$ . In virtù della proprietà associativa, non importa se vengono effettuate per prime le operazioni sulle righe o le operazioni sulle colonne. La relazione  $(E'A)E = E'(AE)$  ci dice che le operazioni sulle righe commutano con le operazioni sulle colonne.

Non è difficile dimostrare (2.9b) mediante calcoli con le matrici; dimostriamo invece (2.9a), utilizzando le basi. Sia  $(u_1, \dots, u_k)$  una base di  $\ker T$  che estendiamo a una base  $\mathbf{B}$  di  $V$ :  $(v_1, \dots, v_r; u_1, \dots, u_k)$ , dove  $r + k = n$ . Poniamo  $w_i = T(v_i)$ . Allora, come si è visto nella dimostrazione di (1.6),  $(w_1, \dots, w_r)$  è una base di  $\text{im } T$ , e può essere estesa a una base  $\mathbf{C}$  di  $W$ :  $(w_1, \dots, w_r; x_1, \dots, x_s)$ . La matrice di  $T$  rispetto alle basi  $\mathbf{B}, \mathbf{C}$  ha la forma richiesta. ■

La proposizione (2.9) è il prototipo di vari risultati che saranno dimostrati più avanti. Essa mostra la potenza dello studio degli spazi vettoriali senza basi fissate (o coordinate), infatti la struttura di una qualsiasi applicazione lineare è collegata alla matrice molto semplice (2.10). Questa proposizione esprime anche una proprietà notevole della moltiplicazione tra matrici, infatti dice che la moltiplicazione a

sinistra per  $A$  su  $F^m$  è un'applicazione lineare. Precisamente, essa afferma che la moltiplicazione a sinistra per  $A$  è la stessa cosa che la moltiplicazione a sinistra per una matrice della forma (2.10), ma rispetto a sistemi di coordinate diversi. Poiché la moltiplicazione per la matrice (2.10) è facile da descrivere, abbiamo imparato qualcosa di nuovo.

### 3 Operatori lineari e autovettori

Consideriamo ora il caso di un *operatore lineare* su  $V$ , cioè un'applicazione lineare  $T : V \rightarrow V$  da uno spazio vettoriale in sé stesso. La moltiplicazione a sinistra per una matrice  $n \times n$  a elementi in  $F$  definisce un operatore lineare sullo spazio  $F^n$  dei vettori colonne.

Per esempio, una rotazione  $\rho_\theta$  del piano di un angolo  $\theta$  è un operatore lineare su  $\mathbb{R}^2$ , la cui matrice rispetto alla base canonica è:

$$(3.1) \quad R = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Per verificare che tale matrice rappresenta una rotazione, scriviamo un vettore  $X \in \mathbb{R}^2$  in coordinate polari, nella forma:  $X = (r, \alpha)$ . Allora, in coordinate cartesiane ortogonali si ha:  $X = \begin{bmatrix} r \cos \alpha \\ r \sin \alpha \end{bmatrix}$ . Le formule di addizione per il seno e il coseno provano che  $RX = \begin{bmatrix} r \cos(\alpha + \theta) \\ r \sin(\alpha + \theta) \end{bmatrix}$ . Dunque, in coordinate polari,  $RX = (r, \alpha + \theta)$ , cioè  $RX$  è ottenuto da  $X$  mediante la rotazione espressa dall'angolo  $\theta$ .

La discussione del paragrafo precedente deve essere modificata leggermente quando trattiamo gli operatori lineari. È chiaro che vogliamo prendere una sola base  $\mathbf{B} = (v_1, \dots, v_n)$  di  $V$ , e usarla al posto delle due basi  $\mathbf{B}$  e  $\mathbf{C}$  considerate nel paragrafo 2. In altre parole, vogliamo scrivere:

$$(3.2) \quad T(\mathbf{B}) = \mathbf{B}A$$

ossia:

$$T(v_j) = \sum_i v_i a_{ij} = v_1 a_{1j} + \dots + v_n a_{nj}.$$

Ciò definisce la matrice  $A = (a_{ij})$  di  $T$ . Essa è una matrice quadrata la cui colonna  $j$ -esima è il vettore delle coordinate di  $T(v_j)$  rispetto alla base  $\mathbf{B}$ . La formula (2.4) resta invariata, a patto di sostituire  $W$  e  $\mathbf{C}$  con  $V$  e  $\mathbf{B}$ . Come si è visto nel paragrafo precedente, se  $X$  e  $Y$  denotano i vettori delle coordinate di  $v$  e  $T(v)$ , rispettivamente, allora:

$$(3.3) \quad Y = AX.$$

Una novità viene fuori quando studiamo l'effetto di un cambiamento di base in  $V$ . Supponiamo di sostituire  $\mathbf{B}$  con una nuova base  $\mathbf{B}' = (v'_1, \dots, v'_n)$ . Allora la formula (2.7) mostra che la nuova matrice  $A'$  ha la forma:

$$(3.4) \quad A' = PAP^{-1},$$

dove  $P$  è la matrice del cambiamento di base. Quindi la regola del cambiamento di base per un'applicazione lineare diventa:

(3.5) PROPOSIZIONE Sia  $A$  la matrice di un operatore lineare  $T$  rispetto a una base  $\mathbf{B}$ . Le matrici  $A'$  che rappresentano  $T$  rispetto ad altre basi sono quelle della forma:

$$A' = PAP^{-1},$$

dove  $P$  è una qualsiasi matrice in  $GL_n(F)$ .

In generale, si dice che una matrice quadrata  $A$  è *simile* ad  $A'$  se  $A' = PAP^{-1}$ , per qualche  $P \in GL_n(F)$ . Si potrebbe usare anche il termine *coniugata* [cfr. cap. 2, (3.4)].

Ora, data una matrice  $A$ , è naturale cercare una matrice simile  $A'$  che sia particolarmente semplice. Si può sperare di ottenere un risultato in qualche modo analogo a (2.10). Qui però il cambiamento ammissibile è molto più limitato, poiché abbiamo una sola base, e quindi una sola matrice  $P$ , da utilizzare.

Possiamo comprendere un po' meglio il problema, scrivendo l'ipotetica matrice  $P$  come un prodotto di matrici elementari:  $P = E_r \cdots E_1$ . Allora:

$$PAP^{-1} = E_r \cdots E_1 A E_1^{-1} \cdots E_r^{-1}.$$

Mediante operazioni elementari, possiamo trasformare  $A$  attraverso una successione di passi:  $A \mapsto EAE^{-1}$ . In altre parole, possiamo effettuare un'arbitraria operazione sulle righe  $E$ , ma allora dobbiamo effettuare anche l'operazione inversa sulle colonne  $E^{-1}$ . Purtroppo, le operazioni sulle righe e sulle colonne interferiscono tra loro e ciò rende difficile la comprensione di tali operazioni. Io non so come utilizzarle. È sorprendente che invece si possa fare molto utilizzando un altro metodo.

Gli strumenti principali per analizzare gli operatori lineari sono i concetti di *autovettore* e di *sottospazio invariante*.

Sia  $T : V \rightarrow V$  un operatore lineare su uno spazio vettoriale. Un sottospazio  $W$  di  $V$  è chiamato un *sottospazio invariante* o un *sottospazio  $T$ -invariante*, se è mandato in se stesso dall'operatore:

$$(3.6) \quad TW \subset W.$$

In altre parole,  $W$  è  $T$ -invariante se  $T(w) \in W$  per ogni  $w \in W$ . Quando ciò accade,  $T$  definisce un operatore lineare su  $W$ , chiamato la *restrizione* di  $T$  a  $W$ .

Sia  $W$  un sottospazio  $T$ -invariante, e scegliamo una base  $\mathbf{B}$  di  $V$  aggiungendo alcuni vettori a una base  $(w_1, \dots, w_k)$  di  $W$ :

$$\mathbf{B} = (w_1, \dots, w_k, v_1, \dots, v_{n-k}).$$

Allora il fatto che  $W$  è invariante si può leggere direttamente dalla matrice  $M$  di  $T$ . Infatti, le colonne di tale matrice sono i vettori delle coordinate dei vettori immagine [cfr. (2.3)], e  $T(w_j)$  appartiene al sottospazio  $W$ , dunque è una combinazione lineare della base  $(w_1, \dots, w_k)$ . Pertanto, quando scriviamo  $T(w_j)$  mediante la base  $\mathbf{B}$ , i coefficienti dei vettori  $v_1, \dots, v_{n-k}$  sono nulli. Ne segue che  $M$  ha la forma a blocchi:

$$(3.7) \quad M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix},$$

dove  $A$  è una matrice  $k \times k$ . Inoltre,  $A$  è la matrice della restrizione di  $T$  a  $W$ .

Supponiamo che  $V = W_1 \oplus W_2$  sia la somma diretta di due sottospazi  $T$ -invarianti, e sia  $\mathbf{B}_i$  una base di  $W_i$ . Allora possiamo formare una base  $\mathbf{B}$  di  $V$ , disponendo gli elementi di  $\mathbf{B}_1$  e di  $\mathbf{B}_2$  in successione [cap. 3, (6.6a)]. In questo caso, la matrice di  $T$  avrà la forma diagonale a blocchi:

$$(3.8) \quad M = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix},$$

dove  $A_i$  è la matrice della restrizione di  $T$  a  $W_i$ .

Il concetto di autovettore è strettamente collegato a quello di sottospazio invariante. Un *autovettore*  $v$  per un operatore lineare  $T$  è un vettore non nullo tale che:

$$(3.9) \quad T(v) = cv$$

per qualche scalare  $c \in F$ . Qui  $c$  può prendere il valore 0, ma il vettore  $v$  non può essere nullo. Geometricamente, se  $V = \mathbb{R}^n$ , un autovettore è un vettore non nullo  $v$  tale che  $v$  e  $T(v)$  sono paralleli.

Lo scalare  $c$  che compare nella relazione (3.9) è chiamato l'*autovalore* associato all'autovettore  $v$ . Quando si parla di un *autovalore* di un operatore lineare  $T$ , si intende uno scalare  $c \in F$  che è l'autovalore associato a qualche autovettore.

Per esempio, il vettore della base canonica  $e_1$  è un autovettore per la moltiplicazione a sinistra per la matrice:

$$\begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}.$$

L'*autovalore* associato all'autovettore  $e_1$  è 3. Un altro esempio: il vettore  $(0, 1, 1)^t$  è un autovettore per la moltiplicazione per la matrice:

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 2 & 1 & 1 \\ 3 & 0 & 2 \end{bmatrix}.$$

definita sullo spazio  $\mathbb{R}^3$  dei vettori colonna, e il suo autovalore è 2.

Talvolta gli autovettori e gli autovalori sono chiamati *vettori caratteristici* e *valori caratteristici*.

Sia  $v$  un autovettore per un operatore lineare  $T$ . Il sottospazio  $W$  generato da  $v$  è  $T$ -invariante, poiché  $T(av) = acv \in W$ , per ogni  $a \in F$ . Viceversa, se tale sottospazio è invariante, allora  $v$  è un autovettore. Quindi un autovettore può essere descritto come una base di un sottospazio  $T$ -invariante di dimensione 1. Se  $v$  è un autovettore, e se lo estendiamo a una base  $(v = v_1, \dots, v_n)$  di  $V$ , allora la matrice di  $T$  avrà la forma a blocchi:

$$\begin{bmatrix} c & B \\ 0 & D \end{bmatrix} = \left[ \begin{array}{c|ccc} c & * & \cdots & * \\ \hline 0 & & & & \\ \vdots & & * & & \\ 0 & & & & \end{array} \right],$$

dove  $c$  è l'autovalore associato a  $v_1$ . Questa è la decomposizione in blocchi (3.7) nel caso di un sottospazio invariante di dimensione 1.

Parlando di un *autovettore* di una matrice  $n \times n$   $A$  si intende un vettore che è un autovettore rispetto alla moltiplicazione a sinistra per  $A$ , ossia un vettore colonna non nullo tale che:

$$AX = cX, \quad \text{per qualche } c \in F.$$

Come prima, lo scalare  $c$  è chiamato *autovalore*. Supponiamo che  $A$  sia la matrice di  $T$  rispetto a una base  $\mathbf{B}$ , e denotiamo con  $X$  il vettore delle coordinate di un vettore  $v \in V$ . Allora  $T(v)$  ha coordinate  $AX$  [cfr. (2.4)]. Pertanto  $X$  è un autovettore per  $A$  se e solo se  $v$  è un autovettore per  $T$ . Inoltre, in tal caso, gli *autovalori* sono gli stessi:  $T$  ed  $A$  hanno gli stessi autovalori.

**(3.10) COROLLARIO** *Matrici simili hanno gli stessi autovalori.*

Ciò segue dal fatto [cfr. (3.5)] che matrici simili rappresentano la stessa applicazione lineare. ■

Gli autovettori non sono sempre facili da trovare, tuttavia è facile stabilire se un vettore assegnato  $X$  è o non è un autovettore per una matrice  $A$ . Occorre verificare soltanto se  $AX$  è o non è un multiplo di  $X$ . Così possiamo stabilire

se un vettore assegnato  $v$  è oppure no un autovettore per un operatore lineare  $T$ , purché siano noti il vettore delle coordinate di  $v$  e la matrice di  $T$  rispetto a una base. Se consideriamo uno dei vettori della base, otteniamo il criterio seguente:

- (3.11) Il vettore  $v_j$  della base è un autovettore di  $T$ , con autovalore  $c$ , se e solo se la colonna  $j$ -esima di  $A$  ha la forma  $ce_j$ .

Infatti la matrice  $A$  è definita dalla proprietà  $T(v_j) = v_1 a_{1j} + \dots + v_n a_{nj}$ . Quindi, se  $T(v_j) = cv_j$ , allora  $a_{jj} = c$  e  $a_{ij} = 0$ , se  $i \neq j$ . ■

- (3.12) COROLLARIO Con le notazioni precedenti,  $A$  è una matrice diagonale se e solo se ogni vettore  $v_j$  della base è un autovettore. ■

- (3.13) COROLLARIO La matrice  $A$  di un operatore lineare è simile a una matrice diagonale se e solo se esiste una base  $\mathbf{B}' = (v'_1, \dots, v'_n)$  di  $V$  costituita da autovettori. ■

Quest'ultimo corollario prova che è possibile rappresentare un operatore lineare in una forma molto semplice, mediante una matrice diagonale, purché esso abbia abbastanza autovettori. Vedremo più avanti che ogni operatore lineare su uno spazio vettoriale complesso possiede almeno un autovettore (§ 4), e che nella maggior parte dei casi gli autovettori formano una base (§ 6). Invece un operatore lineare su uno spazio vettoriale reale non ha necessariamente un autovettore. Per esempio, la rotazione  $\rho_\theta$  (3.1) del piano non porta nessun vettore in un vettore ad esso parallelo, a meno che  $\theta = 0$  oppure  $\theta = \pi$ . Pertanto  $\rho_\theta$  non ha autovettori, a meno che  $\theta = 0$  oppure  $\theta = \pi$ .

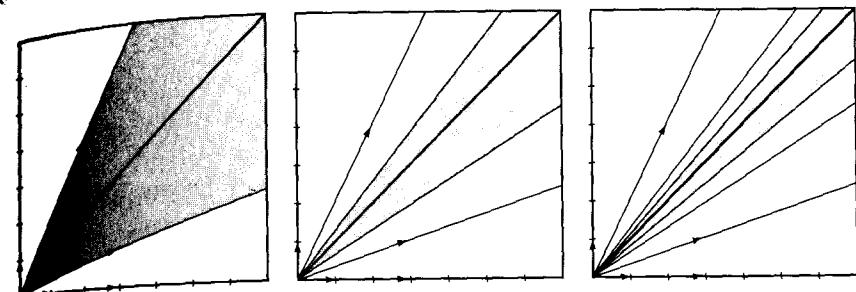
La situazione è del tutto diversa per le matrici reali a elementi positivi. Tali matrici sono chiamate talvolta matrici *positive*. Compiono spesso nelle applicazioni, e una delle loro proprietà più importanti è che hanno sempre un autovettore le cui coordinate sono positive, ossia un autovettore *positivo*. Anziché dimostrare questo fatto, lo illustreremo nel caso di due variabili, esaminando l'effetto della moltiplicazione per una matrice positiva  $2 \times 2$ ,  $A$ , su  $\mathbb{R}^2$ .

Sia  $w_i = Ae_i$ . La regola del parallelogramma per l'addizione tra vettori mostra che  $A$  manda il primo quadrante  $S$  nel settore limitato dai vettori  $w_1, w_2$ . Inoltre il vettore delle coordinate di  $w_i$  è la colonna  $i$ -esima di  $A$ . Poiché gli elementi di  $A$  sono positivi, i vettori  $w_i$  giacciono nel primo quadrante. Pertanto  $A$  porta il primo quadrante in se stesso:  $S \supset AS$ . Applicando di nuovo  $A$ , si ha:  $AS \supset A^2S$ , e così via:

$$(3.14) \quad S \supset AS \supset A^2S \supset A^3S \supset \dots,$$

come mostra la figura (3.15), per la matrice  $A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ .

(3.15)



Immagini del primo quadrante rispetto alla moltiplicazione ripetuta per una matrice positiva.

Ora l'intersezione di un insieme siffatto di settori, ciascuno contenuto nel precedente, o è un settore oppure è una semiretta. Nel nostro caso, l'intersezione  $Z = \cap A^r S$  risulta una semiretta. Ciò è abbastanza intuitivo e può essere dimostrato in vari modi. La dimostrazione è lasciata come esercizio. Moltiplicando ambo i membri della relazione  $Z = \cap A^r S$  per  $A$ , si ottiene:

$$AZ = A \left( \bigcap_0^\infty A^r S \right) = \bigcap_1^\infty A^r S = Z.$$

Dunque  $Z = AZ$ . Ciò prova che i vettori non nulli in  $Z$  sono autovettori. ■

#### 4 Il polinomio caratteristico

In questo paragrafo determineremo gli autovettori di un operatore lineare  $T$  arbitrario. Ricordiamo che un autovettore per  $T$  è un vettore non nullo  $v$  tale che:

$$(4.1) \quad T(v) = cv,$$

per qualche  $c$  in  $F$ . A prima vista, sembra difficile trovare gli autovettori se la matrice dell'operatore lineare è complicata. L'idea ingegnosa è quella di risolvere prima un altro problema, cioè determinare gli *autovalori*. Una volta determinato un *autovalore*  $c$ , l'equazione (4.1) diventa lineare nelle coordinate di  $v$  e la sua *risoluzione* non presenta alcun problema.

Innanzitutto, scriviamo la (4.1) nella forma

$$(4.2) \quad [T - cI](v) = 0,$$

dove l'operatore  $I$  è l'identità e  $T - cI$  è l'operatore lineare definito da

$$(4.3) \quad [T - cI](v) = T(v) - cv.$$

È facile verificare che  $T - cI$  è un operatore lineare. Se  $A$  è la matrice di  $T$  rispetto a una base fissata, allora la matrice di  $T - cI$  è  $A - cI$ .

Possiamo rienunciare la condizione (4.2) nella forma seguente:

$$(4.4) \quad v \text{ appartiene al nucleo di } T - cI.$$

(4.5) LEMMA *Le seguenti condizioni per un operatore lineare  $T : V \rightarrow V$  su uno spazio vettoriale di dimensione finita sono tra loro equivalenti:*

- (a)  $\ker T > 0$ .
- (b)  $\text{im } T < V$ .
- (c) *Se  $A$  è la matrice dell'operatore rispetto a una qualsiasi base, allora  $\det A = 0$ .*
- (d)  *$0$  è un autovalore di  $T$ .*

*Dimostrazione.* La formula della dimensione (1.6) prova che  $\ker T > 0$  se e solo se  $\text{im } T < V$ . Ciò è vero se e solo se  $T$  non è un isomorfismo, ossia se e solo se  $A$  non è una matrice invertibile. D'altra parte, sappiamo che le matrici quadrate  $A$  che non sono invertibili sono quelle con determinante zero. Ciò dimostra l'equivalenza di (a), (b) e (c). Infine, i vettori non nulli del nucleo di  $T$  sono gli autovettori con autovalore zero. Dunque (a) è equivalente a (d). ■

Le condizioni (4.5a) e (4.5b) non sono equivalenti per spazi vettoriali di dimensione infinita. Per esempio, sia  $V = \mathbb{R}^\infty$  lo spazio dei vettori riga infiniti  $(a_1, a_2, \dots)$ , già introdotto nel cap. 3 (§ 5). L'operatore di scorrimento, definito da:

$$(4.6) \quad T(a_1, a_2, \dots) = (0, a_1, a_2, \dots),$$

è un operatore lineare su  $V$ . Per tale operatore,  $\ker T = 0$ , ma  $\text{im } T < V$ .

(4.7) DEFINIZIONE *Un operatore lineare  $T$  su uno spazio vettoriale di dimensione finita  $V$  si dice singolare se soddisfa una qualsiasi delle condizioni equivalenti del lemma (4.5). Altrimenti,  $T$  è non singolare.*

Sappiamo che  $c$  è un autovalore per l'operatore  $T$  se e soltanto se il nucleo di  $T - cI$  è diverso da zero [cfr. (4.4)]. Quindi, se sostituiamo  $T$  con  $T - cI$  nel lemma precedente, otteniamo:

(4.8) COROLLARIO *Gli autovalori di un operatore lineare  $T$  sono gli scalari  $c \in F$  tali che  $T - cI$  è singolare. ■*

Se  $A$  è la matrice di  $T$  rispetto a una base fissata, allora la matrice di  $T - cI$  è  $A - cI$ . Pertanto  $T - cI$  è singolare se e soltanto se  $\det(A - cI) = 0$ .

Questo determinante può essere calcolato esplicitamente, e così facendo abbiamo a disposizione un metodo concreto per determinare gli autovalori e gli autovettori. Supponiamo per esempio che  $A$  sia la matrice:

$$(4.9) \quad \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$$

la cui azione su  $\mathbb{R}^2$  è illustrata nella figura (3.15). Allora:

$$A - cI = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} - \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} 3 - c & 2 \\ 1 & 4 - c \end{bmatrix}$$

e

$$\det(A - cI) = c^2 - 7c + 10 = (c - 5)(c - 2).$$

Tale determinante si annulla se  $c = 5$  oppure  $c = 2$ , quindi abbiamo dimostrato che gli autovalori di  $A$  sono 5 e 2. Per trovare gli autovettori, risolviamo i due sistemi di equazioni lineari:  $[A - 5I]X = 0$  e  $[A - 2I]X = 0$ . Le soluzioni sono determinate a meno di un fattore scalare:

$$(4.10) \quad v_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 2 \\ -1 \end{bmatrix}.$$

Si noti che l'autovettore  $v_1$  con autovalore 5 sta nel primo quadrante e giace sulla semiretta  $Z$  illustrata nella figura (3.15).

Facciamo ora lo stesso calcolo con una matrice qualunque. In tal caso, conviene cambiare segno. È ovvio che  $\det(cI - A) = 0$  se e solo se  $\det(A - cI) = 0$ . Inoltre, di solito si usa sostituire il simbolo  $c$  con una variabile  $t$ . Formiamo la matrice  $tI - A$ :

$$(4.11) \quad tI - A = \begin{bmatrix} (t - a_{11}) & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & (t - a_{22}) & \cdots & -a_{2n} \\ \vdots & & & \vdots \\ -a_{n1} & \cdots & \cdots & (t - a_{nn}) \end{bmatrix}.$$

Allora lo sviluppo completo del determinante [cap. 1 (4.11)] mostra che  $\det(tI - A)$  è un polinomio di grado  $n$  in  $t$ , i cui coefficienti sono scalari.

(4.12) DEFINIZIONE *Il polinomio caratteristico di un operatore lineare  $T$  è il polinomio:*

$$p(t) = \det(tI - A),$$

dove  $A$  è la matrice di  $T$  rispetto a una base fissata.

Gli autovalori di  $T$  si ottengono combinando (4.8) e (4.12):  $c$  è un autovalore se e soltanto se  $p(c) = 0$ .

(4.13) COROLLARIO *Gli autovalori di un operatore lineare sono le radici del suo polinomio caratteristico.* ■

(4.14) COROLLARIO *Gli autovalori di una matrice triangolare superiore o inferiore sono i suoi elementi diagonali.*

*Dimostrazione.* Se  $A$  è una matrice triangolare superiore, allora tale risulta  $tI - A$ . Il determinante di una matrice triangolare è il prodotto dei suoi elementi diagonali, e gli elementi diagonali di  $tI - A$  sono  $t - a_{ii}$ . Pertanto il polinomio caratteristico è  $p(t) = (t - a_{11})(t - a_{22}) \cdots (t - a_{nn})$ , e le sue radici, ossia gli autovalori, sono  $a_{11}, \dots, a_{nn}$ . ■

Il polinomio caratteristico di una matrice  $2 \times 2$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

si calcola facilmente:

$$(4.15) \quad \det(tI - A) = \det \begin{bmatrix} t - a & -b \\ -c & t - d \end{bmatrix} = t^2 - (a + d)t + (ad - bc).$$

Il discriminante di tale polinomio è:

$$(4.16) \quad (a + d)^2 - 4(ad - bc) = (a - d)^2 + 4bc.$$

Se gli elementi di  $A$  sono numeri reali positivi, allora anche il discriminante è positivo, e pertanto il polinomio caratteristico ha radici reali, come è stato osservato alla fine del § 3.

(4.17) PROPOSIZIONE *Il polinomio caratteristico di un operatore  $T$  non dipende dalla scelta della base.*

*Dimostrazione.* Fissata un'altra base, si ottiene una matrice  $A' = PAP^{-1}$  [cfr. (3.4)], e si ha:

$$tI - A' = tI - PAP^{-1} = P(tI)P^{-1} - PAP^{-1} = P(tI - A)P^{-1},$$

■

$$\det(tI - A') = \det(P(tI - A)P^{-1}) = \det P \cdot \det(tI - A) \cdot \det P^{-1} = \det(tI - A).$$

Quindi i polinomi caratteristici calcolati con  $A$  e  $A'$  sono uguali, come asserito. ■

(4.18) PROPOSIZIONE *Il polinomio caratteristico  $p(t)$  ha la forma:*

$$p(t) = t^n - (\text{tr } A)t^{n-1} + (\text{termini intermedi}) + (-1)^n(\det A),$$

dove  $\text{tr } A$ , la traccia di  $A$ , è la somma degli elementi diagonali:

$$\text{tr } A = a_{11} + a_{22} + \cdots + a_{nn}.$$

Tutti i coefficienti sono indipendenti dalla base. Per esempio,  $\text{tr } PAP^{-1} = \text{tr } A$ .

Ciò si dimostra facendo il calcolo. L'indipendenza dalla base segue da (4.17). ■

Dato che il polinomio caratteristico, la traccia e il determinante sono indipendenti dalla base, dipendono soltanto dall'operatore  $T$  e quindi possiamo definire il **polinomio caratteristico**, la **traccia** e il **determinante** di un operatore lineare  $T$  come quelli ottenuti utilizzando la matrice di  $T$  rispetto a una base qualunque.

(4.19) PROPOSIZIONE *Sia  $T$  un operatore lineare su uno spazio vettoriale di dimensione finita  $V$ .*

(a) *Se  $V$  ha dimensione  $n$ , allora  $T$  ha al più  $n$  autovalori.*

(b) *Se  $F$  è il campo dei numeri complessi e  $V \neq 0$ , allora  $T$  ha almeno un autovalore, e quindi ha un autovettore.*

*Dimostrazione.*

(a) Un polinomio di grado  $n$  può avere al più  $n$  radici distinte. Ciò è vero per un campo qualsiasi  $F$ , anche se non è stato ancora dimostrato [cfr. cap. 11, (1.8)]. Pertanto possiamo applicare il corollario (4.13).

(b) Ogni polinomio di grado positivo a coefficienti complessi ha almeno una radice complessa. Tale risultato è chiamato il teorema fondamentale dell'algebra, e una dimostrazione si trova nel capitolo 13 (9.1). ■

Per esempio, sia  $A$  la rotazione (3.1) del piano reale  $\mathbb{R}^2$  di un angolo  $\theta$ . Il suo polinomio caratteristico è:

$$(4.20) \quad p(t) = t^2 - (2 \cos \theta)t + 1,$$

il quale non ha radici reali, a meno che  $\cos \theta = \pm 1$ . Ma se consideriamo  $A$  come un operatore su  $\mathbb{C}^2$ , esistono due autovalori complessi.

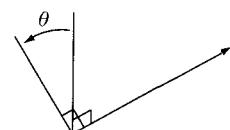
## 5 Matrici ortogonali e rotazioni

In questo paragrafo descriveremo come operatori lineari le rotazioni intorno all'origine degli spazi di dimensione due e tre,  $\mathbb{R}^2$  e  $\mathbb{R}^3$ . Abbiamo già osservato [cfr. (3.1)] che una rotazione di  $\mathbb{R}^2$  di un angolo  $\theta$  è rappresentata come la moltiplicazione per la matrice:

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Una rotazione di  $\mathbb{R}^3$  intorno all'origine può essere descritta mediante una coppia  $(v, \theta)$  costituita da un *vettore unitario*, ossia un vettore di lunghezza 1, che giace sull'asse di rotazione e un angolo  $\theta$  diverso da zero, l'angolo di rotazione. Le due coppie  $(v, \theta)$  e  $(-v, -\theta)$  rappresentano la stessa rotazione. Consideriamo anche l'identità come una rotazione, sebbene il suo asse sia indeterminato.

(5.1)



La matrice che rappresenta una rotazione di un angolo  $\theta$  intorno al vettore  $e_i$  si ottiene facilmente dalla matrice di rotazione  $2 \times 2$ :

$$(5.2) \quad A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{bmatrix}.$$

La moltiplicazione per  $A$  lascia fissa la prima coordinata  $x_1$  di un vettore e opera mediante una rotazione su  $(x_2, x_3)^t$ . Tutte le rotazioni di  $\mathbb{R}^3$  sono operatori lineari, ma le loro matrici possono essere abbastanza complicate. Lo scopo di questo paragrafo è proprio quello di descrivere tali matrici di rotazione.

Una matrice reale  $n \times n$   $A$  si dice *ortogonale* se  $A^t = A^{-1}$ , o, equivalentemente, se  $A^t A = I$ . Le matrici ortogonali  $n \times n$  formano un sottogruppo di  $GL_n(\mathbb{R})$  denotato con  $O_n$  e chiamato il *gruppo ortogonale*:

$$(5.3) \quad O_n = \{A \in GL_n(\mathbb{R}) \mid A^t A = I\}.$$

Il determinante di una matrice ortogonale è  $\pm 1$ , perché se  $A^t A = I$ , allora:

$$(\det A)^2 = (\det A^t)(\det A) = 1.$$

Le matrici ortogonali aventi determinante  $+1$  formano un sottogruppo chiamato il *gruppo ortogonale speciale* e denotato con  $SO_n$ :

$$(5.4) \quad SO_n = \{A \in GL_n(\mathbb{R}) \mid A^t A = I, \det A = 1\}.$$

Questo sottogruppo ha una sola classe laterale oltre a  $SO_n$ , cioè l'insieme degli elementi con determinante  $-1$ ; quindi  $SO_n$  ha indice 2 in  $O_n$ .

Enunciamo ora il risultato principale che dimostreremo a proposito delle rotazioni:

(5.5) TEOREMA *Le rotazioni di  $\mathbb{R}^2$  (o  $\mathbb{R}^3$ ) intorno all'origine sono gli operatori lineari le cui matrici rispetto alla base canonica sono ortogonali e hanno determinante 1. In altre parole, una matrice  $A$  rappresenta una rotazione di  $\mathbb{R}^2$  (o  $\mathbb{R}^3$ ) se e soltanto se  $A \in SO_2$  (o  $SO_3$ ).*

Si noti il seguente corollario:

(5.6) COROLLARIO *La composizione di due rotazioni di  $\mathbb{R}^3$  intorno all'origine è ancora una rotazione.*

Tale corollario segue dal teorema perché la matrice che rappresenta la composizione di due operatori lineari è la matrice prodotto, e perché  $SO_3$  è chiuso rispetto alla moltiplicazione tra matrici, essendo un sottogruppo di  $GL_3(\mathbb{R})$ . Si tratta di un risultato tutt'altro che ovvio, da un punto di vista geometrico. Chiaramente, la composizione di due rotazioni intorno a uno stesso asse è ancora una rotazione intorno a quell'asse. Ma provate a immaginare la composizione di rotazioni intorno ad assi distinti. Qual è l'asse di rotazione dell'operatore composto?

I gruppi  $SO_2$  e  $SO_3$  sono chiamati i *gruppi di rotazione* di dimensione due e tre, poiché i loro elementi rappresentano rotazioni. La situazione diventa più complicata in dimensione  $> 3$ . Per esempio, la matrice:

$$(5.7) \quad \begin{bmatrix} \cos \theta & -\sin \theta & & \\ \sin \theta & \cos \theta & & \\ & & \cos \eta & -\sin \eta \\ & & \sin \eta & \cos \eta \end{bmatrix}$$

è un elemento di  $SO_4$ . La moltiplicazione a sinistra per tale matrice è la composizione di una rotazione di un angolo  $\theta$  sulle prime due coordinate e di una rotazione di un angolo  $\eta$  sulle ultime due coordinate. Questa operazione non può essere realizzata come una singola rotazione.

La dimostrazione del teorema (5.5) non è molto difficile, ma risulterebbe alquanto pesante senza introdurre prima un po' di terminologia. Quindi la dimostrazione sarà spostata alla fine del paragrafo (p. 154).

Per comprendere la relazione tra le matrici ortogonali e le rotazioni avremo bisogno del prodotto scalare di vettori. Per definizione, il *prodotto scalare* di due vettori colonna  $X$  e  $Y$  è:

$$(5.8) \quad (X \cdot Y) = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Talvolta è utile scrivere il prodotto scalare in forma matriciale, nel modo seguente:

$$(5.9) \quad (X \cdot Y) = X^t Y.$$

Ci sono due proprietà fondamentali del prodotto scalare di vettori in  $\mathbb{R}^2$  e in  $\mathbb{R}^3$ . La prima è che il prodotto scalare di un vettore per se stesso è il quadrato della lunghezza del vettore. Si ha cioè:

$$|X|^2 = x_1^2 + x_2^2 \quad \text{oppure} \quad x_1^2 + x_2^2 + x_3^2,$$

rispettivamente. Tale proprietà, che segue dal teorema di Pitagora, è alla base della definizione di lunghezza di un vettore in  $\mathbb{R}^n$ . Infatti, la *lunghezza* di  $X$ , indicata con  $|X|$ , è definita dalla formula:

$$(5.10) \quad |X|^2 = (X \cdot X) = x_1^2 + \cdots + x_n^2.$$

La *distanza* tra due vettori  $X, Y$  è definita come la lunghezza  $|X - Y|$  di  $X - Y$ .

La seconda proprietà notevole del prodotto scalare in  $\mathbb{R}^2$  e  $\mathbb{R}^3$  è data dalla formula:

$$(5.11) \quad (X \cdot Y) = |X| |Y| \cos \theta,$$

dove  $\theta$  è l'angolo tra i vettori. Tale formula è una conseguenza del teorema del coseno (o di Carnot):

$$c^2 = a^2 + b^2 - 2ab \cos \theta,$$

relativo a un triangolo con i lati di lunghezza  $a, b, c$ , dove  $\theta$  è l'angolo formato dai lati  $a, b$ . Per ottenere la (5.11), applichiamo il teorema dei coseni al triangolo di vertici  $0, X, Y$ . Le lunghezze dei suoi lati sono  $|X|, |Y|$  e  $|X - Y|$ , sicché il teorema del coseno può essere scritto nella forma:

$$((X - Y) \cdot (X - Y)) = (X \cdot X) + (Y \cdot Y) - 2 |X| |Y| \cos \theta.$$

Il primo membro si sviluppa nel modo seguente:

$$((X - Y) \cdot (X - Y)) = (X \cdot X) - 2(X \cdot Y) + (Y \cdot Y),$$

e la formula (5.11) si ottiene confrontando le espressioni ottenute.

Una conseguenza più importante della (5.11) è che due vettori  $X$  e  $Y$  sono ortogonali, ossia l'angolo  $\theta$  è  $\pi/2$ , se e soltanto se  $(X \cdot Y) = 0$ . Tale proprietà viene assunta come definizione di ortogonalità tra vettori in  $\mathbb{R}^n$ :

$$(5.12) \quad X \text{ è ortogonale a } Y \text{ se } (X \cdot Y) = 0.$$

**(5.13) PROPOSIZIONE** *Le seguenti condizioni su una matrice reale  $n \times n$   $A$  sono equivalenti:*

- (a)  *$A$  è ortogonale.*
- (b) *La moltiplicazione per  $A$  conserva il prodotto scalare, ossia  $(AX \cdot AY) = (X \cdot Y)$  per ogni scelta dei vettori colonna  $X, Y$ .*
- (c) *Le colonne di  $A$  sono vettori unitari a due a due ortogonali tra loro.*

Una base costituita da vettori unitari a due a due ortogonali è chiamata una *base ortonormale*. Una matrice ortogonale è una matrice le cui colonne formano una base ortonormale.

La moltiplicazione a sinistra per una matrice ortogonale è chiamata anche un *operatore ortogonale*. Dunque gli operatori ortogonali su  $\mathbb{R}^n$  sono quelli che conservano il prodotto scalare.

*Dimostrazione della proposizione (5.13).* Scriviamo  $(X \cdot Y) = X^t Y$ . Se  $A$  è ortogonale, allora  $A^t A = I$ , quindi:

$$(X \cdot Y) = X^t Y = X^t A^t AY = (AX)^t (AY) = (AX \cdot AY).$$

Viceversa, supponiamo che  $X^t Y = X^t A^t AY$  per ogni  $X$  e  $Y$ . Riscriviamo questa uguaglianza nella forma  $X^t BY = 0$ , dove  $B = I - A^t A$ . Ora, per qualsiasi matrice  $B$  si ha:

$$(5.14) \quad e_i^t B e_j = b_{ij}.$$

Pertanto, se  $X^t BY = 0$  per ogni  $X$  e  $Y$ , allora  $e_i^t B e_j = b_{ij} = 0$  per ogni  $i, j$ , e  $B = 0$ . Ne segue che  $I = A^t A$ . Ciò dimostra l'equivalenza tra (a) e (b). Per provare che (a) e (c) sono equivalenti, indichiamo con  $A_j$  la  $j$ -esima colonna della matrice  $A$ . L'elemento  $(i, j)$  della matrice prodotto  $A^t A$  è  $(A_i \cdot A_j)$ ; quindi  $A^t A = I$  se e solo se  $(A_i \cdot A_i) = 1$  per ogni  $i$ , e  $(A_i \cdot A_j) = 0$  per ogni  $i \neq j$ , ossia le colonne hanno lunghezza 1 e sono ortogonali. ■

Il significato geometrico della moltiplicazione per una matrice ortogonale può essere illustrato mediante i movimenti rigidi. Un *movimento rigido* o *isometria* di  $\mathbb{R}^n$  è un'applicazione  $m : \mathbb{R}^n \rightarrow \mathbb{R}^n$  che conserva le distanze, ossia è

un'applicazione che soddisfa la seguente condizione: se  $X, Y$  sono punti di  $\mathbb{R}^n$  la distanza da  $X$  a  $Y$  è uguale alla distanza da  $m(X)$  a  $m(Y)$ :

$$(5.15) \quad |m(X) - m(Y)| = |X - Y|.$$

Un movimento rigido porta un triangolo in un triangolo congruente, e pertanto conserva gli angoli e le forme geometriche in generale.

Si noti che la composizione di due movimenti rigidi è un movimento rigido, e che l'inverso di un movimento rigido è un movimento rigido. Pertanto i movimenti rigidi di  $\mathbb{R}^n$  formano un gruppo  $M_n$ , avente come legge di composizione la composizione di applicazioni. Tale gruppo è chiamato il *gruppo dei movimenti*.

(5.16) PROPOSIZIONE *Sia  $m$  un'applicazione  $\mathbb{R}^n \rightarrow \mathbb{R}^n$ . Le seguenti condizioni su  $m$  sono equivalenti:*

- (a)  *$m$  è un movimento rigido che lascia fissa l'origine.*
- (b)  *$m$  conserva il prodotto scalare, ossia, per ogni  $X, Y \in \mathbb{R}^n$ ,  $(m(X) \cdot m(Y)) = (X \cdot Y)$ .*
- (c)  *$m$  è la moltiplicazione a sinistra per una matrice ortogonale.*

(5.17) COROLLARIO *Un movimento rigido che lascia fissa l'origine è un operatore lineare.*

Ciò segue dall'equivalenza tra (a) e (c).

*Dimostrazione della proposizione (5.16).* Useremo il simbolo ' per denotare l'applicazione  $m$ , scrivendo  $m(X) = X'$ . Supponiamo che  $m$  sia un movimento rigido che lascia fissa l'origine 0. Con la notazione ora introdotta, la proprietà (5.15) che  $m$  conserva le distanze si scrive:

$$(5.18) \quad ((X' - Y') \cdot (X' - Y')) = ((X - Y) \cdot (X - Y))$$

per ogni coppia di vettori  $X, Y$ . Ponendo  $Y = 0$ , si ha:  $(X' \cdot X') = (X \cdot X)$  per ogni  $X$ . Sviluppando entrambi i membri della (5.18) e cancellando  $(X \cdot X)$  e  $(Y \cdot Y)$ , si ottiene:  $(X' \cdot Y') = (X \cdot Y)$ . Ciò prova che  $m$  conserva il prodotto scalare, e quindi che (a) implica (b).

Per dimostrare che (b) implica (c), osserviamo che l'unica applicazione che conserva il prodotto scalare e che lascia fisso inoltre ciascun vettore  $e_i$  della base canonica è l'identità. Infatti, se  $m$  conserva il prodotto scalare, allora  $(X \cdot e_j) = (X' \cdot e'_j)$  per ogni  $X$ . Se per di più,  $e'_j = e_j$ , allora:

$$x_j = (X \cdot e_j) = (X' \cdot e'_j) = (X' \cdot e_j) = x'_j$$

per ogni  $j$ . Pertanto  $X = X'$  e  $m$  è l'identità.

Supponiamo ora che  $m$  conservi il prodotto scalare. Allora le immagini  $e'_1, \dots, e'_n$  dei vettori della base canonica sono ortonormali:  $(e'_i \cdot e'_j) = 1$  e  $(e'_i \cdot e'_j) = 0$ , se  $i \neq j$ . Poniamo  $B' = (e'_1, \dots, e'_n)$  e  $A = [B']$ . In base alla proposizione (5.13),  $A$  è una matrice ortogonale. Poiché le matrici ortogonali formano un gruppo, anche  $A^{-1}$  è ortogonale, sicché anche la moltiplicazione per  $A^{-1}$  conserva il prodotto scalare. Dunque il movimento composto  $A^{-1}m$  conserva il prodotto scalare e lascia fisso ciascun vettore  $e_i$  della base e quindi  $A^{-1}m$  è l'applicazione identica. Ciò prova che  $m$  è la moltiplicazione a sinistra per  $A$ , come richiesto.

Infine, se  $m$  è un operatore lineare la cui matrice  $A$  è ortogonale, allora  $X' - Y' = (X - Y)'$  poiché  $m$  è lineare, e  $|X' - Y'| = |(X - Y)'| = |X - Y|$  in virtù di (5.13b). Dunque  $m$  è un movimento rigido. Inoltre, poiché qualunque operatore lineare lascia fissa l'origine, abbiamo dimostrato che (c) implica (a). ■

Una classe di movimenti rigidi che non fissano l'origine e che pertanto non sono operatori lineari, è costituita dalle traslazioni. Fissato arbitrariamente un vettore  $b = (b_1, \dots, b_n)^t$  in  $\mathbb{R}^n$ , la *traslazione* mediante  $b$  è l'applicazione:

$$(5.19) \quad t_b(X) = X + b = \begin{bmatrix} x_1 + b_1 \\ \vdots \\ x_n + b_n \end{bmatrix}.$$

Tale applicazione è un movimento rigido, poiché  $t_b(X) - t_b(Y) = (X + b) - (Y + b) = X - Y$ , e quindi  $|t_b(X) - t_b(Y)| = |X - Y|$ .

(5.20) PROPOSIZIONE *Ogni movimento rigido  $m$  è la composizione di un operatore lineare ortogonale e di una traslazione. In altre parole, esso ha la forma  $m(X) = AX + b$ , essendo  $A$  una matrice ortogonale e  $b$  un vettore.*

*Dimostrazione.* Poniamo  $b = m(0)$ . Allora, dato che  $t_{-b}(b) = 0$ , l'applicazione composta  $t_{-b}m$  è un movimento rigido che lascia fissa l'origine:  $t_{-b}(m(0)) = 0$ . In base alla proposizione (5.16), l'applicazione  $t_{-b}m$  è la moltiplicazione a sinistra per una matrice ortogonale  $A$ , ossia:  $t_{-b}m(X) = AX$ . Applicando  $t_b$  a entrambi i membri di questa equazione, si ottiene:  $m(X) = AX + b$ .

Si noti che sia il vettore  $b$  che la matrice  $A$  sono univocamente determinati da  $m$ , poiché  $b = m(0)$  e  $A$  è l'operatore  $t_{-b}m$ . ■

Ricordiamo che il determinante di una matrice ortogonale è  $\pm 1$ . Si dice che un operatore ortogonale *conserva l'orientazione* se il suo determinante è  $+1$ , e *inverte l'orientazione* se il suo determinante è  $-1$ . Analogamente, sia  $m$  un movimento rigido e scriviamo:  $m(X) = AX + b$ , come sopra. Si dice allora che  $m$  *conserva l'orientazione* se  $\det A = 1$  e *inverte l'orientazione* se  $\det A = -1$ . Un movimento di  $\mathbb{R}^2$  inverte l'orientazione se "ribalta" il piano su se stesso, altrimenti conserva l'orientazione.

Utilizzando il teorema (5.5) e la proposizione (5.16), si ottiene la seguente caratterizzazione delle rotazioni:

(5.21) COROLLARIO *Le rotazioni di  $\mathbb{R}^2$  e  $\mathbb{R}^3$  sono i movimenti rigidi che conservano l'orientazione e lasciano fissa l'origine.* ■

Passiamo ora alla dimostrazione del teorema (5.5), che caratterizza le rotazioni di  $\mathbb{R}^2$  e  $\mathbb{R}^3$  intorno all'origine. Ogni rotazione  $\rho$  è un movimento rigido, sicché, in base alla proposizione (5.16),  $\rho$  è la moltiplicazione per una matrice ortogonale  $A$ . Inoltre il determinante di  $A$  è 1, poiché  $\det A = \pm 1$  per una matrice ortogonale arbitraria e poiché il determinante varia con continuità al variare dell'angolo di rotazione. Quando l'angolo è zero,  $A$  è la matrice identica, che ha determinante 1. Dunque la matrice di una rotazione è un elemento di  $SO_2$  o  $SO_3$ .

Viceversa, sia  $A \in SO_2$  una matrice  $2 \times 2$  ortogonale con determinante 1. Denotiamo con  $v_1$  la prima colonna  $Ae_1$  di  $A$ . Poiché  $A$  è ortogonale,  $v_1$  è un vettore unitario. Inoltre esiste una rotazione  $R$  (3.1) tale che  $Re_1 = v_1$ . Allora  $B = R^{-1}A$  lascia fisso  $e_1$ . D'altra parte,  $A$  e  $R$  sono elementi di  $SO_2$ , e ciò implica che  $B$  appartiene a  $SO_2$ . Pertanto le colonne di  $B$  formano una base ortonormale di  $\mathbb{R}^2$ , e la prima colonna è  $e_1$ . La seconda colonna, essendo di lunghezza 1 e ortogonale a  $e_1$ , deve essere uguale a  $e_2$  o a  $-e_2$ , e il secondo caso è da scartare poiché  $\det B = 1$ . Ne segue che  $B = I$  e che  $A = R$ . Dunque  $A$  è una rotazione.

Per dimostrare che un elemento  $A$  di  $SO_3$  rappresenta una rotazione, conviene innanzitutto definire le rotazioni  $\rho$  di  $\mathbb{R}^3$  intorno all'origine. Richiederemo le seguenti proprietà:

- (5.22) (i)  $\rho$  è un movimento rigido che lascia fissa l'origine;  
(ii)  $\rho$  lascia fisso inoltre un vettore non nullo  $v$ ;  
(iii)  $\rho$  agisce come una rotazione sul piano  $P$  passante per l'origine e ortogonale a  $v$ .

In base alla proposizione (5.16), la prima proprietà equivale a dire che  $\rho$  è un operatore ortogonale. Pertanto la matrice  $A \in SO_3$  soddisfa tale condizione. La proprietà (ii) può essere enunciata dicendo che  $v$  è un autovettore per l'operatore  $\rho$ , con autovalore 1. Allora, poiché  $\rho$  conserva l'ortogonalità, esso manda il sottospazio ortogonale  $P$  in se stesso. In altre parole,  $P$  è un sottospazio invariante. La proprietà (iii) dice che la restrizione di  $\rho$  a tale sottospazio invariante è una rotazione.

Si noti che la matrice (5.2) soddisfa tali proprietà, con  $v = e_1$ .

(5.23) LEMMA *Ogni elemento  $A \in SO_3$  ha l'autovalore 1.*

**Dimostrazione.** In virtù di (4.8), occorre dimostrare che  $\det(A - I) = 0$ . Questa dimostrazione è artificiosa, ma efficiente. Ricordiamo che, per una qualsiasi matrice  $A$ , si ha:  $\det A = \det A^t$ , sicché  $\det A^t = 1$ . Poiché  $A$  è ortogonale,  $A^t(A - I) = (I - A)^t$ . Allora:

$$\det(A - I) = \det A^t(A - I) = \det(I - A)^t = \det(I - A).$$

D'altra parte, se  $B$  è una matrice  $3 \times 3$  arbitraria, si ha:  $\det(-B) = -\det B$ . Pertanto  $\det(A - I) = -\det(I - A)$  e quindi  $\det(A - I) = 0$ . ■

Ora, data una matrice  $A \in SO_3$ , il lemma prova che la moltiplicazione a sinistra per  $A$  lascia fisso un vettore non nullo  $v_1$ . Normalizziamo  $v_1$ , così che la sua lunghezza sia 1, e scegliamo due vettori unitari ortogonali  $v_2, v_3$  appartenenti al piano  $P$  passante per l'origine e ortogonale a  $v_1$ . Allora  $\mathbf{B} = (v_1, v_2, v_3)$  è una base ortonormale di  $\mathbb{R}^3$ . La matrice  $P = [\mathbf{B}]^{-1}$  è ortogonale perché  $[\mathbf{B}]$  è ortogonale, e  $A' = PAP^{-1}$  rappresenta, rispetto alla base  $\mathbf{B}$ , lo stesso operatore rappresentato da  $A$ . Poiché  $A$  e  $P$  sono ortogonali, tale risulta  $A'$ . Inoltre  $\det A' = \det A = 1$ . Dunque  $A' \in SO_3$ .

Poiché  $v_1$  è un autovettore con autovalore 1, la prima colonna di  $A'$  è  $e_1$ . Poiché  $A'$  è ortogonale, le altre colonne sono ortogonali a  $e_1$ , e  $A'$  ha la forma a blocchi:

$$\left[ \begin{array}{c|c} 1 & 0 \\ \hline 0 & R \end{array} \right].$$

Utilizzando il fatto che  $A' \in SO_3$ , si ottiene che  $R \in SO_2$ . Dunque  $R$  è una rotazione. Ciò prova che  $A'$  ha la forma (5.2) e che essa rappresenta una rotazione. Ne segue che anche  $A$  rappresenta una rotazione, e ciò completa la dimostrazione del teorema (5.5). ■

(5.24) **Osservazione.** Per mantenere la nuova base separata dalla vecchia base, l'abbiamo denotata nel cap. 3 con  $\mathbf{B}'$ . L'apice non è necessario quando la vecchia base è la base canonica, e poiché esso appesantisce le notazioni, spesso lo eliminiamo, come abbiamo fatto sopra.

## 6 Diagonalizzazione

In questo paragrafo proveremo che per "la maggior parte" degli operatori lineari su uno spazio vettoriale complesso, esiste una base tale che la matrice dell'operatore è diagonale. L'argomento chiave, già illustrato alla fine del paragrafo 4, è che ogni polinomio complesso di grado positivo possiede una radice, da cui segue che ogni operatore lineare ha un autovettore.

## (6.1) PROPOSIZIONE

- (a) (Spazi vettoriali) Sia  $T$  un operatore lineare su uno spazio vettoriale complesso  $V$  di dimensione finita. Allora esiste una base  $\mathbf{B}$  di  $V$  tale che la matrice  $A$  di  $T$  sia triangolare superiore.
- (b) (Matrici) Ogni matrice  $n \times n$  complessa  $A$  è simile a una matrice triangolare superiore. In altre parole, esiste una matrice  $P \in GL_n(\mathbb{C})$  tale che  $PAP^{-1}$  è triangolare superiore.

*Dimostrazione.* I due enunciati sono equivalenti, in virtù di (3.5). Cominciamo con l'applicare (4.19b), che prova l'esistenza di un autovettore, diciamo  $v'_1$ . Estendiamo tale vettore ad una base  $\mathbf{B}' = (v'_1, \dots, v'_n)$  di  $V$ . Allora, in base a (3.11), la prima colonna della matrice  $A'$  di  $T$  rispetto a  $\mathbf{B}'$  sarà:  $(c_1, 0, \dots, 0)^t$ , dove  $c_1$  è l'autovalore di  $v'_1$ . Pertanto  $A'$  ha la forma:

$$A' = \begin{array}{|c|c|} \hline c_1 & * \cdots * \\ \hline 0 & \vdots \\ \vdots & B \\ 0 & \vdots \\ \hline \end{array},$$

dove  $B$  è una matrice  $(n-1) \times (n-1)$ . La versione matriciale di tale riduzione è la seguente: data una matrice  $n \times n$  arbitraria  $A$ , esiste una matrice  $P \in GL_n(\mathbb{C})$  tale che  $A' = PAP^{-1}$  ha la forma sopra descritta. Procediamo ora per induzione su  $n$ . Per l'ipotesi induttiva, possiamo supporre che esista una matrice  $Q \in GL_{n-1}(\mathbb{C})$  tale che  $QBQ^{-1}$  sia triangolare. Sia  $Q_1$  la matrice  $n \times n$ :

$$\begin{array}{|c|c|} \hline 1 & 0 \cdots 0 \\ \hline 0 & \vdots \\ \vdots & Q \\ 0 & \vdots \\ \hline \end{array}.$$

Allora la matrice:

$$(Q_1 P) A (Q_1 P)^{-1} = Q_1 (PAP^{-1}) Q_1^{-1} = Q_1 A' Q_1^{-1}$$

ha la forma:

$$\begin{array}{|c|c|} \hline c_1 & * \cdots * \\ \hline 0 & \vdots \\ \vdots & QBQ^{-1} \\ 0 & \vdots \\ \hline \end{array},$$

dunque è triangolare superiore. ■

Come già abbiamo accennato, il punto centrale nella dimostrazione è il fatto che ogni polinomio complesso possiede una radice. La stessa dimostrazione continua a valere per un campo  $F$  arbitrario, purché tutte le radici del polinomio caratteristico siano nel campo.

(6.2) COROLLARIO Sia  $F$  un campo.

- (a) (Spazi vettoriali) Sia  $T$  un operatore lineare su uno spazio vettoriale di dimensione finita  $V$  su  $F$ , e supponiamo che il polinomio caratteristico di  $T$  si scriva come il prodotto di fattori lineari in  $F$ . Allora esiste una base  $\mathbf{B}$  di  $V$  tale che la matrice  $A$  di  $T$  è triangolare.
- (b) (Matrici) Sia  $A$  una matrice  $n \times n$  il cui polinomio caratteristico si scriva come il prodotto di fattori lineari in  $F$ . Allora esiste una matrice  $P \in GL_n(F)$  tale che  $PAP^{-1}$  è triangolare.

*Dimostrazione.* La dimostrazione è la stessa, tranne che, per effettuare l'induzione, occorre verificare che il polinomio caratteristico della matrice  $B$  è  $p(t)/(t - c_1)$ , dove  $p(t)$  è il polinomio caratteristico di  $A$ . Ciò è vero perché  $p(t)$  è anche il polinomio caratteristico di  $A'$  (4.17), e perché  $\det(tI - A') = -(t - c_1) \det(tI - B)$ . Pertanto l'ipotesi che il polinomio caratteristico si spezza in un prodotto di fattori lineari si trasmette da  $A$  a  $B$ . ■

Chiediamoci ora quali sono le matrici  $A$  simili a matrici diagonali. Come si è visto in (3.12), esse sono le matrici  $A$  che hanno una base di autovettori. Supponiamo di nuovo che  $F = \mathbb{C}$  e consideriamo le radici del polinomio caratteristico  $p(t)$ . Ciascuna radice è l'autovalore associato a qualche autovettore, e ogni autovettore ha un unico autovalore. La maggior parte dei polinomi complessi di grado  $n$  ha  $n$  radici distinte. Pertanto la maggior parte delle matrici complesse ha  $n$  autovettori con autovalori distinti, ed è ragionevole supporre che tali autovettori formino una base. Infatti:

(6.3) PROPOSIZIONE Siano  $v_1, \dots, v_r \in V$  autovettori per un operatore lineare  $T$ , con autovalori distinti  $c_1, \dots, c_r$ . Allora l'insieme  $(v_1, \dots, v_r)$  è linearmente indipendente.

*Dimostrazione.* Procediamo per induzione su  $r$ . Supponiamo che sia data una relazione lineare della forma:

$$0 = a_1 v_1 + \dots + a_r v_r.$$

Dobbiamo dimostrare che  $a_i = 0$  per ogni  $i$ , e per fare ciò applichiamo l'operatore  $T$ :

$$0 = T(0) = a_1 T(v_1) + \cdots + a_r T(v_r) = a_1 c_1 v_1 + \cdots + a_r c_r v_r.$$

Questa è una seconda relazione lineare tra  $v_1, \dots, v_r$ . Eliminiamo  $v_r$  dalle due relazioni, moltiplicando la prima relazione per  $c_r$  e sottraendo la seconda:

$$0 = a_1(c_r - c_1)v_1 + \cdots + a_{r-1}(c_r - c_{r-1})v_{r-1}.$$

Applicando il principio di induzione, possiamo supporre che  $v_1, \dots, v_{r-1}$  sono indipendenti. Allora i coefficienti  $a_1(c_r - c_1), \dots, a_{r-1}(c_r - c_{r-1})$  sono tutti nulli. Poiché i  $c_i$  sono distinti, si ha  $c_r - c_i \neq 0$ , se  $i < r$ . Pertanto  $a_1 = \dots = a_{r-1} = 0$ , e la relazione di partenza si riduce a  $0 = a_r v_r$ . Poiché un autovettore è diverso dal vettore nullo, anche  $a_r = 0$ . ■

Il teorema seguente si ottiene combinando (3.12) e (6.3):

**(6.4) TEOREMA** *Sia  $T$  un operatore lineare su uno spazio vettoriale  $V$  di dimensione  $n$  su un campo  $F$ . Supponiamo che il suo polinomio caratteristico abbia  $n$  radici distinte in  $F$ . Allora esiste una base di  $V$  rispetto alla quale la matrice di  $T$  è diagonale. ■*

Si noti che gli elementi diagonali sono determinati, a parte l'ordine, dall'operatore lineare  $T$ : sono gli autovalori.

Quando  $p(t)$  possiede radici multiple, non esiste di solito una base di autovettori, ed è più difficile trovare una matrice semplice per  $T$ . Lo studio di questo caso porta alla cosiddetta *forma canonica di Jordan* di una matrice, che sarà discussa nel cap. 12.

Come esempio di diagonalizzazione, consideriamo la matrice:

$$A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$$

i cui autovettori sono stati calcolati in (4.10). Tali autovettori formano una base  $\mathbf{B} = (v_1, v_2)$  di  $\mathbb{R}^2$ . In base alle (4.20) (cap. 3) e (5.24) (cap. 4), la matrice che collega la base canonica  $\mathbf{E}$  a tale base  $\mathbf{B}$  è

$$(6.5) \quad P = [\mathbf{B}]^{-1} = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}^{-1} = -\frac{1}{3} \begin{bmatrix} -1 & -2 \\ -1 & 1 \end{bmatrix},$$

e  $PAP^{-1} = A'$  è diagonale:

$$(6.6) \quad -\frac{1}{3} \begin{bmatrix} -1 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 0 & 2 \end{bmatrix} = A'.$$

La generale è stabilità nel corollario seguente:

**(6.7) COROLLARIO** *Se  $\mathbf{B}$  è una base di autovettori di  $A$  in  $F^n$  e se  $P = [\mathbf{B}]^{-1}$ , allora  $A' = PAP^{-1}$  è diagonale. ■*

L'importanza del teorema 6.4 è dovuta al fatto che è facile operare con matrici diagonali. Per esempio, se  $A' = PAP^{-1}$  è diagonale, allora possiamo calcolare le potenze della matrice  $A$  utilizzando la formula:

$$(6.8) \quad A^k = (P^{-1}A'P)^k = P^{-1}(A')^k P.$$

In particolare, se  $A$  è la matrice (4.9), allora:

$$A^k = -\frac{1}{3} \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 2 \end{bmatrix}^k \begin{bmatrix} -1 & -2 \\ -1 & 1 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 5^k + 2 \cdot 2^k & 2(5^k - 2^k) \\ 5^k - 2^k & 2 \cdot 5^k + 2^k \end{bmatrix}.$$

## 7 Sistemi di equazioni differenziali

Sappiamo dall'analisi matematica che le soluzioni dell'equazione differenziale lineare del primo ordine:

$$(7.1) \quad \frac{dx}{dt} = ax$$

sono date da  $x(t) = ce^{at}$ , essendo  $c$  una costante arbitraria. Infatti,  $ce^{at}$  è ovviamente una soluzione di (7.1). Per dimostrare che ogni soluzione è di questa forma, consideriamo una qualsiasi funzione derivabile  $x(t)$  che sia soluzione della (7.1). Calcolando la derivata di  $e^{-at}x(t)$  mediante la regola del prodotto, si ha:

$$\frac{d}{dt}(e^{-at}x(t)) = -ae^{-at}x(t) + e^{-at}ax(t) = 0.$$

Dunque  $e^{-at}x(t)$  è una costante  $c$ , e  $x(t) = ce^{at}$ .

Come applicazione della diagonalizzazione, estenderemo tale soluzione ai sistemi di equazioni differenziali. Per scrivere le equazioni con notazione matriciale, useremo la seguente terminologia. Una *funzione a valori vettoriali*  $X(t)$  è un vettore le cui componenti sono funzioni di  $t$ . Analogamente, una *funzione a valori matriciali*  $A(t)$  è una matrice i cui elementi sono funzioni:

$$(7.2) \quad X(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix}, \quad A(t) = \begin{bmatrix} a_{11}(t) & \cdots & a_{1n}(t) \\ \vdots & \ddots & \vdots \\ a_{m1}(t) & \cdots & a_{mn}(t) \end{bmatrix}.$$

Le operazioni relative al calcolo dei limiti, delle derivate, e così via si estendono alle funzioni a valori vettoriali e a valori matriciali, effettuando le operazioni separatamente su ciascun elemento. Così, per definizione:

$$(7.3) \quad \lim_{t \rightarrow t_0} X(t) = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \quad \text{dove } \xi_i = \lim_{t \rightarrow t_0} x_i(t).$$

Pertanto tale limite esiste se e solo se  $\lim x_i(t)$  esiste per ogni  $i$ . Analogamente, la derivata di una funzione a valori vettoriali o matriciali è la funzione ottenuta derivando separatamente ciascun elemento:

$$\frac{dX}{dt} = \begin{bmatrix} x'_1(t) \\ \vdots \\ x'_n(t) \end{bmatrix}, \quad \frac{dA}{dt} = \begin{bmatrix} a'_{11}(t) & \cdots & a'_{1n}(t) \\ \vdots & & \vdots \\ a'_{m1}(t) & \cdots & a'_{mn}(t) \end{bmatrix},$$

dove  $x'_i(t)$  è la derivata di  $x_i(t)$ , e così via. Pertanto  $dX/dt$  è definita se e solo se ciascuna delle funzioni  $x_i(t)$  è derivabile. La derivata può essere descritta anche con notazione vettoriale, nella forma:

$$(7.4) \quad \frac{dX}{dt} = \lim_{h \rightarrow 0} \frac{X(t+h) - X(t)}{h},$$

dove  $X(t+h) - X(t)$  si calcola mediante l'addizione tra vettori e il simbolo  $h$  al denominatore sta a indicare la moltiplicazione per lo scalare  $h^{-1}$ . Il limite si ottiene calcolando separatamente il limite di ciascun elemento, come sopra. Quindi gli elementi di (7.4) sono le derivate  $x'_i(t)$ . Lo stesso vale per le funzioni a valori matriciali.

Un sistema di equazioni differenziali del primo ordine, lineari omogenee a coefficienti costanti è un'equazione matriciale della forma:

$$(7.5) \quad \frac{dX}{dt} = AX,$$

dove  $A$  è una matrice  $n \times n$  reale o complessa e  $X(t)$  è una funzione a valori vettoriali di dimensione  $n$ . Scrivendo esplicitamente un sistema di questo tipo, si ottiene un sistema di  $n$  equazioni differenziali, della forma:

$$(7.6) \quad \begin{aligned} \frac{dx_1}{dt} &= a_{11}x_1(t) + \cdots + a_{1n}x_n(t) \\ \vdots &\quad \vdots &\quad \vdots \\ \frac{dx_n}{dt} &= a_{n1}x_1(t) + \cdots + a_{nn}x_n(t) \end{aligned}$$

$x_i(t)$  sono funzioni incognite e gli  $a_{ij}$  sono scalari. Per esempio, se sostituiamo a la matrice  $\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ , l'equazione (7.5) diventa un sistema di due equazioni in due incognite:

$$(7.7) \quad \begin{aligned} \frac{dx_1}{dt} &= 3x_1 + 2x_2 \\ \frac{dx_2}{dt} &= x_1 + 4x_2. \end{aligned}$$

I più semplici sistemi (7.5) sono quelli in cui  $A$  è una matrice diagonale. Siano  $a_i$  gli elementi diagonali. Allora l'equazione (7.5) diventa:

$$(7.8) \quad \frac{dx_i}{dt} = a_i x_i(t), \quad i = 1, \dots, n.$$

In tal caso le funzioni incognite  $x_i$  non sono mischiate dalle equazioni, e quindi possiamo trovare la soluzione per ciascuna di esse separatamente:

$$(7.9) \quad x_i = c_i e^{a_i t},$$

essendo  $c_i$  una costante arbitraria.

L'osservazione che ci permette di risolvere l'equazione differenziale (7.5) nella maggior parte dei casi è la seguente: se  $v$  è un autovettore di  $A$  con autovalore  $a$ , allora

$$(7.10) \quad X = e^{at} v$$

è una soluzione particolare di (7.5). Qui la funzione  $e^{at}v$  va pensata come moltiplicazione della funzione scalare  $e^{at}$  per il vettore  $v$ . La derivazione agisce sulla funzione scalare, lasciando fisso il vettore costante  $v$ , mentre la moltiplicazione per  $A$  agisce sul vettore  $v$ , lasciando fissa la funzione scalare  $e^{at}$ . Dunque  $\frac{d}{dt} e^{at}v = ae^{at}v = Ae^{at}v$ . Per esempio,  $(2, -1)^t$  è un autovettore con autovalore 2 della matrice  $\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ , e  $\begin{bmatrix} 2e^{2t} \\ -e^{2t} \end{bmatrix}$  è una soluzione del sistema di equazioni differenziali (7.7).

Questa osservazione ci permette di risolvere il sistema (7.5) ogniqualvolta la matrice  $A$  possiede autovalori reali distinti. In tal caso, ogni soluzione risulta una combinazione lineare delle soluzioni particolari (7.10). Per verificare ciò, conviene diagonalizzare. Sostituendo qui la notazione  $\tilde{\cdot}$  usata nel paragrafo precedente con la notazione  $\tilde{\cdot}$ , per evitare confusione con la derivazione. Sia  $P$  una matrice invertibile tale che  $PAP^{-1} = \tilde{A}$  sia diagonale. Pertanto  $P = [\mathbf{B}]^{-1}$ , dove  $\mathbf{B}$  è una base di autovettori. Effettuiamo il cambiamento lineare di variabili:

$$(7.11) \quad X = P^{-1} \tilde{X}.$$

Allora:

$$(7.12) \quad \frac{dX}{dt} = P^{-1} \frac{d\tilde{X}}{dt}.$$

Sostituendo in (7.5), si ottiene:

$$(7.13) \quad \frac{d\tilde{X}}{dt} = PAP^{-1}\tilde{X} = \tilde{A}\tilde{X}.$$

Poiché  $\tilde{A}$  è diagonale, le variabili  $\tilde{x}_i$  sono state separate, e pertanto l'equazione può essere risolta in termini di esponenziali. Gli elementi diagonali di  $\tilde{A}$  sono gli autovalori  $\lambda_1, \dots, \lambda_n$  di  $A$ , sicché la soluzione del sistema (7.13) è:

$$(7.14) \quad \tilde{x}_i = c_i e^{\lambda_i t}, \quad \text{essendo } c_i \text{ costanti arbitrarie.}$$

Sostituendo in (7.11), si ha che

$$(7.15) \quad X = P^{-1}\tilde{X}$$

risolve il sistema di partenza (7.5). Ciò dimostra la seguente:

(7.16) PROPOSIZIONE *Sia  $A$  una matrice  $n \times n$ , e sia  $P$  una matrice invertibile tale che  $PAP^{-1} = \tilde{A}$  sia diagonale, con elementi diagonali  $\lambda_1, \dots, \lambda_n$ . La soluzione generale del sistema  $\frac{dX}{dt} = AX$  è  $X = P^{-1}\tilde{X}$ , dove  $\tilde{x}_i = c_i e^{\lambda_i t}$ , essendo  $c_i$  costanti arbitrarie. ■*

Una matrice che diagonalizza  $A$  nell'esempio (7.7) è stata calcolata in (6.5):

$$(7.17) \quad P^{-1} = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}, \quad \text{e} \quad \tilde{A} = \begin{bmatrix} 5 & \\ & 2 \end{bmatrix}.$$

Allora:

$$(7.18) \quad \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} c_1 e^{5t} \\ c_2 e^{2t} \end{bmatrix},$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} c_1 e^{5t} \\ c_2 e^{2t} \end{bmatrix} = \begin{bmatrix} c_1 e^{5t} + 2c_2 e^{2t} \\ c_1 e^{5t} - c_2 e^{2t} \end{bmatrix}.$$

In altre parole, ogni soluzione è una combinazione lineare delle due soluzioni fondamentali:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} e^{5t} \\ e^{5t} \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2e^{2t} \\ -e^{2t} \end{bmatrix}.$$

sono le soluzioni (7.10) corrispondenti agli autovettori  $(1, 1)^t$  e  $(2, -1)^t$ . I coefficienti  $c_i$  che compaiono in tali soluzioni sono arbitrari. Essi vengono determinati di solito assegnando *condizioni iniziali*, ossia il valore di  $X$  per un certo valore particolare  $t_0$ .

Consideriamo ora il caso in cui la matrice dei coefficienti  $A$  possiede autovalori distinti, ma non tutti reali. Per imitare il metodo sopra esposto, dobbiamo considerare innanzitutto equazioni differenziali della forma (7.1), in cui  $a$  è un numero complesso. Le soluzioni di una tale equazione differenziale, interpretate correttamente, hanno ancora la forma  $ce^{at}$ . L'unica cosa da ricordare è che  $e^{at}$  è ora una funzione di  $t$  a valori complessi. Per non complicare troppo le cose, restringiamo la variabilità di  $t$  ai valori reali, sebbene questa non sia la scelta più naturale lavorando con le funzioni a valori complessi. D'altra parte, lasciando assumere a  $t$  valori complessi, le cose non cambierebbero di molto.

La definizione della derivata di una funzione a valori complessi è la stessa di quella per le funzioni a valori reali:

$$(7.19) \quad \frac{dx}{dt} = \lim_{h \rightarrow 0} \frac{x(t+h) - x(t)}{h},$$

purché tale limite esista. Non vi sono novità particolari. È possibile esprimere un'arbitraria funzione complessa  $x(t)$  mediante la sua parte reale e la sua parte immaginaria, che sono funzioni a valori reali:

$$(7.20) \quad x(t) = u(t) + iv(t).$$

Allora  $x$  è derivabile se e soltanto se  $u$  e  $v$  sono derivabili, e in tal caso, la derivata di  $x$  è  $x' = u' + iv'$ . Ciò segue direttamente dalla definizione. Le regole usuali per la derivazione, come la regola del prodotto, continuano a valere per le funzioni a valori complessi. Esse si possono dimostrare applicando a  $u$  e  $v$  i teoremi corrispondenti relativi alle funzioni reali, oppure estendendo la dimostrazione per le funzioni reali al caso complesso.

Richiamiamo la formula:

$$(7.21) \quad e^{r+si} = e^r(\cos s + i \sin s).$$

Derivando tale formula, si ottiene che  $de^{at}/dt = ae^{at}$  per ogni numero complesso  $a = r + si$ . Pertanto  $ce^{at}$  è una soluzione dell'equazione differenziale (7.1), e la dimostrazione data all'inizio del paragrafo prova che queste sono le uniche soluzioni.

Avendo esteso lo studio di un'equazione al caso dei coefficienti complessi, possiamo usare ora il metodo della diagonalizzazione per risolvere un sistema di equazioni (7.5), quando  $A$  è una matrice complessa arbitraria con autovalori distinti.

Per esempio, sia  $A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ . I vettori  $v_1 = \begin{bmatrix} 1 \\ i \end{bmatrix}$  e  $v_2 = \begin{bmatrix} i \\ 1 \end{bmatrix}$  sono autovettori, rispettivamente con autovalori  $1+i$  e  $1-i$ . Poniamo  $\mathbf{B} = (v_1, v_2)$ . In base a (6.7),  $A$  è diagonalizzata dalla matrice  $P$ , dove

$$(7.22) \quad P^{-1} = [\mathbf{B}] = \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}.$$

La formula (7.14) ci dà  $\tilde{X} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} c_1 e^{t+it} \\ c_2 e^{t-it} \end{bmatrix}$ . Le soluzioni di (7.5) sono:

$$(7.23) \quad \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = P^{-1} \tilde{X} = \begin{bmatrix} c_1 e^{t+it} + i c_2 e^{t-it} \\ i c_1 e^{t+it} + c_2 e^{t-it} \end{bmatrix},$$

dove  $c_1, c_2$  sono numeri complessi arbitrari. Pertanto ogni soluzione è una combinazione lineare delle due soluzioni fondamentali:

$$(7.24) \quad \begin{bmatrix} e^{t+it} \\ ie^{t+it} \end{bmatrix}, \quad \begin{bmatrix} ie^{t-it} \\ e^{t-it} \end{bmatrix}.$$

Tuttavia, queste soluzioni non sono completamente soddisfacenti, poiché siamo partiti da un sistema di equazioni differenziali a coefficienti reali e le soluzioni ottenute sono complesse. Quando la matrice di partenza è reale, vogliamo avere soluzioni reali. A tal fine, osserviamo il lemma seguente:

(7.25) LEMMA *Sia  $A$  una matrice  $n \times n$  reale e sia  $X(t)$  una soluzione a valori complessi dell'equazione differenziale (7.5). Allora la parte reale e la parte immaginaria di  $X(t)$  sono soluzioni della stessa equazione.* ■

Ora ogni soluzione dell'equazione di partenza (7.5), reale o complessa, ha la forma (7.23), essendo i  $c_i$  numeri complessi. Pertanto le soluzioni reali stanno tra quelle che abbiamo trovato. Per scriverle esplicitamente, possiamo prendere le parti reali e le parti immaginarie delle soluzioni complesse.

Le parti reali e le parti immaginarie delle (7.24) si determinano utilizzando la (7.21). Esse sono, rispettivamente:

$$(7.26) \quad \begin{bmatrix} e^t \cos t \\ -e^t \sin t \end{bmatrix}, \quad \begin{bmatrix} e^t \sin t \\ e^t \cos t \end{bmatrix}.$$

Ogni soluzione reale è combinazione lineare reale di queste soluzioni particolari.

## L'esponenziale di una matrice

I sistemi di equazioni differenziali lineari a coefficienti costanti del primo ordine possono anche essere risolti formalmente, utilizzando l'*esponenziale di una matrice*. L'esponenziale di una matrice  $n \times n$  reale o complessa  $A$  si ottiene sostituendo una matrice nella serie di Taylor di  $e^x$ :

$$(8.1) \quad 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Dunque, per definizione:

$$(8.2) \quad e^A = I + A + \frac{1}{2!} A^2 + \frac{1}{3!} A^3 + \dots$$

Questa è una matrice  $n \times n$ .

(8.3) PROPOSIZIONE *La serie (8.2) converge assolutamente per ogni matrice complessa  $A$ .*

Per non interrompere la trattazione, abbiamo raccolto tutte le dimostrazioni alla fine del paragrafo.

Poiché la moltiplicazione tra matrici è relativamente complicata, non è facile scrivere esplicitamente, in modo diretto, gli elementi della matrice  $e^A$ . In generale questi non si ottengono come esponenziali degli elementi di  $A$ . Fa eccezione il caso in cui  $A$  è una matrice diagonale, diciamo con elementi diagonali  $a_{ii}$ . L'esame della serie rivela che in questo caso anche  $e^A$  è diagonale, e che i suoi elementi diagonali sono  $e^{a_{ii}}$ .

L'esponenziale è anche relativamente facile da calcolare per una matrice  $2 \times 2$  triangolare. Per esempio, sia:

$$(8.4) \quad A = \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix}.$$

Allora:

$$(8.5) \quad e^A = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 & 3 \\ & 4 \end{bmatrix} + \dots = \begin{bmatrix} e & * \\ & e^2 \end{bmatrix}.$$

Calcolando gli esponenziali degli elementi diagonali si ottengono gli elementi diagonali di  $e^A$ . È un buon esercizio calcolare l'elemento mancante \* direttamente dalla definizione.

L'esponenziale di una matrice  $A$  può essere determinata anche nel caso in cui sia data una matrice  $P$  tale che  $PAP^{-1}$  sia diagonale. Utilizzando la regola:

$PA^k P^{-1} = (PAP^{-1})^k$  e la proprietà distributiva della moltiplicazione tra matrici, si ottiene:

$$(8.6) \quad Pe^A P^{-1} = PIP^{-1} + (PAP^{-1}) + \frac{1}{2!} (PAP^{-1})^2 + \dots = e^{PAP^{-1}}.$$

Supponiamo che  $PAP^{-1} = \tilde{A}$  sia diagonale, con elementi diagonali  $\lambda_i$ . Allora anche  $e^{\tilde{A}}$  è diagonale, e i suoi elementi diagonali sono  $e^{\lambda_i}$ . Pertanto possiamo calcolare esplicitamente  $e^A$ :

$$(8.7) \quad e^A = P^{-1} e^{\tilde{A}} P.$$

Allo scopo di utilizzare l'esponenziale di una matrice per risolvere i sistemi di equazioni differenziali, occorre estendere ad essa alcune proprietà della funzione esponenziale ordinaria. La proprietà più importante è:  $e^{x+y} = e^x e^y$ . Tale proprietà può essere espressa come un'identità formale tra le due serie infinite che si ottengono dagli sviluppi in serie:

$$(8.8) \quad \begin{aligned} e^{x+y} &= 1 + \frac{x+y}{1!} + \frac{(x+y)^2}{2!} + \dots, \\ e^x \cdot e^y &= \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots\right) \left(1 + \frac{y}{1!} + \frac{y^2}{2!} + \dots\right). \end{aligned}$$

Non possiamo sostituire le matrici in tale identità poiché per ottenere l'uguaglianza delle due serie occorre la proprietà commutativa. Per esempio, i termini quadratici di (8.8), calcolati senza la proprietà commutativa, sono  $\frac{1}{2}(x^2 + xy + yx + y^2)$  e  $\frac{1}{2}x^2 + xy + \frac{1}{2}y^2$ , e quindi non sono uguali, a meno che  $xy = yx$ . Pertanto non vi è alcun motivo per aspettarsi che  $e^{A+B}$  sia uguale a  $e^A e^B$  in generale. Tuttavia, se due matrici  $A$  e  $B$  commutano tra loro, allora vale l'identità formale.

### (8.9) PROPOSIZIONE

(a) *Gli sviluppi formali di (8.8), con  $x, y$  variabili che commutano tra loro, sono uguali.*

(b) *Siano  $A, B$  matrici  $n \times n$  complesse tali che  $AB = BA$ . Allora  $e^{A+B} = e^A e^B$ .*

Dimostrazione a p. 170. ■

(8.10) COROLLARIO *Data una matrice complessa  $n \times n$   $A$ , l'esponenziale  $e^A$  è invertibile, e la sua inversa è  $e^{-A}$ .*

Ciò segue dalla proposizione, poiché  $A$  e  $-A$  commutano tra loro, e quindi  $e^A e^{-A} = e^{A-A} = e^0 = I$ . ■

Come esempio di applicazione della proposizione (8.9b), consideriamo la ma-

trice:

$$(8.11) \quad A = \begin{bmatrix} 2 & 3 \\ & 2 \end{bmatrix}.$$

Possiamo calcolarne l'esponenziale, scrivendo  $A$  nella forma:  $A = 2I + B$ , dove  $B = 3e_{12}$ . Poiché  $2I$  commuta con  $B$ , possiamo applicare la proposizione (8.9b):  $e^A = e^{2I} e^B$ , e dallo sviluppo in serie si ottengono direttamente i valori:  $e^{2I} = e^2 I$ ,  $e^B = I + B$ . Dunque

$$e^A = \begin{bmatrix} e^2 & \\ & e^2 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ & 1 \end{bmatrix} = \begin{bmatrix} e^2 & 3e^2 \\ & e^2 \end{bmatrix}.$$

Passiamo ora al risultato principale che collega l'esponenziale di una matrice alle equazioni differenziali. Data una matrice  $n \times n$   $A$ , consideriamo l'esponenziale  $e^{tA}$ , essendo  $t$  una variabile scalare, come una funzione a valori matriciali:

$$(8.12) \quad e^{tA} = I + tA + \frac{t^2}{2!} A^2 + \frac{t^3}{3!} A^3 + \dots$$

(8.13) PROPOSIZIONE *La funzione  $e^{tA}$  è derivabile rispetto a  $t$ , e la sua derivata è  $Ae^{tA}$ .*

Dimostrazione a p. 171. ■

(8.14) TEOREMA *Sia  $A$  una matrice  $n \times n$  reale o complessa. Le colonne della matrice  $e^{tA}$  formano una base dello spazio vettoriale delle soluzioni dell'equazione differenziale:*

$$\frac{dX}{dt} = AX.$$

Avremo bisogno del lemma seguente, la cui dimostrazione è lasciata per esercizio:

(8.15) LEMMA (Regola del prodotto) *Siano  $A(t)$  e  $B(t)$  funzioni a valori matriciali derivabili rispetto a  $t$ , tali che il loro prodotto sia definito. Allora la matrice prodotto  $A(t)B(t)$  è derivabile, e la sua derivata è:*

$$\frac{d}{dt} A(t)B(t)) = \frac{dA}{dt} B + A \frac{dB}{dt}. \quad ■$$

Dimostrazione del teorema (8.14). La proposizione (8.13) prova che le colonne  $A$  sono soluzioni dell'equazione differenziale, poiché la derivazione e la moltiplicazione per  $A$  agiscono indipendentemente sulle colonne della matrice  $e^{tA}$ . Per

dimostrare che ogni soluzione è una combinazione lineare delle colonne, imitiamo la dimostrazione data all'inizio del paragrafo 7. Sia  $X(t)$  una soluzione qualsiasi di (7.5). Derivando la matrice prodotto  $e^{-tA}X(t)$ , otteniamo:

$$(8.17) \quad \frac{d}{dt}(e^{-tA}X(t)) = -Ae^{-tA}X(t) + e^{-tA}AX(t).$$

Fortunatamente,  $A$  e  $e^{-tA}$  commutano tra loro (ciò segue direttamente dalla definizione dell'esponenziale), quindi la derivata è zero. Pertanto  $e^{-tA}X(t)$  è un vettore colonna costante, diciamo  $C = (c_1, \dots, c_n)^t$ , e  $X(t) = e^{tA}C$ . Ciò esprime  $X(t)$  come una combinazione lineare delle colonne di  $e^{tA}$  e tale espressione è unica, poiché  $e^{tA}$  è una matrice invertibile. ■

In base al teorema (8.14), l'esponenziale di una matrice risolve sempre l'equazione differenziale (7.5). Dato che il calcolo diretto dell'esponenziale può essere piuttosto difficile, a volte non è facile applicare questo teorema in una situazione concreta. Ma se  $A$  è una matrice diagonalizzabile, allora l'esponenziale di  $A$  può essere calcolata come nella (8.7):  $e^A = P^{-1}e^{\tilde{A}}P$ . Possiamo usare questo metodo di calcolo per  $e^{tA}$ , per risolvere l'equazione (7.5), ma naturalmente esso dà lo stesso risultato di prima. Così, se  $A$  è la matrice usata nell'esempio (7.7), e  $P, \tilde{A}$  si ottengono da (7.17), si ha:

$$e^{t\tilde{A}} = \begin{bmatrix} e^{5t} & \\ & e^{2t} \end{bmatrix}$$

e

$$\begin{aligned} e^{tA} &= P^{-1}e^{t\tilde{A}}P = -\frac{1}{3} \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} e^{5t} & \\ & e^{2t} \end{bmatrix} \begin{bmatrix} -1 & -2 \\ -1 & 1 \end{bmatrix} = \\ &= \frac{1}{3} \begin{bmatrix} e^{5t} + 2e^{2t} & 2e^{5t} - 2e^{2t} \\ e^{5t} - e^{2t} & 2e^{5t} + e^{2t} \end{bmatrix}. \end{aligned}$$

Le colonne della matrice che abbiamo ottenuto formano un'altra base per la soluzione generale (7.18).

D'altra parte, la matrice  $A = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ , che rappresenta il sistema di equazioni:

$$(8.16) \quad \frac{dx}{dt} = x, \quad \frac{dy}{dt} = x + y,$$

non è diagonalizzabile. Pertanto il metodo illustrato nel § 7 non può essere applicato. Per risolvere il sistema, scriviamo  $At = It + Bt$ , dove  $B = e_{21}$ , e otteniamo, come nella discussione di (8.11):

$$(8.17) \quad e^{At} = e^{It}e^{Bt} = \begin{bmatrix} e^t & \\ te^t & e^t \end{bmatrix}.$$

le soluzioni di (8.16) sono combinazioni lineari delle colonne:

$$(8.18) \quad \begin{bmatrix} e^t \\ te^t \end{bmatrix}, \quad \begin{bmatrix} 0 \\ e^t \end{bmatrix}.$$

Per calcolare esplicitamente l'esponenziale in tutti i casi, occorre scrivere la matrice nella forma di Jordan (cfr. cap. 12).

Torniamo ora indietro a dimostrare le proposizioni (8.3), (8.9) e (8.13). Per ottenere una notazione più compatta, denoteremo qui l'elemento di indici  $i, j$  di una matrice  $A$  con  $A_{ij}$ . Così  $(AB)_{ij}$  denoterà l'elemento della matrice prodotto  $AB$ , e  $(A^k)_{ij}$  l'elemento di  $A^k$ . Con tale notazione, l'elemento di indici  $i, j$  di  $e^A$  è la somma della serie:

$$(8.19) \quad (e^A)_{ij} = I_{ij} + A_{ij} + \frac{1}{2!}(A^2)_{ij} + \frac{1}{3!}(A^3)_{ij} + \dots$$

Per dimostrare che la serie relativa all'esponenziale converge, occorre provare che gli elementi delle potenze  $A^k$  di una matrice assegnata  $A$  non crescono troppo rapidamente, in modo tale che i valori assoluti degli elementi di indici  $i, j$  formano una serie limitata (e quindi convergente). A tale scopo, definiamo la norma di una matrice  $n \times n$   $A$  come il massimo valore assoluto degli elementi della matrice:

$$(8.20) \quad \|A\| = \max_{i,j} |A_{ij}|.$$

In altre parole,  $\|A\|$  è il più piccolo numero reale tale che

$$(8.21) \quad |A_{ij}| \leq \|A\| \quad \text{per ogni } i, j.$$

Questa è una delle varie definizioni possibili per la norma. La sua proprietà fondamentale è la seguente:

(8.22) LEMMA Siano  $A, B$  matrici  $n \times n$  complesse. Allora si ha  $\|AB\| \leq n\|A\|\|B\|$ ,  $\|A^k\| \leq n^{k-1}\|A\|^k$  per ogni  $k > 0$ .

*Dimostrazione.* Scriviamo una stima per il valore assoluto dell'elemento di indici  $i, j$  di  $AB$ :

$$|(AB)_{ij}| = \left| \sum_{\nu=1}^n A_{i\nu} B_{\nu j} \right| \leq \sum_{\nu=1}^n |A_{i\nu}| |B_{\nu j}| \leq n\|A\|\|B\|.$$

Dunque  $\|AB\| \leq n\|A\|\|B\|$ . La seconda diseguaglianza segue per induzione dalla prima. ■

**Dimostrazione della proposizione (8.3).** Per dimostrare che l'esponenziale di una matrice converge assolutamente, calcoliamo una stima per la serie. Precisamente, posto:  $a = n\|A\|$ , otteniamo:

$$\begin{aligned} |(e^A)_{ij}| &\leq |I_{ij}| + |A_{ij}| + \frac{1}{2!} |(A^2)_{ij}| + \frac{1}{3!} |(A^3)_{ij}| + \dots \leq \\ (8.23) \quad &\leq 1 + \|A\| + \frac{1}{2!} n\|A\|^2 + \frac{1}{3!} n^2\|A\|^3 + \dots = \\ &= 1 + \left( a + \frac{1}{2!} a^2 + \frac{1}{3!} a^3 + \dots \right) \frac{1}{n} = 1 + \frac{e^a - 1}{n}. \blacksquare \end{aligned}$$

**Dimostrazione della proposizione (8.9)**

(a) I termini di grado  $k$  negli sviluppi di (8.8) sono:

$$\frac{(x+y)^k}{k!} = \sum_{r+s=k} \binom{k}{r} \frac{x^r y^s}{k!} \quad \text{e} \quad \sum_{r+s=k} \frac{x^r}{r!} \frac{y^s}{s!}.$$

Per dimostrare che tali termini sono uguali, dobbiamo far vedere che

$$\binom{k}{r} \frac{1}{k!} = \frac{1}{r!s!} \quad \text{oppure} \quad \binom{k}{r} = \frac{k!}{r!s!},$$

per ogni  $k$  e per ogni  $r, s$  tali che  $r+s=k$ , e questa è una formula standard relativa ai coefficienti binomiali.

(b) Indichiamo con  $S_n(x)$  la somma parziale:  $1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$ . Allora risulta:

$$\begin{aligned} S_n(x)S_n(y) &= \left( 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!} \right) \left( 1 + \frac{y}{1!} + \frac{y^2}{2!} + \dots + \frac{y^n}{n!} \right) = \\ &= \sum_{r,s=0}^n \frac{x^r}{r!} \frac{y^s}{s!}, \end{aligned}$$

mentre d'altra parte si ha:

$$\begin{aligned} S_n(x+y) &= \left( 1 + \frac{(x+y)}{1!} + \frac{(x+y)^2}{2!} + \dots + \frac{(x+y)^n}{n!} \right) = \\ &= \sum_{k=0}^n \sum_{r+s=k} \binom{k}{r} \frac{x^r y^s}{k!} = \sum_{k=0}^n \sum_{r+s=k} \frac{x^r}{r!} \frac{y^s}{s!}. \end{aligned}$$

confrontando i termini, troviamo che lo sviluppo della somma parziale  $S_n(x+y)$  è costituito dai termini in  $S_n(x)S_n(y)$  tali che  $r+s \leq n$ . Lo stesso vale sostituendo a  $x, y$  due matrici  $A, B$  che commutano tra loro. Dobbiamo dimostrare che la somma dei termini rimanenti tende a zero per  $k \rightarrow \infty$ .

**(8.24) LEMMA** La serie  $\sum_{k=0}^{\infty} \sum_{r+s=k} \left| \left( \frac{A^r}{r!} \frac{B^s}{s!} \right)_{ij} \right|$  converge per ogni  $i, j$ .

**Dimostrazione.** Poniamo  $a = n\|A\|$  e  $b = n\|B\|$ . Cerchiamo una stima per i termini della somma. In base a (8.22), si ha  $|(A^r B^s)_{ij}| \leq n(n^{r-1}\|A\|^r)(n^{s-1}\|B\|^s) \leq a^r b^s$ . Quindi

$$\sum_k \sum_{r+s=k} \left| \left( \frac{A^r}{r!} \frac{B^s}{s!} \right)_{ij} \right| \leq \sum_k \sum_{r+s=k} \frac{a^r}{r!} \frac{b^s}{s!} = e^{a+b}.$$

La proposizione segue da questo lemma perché, d'altra parte, il valore assoluto dell'elemento di indici  $i, j$  di  $S_k(A)S_k(B) - S_k(A+B)$  è maggiorato da  $\sum_{r+s>k} \left| \left( \frac{A^r}{r!} \frac{B^s}{s!} \right)_{ij} \right|$ . In base al lemma, questa somma tende a zero per  $k \rightarrow \infty$ , e d'altra parte si ha:

$$(S_k(A)S_k(B) - S_k(A+B)) \rightarrow (e^A e^B - e^{A+B}). \blacksquare$$

**Dimostrazione della proposizione (8.13).** Per definizione, si ha:

$$\frac{d}{dt} (e^{tA}) = \lim_{h \rightarrow 0} \frac{e^{(t+h)A} - e^{tA}}{h}.$$

Poiché le matrici  $tA$  e  $hA$  commutano tra loro, la proposizione (8.9) prova che:

$$\frac{e^{(t+h)A} - e^{tA}}{h} = \left( \frac{e^{hA} - I}{h} \right) e^{tA}.$$

Pertanto la proposizione segue dal lemma:

**(8.25) LEMMA**  $\lim_{h \rightarrow 0} \frac{e^{hA} - I}{h} = A$ .

**Dimostrazione.** Lo sviluppo in serie dell'esponenziale prova che:

$$(26) \quad \frac{e^{hA} - I}{h} - A = \frac{h}{2!} A^2 + \frac{h^2}{3!} A^3 + \dots$$

Cerchiamo una stima per tale serie. Allora, posto:  $a = |h|n\|A\|$ , otteniamo:

$$\begin{aligned} \left| \left( \frac{h}{2!} A^2 + \frac{h^2}{3!} A^3 + \dots \right)_{ij} \right| &\leq \left| \frac{h}{2!} (A^2)_{ij} \right| + \left| \frac{h^2}{3!} (A^3)_{ij} \right| + \dots \leq \\ &\leq \frac{1}{2!} |h| n \|A\|^2 + \frac{1}{3!} |h|^2 n^2 \|A\|^3 + \dots = \|A\| \left( \frac{1}{2!} a + \frac{1}{3!} a^2 + \dots \right) = \\ &= \frac{\|A\|}{a} (e^a - 1 - a) = \|A\| \left( \frac{e^a - 1}{a} - 1 \right). \end{aligned}$$

Si noti che  $a \rightarrow 0$  per  $h \rightarrow 0$ . Poiché la derivata di  $e^x$  è  $e^x$ , si ha

$$\lim_{a \rightarrow 0} \frac{e^a - 1}{a} = \frac{d}{dx} e^x \Big|_{x=0} = e^0 = 1.$$

Pertanto l'espressione (8.26) tende a zero per  $h \rightarrow 0$ . ■

Useremo ancora le proprietà notevoli dell'esponenziale di una matrice nel cap. 8.

Non ho giudicato necessario affrontare la fatica di una dimostrazione formale del teorema nel caso generale.

Arthur Cayley

### Esercizi

#### 1 La formula della dimensione

1. Sia  $T$  la moltiplicazione a sinistra per la matrice  $\begin{bmatrix} 1 & 2 & 0 & -1 & 5 \\ 2 & 0 & 2 & 0 & 1 \\ 1 & 1 & -1 & 3 & 2 \\ 0 & 3 & -3 & 2 & 6 \end{bmatrix}$ . Calcolare esplicitamente  $\ker T$  e  $\text{im } T$  descrivendo basi per tali spazi, e verificare (1.7).

2. Determinare il rango della matrice  $\begin{bmatrix} 11 & 12 & 13 & 14 \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{bmatrix}$ .

3. Sia  $T : V \rightarrow W$  un'applicazione lineare. Dimostrare che  $\ker T$  è un sottospazio di  $V$  e che  $\text{im } T$  è un sottospazio di  $W$ .

4. Sia  $A$  una matrice  $m \times n$ . Dimostrare che lo spazio delle soluzioni del sistema lineare  $AX = 0$  ha dimensione almeno  $n - m$ .

5. Sia  $A$  una matrice  $k \times m$  e sia  $B$  una matrice  $n \times p$ . Dimostrare che la legge  $M \mapsto AMB$  definisce un'applicazione lineare dallo spazio  $F^{m \times n}$  delle matrici  $m \times n$  allo spazio  $F^{k \times p}$ .

6. Sia  $(v_1, \dots, v_n)$  un sottoinsieme di uno spazio vettoriale  $V$ . Dimostrare che l'applicazione  $\varphi : F^n \rightarrow V$  definita da:  $\varphi(X) = v_1 x_1 + \dots + v_n x_n$  è un'applicazione lineare.

Se il campo  $F$  è uno dei campi  $F_p$ , gli spazi vettoriali di dimensione finita su  $F$  hanno un numero finito di elementi. In tal caso, la (1.6) (cap. 4) e la (6.15) (cap. 2) valgono entrambe. Collegare tali formule tra loro.

Dimostrare che ogni matrice  $m \times n$   $A$  di rango 1 ha la forma:  $A = XY^t$ , dove  $X, Y$  sono, rispettivamente, un vettore colonna  $m$ -dimensionale e un vettore colonna  $n$ -dimensionale.

9. (a) L'operatore *spostamento a sinistra*  $S^-$  su  $V = \mathbb{R}^\infty$  è definito da:  $(a_1, a_2, \dots) \mapsto (a_2, a_3, \dots)$ . Dimostrare che  $\ker S^- > 0$ , ma  $\text{im } S^- = V$ .  
(b) L'operatore *spostamento a destra*  $S^+$  su  $V = \mathbb{R}^\infty$  è definito da:  $(a_1, a_2, \dots) \mapsto (0, a_1, a_2, \dots)$ . Dimostrare che  $\ker S^+ = 0$ , ma  $\text{im } S^+ < V$ .

#### 2 La matrice di un'applicazione lineare

1. Determinare la matrice dell'operatore di derivazione  $\frac{d}{dx} : P_n \rightarrow P_{n-1}$  rispetto alle basi canoniche (cfr. (1.4)).  
2. Trovare tutte le applicazioni lineari  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  che portano la retta di equazione  $y = x$  nella retta di equazione  $y = 3x$ .  
3. Dimostrare la proposizione (2.9b) utilizzando le operazioni sulle righe e sulle colonne.  
4. Sia  $T : \mathbb{R}^3 \rightarrow \mathbb{R}^2$  l'applicazione lineare definita da  $T(x_1, x_2, x_3)^t = (x_1 + x_2, 2x_3 - x_1)^t$ . Qual è la matrice di  $T$  rispetto alle basi canoniche?  
5. Sia  $A$  una matrice  $n \times n$ , e si denoti con  $V = F^n$  lo spazio dei vettori riga. Qual è la matrice dell'applicazione lineare "moltiplicazione a destra per  $A$ " da  $V$  a  $V$ , rispetto alla base canonica di  $V$ ?  
6. Dimostrare che matrici diverse tra loro definiscono applicazioni lineari diverse tra loro.  
7. Descrivere la moltiplicazione a sinistra e la moltiplicazione a destra per la matrice (2.10), e dimostrare che il rango di tale matrice è  $r$ .  
8. Provare che  $A$  e  $A^t$  hanno lo stesso rango.  
9. Siano  $T_1, T_2$  applicazioni lineari da  $V$  a  $W$ . Definiamo  $T_1 + T_2$  e  $cT$  mediante le regole:  $[T_1 + T_2](v) = T_1(v) + T_2(v)$  e  $[cT](v) = cT(v)$ .  
(a) Dimostrare che  $T_1 + T_2$  e  $cT_1$  sono applicazioni lineari, e descrivere le matrici ad esse associate mediante le matrici di  $T_1, T_2$ .  
(b) Sia  $L$  l'insieme di tutte le applicazioni lineari da  $V$  a  $W$ . Dimostrare che  $L$  risulta uno spazio vettoriale rispetto alle operazioni definite sopra, e calcolare la sua dimensione.

#### 3 Operatori lineari e autovettori

1. Sia  $V$  lo spazio vettoriale delle matrici reali simmetriche  $2 \times 2$   $X = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ , e si consideri la matrice  $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ . Determinare la matrice dell'operatore lineare su  $V$  definito da  $X \mapsto AXA^t$ , rispetto a una base opportuna.

2. Sia  $F^{2 \times 2}$  lo spazio delle matrici  $2 \times 2$ , siano  $A, B \in F^{2 \times 2}$  fissate, e sia  $T : F^{2 \times 2} \rightarrow F^{2 \times 2}$  l'operatore definito da  $T(M) = AMB$ . Trovare la matrice di  $T$  rispetto alla base  $(e_{11}, e_{12}, e_{21}, e_{22})$  di  $F^{2 \times 2}$ .
3. Sia  $T : V \rightarrow V$  un operatore lineare su uno spazio vettoriale di dimensione 2, e supponiamo che  $T$  non sia la moltiplicazione per uno scalare. Dimostrare che esiste un vettore  $v \in V$  tale che  $(v, T(v))$  è una base di  $V$ , e descrivere la matrice di  $T$  rispetto a tale base.
4. Sia  $T$  un operatore lineare su uno spazio vettoriale  $V$ , e sia  $c \in F$  un autovalore di  $T$ . Sia  $W$  l'insieme degli autovettori di  $T$  associati all'autovalore  $c$ , con l'aggiunta del vettore nullo. Dimostrare che  $W$  è un sottospazio  $T$ -invariante.
5. Trovare tutti i sottospazi invarianti degli operatori lineari reali rappresentati dalle matrici:
- (a)  $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$  (b)  $\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$ .
6. Un operatore lineare su uno spazio vettoriale  $V$  si dice *nilpotente*, se  $T^k = 0$  per qualche intero  $k$ . Sia  $T$  un operatore nilpotente e si ponga  $W_i = \text{im } T^i$ .
- (a) Dimostrare che, se  $W_i \neq 0$ , allora si ha  $\dim W_{i+1} < \dim W_i$ .
- (b) Dimostrare che, se  $V$  è uno spazio di dimensione  $n$  e se  $T$  è nilpotente, allora risulta  $T^n = 0$ .
7. Sia  $T$  un operatore lineare su  $\mathbb{R}^2$ . Dimostrare che, se  $T$  porta una retta  $\ell$  in  $\ell$ , allora  $T$  porta anche ogni retta parallela a  $\ell$  in un'altra retta parallela a  $\ell$ .
8. Dimostrare che la composizione  $T_1 \circ T_2$  di operatori lineari su uno spazio vettoriale è un operatore lineare, e calcolare la matrice ad essa associata mediante le matrici  $A_1, A_2$  di  $T_1, T_2$ .
9. Sia  $P$  lo spazio vettoriale reale dei polinomi  $p(x) = a_0 + a_1x + \dots + a_nx^n$  di grado  $\leq n$ , e si denoti con  $D$  la derivata  $\frac{d}{dx}$ , considerata come un operatore lineare su  $P$ .
- (a) Trovare la matrice di  $D$  rispetto a una base opportuna, e dimostrare che  $D$  è un operatore nilpotente.
- (b) Determinare tutti i sottospazi  $D$ -invarianti.
10. Dimostrare che le matrici  $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$  e  $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$  ( $b \neq 0$ ) sono simili tra loro se e soltanto se  $a \neq d$ .
11. Sia  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  una matrice reale  $2 \times 2$ . Dimostrare che  $A$  può essere ridotta a una matrice  $\begin{bmatrix} 0 & * \\ 1 & * \end{bmatrix}$  mediante operazioni sulle righe e sulle colonne della forma:  $A \rightarrow EAE^{-1}$ , a meno che  $b = c = 0$  e  $a = d$ . Analizzare con cura i vari casi, considerando l'eventualità che  $b \circ c$  sia uguale a zero.
12. Sia  $T$  un operatore lineare su  $\mathbb{R}^2$  con due autovettori linearmente indipendenti  $v_1, v_2$ . Supponiamo che gli autovalori  $c_1, c_2$  associati a tali autovettori siano positivi e che  $c_1 > c_2$ . Sia  $\ell_i$  la retta generata da  $v_i$  ( $i = 1, 2$ ).

(a) L'operatore  $T$  porta ogni retta  $\ell$  passante per l'origine in un'altra retta. Utilizzando la regola del parallelogramma per l'addizione tra vettori, verificare che ogni retta  $\ell \neq \ell_2$  viene spostata lontano da  $\ell_2$  verso  $\ell_1$ .

(b) Utilizzare (a) per dimostrare che gli autovettori di  $T$  sono necessariamente multipli di  $v_1$  o di  $v_2$ .

(c) Descrivere l'effetto sulle rette nel caso in cui vi è una sola retta portata in se stessa, con autovalore positivo.

13. Si consideri una matrice  $2 \times 2$  arbitraria  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ . La condizione affinché un vettore colonna  $X$  sia un autovettore per la moltiplicazione a sinistra per  $A$  è che  $Y = AX$  sia parallelo a  $X$ , ciò che significa che i rapporti  $s = x_2/x_1$  e  $s' = y_2/y_1$  sono uguali.

(a) Trovare l'equazione in  $s$  che esprime tale uguaglianza.

(b) Per quali matrici  $A$   $s = 0$  oppure  $s = \infty$  è una soluzione?

(c) Dimostrare che, se gli elementi di  $A$  sono numeri reali positivi, allora esiste un autovettore nel primo quadrante e anche un autovettore nel secondo quadrante.

#### 4 Il polinomio caratteristico

1. Calcolare i polinomi caratteristici, gli autovalori e gli autovettori delle seguenti matrici complesse:

(a)  $\begin{bmatrix} -2 & 2 \\ -2 & 3 \end{bmatrix}$ ; (b)  $\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$ .

2. (a) Dimostrare che gli autovalori di una matrice reale simmetrica  $2 \times 2$  sono numeri reali.

(b) Dimostrare che una matrice reale  $2 \times 2$  tale che gli elementi non appartenenti alla diagonale principale siano positivi ha autovalori reali.

3. Trovare gli autovalori complessi e gli autovettori della matrice di rotazione:

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

4. Dimostrare che una matrice reale  $3 \times 3$  ha almeno un autovalore reale.

5. Determinare il polinomio caratteristico della matrice:

$$\begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & 1 & & \\ & 1 & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 1 & 0 \end{bmatrix}.$$

6. Dimostrare la proposizione (4.18).

7. (a) Sia  $T$  un operatore lineare avente due autovettori linearmente indipendenti associati a uno stesso autovalore  $\lambda$ . È vero che  $\lambda$  è una radice multipla del polinomio caratteristico di  $T$ ?

(b) Supponiamo che  $\lambda$  sia una radice multipla del polinomio caratteristico. È vero che  $T$  ha due autovettori linearmente indipendenti con autovalore  $\lambda$ ?

8. Sia  $V$  uno spazio vettoriale su un campo  $F$  con base  $(v_1, \dots, v_n)$ , e siano  $a_1, \dots, a_{n-1}$  elementi di  $F$ . Si consideri l'operatore lineare su  $V$  definito da:

$$T(v_i) = v_{i+1}, \text{ se } i < n \quad \text{e} \quad T(v_n) = a_1 v_1 + a_2 v_2 + \dots + a_{n-1} v_{n-1}.$$

(a) Determinare la matrice di  $T$  rispetto alla base assegnata.

(b) Determinare il polinomio caratteristico di  $T$ .

9. È vero che  $A$  e  $A^t$  hanno gli stessi autovalori e gli stessi autovettori?

10. (a) Utilizzare il polinomio caratteristico per dimostrare che una matrice reale  $2 \times 2 P$  avente tutti gli elementi positivi possiede due autovalori reali distinti.

(b) Dimostrare che l'autovalore più grande ha un autovettore nel primo quadrante, e che l'autovalore più piccolo ha un autovettore nel secondo quadrante.

11. (a) Sia  $A$  una matrice  $3 \times 3$ , con polinomio caratteristico:

$$p(t) = t^3 - (\operatorname{tr} A)t^2 + s_1 t - (\det A).$$

Dimostrare che  $s_1$  è la somma dei sottodeterminanti simmetrici  $2 \times 2$ :

$$s_1 = \det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \det \begin{bmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{bmatrix} + \det \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix}.$$

(b) Generalizzare il risultato precedente per le matrici  $n \times n$ .

12. Sia  $T$  un operatore lineare su uno spazio di dimensione  $n$ , con autovalori  $\lambda_1, \dots, \lambda_n$ .

(a) Dimostrare che  $\operatorname{tr} T = \lambda_1 + \dots + \lambda_n$  e che  $\det T = \lambda_1 \cdots \lambda_n$ .

(b) Determinare gli altri coefficienti del polinomio caratteristico mediante gli autovalori.

13. Si consideri l'operatore lineare definito dalla moltiplicazione a sinistra per una matrice  $n \times n$   $A$ , sullo spazio  $F^{n \times n}$  di tutte le matrici  $n \times n$ . Calcolare la traccia e il determinante di tale operatore.

14. Sia  $P$  una matrice reale tale che  $P^t = P^2$ . Quali sono gli autovalori possibili per  $P$ ?

15. Sia  $A$  una matrice tale che  $A^n = I$ . Dimostrare che gli autovalori di  $A$  sono potenze della radice  $n$ -esima dell'unità:  $\zeta_n = e^{2\pi i/n}$ .

## 5 Matrici ortogonali e rotazioni

1. In  $\mathbb{R}^3$  qual è la matrice di rotazione di un angolo  $\theta$  intorno all'asse  $e_2$ ?

Dimostrare che ogni insieme ortonormale di  $n$  vettori in  $\mathbb{R}^n$  è una base.

3. Dimostrare algebricamente che una matrice reale  $2 \times 2 \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  rappresenta una rotazione se e solo se appartiene a  $SO_2$ .

4. (a) Dimostrare che  $O_n$  e  $SO_n$  sono sottogruppi di  $GL_n(\mathbb{R})$ , e determinare l'indice di  $SO_n$  in  $O_n$ .

(b) È vero che  $O_2$  è isomorfo al gruppo prodotto  $SO_2 \times \{\pm I\}$ ? È vero che  $O_3$  è isomorfo a  $SO_3 \times \{\pm I\}$ ?

5. Quali sono gli autovalori della matrice  $A$  che in  $\mathbb{R}^3$  rappresenta la rotazione di un angolo  $\theta$  intorno a un asse  $v$ ?

6. Sia  $A$  una matrice di  $O_3$  con determinante  $-1$ . Dimostrare che  $-1$  è un autovalore di  $A$ .

7. Sia  $A$  una matrice ortogonale  $2 \times 2$  con determinante  $-1$ . Dimostrare che  $A$  rappresenta una riflessione intorno a una retta passante per l'origine.

8. Sia  $A$  un elemento di  $SO_3$ , con angolo di rotazione  $\theta$ . Dimostrare che  $\cos \theta = \frac{1}{2}(\operatorname{tr} A - 1)$ .

9. Ogni polinomio reale di grado 3 ha una radice reale. Utilizzare questo fatto per dare una dimostrazione meno artificiosa del lemma (5.23).

\*10. Determinare in modo geometrico l'asse di rotazione della composizione di due rotazioni in  $\mathbb{R}^3$ .

11. Sia  $v$  un vettore di lunghezza 1, e sia  $P$  il piano di  $\mathbb{R}^3$  ortogonale a  $v$ . Descrivere una corrispondenza biunivoca tra i punti della circonferenza unitaria in  $P$  e le matrici  $A \in SO_3$  la cui prima colonna sia  $v$ .

12. Descrivere geometricamente l'azione di una matrice ortogonale con determinante  $-1$ .

13. Dimostrare che un movimento rigido, definito dalla condizione (5.15), è un'applicazione biiettiva.

\*14. Sia  $A$  un elemento di  $SO_3$ . Dimostrare che, se è definito, il vettore:

$$((a_{23} + a_{32})^{-1}, (a_{13} + a_{31})^{-1}, (a_{12} + a_{21})^{-1})$$

è un autovettore con autovalore 1.

## 6 Diagonalizzazione

1. (a) Trovare gli autovettori e gli autovalori della matrice:

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

(b) Trovare una matrice  $P$  tale che  $PAP^{-1}$  sia diagonale.

$$(c) \text{Calcolare } \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^{30}.$$

2. Diagonalizzare la matrice di rotazione  $\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$ , utilizzando i numeri complessi.
3. Dimostrare che, se  $A, B$  sono matrici  $n \times n$  e se  $A$  è non singolare, allora  $AB$  è simile a  $BA$ .
4. Sia  $A$  una matrice complessa avente zero come unico autovalore. È vero che  $A$  è nilpotente?
5. In ciascuno dei casi seguenti, se la matrice è diagonalizzabile, trovare una matrice  $P$  tale che  $PAP^{-1}$  sia diagonale:

(a)  $\begin{bmatrix} -2 & 2 \\ -2 & 3 \end{bmatrix}$  (b)  $\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$  (c)  $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}$  (d)  $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ .

6. È possibile effettuare la diagonalizzazione (6.1) con una matrice  $P \in SL_n$ ?
7. Dimostrare che un operatore lineare  $T$  è nilpotente se e solo se esiste una base di  $V$  tale che la matrice di  $T$  sia triangolare superiore, con gli elementi diagonali uguali a zero.
8. Sia  $T$  un operatore lineare su uno spazio di dimensione 2. Supponiamo che il polinomio caratteristico di  $T$  sia  $(t-a)^2$ . Dimostrare che esiste una base di  $V$  tale che la matrice di  $T$  ha una delle due forme seguenti:

$$\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}, \quad \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

9. Sia  $A$  una matrice nilpotente. Dimostrare che  $\det(I+A)=1$ .
10. Dimostrare che, se  $A$  è una matrice nilpotente  $n \times n$ , allora  $A^n=0$ .
11. Trovare tutte le matrici reali  $2 \times 2$  tali che  $A^2=I$ , e descrivere geometricamente il modo in cui esse operano su  $\mathbb{R}^2$  mediante la moltiplicazione a sinistra.
12. Sia  $M$  una matrice formata da due blocchi diagonali:  $M = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$ . Provare che  $M$  è diagonalizzabile se e solo se  $A$  e  $D$  sono diagonalizzabili.
13. (a) Sia  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  una matrice  $2 \times 2$  con un autovalore  $\lambda$ . Dimostrare che  $(b, \lambda-a)$  è un autovettore per  $A$ .
- (b) Trovare una matrice  $P$  tale che  $PAP^{-1}$  sia diagonale, se  $A$  ha due autovalori distinti  $\lambda_1 \neq \lambda_2$ .
14. Sia  $A$  una matrice complessa  $n \times n$ . Dimostrare che esiste una matrice  $B$  arbitrariamente vicina ad  $A$  (nel senso che il valore assoluto  $|b_{ij}-a_{ij}|$  può essere reso arbitrariamente piccolo per ogni  $i, j$ ) tale che  $B$  ha  $n$  autovalori distinti.

- \*15. Sia  $A$  una matrice complessa  $n \times n$  con  $n$  autovalori distinti  $\lambda_1, \dots, \lambda_n$ . Supponiamo che  $\lambda_1$  sia l'autovalore più grande, ossia che  $|\lambda_1| > |\lambda_i|$  per ogni  $i > 1$ . Dimostrare che, per la maggior parte dei vettori  $X$ , la successione  $X_k = \lambda_1^{-k} A^k X$  converge ad un

autovettore  $Y$  con autovalore  $\lambda_1$ , e descrivere precisamente quali sono le condizioni su  $X$  affinché ciò accada.

16. (a) Utilizzare il metodo del problema precedente per calcolare l'autovalore più grande della matrice  $\begin{bmatrix} 3 & 1 \\ 3 & 4 \end{bmatrix}$ , con una precisione di tre cifre.

- (b) Calcolare l'autovalore più grande della matrice  $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ , con una precisione di tre cifre.

- \*17. Siano  $A$  e  $B$  matrici complesse  $m \times m$  e  $n \times n$ , rispettivamente, sia  $F^{m \times n}$  lo spazio delle matrici complesse  $m \times n$  e sia  $T : F^{m \times n} \rightarrow F^{m \times n}$  l'operatore definito da:  $T(M) = AMB$ .

- (a) Costruire un autovettore per  $T$  a partire da una coppia di vettori colonna  $X, Y$ , dove  $X$  è un autovettore per  $A$  e  $Y$  è un autovettore per  $B^t$ .

- (b) Determinare gli autovalori di  $T$  mediante gli autovalori di  $A$  e  $B$ .

- \*18. Sia  $A$  una matrice complessa  $n \times n$ , sia  $F^{n \times n}$  lo spazio di tutte le matrici complesse  $n \times n$ , e sia  $T : F^{n \times n} \rightarrow F^{n \times n}$  l'operatore definito da  $T(B) = AB - BA$ .

- (a) Dimostrare che il rango di tale operatore è al più  $n^2 - n$ .

- (b) Determinare gli autovalori di  $T$  mediante gli autovalori  $\lambda_1, \dots, \lambda_n$  di  $A$ .

## 7 Sistemi di equazioni differenziali

1. Sia  $v$  un autovettore per una matrice  $A$ , con autovalore  $c$ . Provare che  $e^{ct}v$  è una soluzione dell'equazione differenziale  $\frac{dX}{dt} = AX$ .

2. Risolvere l'equazione  $\frac{dX}{dt} = AX$  per le seguenti matrici  $A$ :

(a)  $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ ; (b)  $\begin{bmatrix} -2 & 2 \\ -2 & 3 \end{bmatrix}$ ; (c)  $\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$ ; (d)  $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}$  (e)  $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ .

3. Spiegare perché la diagonalizzazione fornisce la soluzione generale.

4. (a) Dimostrare la proposizione (7.16).

- (b) Perché è sufficiente scrivere esplicitamente le parti reali e le parti immaginarie per ottenere la soluzione generale?

5. Dimostrare il lemma (7.25).

- Risolvere l'equazione differenziale non omogenea:  $\frac{dX}{dt} = AX + B$ , a partire dalle soluzioni dell'equazione omogenea:  $\frac{dX}{dt} = AX$ .

7. Un'equazione differenziale della forma:  $\frac{d^n x}{dt^n} + a_{n-1} \frac{d^{n-1}x}{dt^{n-1}} + \dots + a_1 \frac{dx}{dt} + a_0 x = 0$  può essere riscritta come un sistema di equazioni differenziali del primo ordine, mediante un semplice artificio. Precisamente, introduciamo funzioni incognite  $x_0, x_1, \dots, x_{n-1}$  con  $x = x_0$ , e poniamo:  $dx_i/dt = x_{i+1}$  per  $i = 0, \dots, n-2$ . L'equazione di partenza  $= -(a_{n-1}x_{n-1} + \dots + a_1x_1 + a_0x)$ . Determinare la matrice che rappresenta tale sistema di equazioni.

8. (a) Riscrivere l'equazione lineare del secondo ordine in una variabile:

$$\frac{d^2 x}{dt^2} + b \frac{dx}{dt} + cx = 0,$$

come un sistema di due equazioni del primo ordine in due incognite:  $x_0 = x$ ,  $x_1 = dx/dt$ .

- (b) Risolvere tale sistema per  $b = -4$  e  $c = 3$ .

9. Sia  $A$  una matrice  $n \times n$ , e sia  $B(t)$  un vettore colonna di funzioni continue nell'intervallo  $[\alpha, \beta]$ . Si ponga, per definizione:  $F(t) = \int_{\alpha}^t e^{-tA} B(t) dt$ .

- (a) Dimostrare che  $X = F(t)$  è una soluzione dell'equazione differenziale:  $X' = AX + B(t)$  nell'intervallo  $(\alpha, \beta)$ .

- (b) Determinare tutte le soluzioni di tale equazione nell'intervallo.

### 8 L'esponenziale di una matrice

1. Calcolare  $e^A$  per le seguenti matrici  $A$ :

(a)  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ ; (b)  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ .

2. Sia  $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ .

- (a) Calcolare  $e^A$  direttamente dallo sviluppo.

- (b) Calcolare  $e^A$  diagonalizzando la matrice.

3. Calcolare  $e^A$  per le seguenti matrici  $A$ :

(a)  $\begin{bmatrix} 0 & -b \\ b & 0 \end{bmatrix}$ ; (b)  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ ; (c)  $\begin{bmatrix} 0 & 1 & & \\ & \ddots & 1 & \\ & & \ddots & \ddots \\ & & & 0 \end{bmatrix}$ .

4. Calcolare  $e^A$  per le seguenti matrici  $A$ :

(a)  $\begin{bmatrix} 2\pi i & 2\pi i \\ 2\pi i & 2\pi i \end{bmatrix}$ ; (b)  $\begin{bmatrix} 6\pi i & 4\pi i \\ 2\pi i & 8\pi i \end{bmatrix}$ .

Sia  $A$  una matrice  $n \times n$ . Dimostrare che l'applicazione  $t \mapsto e^{tA}$  è un omomorfismo dal gruppo additivo  $\mathbb{R}$  a  $GL_n(\mathbb{C})$ .

6. Trovare due matrici  $A, B$  tali che  $e^{A+B} \neq e^A e^B$ .

7. Dimostrare la formula:  $e^{\text{tr } A} = \det(e^A)$ , dove  $\text{tr } A$  denota la traccia di  $A$ .

8. Risolvere l'equazione differenziale:  $\frac{dX}{dt} = AX$ , con  $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$ .

9. Sia  $f(t)$  un polinomio, e sia  $T$  un operatore lineare. Dimostrare che  $f(T)$  è un operatore lineare.

10. Sia  $A$  una matrice simmetrica, e sia  $f(t)$  un polinomio. Dimostrare che  $f(A)$  è una matrice simmetrica.

11. Dimostrare la regola del prodotto per la derivata di funzioni a valori matriciali.

12. Siano  $A(t)$ ,  $B(t)$  funzioni a valori matriciali derivabili rispetto a  $t$ . Calcolare le seguenti funzioni:

(a)  $\frac{d}{dt}(A^3(t))$ ;

(b)  $\frac{d}{dt}(A^{-1}(t))$ , supponendo che  $A(t)$  sia invertibile per ogni  $t$ ;

(c)  $\frac{d}{dt}(A^{-1}(t)B(t))$ .

13. Sia  $X$  un autovettore di una matrice  $n \times n$   $A$ , con autovalore  $\lambda$ .

- (a) Dimostrare che, se  $A$  è invertibile, allora  $X$  è un autovettore anche per  $A^{-1}$  e il suo autovalore è  $\lambda^{-1}$ .

- (b) Sia  $p(t)$  un polinomio. Allora  $X$  è un autovettore per  $p(A)$ , con autovalore  $p(\lambda)$ .

- (c) Dimostrare che  $X$  è un autovettore per  $e^A$ , con autovalore  $e^\lambda$ .

14. Per una matrice  $n \times n$   $A$ , si definiscono le matrici  $\sin A$  e  $\cos A$ , utilizzando gli sviluppi in serie di Taylor di  $\sin x$  e  $\cos x$ .

- (a) Dimostrare che tali serie convergono per ogni  $A$ .

- (b) Dimostrare che  $\sin tA$  è una funzione derivabile rispetto a  $t$  e che risulta:  $d(\sin tA)/dt = A \cos tA$ .

15. Discutere il campo di validità delle seguenti identità:

(a)  $\cos^2 A + \sin^2 A = I$ ;

(b)  $e^{iA} = \cos A + i \sin A$ ;

(c)  $\sin(A+B) = \sin A \cos B + \cos A \sin B$ ;

(d)  $\cos(A+B) = \cos A \cos B - \sin A \sin B$ ;

(e)  $e^{2\pi i A} = I$ ;

(f)  $d(e^{A(t)})/dt = e^{A(t)} A'(t)$ , essendo  $A(t)$  una funzione a valori matriciali derivabile rispetto a  $t$ .

16. (a) Dimostrare la regola del prodotto per la derivata di funzioni a valori complessi in due modi: direttamente, e scrivendo  $x(t) = u(t) + iv(t)$  e applicando poi la regola del prodotto per le funzioni a valori reali.
- (b) Sia  $f(t)$  una funzione di una variabile reale  $t$  a valori complessi, e sia  $\varphi(u)$  una funzione di  $u$  a valori reali. Enunciare e dimostrare la regola della derivazione della funzione composta per  $f(\varphi(u))$ .
17. (a) Sia  $B_k$  una successione di matrici  $m \times n$  convergente ad una matrice  $B$ , e sia  $P$  una matrice  $m \times m$ . Dimostrare che  $PB_k$  converge a  $PB$ .
- (b) Provare che, se  $m = n$  e  $P$  è invertibile, allora la successione  $PB_kP^{-1}$  converge a  $PBP^{-1}$ .
18. Sia  $f(x) = \sum c_k x^k$  una serie di potenze tale che  $\sum c_k A^k$  converge quando  $A$  è una matrice  $n \times n$  sufficientemente piccola. Dimostrare che  $A$  e  $f(A)$  commutano tra loro.
19. Determinare  $\frac{d}{dt} \det A(t)$ , essendo  $A(t)$  una funzione a valori matriciali derivabile rispetto a  $t$ .

*Esercizi vari*

1. Quali sono gli autovalori possibili di un operatore lineare  $T$  tale che:
- (a)  $T^r = I$ , (b)  $T^r = 0$ , (c)  $T^2 - 5T + 6 = 0$ ?
2. Un operatore lineare  $T$  si dice *nilpotente* se qualche potenza di  $T$  è zero.
- (a) Dimostrare che  $T$  è nilpotente se e soltanto se il suo polinomio caratteristico è  $t^n$ , con  $n = \dim V$ .
- (b) Dimostrare che, se  $T$  è un operatore nilpotente su uno spazio vettoriale di dimensione  $n$ , allora  $T^n = 0$ .
- (c) Un operatore lineare  $T$  si dice *unipotente* se  $T - I$  è nilpotente. Determinare il polinomio caratteristico di un operatore unipotente. Quali sono i suoi autovalori possibili?
3. Sia  $A$  una matrice complessa  $n \times n$ . Provare che, se  $\operatorname{tr} A^i = 0$  per ogni  $i$ , allora  $A$  è nilpotente.
- \*4. Siano  $A, B$  matrici complesse  $n \times n$ , e sia  $C = AB - BA$ . Dimostrare che, se  $C$  commuta con  $A$ , allora  $C$  è nilpotente.
5. Siano  $\lambda_1, \dots, \lambda_n$  le radici del polinomio caratteristico  $p(t)$  di una matrice complessa  $A$ . Dimostrare le formule:  $\operatorname{tr} A = \lambda_1 + \dots + \lambda_n$  e  $\det A = \lambda_1 \cdots \lambda_n$ .
6. Sia  $T$  un operatore lineare su uno spazio vettoriale reale  $V$  tale che  $T^2 = I$ . Si considerino i seguenti sottospazi:
- $$W^+ = \{v \in V \mid T(v) = v\}, \quad W^- = \{v \in V \mid T(v) = -v\}.$$
- Dimostrare che  $V$  è isomorfo alla somma diretta  $W^+ \oplus W^-$ .
7. La norma di Frobenius  $|A|$  di una matrice  $n \times n$   $A$  è definita come la lunghezza di  $A$ , considerata come un vettore  $n^2$ -dimensionale, ossia:  $|A|^2 = \sum |a_{ij}|^2$ . Dimostrare le seguenti diseguaglianze:  $|A + B| \leq |A| + |B|$  e  $|AB| \leq |A||B|$ .

- Sia  $T : V \rightarrow V$  un operatore lineare su uno spazio vettoriale di dimensione finita  $V$ . Dimostrare che esiste un intero  $n$  tale che:  $(\ker T^n) \cap (\operatorname{im} T^n) = 0$ .
- Quali matrici infinite rappresentano gli operatori lineari sullo spazio  $Z$  [cap. 3 (5.2d)?]
10. I minori  $k \times k$  di una matrice  $m \times n$   $A$  sono le sottomatrici quadrate ottenute cancellando  $m-k$  righe e  $n-k$  colonne. Sia  $A$  una matrice di rango  $r$ . Dimostrare che qualche minore  $r \times r$  è invertibile e che nessun minore  $(r+1) \times (r+1)$  è invertibile.
11. Sia  $\varphi : F^n \rightarrow F^m$  la moltiplicazione a sinistra per una matrice  $m \times n$   $A$ . Dimostrare che le seguenti condizioni sono equivalenti:
- (a)  $A$  ha un'inversa destra, ossia una matrice  $B$  tale che  $AB = I$ .
  - (b)  $\varphi$  è suriettiva.
  - (c) Esiste un minore  $m \times m$  di  $A$  il cui determinante è diverso da zero.
12. Sia  $\varphi : F^n \rightarrow F^m$  la moltiplicazione a sinistra per una matrice  $m \times n$   $A$ . Dimostrare che le seguenti condizioni sono equivalenti:
- (a)  $A$  ha un'inversa sinistra, ossia una matrice  $B$  tale che  $BA = I$ .
  - (b)  $\varphi$  è iniettiva.
  - (c) Esiste un minore  $n \times n$  di  $A$  il cui determinante è diverso da zero.
- \*13. Sia  $A$  una matrice  $n \times n$  tale che  $A^r = I$ . Dimostrare che, se  $A$  ha un solo autovalore  $\zeta$ , allora  $A = \zeta I$ .
14. (a) Senza utilizzare il polinomio caratteristico, dimostrare che un operatore lineare su uno spazio vettoriale di dimensione  $n$  può avere al più  $n$  autovalori distinti.
- (b) Utilizzare (a) per provare che un polinomio di grado  $n$  a coefficienti in un campo  $F$  ha al più  $n$  radici in  $F$ .
15. Sia  $A$  una matrice  $n \times n$ , e sia  $p(t) = t^n + c_{n-1}t^{n-1} + \dots + c_1t + c_0$  il suo polinomio caratteristico. Il teorema di Cayley-Hamilton afferma che:
- $$p(A) = A^n + c_{n-1}A^{n-1} + \dots + c_1A + c_0I = 0.$$
- (a) Dimostrare il teorema di Cayley-Hamilton per le matrici  $2 \times 2$ .
- (b) Dimostrarlo per le matrici diagonali.
- (c) Dimostrarlo per le matrici diagonalizzabili.
- \*16. (d) Dimostrare che ogni matrice complessa  $n \times n$  è arbitrariamente vicina ad una matrice diagonalizzabile, e utilizzare questo fatto per estendere per continuità la dimostrazione per le matrici diagonalizzabili a tutte le matrici complesse.
16. (a) Utilizzare il teorema di Cayley-Hamilton per scrivere un'espressione di  $A^{-1}$  in termini di  $A$ ,  $(\det A)^{-1}$  e i coefficienti del polinomio caratteristico.
- (b) Verificare tale espressione nel caso  $2 \times 2$  con un calcolo esplicito.
17. Sia  $A$  una matrice  $2 \times 2$ . Il teorema di Cayley-Hamilton permette di scrivere tutte le potenze di  $A$  come combinazioni lineari di  $I$  e  $A$ . Pertanto è plausibile che anche  $e^A$  sia una tale combinazione lineare.

(a) Dimostrare che, se  $a, b$  sono gli autovalori di  $A$  e se  $a \neq b$ , allora:

$$e^A = \frac{ae^b - be^a}{a - b} I + \frac{e^a - e^b}{a - b} A.$$

(b) Trovare la formula corretta nel caso in cui  $A$  ha due autovalori uguali.

- 18.** I numeri di Fibonacci  $0, 1, 1, 2, 3, 5, 8, \dots$  sono definiti mediante la relazione ricorsiva:  $f_n = f_{n-1} + f_{n-2}$ , con le condizioni iniziali:  $f_0 = 0$ ,  $f_1 = 1$ . Tale relazione ricorsiva può essere scritta in forma matriciale:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} f_{n-2} \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} f_{n-1} \\ f_n \end{bmatrix}.$$

(a) Dimostrare la formula:

$$f_n = \frac{1}{\alpha} \left[ \left( \frac{1+\alpha}{2} \right)^n - \left( \frac{1-\alpha}{2} \right)^n \right],$$

dove  $\alpha = \sqrt{5}$ .

(b) Supponiamo che la successione  $\{a_n\}$  sia definita mediante la relazione:  $a_n = \frac{1}{2}(a_{n-1} + a_{n-2})$ . Calcolare  $\lim a_n$  in termini di  $a_0, a_1$ .

- \*19.** Sia  $A$  una matrice reale positiva  $n \times n$ , e sia  $X \in \mathbb{R}^n$  un vettore colonna. Utilizziamo le notazioni abbreviate  $X > 0$  e  $X \geq 0$  per indicare che gli elementi del vettore  $X$  sono positivi oppure non negativi, rispettivamente. Per “quadrante positivo” intendiamo l’insieme dei vettori  $X \geq 0$ . (Tuttavia si noti che  $X \geq 0$  e  $X \neq 0$  non implicano  $X > 0$ , nel nostro senso.)

(a) Dimostrare che, se  $X \geq 0$  e  $X \neq 0$ , allora  $AX > 0$ .

(b) Si denoti con  $C$  l’insieme delle coppie ordinate  $(X, t)$ , con  $t \in \mathbb{R}$ , tali che  $X \geq 0$ ,  $|X| = 1$  e  $(A - tI)X \geq 0$ . Dimostrare che  $C$  è un sottoinsieme compatto di  $\mathbb{R}^{n+1}$ .

(c) La funzione  $t$  assume un valore massimo su  $C$ , diciamo nel punto  $(X_0, t_0)$ . Allora  $(A - t_0 I)X_0 \geq 0$ . Dimostrare che  $(A - t_0 I)X_0 = 0$ .

(d) Dimostrare che  $X_0$  è un autovettore con autovalore  $t_0$ , facendo vedere che altrimenti il vettore  $AX_0 = X_1$  contraddirebbe la massimalità di  $t_0$ .

(e) Dimostrare che  $t_0$  è l’autovalore di  $A$  con il più grande valore assoluto.

- \*20.** Sia  $A = A(t)$  una matrice di funzioni. Cos’è che non va bene quando si cerca di dimostrare che, in analogia col caso  $n = 1$ , la matrice

$$\exp \left( \int_{t_0}^t A(u) du \right)$$

è una soluzione del sistema:  $dX/dt = AX$ ? È possibile trovare delle condizioni sulla funzione a valori matriciali  $A(t)$ , affinché la matrice scritta sopra risulti una soluzione?

## Capitolo 5 Simmetria

L’algebra non è che geometria scritta; la geometria non è che algebra figurata.

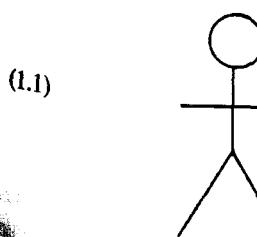
Sophie Germain

Lo studio della simmetria fornisce una delle più belle applicazioni della teoria dei gruppi. I gruppi furono inventati innanzitutto per analizzare le simmetrie di certe strutture algebriche chiamate estensioni di campi, e poiché la simmetria è un fenomeno che si presenta comunemente in tutte le scienze, costituisce ancora uno dei due modi principali in cui viene applicata la teoria dei gruppi. L’altro modo riguarda le rappresentazioni dei gruppi, e verrà discusso nel capitolo 9. Nei primi quattro paragrafi di questo capitolo studieremo la simmetria delle figure piane mediante i gruppi di movimenti rigidi del piano. Le figure piane forniscono una ricca fonte di esempi e un ambiente per la nozione generale di *azione di un gruppo*, che verrà introdotta nel paragrafo 5.

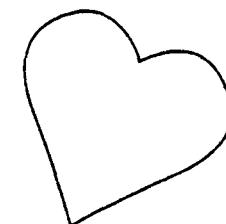
In questo capitolo, utilizzeremo argomentazioni di tipo geometrico, ma senza preoccuparci di risalire agli assiomi della geometria.

### 1 Simmetria delle figure piane

Le simmetrie possibili delle figure piane vengono classificate di solito nei seguenti tipi principali, descritti nelle figure (1.1-1.3):

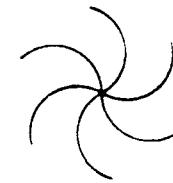
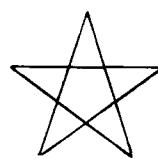


(1.1)



Simmetria bilaterale.

(1.2)



(1.3)

Simmetria di rotazione.



Simmetria di traslazione.

Esiste anche un quarto tipo di simmetria, anche se un po' meno familiare:

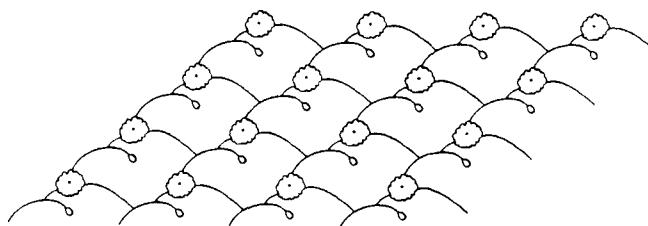
(1.4)



Simmetria di glissoriflessione.

Figure come i disegni delle carte da parati possono avere due simmetrie di traslazione indipendenti, come mostra la figura (1.5):

(1.5)



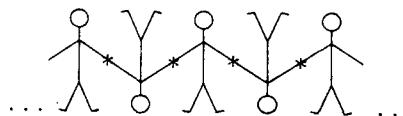
Possono presentarsi inoltre altre combinazioni di simmetrie. Per esempio, la stella possiede simmetria bilaterale e simmetria di rotazione. La figura (1.6) è un esempio in cui sono combinate la simmetria di traslazione e la simmetria di rotazione:

(1.6)



Un altro esempio è illustrato dalla figura (1.7):

(1.7)



si ricorderà (cfr. cap. 4 § 5) si dice che un'applicazione  $m : P \rightarrow P$  del piano  $P$  in sé è un *movimento rigido*, o un'*isometria*, se conserva le distanze, cioè se, dati due punti  $p, q \in P$ , la distanza da  $p$  a  $q$  è uguale alla distanza da  $m(p)$  a  $m(q)$ . Dimostreremo nel prossimo paragrafo che i movimenti rigidi sono le *traslazioni*, le rotazioni, le riflessioni e le glissoriflessioni. Essi formano un gruppo  $M$ , la cui legge di composizione è la composizione di applicazioni.

Se un movimento rigido  $m$  porta un sottoinsieme  $F$  del piano in sé, si dice che  $m$  è una *simmetria* di  $F$ . L'insieme di tutte le simmetrie di  $F$  costituisce sempre un sottogruppo  $G$  di  $M$ , chiamato il *gruppo delle simmetrie* della figura  $F$ . È chiaro che  $G$  è un sottogruppo. Infatti, se  $m$  e  $m'$  portano  $F$  in  $F$ , allora anche l'applicazione composta  $mm'$  porta  $F$  in  $F$ , e così via.

Il gruppo delle simmetrie della figura (1.1), dotata di simmetria bilaterale, è formato da due elementi: l'identità  $1$  e la riflessione  $r$  intorno a una retta chiamata *asse di simmetria*. Vale la relazione:  $rr = 1$ , ciò che prova che  $G$  è un gruppo ciclico di ordine 2, come deve essere, poiché non esistono altri gruppi di ordine 2.

Il gruppo delle simmetrie della figura (1.3) è un gruppo ciclico infinito generato dal movimento che sposta la figura a sinistra di un'unità. Si dice che un movimento siffatto è una *traslazione*  $t$ , sicché:

$$G = \{\dots, t^{-2}, t^{-1}, 1, t, t^2, \dots\}.$$

I gruppi di simmetria delle figure (1.4), (1.6), (1.7) contengono altri elementi oltre le traslazioni e pertanto sono più ampi. È un buon esercizio descrivere i loro elementi.

## 2 Il gruppo dei movimenti del piano

In questo paragrafo viene descritto il gruppo  $M$  di tutti i movimenti rigidi del piano. La distinzione più grossolana è tra movimenti che *conservano l'orientazione* e movimenti che *invertono l'orientazione* (questi ultimi ribaltano il piano: cfr. cap. 4, § 5). In base a questa partizione di  $M$  possiamo definire un'applicazione:

$$M \rightarrow \{\pm 1\},$$

la quale manda i movimenti che conservano l'orientazione in  $1$  e quelli che la invertono in  $-1$ . Non è difficile convincersi che tale applicazione è un omomorfismo di gruppi: il prodotto di due movimenti che invertono l'orientazione è un movimento che conserva l'orientazione, e così via.

Una classificazione più fine è la seguente:

(2.1) (a) *Movimenti che conservano l'orientazione:*

*Traslazione:* movimento parallelo del piano mediante un vettore  $a$ :  $p \mapsto p + a$ .

*Rotazione:* movimento che ruota il piano di un angolo  $\theta \neq 0$  intorno a un punto.

(b) *Movimenti che invertono l'orientazione:*

*Riflessione* intorno a una retta  $\ell$ .

*Glissoriflessione:* movimento ottenuto componendo una riflessione intorno a una retta  $\ell$  e una traslazione mediante un vettore non nullo  $a$  parallelo a  $\ell$ .

(2.2) **TEOREMA** *L'elenco precedente comprende tutti i casi possibili. Ogni movimento rigido del piano è una traslazione, o una rotazione, o una riflessione, o una glissoriflessione, oppure l'identità.*

Questo risultato è davvero notevole. Una sua conseguenza è che la composizione di due rotazioni intorno a due punti distinti è una rotazione intorno a un terzo punto, oppure è una traslazione. Ciò segue dal teorema, poiché la composizione conserva l'orientazione, tuttavia non è ovvio.

Alcune delle altre composizioni sono più facili da visualizzare. La composizione di due rotazioni di angoli  $\theta$  e  $\eta$  intorno a uno stesso punto è ancora una rotazione, di angolo  $\theta + \eta$ , intorno a quel punto. La composizione di due traslazioni mediante vettori  $a$  e  $b$  è la traslazione mediante il vettore somma  $a + b$ .

Si noti che una traslazione non lascia fisso alcun punto (a meno che il vettore  $a$  non sia il vettore nullo, nel qual caso essa è l'identità) e così pure le glissoriflessioni non hanno punti fissi. Inoltre, una rotazione lascia fisso un unico punto, il centro di rotazione, e una riflessione lascia fissi i punti sulla retta di riflessione, quindi la composizione di due riflessioni intorno a due rette non parallele  $\ell_1, \ell_2$  è una rotazione intorno al punto di intersezione  $p = \ell_1 \cap \ell_2$ . Ciò segue dal teorema, poiché la composizione lascia fisso  $p$  e conserva l'orientazione. La composizione di due riflessioni intorno a rette parallele è una traslazione mediante un vettore ortogonale alle rette.

Per dimostrare il teorema (2.2), e per poter eseguire agevolmente i calcoli nel gruppo  $M$ , sceglieremo alcuni movimenti particolari come generatori per il gruppo. Otterremo delle relazioni simili alle (1.18) del capitolo 2, che definiscono il gruppo simmetrico  $S_3$ , ma essendo  $M$  infinito, saranno più numerose.

Identifichiamo il piano con lo spazio  $\mathbf{R}^2$  dei vettori colonna, scegliendo un sistema di coordinate, poi prendiamo come generatori le traslazioni, le rotazioni intorno all'origine e la riflessione intorno all'asse  $x_1$ :

2.3)

(a) *Traslazione  $t_a$  mediante un vettore  $a$ :*  $t_a(x) = x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$ .

(b) *Rotazione  $\rho_\theta$  di un angolo  $\theta$  intorno all'origine:*

$$\rho_\theta(x) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

(c) *Riflessione  $r$  intorno all'asse  $x_1$ :*  $r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$ .

Poiché lasciano fissa l'origine, le rotazioni  $\rho_\theta$  e la riflessione  $r$  sono operatori ortogonali su  $\mathbf{R}^2$ . Una traslazione non è un operatore lineare, infatti non manda il vettore nullo in sé, a meno che, naturalmente, non si tratti della traslazione mediante il vettore nullo.

I movimenti (2.3) non sono tutti gli elementi di  $M$ . Per esempio, essi non comprendono le rotazioni intorno a un punto diverso dall'origine e neppure le riflessioni intorno ad altre rette. Tuttavia, essi generano il gruppo, ossia ogni elemento di  $M$  è un prodotto di questi elementi. Si vede facilmente che ogni movimento rigido  $m$  può essere ottenuto da essi, per composizione. Precisamente, si ha:

$$(2.4) \quad m = t_a \rho_\theta \quad \text{oppure} \quad m = t_a \rho_\theta r,$$

per qualche vettore  $a$  e qualche angolo  $\theta$ , eventualmente nulli. Per verificare ciò, ricordiamo che ogni movimento rigido è la composizione di un operatore ortogonale e di una traslazione [cap. 4 (5.20)], quindi possiamo scrivere  $m$  nella forma:  $m = t_a m'$ , dove  $m'$  è un operatore ortogonale. Ora, se  $\det m' = 1$ , allora  $m'$  è una delle rotazioni  $\rho_\theta$  (ciò segue dal teorema (5.5) del capitolo 4) pertanto, in questo caso,  $m = t_a \rho_\theta$ . Infine, se  $\det m' = -1$ , allora  $\det m' r = 1$ , sicché  $m' r$  è una rotazione  $\rho_\theta$ . Poiché  $r^2 = 1$ , in tal caso  $m' = \rho_\theta r$ , e  $m = t_a \rho_\theta r$ .

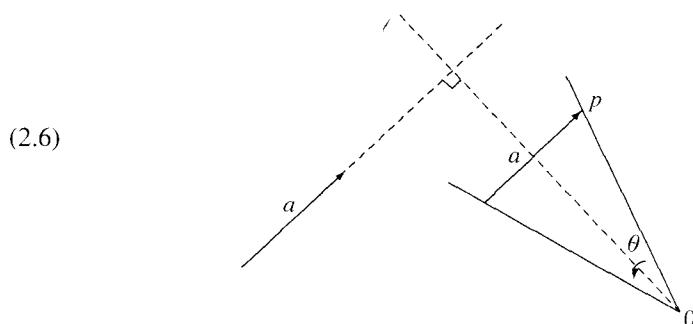
L'espressione di un movimento  $m$  come un prodotto (2.4) è unica. Infatti, supponiamo che  $m$  sia espresso in due modi:  $m = t_a \rho_\theta r^i = t_b \rho_\eta r^j$ , dove  $i, j$  sono 0 o 1. Poiché  $m$  conserva l'orientazione se  $i = 0$  e inverte l'orientazione se  $i = 1$ , risulta necessariamente  $i = j$ , e quindi possiamo cancellare  $r$  in entrambi i membri, se necessario, per ottenere l'uguaglianza:  $t_a \rho_\theta = t_b \rho_\eta$ . Moltiplicando entrambi i membri a sinistra per  $t_{-b}$  e a destra per  $\rho_{-\theta}$ , si ottiene:  $t_{a-b} = \rho_{\eta-\theta}$ . Ma una traslazione non è una rotazione, a meno che entrambi non siano l'identità. Dunque  $a = b$  e  $\theta = \eta$ . ■

I calcoli in  $M$  possono essere effettuati con i simboli  $t_a, \rho_\theta, r$ , utilizzando regole di composizione che possono essere ottenute a partire dalle formule (2.3). Le regole necessarie sono le seguenti:

$$(2.5) \quad \begin{aligned} t_a t_b &= t_{a+b}, & \rho_\theta \rho_\eta &= \rho_{\theta+\eta}, & rr &= 1, \\ \rho_\theta t_a &= t_{a'} \rho_\theta, & \text{dove } a' &= \rho_\theta(a), \\ rt_a &= t_{a'} r, & \text{dove } a' &= r(a), \\ r\rho_\theta &= \rho_{-\theta} r. \end{aligned}$$

Utilizzando queste regole, possiamo ridurre un qualsiasi prodotto di generatori a una delle due forme (2.4). La forma così ottenuta è univocamente determinata, poiché vi è un'unica espressione della forma (2.4) per un dato movimento.

*Dimostrazione del teorema (2.2).* Sia  $m$  un movimento rigido che conserva l'orientazione, ma non è una traslazione. Vogliamo dimostrare che  $m$  è una rotazione intorno a un punto. È chiaro che un movimento che conserva l'orientazione lasciando fisso un punto  $p$  nel piano dev'essere una rotazione intorno a  $p$ . Dunque dobbiamo far vedere che ogni movimento  $m$  che conserva l'orientazione e non è una traslazione lascia fisso qualche punto. Scriviamo:  $m = t_a \rho_\theta$ , come in (2.4). Per ipotesi,  $\theta \neq 0$ . Possiamo utilizzare la rappresentazione geometrica illustrata nella figura (2.6) per trovare il punto fisso. In essa,  $\ell$  è la retta per l'origine perpendicolare ad  $a$ , e il settore di angolo  $\theta$  è disposto in modo da essere bisecato da  $\ell$ . Il punto  $p$  si determina inserendo il vettore  $a$  nel settore, come mostrato in figura. Per verificare che  $m$  lascia fisso  $p$ , basta ricordare che l'operazione  $\rho_\theta$  è quella che viene effettuata per prima, ed è seguita da  $t_a$ .



Punto fisso di un movimento che conserva l'orientazione.

Un altro modo per trovare il punto fisso consiste nel risolvere algebricamente l'equazione  $x = t_a \rho_\theta(x)$  in  $x$ . Per definizione di traslazione,  $t_a(\rho_\theta(x)) = \rho_\theta(x) + a$ .

Pertanto l'equazione che occorre risolvere è  $x - \rho_\theta(x) = a$ , ossia

$$(2.7) \quad \begin{bmatrix} 1 - \cos \theta & \sin \theta \\ -\sin \theta & 1 - \cos \theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

Si noti che  $\det(1 - \rho_\theta) = 2 - 2 \cos \theta$ . Se  $\theta \neq 0$  il determinante è non nullo e pertanto vi è un'unica soluzione per  $x$ .

(2.8) COROLLARIO Il movimento  $m = t_a \rho_\theta$  è la rotazione di un angolo  $\theta$  intorno al suo punto fisso.

*Dimostrazione.* Come si è appena visto, il punto fisso di  $m$  è quello che soddisfa la relazione  $p = \rho_\theta(p) + a$ . Allora, per ogni  $x$ , si ha:

$$m(p+x) = t_a \rho_\theta(p+x) = \rho_\theta(p+x) + a = \rho_\theta(p) + \rho_\theta(x) + a = p + \rho_\theta(x).$$

Dunque  $m$  manda  $p+x$  in  $p+\rho_\theta(x)$  e quindi è la rotazione intorno a  $p$  di un angolo  $\theta$ , come richiesto. ■

Passiamo ora a dimostrare che ogni movimento che inverte l'orientazione, diciamo  $m = t_a \rho_\theta r$ , è una glissoriflessione oppure una riflessione (la quale può essere considerata una glissoriflessione con vettore di spostamento nullo). Proveremo ciò trovando una retta  $\ell$  che  $m$  manda in se stessa, così che la restrizione di  $m$  a  $\ell$  sia una traslazione. È geometricamente evidente che un movimento che inverte l'orientazione e agisce in tal modo su una retta è una glissoriflessione.

La geometria in questo caso è più complicata e pertanto affronteremo il problema in due tappe. Innanzitutto, il movimento  $\rho_\theta r = r'$  è una riflessione intorno a una retta, e precisamente la retta che interseca l'asse  $x_1$  nell'origine, formando con esso un angolo di ampiezza  $\frac{1}{2}\theta$  (ciò non è difficile da vedere, geometricamente o algebricamente). Quindi il movimento  $m$  in esame è il prodotto della traslazione  $t_a$  e della riflessione  $r'$ . Con una rotazione degli assi coordinati possiamo far sì che l'asse  $x_1$  diventi la retta di riflessione di  $r'$ ; allora  $r'$  diventa la riflessione standard  $r$ , e la traslazione  $t_a$  rimane una traslazione, sebbene le coordinate del vettore  $a$  siano cambiate. Rispetto a questo nuovo sistema di coordinate, il movimento  $m$  si scrive nella forma:  $m = t_a r$ , ed opera nel modo seguente:

$$m \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 + a_1 \\ -x_2 + a_2 \end{bmatrix}.$$

Tale movimento manda la retta  $x_2 = \frac{1}{2}a_2$  in sé, mediante la traslazione

$$\left( x_1, \frac{1}{2}a_2 \right)^t \mapsto \left( x_1 + a_1, \frac{1}{2}a_2 \right)^t,$$

Pertanto è una glissoriflessione rispetto a questa retta. ■

Vi sono due sottogruppi notevoli di  $M$ , per i quali occorre introdurre delle notazioni:

(2.9)  $T$ , il gruppo delle traslazioni.

$\mathbf{O}$ , il gruppo degli operatori ortogonali.

Il gruppo  $\mathbf{O}$  è costituito dai movimenti che lasciano fissa l'origine. Esso contiene le rotazioni intorno all'origine e le riflessioni intorno alle rette passanti per l'origine.

Si noti che, fissato un sistema di coordinate nel piano, si ottiene una corrispondenza biunivoca:

$$(2.10) \quad \begin{aligned} \mathbb{R}^2 &\longrightarrow T \\ a &\longmapsto t_a. \end{aligned}$$

Essa è un isomorfismo del gruppo additivo  $\mathbb{R}^2$  con il sottogruppo  $T$ , poiché  $t_a t_b = t_{a+b}$ .

Gli elementi di  $\mathbf{O}$  sono operatori lineari. Utilizzando ancora il sistema di coordinate scelto, possiamo associare un elemento  $m \in \mathbf{O}$  alla sua matrice. In tal modo, otteniamo un isomorfismo:

$$O_2 \xrightarrow{\sim} \mathbf{O}$$

dal gruppo  $O_2$  delle matrici  $2 \times 2$  ortogonali a  $\mathbf{O}$  [cfr. cap. 4, (5.16)].

Possiamo considerare inoltre il sottogruppo di  $M$  costituito dai movimenti che lasciano fisso un punto del piano diverso dall'origine. Tale sottogruppo è collegato a  $\mathbf{O}$  nel modo seguente:

### (2.11) PROPOSIZIONE

(a) Sia  $p$  un punto del piano. Denotiamo con  $\rho'_\theta$  la rotazione intorno a  $p$  di un angolo  $\theta$  e con  $r'$  la riflessione intorno alla retta passante per  $p$  e parallela all'asse  $x$ . Allora risulta:

$$\rho'_\theta = t_p \rho_\theta t_p^{-1}, \quad r' = t_p r t_p^{-1}.$$

(b) Il sottogruppo di  $M$  costituito dai movimenti che lasciano fisso  $p$  è il sottogruppo coniugato:

$$\mathbf{O}' = t_p \mathbf{O} t_p^{-1}.$$

*Dimostrazione.* Per ottenere la rotazione  $\rho'_\theta$ , innanzitutto trasportiamo il punto  $p$  nell'origine, poi facciamo ruotare il piano intorno all'origine di un angolo  $\theta$  e infine riportiamo l'origine in  $p$ :

$$\rho'_\theta = t_p \rho_\theta t_p^{-1} = t_p \rho_\theta t_p^{-1}.$$

La riflessione  $r'$  può essere ottenuta nello stesso modo a partire da  $r$ :

$$r' = t_p r t_p^{-1} = t_p r t_p^{-1}.$$

Ciò dimostra (a). Poiché ogni movimento che lascia fisso  $p$  ha la forma  $\rho'_\theta$  oppure  $\rho'_\theta r'$  [si veda la dimostrazione di (2.4)], (b) segue da (a). ■

Esiste un omomorfismo notevole  $\varphi$  da  $M$  a  $\mathbf{O}$ , con nucleo  $T$ , che si ottiene eliminando la traslazione dai prodotti (2.4):

$$(2.12) \quad \begin{aligned} M &\xrightarrow{\varphi} \mathbf{O} \\ t_a \rho_\theta &\longmapsto \rho_\theta \\ t_a \rho_\theta r &\longmapsto \rho_\theta r. \end{aligned}$$

Tale definizione può sembrare troppo semplicistica, ma le formule (2.5) dimostrano che  $\varphi$  è un omomorfismo:

$$(t_a \rho_\theta)(t_b \rho_\eta) = t_a t_b \rho_\theta \rho_\eta = t_{a+b} \rho_{\theta+\eta},$$

da cui:

$$\varphi(t_a \rho_\theta t_b \rho_\eta) = \rho_{\theta+\eta},$$

e così via. Poiché  $T$  è il nucleo di un omomorfismo è un sottogruppo normale di  $M$ .

Si noti che non è possibile definire, in modo analogo, un omomorfismo da  $M$  a  $T$ .

(2.13) PROPOSIZIONE Sia  $p$  un punto arbitrario del piano, e denotiamo con  $\rho'_\theta$  la rotazione intorno a  $p$  di un angolo  $\theta$ . Allora  $\varphi(\rho'_\theta) = \rho_\theta$ . Analogamente, se  $r'$  è la riflessione intorno alla retta passante per  $p$  e parallela all'asse  $x$ , allora  $\varphi(r') = r$ .

Ciò segue da (2.11a), perché  $t_p$  appartiene al nucleo di  $\varphi$ . La proposizione può essere enunciata anche nel modo seguente:

(2.14) L'omomorfismo  $\varphi$  non dipende dalla scelta dell'origine. ■

### 3 Gruppi finiti di movimenti

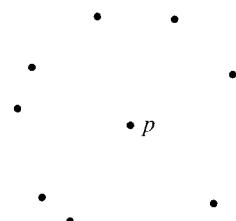
In questo paragrafo ci proponiamo di studiare i possibili gruppi finiti di simmetrie di figure quali la (1.1) e la (1.2). Siamo così condotti allo studio dei sottogruppi finiti  $G$  del gruppo  $M$  dei movimenti rigidi del piano.

L'osservazione fondamentale che permette di descrivere tutti i sottogruppi finiti è espressa dal seguente teorema:

(3.1) TEOREMA (Teorema del punto fisso) *Sia  $G$  un sottogruppo finito del gruppo dei movimenti  $M$ . Allora esiste un punto  $p$  nel piano che è lasciato fisso da ogni elemento di  $G$ , ossia esiste un punto  $p$  tale che  $g(p) = p$  per ogni  $g \in G$ .*

Ne segue, per esempio, che ogni sottogruppo di  $M$  che contiene rotazioni intorno a due punti distinti è infinito.

Ecco ora una bella dimostrazione geometrica del teorema. Sia  $s$  un punto del piano e sia  $S$  l'insieme dei punti che sono immagini di  $s$  rispetto ai vari movimenti di  $G$ . Pertanto ogni elemento  $s' \in S$  ha la forma:  $s' = g(s)$  per qualche  $g \in G$ . Tale insieme è chiamato l'*orbita* di  $s$  rispetto all'azione di  $G$ . L'elemento  $s$  appartiene all'orbita, poiché  $1$  sta in  $G$ , e  $s = 1(s)$ . Una tipica orbita è rappresentata qui sotto, nel caso in cui  $G$  è il gruppo delle simmetrie di un pentagono regolare.



Ogni elemento del gruppo  $G$  permuta l'orbita  $S$ . In altre parole, se  $s' \in S$  e  $x \in G$ , allora  $x(s') \in S$ . Infatti, sia  $s' = g(s)$ , con  $g \in G$ . Poiché  $G$  è un gruppo,  $xg \in G$ . Pertanto, per definizione,  $xg(s) \in S$ . Poiché  $xg(s) = x(s')$ , ciò prova che  $x(s') \in S$ .

Elenchiamo ora gli elementi di  $S$  in un ordine arbitrario, scrivendo  $S = \{s_1, \dots, s_n\}$ . Il punto fisso che andiamo cercando è il *centro di gravità* dell'orbita, definito da

$$(3.2) \quad p = \frac{1}{n} (s_1 + \dots + s_n),$$

dove l'espressione a secondo membro è calcolata mediante l'addizione tra vettori, in un arbitrario sistema di coordinate nel piano. Il centro di gravità dovrebbe essere considerato come una *media* dei punti  $s_1, \dots, s_n$ .

(3.3) LEMMA *Sia  $S = \{s_1, \dots, s_n\}$  un insieme finito di punti del piano, e sia  $p$  il suo centro di gravità, definito da (3.2). Sia  $m$  un movimento rigido, e poniamo  $m(s_i) = s'_i$  e  $m(p) = p'$ . Allora  $p' = \frac{1}{n} (s'_1 + \dots + s'_n)$ . In altre parole, i movimenti rigidi mandano centri di gravità in centri di gravità.*

**Dimostrazione.** Ciò è chiaro per ragioni fisiche, ma può essere dimostrato anche mediante i calcoli. Per fare questo, basta trattare separatamente i casi  $m = t_a$ ,  $m = \rho_\theta$  e  $m = r$ , poiché ogni movimento si ottiene da questi per composizione.

**Caso 1:**  $m = t_a$ . Allora  $p' = p + a$  e  $s'_i = s_i + a$ , e d'altra parte:

$$p + a = \frac{1}{n} ((s_1 + a) + \dots + (s_n + a)).$$

**Caso 2:**  $m = \rho_\theta$  oppure  $r$ . Allora  $m$  è un operatore lineare. Pertanto

$$\begin{aligned} p' &= m \left( \frac{1}{n} (s_1 + \dots + s_n) \right) = \frac{1}{n} (m(s_1) + \dots + m(s_n)) \\ &= \frac{1}{n} (s'_1 + \dots + s'_n). \blacksquare \end{aligned}$$

Il centro di gravità dell'insieme  $S$  è un punto fisso rispetto all'azione di  $G$ . Infatti, un elemento arbitrario  $g_i$  di  $G$  permuta l'orbita  $\{s_1, \dots, s_n\}$ , sicché il lemma 3.3 prova che esso manda il centro di gravità in sé. Ciò completa la dimostrazione del teorema. ■

Sia ora  $G$  un sottogruppo finito di  $M$ . Il teorema (3.1) ci assicura che esiste un punto lasciato fisso da ogni elemento di  $G$ , e possiamo scegliere le coordinate in modo tale che questo punto sia l'origine. Allora  $G$  risulterà un sottogruppo di **O**. Quindi, per descrivere i sottogruppi finiti  $G$  di  $M$ , basta descrivere i sottogruppi finiti di **O** (ossia, essendo **O** isomorfo al gruppo delle matrici  $2 \times 2$  ortogonali, i sottogruppi finiti del gruppo ortogonale  $O_2$ ). Tali sottogruppi sono descritti nel teorema seguente:

(3.4) TEOREMA *Sia  $G$  un sottogruppo finito del gruppo **O** dei movimenti rigidi che lasciano fissa l'origine. Allora  $G$  è uno dei gruppi seguenti:*

- (a)  $G = C_n$ , il gruppo ciclico di ordine  $n$ , generato dalla rotazione  $\rho_\theta$ , dove  $\theta = 2\pi/n$ .
- (b)  $G = D_n$ , il gruppo diedrale di ordine  $2n$ , generato da due elementi: la rotazione  $\rho_\theta$ , dove  $\theta = 2\pi/n$ , e una riflessione  $r'$  intorno a una retta per l'origine.

La dimostrazione è data alla fine del paragrafo (p. 197).

Il gruppo  $D_n$  dipende dalla retta di riflessione, ma naturalmente possiamo scegliere le coordinate in modo tale che essa diventi l'asse  $x$ , e allora  $r'$  diventa la riflessione standard  $r$ . Se pensiamo  $G$  come sottogruppo finito di  $M$ , dobbiamo spostare l'origine nel punto fisso, per poter applicare il teorema (3.4).

Pertanto il risultato finale relativo ai gruppi finiti di movimenti è il corollario seguente:

(3.5) COROLLARIO *Sia  $G$  un sottogruppo finito del gruppo dei movimenti  $M$ . Allora, introdotto un sistema di coordinate opportuno,  $G$  diventa uno dei gruppi  $C_n$  o  $D_n$ , dove  $C_n$  è generato da  $\rho_\theta$ , con  $\theta = 2\pi/n$ , e  $D_n$  è generato da  $\rho_\theta$  e  $r$ .*

Per  $n \geq 3$ , segue dal teorema che il gruppo diedrale  $D_n$  è il gruppo delle simmetrie di un poligono regolare di  $n$  lati. Infatti un poligono regolare di  $n$  lati ha un gruppo di simmetria che contiene la rotazione di  $2\pi/n$  intorno al suo centro, e contiene anche alcune riflessioni. Il teorema (3.4) ci assicura che esso è  $D_n$ .

I gruppi diedrali  $D_1, D_2$  sono troppo piccoli per essere i gruppi di simmetria di un poligono regolare di  $n$  lati, nel senso usuale.  $D_1$  è il gruppo  $\{1, r\}$  di due elementi, e quindi è un gruppo ciclico, come  $C_2$ . Tuttavia l'elemento non banale di  $D_1$  è una riflessione, mentre in  $C_2$  è la rotazione di  $\pi$ . Il gruppo  $D_2$  contiene i 4 elementi  $\{1, \rho, r, \rho r\}$ , dove  $\rho = \rho_\pi$  ed è isomorfo al gruppo quadrinomio di Klein. Volendo, si può pensare a  $D_1$  e  $D_2$  come ai gruppi delle simmetrie dell'1-agono e del 2-agono:



I gruppi diedrali costituiscono una classe importante di esempi, ed è utile avere per essi un insieme completo di relazioni che li definiscono. Esse possono essere ricavate direttamente dalla lista delle relazioni (2.5) che definiscono  $M$ . Denotiamo la rotazione  $\rho_\theta$  ( $\theta = 2\pi/n$ ) con  $x$ , e la riflessione  $r$  con  $y$ .

(3.6) PROPOSIZIONE *Il gruppo diedrale  $D_n$  è generato da due elementi  $x, y$  che soddisfano le relazioni:*

$$x^n = 1, \quad y^2 = 1, \quad yx = x^{-1}y.$$

*Gli elementi di  $D_n$  sono:*

$$\{1, x, x^2, \dots, x^{n-1}; y, xy, x^2y, \dots, x^{n-1}y\} = \{x^i y^j \mid 0 \leq i < n, 0 \leq j < 2\}.$$

*Dimostrazione.* Gli elementi  $x = \rho_\theta$  e  $y = r$  generano il gruppo  $D_n$ , per definizione. Le relazioni  $y^2 = 1$  e  $yx = x^{-1}y$  sono incluse nell'elenco delle relazioni (2.5) per  $M$ : esse sono  $rr = 1$  e  $r\rho_\theta = \rho_{-\theta}r$ . La relazione  $x^n = 1$  segue dal fatto che  $\theta = 2\pi/n$ , il che prova anche che gli elementi  $1, x, \dots, x^{n-1}$  sono distinti. Ne segue che anche gli elementi  $y, xy, x^2y, \dots, x^{n-1}y$  sono distinti, e quindi, poiché essi sono riflessioni, mentre le potenze di  $x$  sono rotazioni, non vi sono ripetizioni.

nella lista degli elementi. Infine, le relazioni possono essere usate per ridurre un prodotto arbitrario di  $x, y, x^{-1}, y^{-1}$  nella forma  $x^i y^j$ , con  $0 \leq i < n$ ,  $0 \leq j < 2$ . Pertanto la lista contiene tutti gli elementi del gruppo generato da  $x, y$ , e poiché tali elementi generano  $D_n$ , la lista è completa. ■

Utilizzando le prime due relazioni (3.6), la terza relazione può essere scritta in vari modi. Essa è equivalente a:

$$(3.7) \quad yx = x^{n-1}y \quad \text{oppure} \quad xyxy = 1.$$

Si noti che, per  $n = 3$ , le relazioni (3.6) coincidono con le relazioni che definiscono il gruppo simmetrico  $S_3$  [cap. 2, (1.18)].

(3.8) COROLLARIO *Il gruppo diedrale  $D_3$  e il gruppo simmetrico  $S_3$  sono isomorfi tra loro.* ■

Per  $n > 3$ , il gruppo diedrale e il gruppo simmetrico certamente non sono isomorfi, poiché  $D_n$  ha ordine  $2n$ , mentre  $S_n$  ha ordine  $n!$ .

*Dimostrazione del teorema (3.4).* Sia  $G$  un sottogruppo finito di  $\mathbf{O}$ . Occorre ricordare che gli elementi di  $\mathbf{O}$  sono le rotazioni  $\rho_\theta$  e le riflessioni  $\rho_\theta r$ .

*Caso 1:* Tutti gli elementi di  $G$  sono rotazioni. In tal caso, occorre provare che  $G$  è ciclico. La dimostrazione è simile a quella usata per determinare i sottogruppi del gruppo additivo  $\mathbf{Z}$  degli interi [cap. 2 (2.3)]. Se  $G = \{1\}$ , allora  $G = C_1$ . Altrimenti  $G$  contiene una rotazione non banale  $\rho_\theta$ . Sia  $\theta$  il più piccolo angolo di rotazione positivo tra gli elementi di  $G$ , allora  $G$  è generato da  $\rho_\theta$ . Infatti, sia  $\rho_\alpha$  un elemento arbitrario di  $G$ , dove l'angolo di rotazione  $\alpha$  è rappresentato, come al solito, da un numero reale. Sia  $n\theta$  il più grande multiplo intero di  $\theta$  minore di  $\alpha$ , sicché  $\alpha = n\theta + \beta$ , con  $0 \leq \beta < \theta$ . Poiché  $G$  è un gruppo e poiché  $\rho_\alpha$  e  $\rho_\theta$  sono elementi di  $G$ , anche il prodotto  $\rho_\beta = \rho_\alpha \rho_{-n\theta}$  è un elemento di  $G$ . Ma, per ipotesi,  $\theta$  è il più piccolo angolo di rotazione positivo in  $G$ , quindi  $\beta = 0$  e  $\alpha = n\theta$ . Ciò prova che  $G$  è ciclico. Sia  $n\theta$  il più piccolo multiplo di  $\theta$  che sia  $\geq 2\pi$ , sicché  $2\pi \leq n\theta < 2\pi + \theta$ . Poiché  $\theta$  è il più piccolo angolo di rotazione positivo in  $G$ , si ha:  $n\theta = 2\pi$ . Dunque  $\theta = 2\pi/n$  per qualche intero  $n$ .

*Caso 2:*  $G$  contiene una riflessione. A meno di un eventuale cambiamento di coordinate, possiamo supporre che la riflessione standard  $r$  appartenga a  $G$ . Indicando con  $H$  il sottogruppo delle rotazioni in  $G$ , possiamo applicare ciò che è stato dimostrato nel caso 1 al gruppo  $H$ , per concludere che esso è un gruppo ciclico:  $H = C_n$ . Allora i  $2n$  prodotti  $\rho_\theta^i, \rho_\theta^i r$ ,  $0 \leq i \leq n-1$ , appartengono a  $G$  e pertanto  $G$  contiene il gruppo diedrale  $D_n$ . Dobbiamo dimostrare che  $G = D_n$ . Ora, se un elemento  $g$  di  $G$  è una rotazione, allora  $g \in H$  per definizione di  $H$ ; dunque  $g$  è un elemento di  $D_n$ . Se  $g$  è una riflessione, allora  $g$  può essere scritto nella forma

$\rho_\alpha r$  per qualche rotazione  $\rho_\alpha$  (2.8). Poiché  $r$  è un elemento di  $G$ , tale risulta il prodotto  $\rho_\alpha rr = \rho_\alpha$ . Pertanto  $\rho_\alpha$  è una potenza di  $\rho_\theta$ , e anche  $g$  appartiene a  $D_n$ . Quindi  $G = D_n$ . Ciò completa la dimostrazione del teorema. ■

#### 4 Gruppi discreti di movimenti

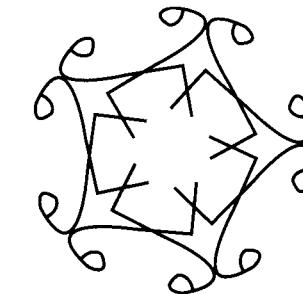
In questo paragrafo studieremo i gruppi delle simmetrie di figure illimitate quali i disegni delle carte da parati. Innanzitutto dobbiamo descrivere una condizione che sostituisca quella di finitezza per il gruppo, e che includa i gruppi di simmetria di figure illimitate interessanti. Ora una proprietà delle figure illustrate nel testo è che esse non ammettono traslazioni o rotazioni arbitrariamente piccole. Figure molto particolari, come la retta, hanno simmetrie di traslazione arbitrariamente piccole, e una circonferenza, per esempio, possiede simmetrie di rotazione arbitrariamente piccole. Ebbene, se si escludono tali figure, allora i gruppi di simmetrie possono essere classificati.

(4.1) DEFINIZIONE Un sottogruppo  $G$  del gruppo dei movimenti  $M$  si dice discreto se non contiene traslazioni o rotazioni arbitrariamente piccole. Più precisamente,  $G$  è discreto se esiste un numero reale  $\epsilon > 0$  tale che:

- (i) se  $t_a$  è una traslazione in  $G$  mediante un vettore non nullo  $a$ , allora la lunghezza di  $a$  è non minore di  $\epsilon$ :  $|a| \geq \epsilon$ ;
- (ii) se  $\rho$  è una rotazione in  $G$  intorno a un punto di un angolo non nullo  $\theta$ , allora l'ampiezza di  $\theta$  è non minore di  $\epsilon$ :  $|\theta| \geq \epsilon$ .

Poiché le traslazioni e le rotazioni esauriscono i movimenti che conservano l'orientazione (2.1), tale condizione si applica a tutti gli elementi di  $G$  che conservano l'orientazione. Non imponiamo condizioni alle riflessioni e alle glissoriflessioni, perché l'unica condizione che potremmo richiedere segue automaticamente dalla condizione imposta ai movimenti che conservano l'orientazione.

Il principio del caleidoscopio può essere usato per dimostrare che ogni gruppo discreto di movimenti è il gruppo delle simmetrie di una figura piana. (Non svilupperemo un'argomentazione rigorosa per dimostrarlo). Partiamo da una figura piana  $R$  "a caso", cioè che non abbia altre simmetrie al di fuori dell'identità. Allora ogni elemento  $g$  del gruppo in esame sposterà  $R$  in una posizione diversa, diciamo  $gR$ . La figura cercata  $F$  è l'unione di tutte le figure  $gR$ . Un elemento  $x$  di  $G$  manda  $gR$  in  $xgR$ , che è ancora un sottoinsieme di  $F$ , e quindi trasforma  $F$  in sé. Se  $R$  è sufficientemente arbitraria,  $G$  sarà il gruppo delle simmetrie di  $F$  (che può essere una figura estremamente suggestiva). Ecco qui il risultato dell'applicazione di questo procedimento nel caso in cui  $G$  è il gruppo diedrale delle simmetrie di un pentagono regolare:



Naturalmente figure diverse possono avere gli stessi gruppi oppure gruppi simili di simmetria. Tuttavia è interessante e istruttivo classificare le figure in base ai loro gruppi di simmetria. Esamineremo ora una prima classificazione di tali gruppi, che verrà ripresa e arricchita negli esercizi.

I due strumenti principali per studiare un gruppo discreto  $G$  sono il suo gruppo delle traslazioni e il suo gruppo puntuale. Il gruppo delle traslazioni di  $G$  è l'insieme dei vettori  $a$  tali che  $t_a \in G$ . Poiché  $t_a t_b = t_{a+b}$  e  $t_{-a} = t_a^{-1}$ , esso è un sottogruppo additivo dei vettori, che verrà denotato con  $L_G$ . Con una scelta opportuna delle coordinate, possiamo identificare lo spazio dei vettori con  $\mathbb{R}^2$ . Allora si ha:

$$(4.2) \quad L_G = \{a \in \mathbb{R}^2 \mid t_a \in G\}.$$

Tale gruppo è isomorfo al sottogruppo  $T \cap G$  delle traslazioni in  $G$ , mediante l'isomorfismo (2.10):  $a \mapsto t_a$ . Ora  $T \cap G$ , essendo un sottogruppo di  $G$ , è discreto, poiché un sottogruppo di un gruppo discreto è discreto. In  $L_G$  questa condizione diventa:

(4.3)  $L_G$  non contiene vettori di lunghezza  $< \epsilon$ , tranne il vettore nullo.

Un sottogruppo  $L$  del gruppo additivo  $\mathbb{R}^n$ , che soddisfa la condizione (4.3) per qualche  $\epsilon > 0$  è chiamato sottogruppo discreto di  $\mathbb{R}^n$ . Qui l'aggettivo "discreto" sta a significare che gli elementi di  $L$  sono separati da una distanza fissa:

(4.4) La distanza tra due vettori arbitrari  $a, b \in L$  è almeno  $\epsilon$ , se  $a \neq b$ .

Infatti, la distanza è la lunghezza di  $b - a$ , e  $b - a \in L$  poiché  $L$  è un sottogruppo.

(4.5) PROPOSIZIONE Ogni sottogruppo discreto  $L$  di  $\mathbb{R}^2$  ha una delle forme seguenti:

- (i)  $L = \{0\}$ .

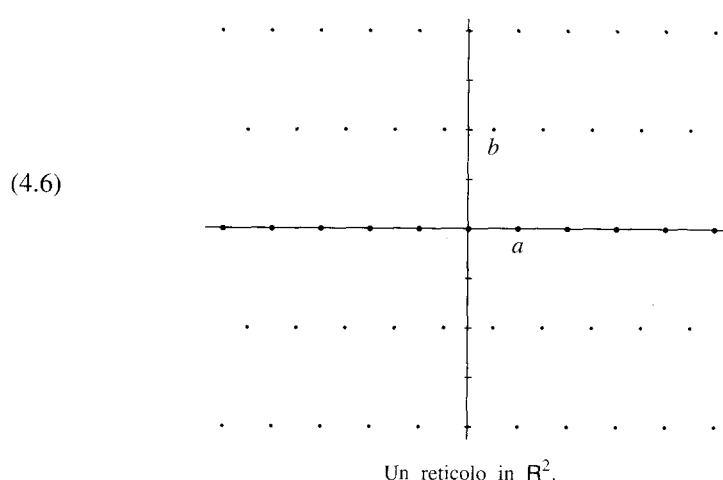
(b)  $L$  è generato come gruppo additivo da un vettore non nullo  $a$ :

$$L = \{ma \mid m \in \mathbf{Z}\}.$$

(c)  $L$  è generato da due vettori linearmente indipendenti  $a, b$ :

$$L = \{ma + nb \mid m, n \in \mathbf{Z}\}.$$

I gruppi del terzo tipo sono chiamati *reticolli piani*, e l'insieme di generatori  $(a, b)$  è chiamato *base del reticolo*.



Rimandiamo la dimostrazione della proposizione (4.5) e passiamo a esaminare il secondo strumento per studiare un gruppo discreto di movimenti: il suo gruppo puntuale. Ricordiamo che esiste un omomorfismo (2.12)  $\varphi: M \rightarrow \mathbf{O}$ , il cui nucleo è  $T$ . Se restringiamo tale omomorfismo a  $G$ , otteniamo un omomorfismo:

$$(4.7) \quad \varphi|_G: G \rightarrow \mathbf{O}.$$

Il suo nucleo è  $T \cap G$  (che è un sottogruppo isomorfo al gruppo delle traslazioni  $L_G$ ). Il gruppo puntuale  $\bar{G}$  è l'immagine di  $G$  in  $\mathbf{O}$ . Dunque  $\bar{G}$  è un sottogruppo di  $\mathbf{O}$ .

Per definizione, una rotazione  $\rho_\theta$  appartiene a  $\bar{G}$ , se  $G$  contiene qualche elemento della forma  $t_a \rho_\theta$ . D'altra parte, abbiamo visto (2.8) che  $t_a \rho_\theta$  è una rotazione di un angolo  $\theta$  intorno a qualche punto del piano. Pertanto l'immagine inversa di un elemento  $\rho_\theta \in \bar{G}$  è costituita da tutti gli elementi di  $G$  che sono rotazioni di un angolo  $\theta$  intorno a qualche punto.

Analogamente, denotiamo con  $\ell$  la retta di riflessione di  $\rho_\theta r$ . Come abbiamo osservato in precedenza, il suo angolo con l'asse  $x$  è  $\frac{1}{2}\theta$ . Il gruppo puntuale  $\bar{G}$

contiene  $\rho_\theta r$  se esiste qualche elemento  $t_a \rho_\theta r$  in  $G$ , e  $t_a \rho_\theta r$  è una riflessione o una glissoriflessione rispetto a una retta parallela a  $\ell$ . Pertanto l'immagine inversa di  $\rho_\theta r$  è costituita da tutti gli elementi di  $G$  che sono riflessioni o glissoriflessioni rispetto a rette parallele a  $\ell$ .

Poiché  $G$  non contiene piccole rotazioni, lo stesso accade per il suo gruppo puntuale  $\bar{G}$ . Pertanto anche  $\bar{G}$  è discreto, e quindi  $\bar{G}$  è un sottogruppo discreto di  $\mathbf{O}$ .

**(4.8) PROPOSIZIONE** *Un sottogruppo discreto di  $\mathbf{O}$  è un gruppo finito.*

La dimostrazione di questa proposizione è lasciata come esercizio. ■

Combinando la proposizione (4.8) con il teorema (3.4), si ottiene il seguente corollario:

**(4.9) COROLLARIO** *Il gruppo puntuale  $\bar{G}$  di un gruppo discreto  $G$  è ciclico oppure diedrale.*

Ecco qui l'osservazione fondamentale che collega il gruppo puntuale con il gruppo delle traslazioni:

**(4.10) PROPOSIZIONE** *Sia  $G$  un sottogruppo discreto di  $M$ , con gruppo delle traslazioni  $L = L_G$  e gruppo puntuale  $\bar{G}$ . Gli elementi di  $\bar{G}$  mandano il gruppo  $L$  in sé, cioè, se  $\bar{g} \in \bar{G}$  e  $a \in L$ , allora  $\bar{g}(a) \in L$ .*

Tale proposizione può essere rienunciata dicendo che  $\bar{G}$  è contenuto nel gruppo delle simmetrie di  $L$ , dove  $L$  viene considerato come un insieme di punti del piano  $\mathbf{R}^2$ . Tuttavia, è importante osservare che il gruppo di partenza  $G$  non opera necessariamente su  $L$ .

**Dimostrazione.** Dire che  $a \in L$  significa che  $t_a \in G$ . Pertanto occorre provare che se  $t_a \in G$  e  $\bar{g} \in \bar{G}$ , allora  $t_{\bar{g}(a)} \in G$ . Ora, in base alla definizione del gruppo puntuale,  $\bar{g}$  è l'immagine di qualche elemento  $g$  di  $G$ :  $\varphi(g) = \bar{g}$ . Dimostreremo la proposizione, provando che  $t_{\bar{g}(a)}$  è il coniugato di  $t_a$  mediante  $g$ . Scriviamo:  $g = t_b \rho$  oppure  $t_b \rho r$ , dove  $\rho = \rho_\theta$ . Allora  $\bar{g} = \rho$  oppure  $\rho r$ , rispettivamente. Nel primo caso,

$$gt_ag^{-1} = t_b \rho t_a \rho^{-1} t_{-b} = t_b t_{\rho(a)} \rho \rho^{-1} t_{-b} = t_{\rho(a)},$$

come richiesto. Il calcolo è simile nell'altro caso. ■

La proposizione seguente descrive i gruppi puntuali che possono venir fuori quando il gruppo delle traslazioni  $L_G$  è un reticolo.

(4.11) PROPOSIZIONE Sia  $H \subset \mathbf{O}$  un sottogruppo finito del gruppo delle simmetrie di un reticolo  $L$ . Allora:

- (a) ogni rotazione in  $H$  ha ordine 1, 2, 3, 4, oppure 6.
- (b)  $H$  è uno dei gruppi  $C_n$ ,  $D_n$ , dove  $n = 1, 2, 3, 4$ , oppure 6.

Tale proposizione è spesso citata come la *restrizione cristalografica*. Si noti che in base ad essa una rotazione di ordine 5 è esclusa. Non esistono disegni di carte da parati con simmetria di rotazione di ordine 5. (Tuttavia, esistono disegni "quasi-periodici" con simmetria di ordine 5).

Per dimostrare le proposizioni (4.5) e (4.11), cominciamo a considerare un semplice risultato, dato dal lemma seguente:

(4.12) LEMMA Sia  $L$  un sottogruppo discreto di  $\mathbb{R}^2$ .

- (a) Un sottoinsieme limitato  $S$  di  $\mathbb{R}^2$  contiene soltanto un numero finito di elementi di  $L$ .
- (b) Se  $L \neq \{0\}$ , allora  $L$  contiene un vettore non nullo di lunghezza minima.

*Dimostrazione*

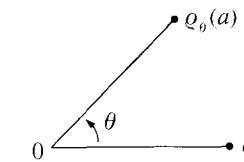
(a) Ricordiamo che un sottoinsieme  $S$  di  $\mathbb{R}^n$  si dice *limitato* se è contenuto in qualche grande "scatola", cioè se i punti di  $S$  non hanno coordinate arbitrariamente grandi. Ovviamente, se  $S$  è limitato, tale risulta  $L \cap S$ . Ora, per il teorema di Bolzano-Weierstrass, un sottoinsieme limitato e infinito deve contenere alcuni elementi arbitrariamente vicini gli uni agli altri, ossia gli elementi non possono essere separati da una distanza positiva prefissata  $\epsilon$ . Ciò non accade per  $L$ , in virtù di (4.4). Dunque  $L \cap S$  è un insieme finito.

(b) Quando diciamo che un vettore non nullo  $a$  ha lunghezza minima, intendiamo dire che ogni vettore non nullo  $v \in L$  ha lunghezza maggiore o uguale a  $|a|$ . Non richiediamo che il vettore  $a$  sia univocamente determinato. (In realtà, non potremmo richiedere ciò, poiché se  $a$  ha lunghezza minima, anche  $-a$  ha lunghezza minima.)

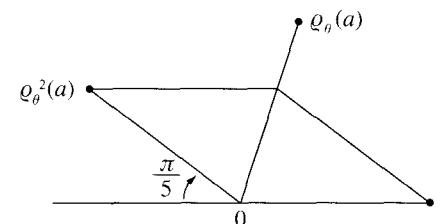
Supponiamo che  $L \neq \{0\}$ . Per dimostrare che esiste un vettore di lunghezza minima, consideriamo un vettore non nullo arbitrario  $b \in L$ , e sia  $S$  il disco di raggio  $|b|$  intorno all'origine. Tale disco è un insieme limitato, quindi contiene soltanto un numero finito di elementi di  $L$ , incluso  $b$ . In questo insieme finito di vettori non nulli ne esiste uno di lunghezza minima, che sarà il vettore richiesto.

*Dimostrazione della proposizione (4.11).* La seconda parte della proposizione segue dalla prima, in virtù di (3.6). Per dimostrare (a), sia  $\theta$  il più piccolo angolo di rotazione non nullo in  $H$ , e sia  $a$  un vettore non nullo in  $L$  di lunghezza minima.

Allora, poiché  $H$  agisce su  $L$ , anche  $\rho_\theta(a)$  sta in  $L$ ; pertanto  $b = \rho_\theta(a) - a \in L$ . Dato che  $a$  ha lunghezza minima,  $|b| \geq |a|$ . Ne segue che  $\theta \geq 2\pi/5$ .



Dunque  $\rho_\theta$  ha ordine  $\leq 6$ . Inoltre il caso  $\theta = 2\pi/5$  è da scartare, poiché allora il vettore  $b' = \rho_\theta^2(a) + a$  è più corto di  $a$ :

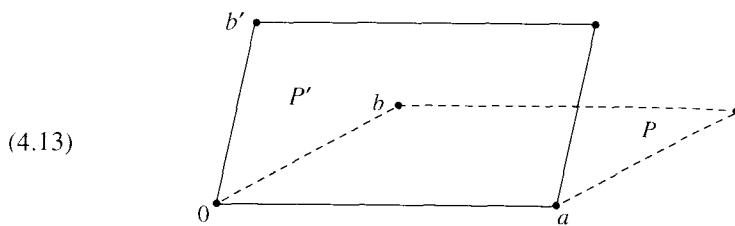


Ciò completa la dimostrazione. ■

*Dimostrazione della proposizione (4.5).* Sia  $L$  un sottogruppo discreto di  $\mathbb{R}^2$ . Il caso in cui  $L = \{0\}$  è incluso nella lista. Se  $L \neq \{0\}$ , esiste un vettore non nullo  $a \in L$ , e vi sono due possibilità:

**Caso 1:** Tutti i vettori di  $L$  giacciono su una retta  $\ell$  passante per l'origine. Ripetiamo un'argomentazione usata più volte in precedenza, e scegliamo un vettore non nullo  $a \in L$  di lunghezza minima. Vogliamo provare che  $L$  è generato da  $a$ . Sia  $v$  un elemento arbitrario di  $L$ . Allora esso è un multiplo reale  $v = ra$  di  $a$ , poiché  $L \subset \ell$ . Prendiamo la parte intera di  $r$ , scrivendo  $r = n + r_0$ , dove  $n$  è un intero e  $0 \leq r_0 < 1$ . Allora  $v - na = r_0a$  ha lunghezza minore di  $|a|$ , e poiché  $L$  è un gruppo, tale elemento sta in  $L$ . Pertanto  $r_0 = 0$ . Ciò prova che  $v$  è un multiplo intero di  $a$ , e quindi che  $v$  appartiene al sottogruppo generato da  $a$ , come richiesto.

**Caso 2:** Gli elementi di  $L$  non giacciono su una retta. Allora  $L$  contiene due vettori linearmente indipendenti  $a', b'$ . Partiamo da una coppia arbitraria di vettori indipendenti, e cerchiamo di costruire due vettori che genereranno il gruppo  $L$ . Per cominciare, sostituiamo  $a'$  con un vettore non nullo di lunghezza minima  $a$  sulla retta  $\ell$  generata da  $a'$ . L'argomentazione sviluppata nel caso 1 prova che il sottogruppo  $\ell \cap L$  è generato da  $a$ . Successivamente, consideriamo il parallelogramma di vertici  $0, a, b', a + b'$ :



Poiché  $P'$  è un insieme limitato, per il lemma (4.12) contiene soltanto un numero finito di elementi di  $L$ . Possiamo scegliere allora in questo insieme finito un vettore  $b$  avente distanza più piccola possibile, ma positiva, dalla retta  $\ell$ . Vogliamo ora dimostrare che  $a$  e  $b$  generano  $L$ . Sia  $P$  il parallelogramma di vertici  $0, a, b, a+b$ . Ebbene,  $P$  non contiene punti di  $L$  all'infuori dei vertici. Per verificare ciò, osserviamo innanzitutto che un punto arbitrario  $c$  del reticolo appartenente a  $P$ , che non sia un vertice, deve trovarsi su uno dei segmenti di retta  $[b, a+b]$  o  $[0, a]$ . Altrimenti i due punti  $c$  e  $c-a$  sarebbero più vicini a  $b$  di  $b$ , e uno di tali punti apparterrebbe a  $P'$ . Ora, il segmento  $[0, a]$  è da scartare, poiché  $a$  è un vettore di lunghezza minima su  $\ell$ . Infine, se vi fosse un punto  $c$  sul segmento  $[b, a+b]$ , allora  $c-b$  sarebbe un elemento di  $L$  sul segmento  $[0, a]$ . La dimostrazione è completata dal lemma seguente:

(4.14) LEMMA *Siano  $a, b$  vettori linearmente indipendenti appartenenti a un sottogruppo  $L$  di  $\mathbf{R}^2$ . Supponiamo che il parallelogramma  $P$  da essi generato non contenga elementi di  $L$  all'infuori dei vertici  $0, a, b, a+b$ . Allora  $L$  è generato da  $a$  e  $b$ , ossia:*

$$L = \{ma + nb \mid m, n \in \mathbf{Z}\}.$$

*Dimostrazione.* Sia  $v$  un elemento di  $L$ . Allora, poiché  $(a, b)$  è una base di  $\mathbf{R}^2$ ,  $v$  è una combinazione lineare del tipo  $v = ra + sb$ , dove  $r, s$  sono numeri reali. Prendiamo le parti intere di  $r, s$ , scrivendo:  $r = m + r_0$ ,  $s = n + s_0$ , dove  $m, n$  sono interi e  $0 \leq r_0, s_0 < 1$ . Consideriamo il vettore  $v_0 = r_0a + s_0b = v - ma - nb$ . Esso è contenuto nel parallelogramma  $P$ , e inoltre appartiene a  $L$ . Ne segue che  $v_0$  è uno dei vertici, e poiché  $r_0, s_0 < 1$ , deve essere l'origine. Dunque  $v = ma + nb$ . Ciò completa la dimostrazione del lemma e della proposizione (4.5). ■

Sia  $L$  un reticolo di  $\mathbf{R}^2$ . Un elemento  $v \in L$  si dice *primitivo*, se non è un multiplo intero di un altro vettore di  $L$ . La dimostrazione precedente prova in realtà il seguente risultato:

(4.15) COROLLARIO *Sia  $L$  un reticolo e sia  $v$  un elemento primitivo di  $L$ . Allora esiste un elemento  $w \in L$  tale che l'insieme  $(v, w)$  è una base del reticolo.* ■

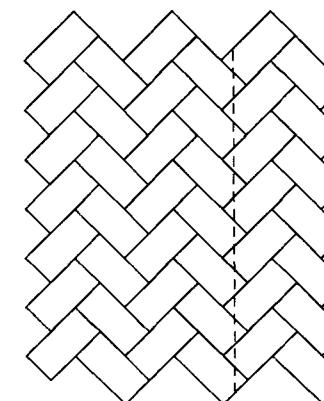
Ritorniamo ora ad esaminare un gruppo discreto di movimenti  $G \subset M$  e consideriamo una prima classificazione di  $G$  in base alla struttura del suo gruppo delle traslazioni  $L_G$ . Se  $L_G$  è il gruppo banale, allora l'omomorfismo da  $G$  al suo gruppo dei punti è biiettivo e  $G$  è finito. Abbiamo esaminato questo caso nel paragrafo 3.

I gruppi discreti  $G$  tali che  $L_G$  sia ciclico infinito sono i gruppi di simmetria dei disegni dei fregi, come (1.3). La classificazione di tali gruppi è lasciata come esercizio.

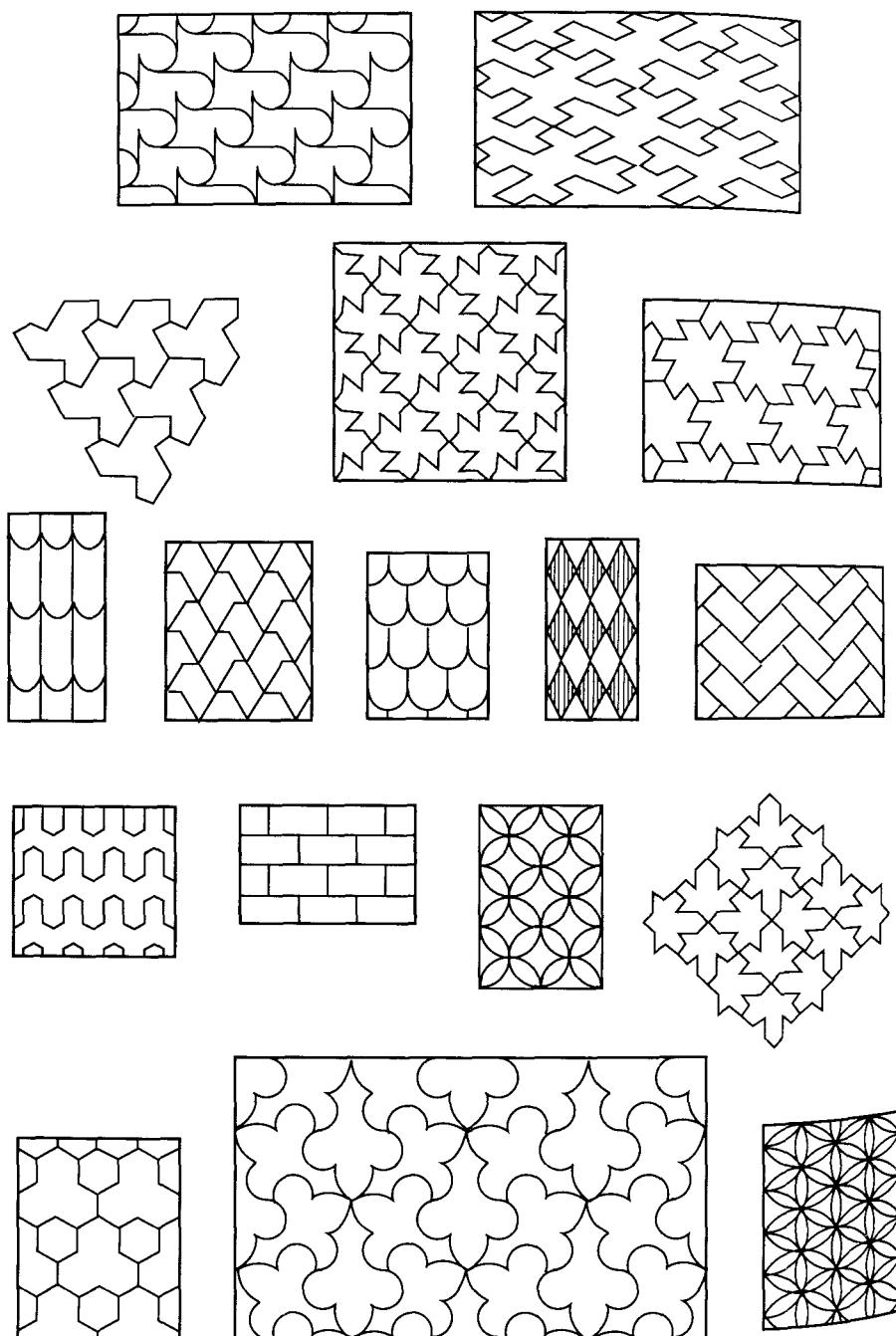
Se  $L_G$  è un reticolo, allora  $G$  è chiamato *gruppo cristalografico piano* (in inglese *lattice group*). Tali gruppi sono i gruppi delle simmetrie dei disegni delle carte da parati e dei cristalli in dimensione due.

Il fatto che qualsiasi disegno di carta da parati si ripete in due direzioni si riflette nel fatto che il suo gruppo di simmetria contiene sempre due traslazioni indipendenti, il che prova che  $L_G$  è un reticolo. Esso può contenere anche altri elementi (rotazioni, riflessioni o glissoriflessioni), tuttavia la restrizione cristalografica limita i casi possibili e permette di classificare i gruppi cristalografici piani in 17 tipi. La classificazione tiene conto non soltanto della struttura intrinseca del gruppo, ma anche del tipo di movimento che ciascun elemento del gruppo rappresenta. I campioni dei disegni con i vari tipi di simmetria sono illustrati nella figura (4.16).

La proposizione (4.11) è utile per determinare il gruppo puntuale di un gruppo cristalografico. Per esempio, il motivo a "mattoni" raffigurato qui sotto possiede una simmetria di rotazione di un angolo  $\pi$  intorno ai centri dei mattoni. Tutte queste rotazioni rappresentano lo stesso elemento  $\rho_\pi$  del gruppo puntuale  $\overline{G}$ . La figura possiede anche una simmetria di glissoriflessione lungo la linea tratteggiata indicata. Pertanto il gruppo puntuale  $\overline{G}$  contiene una riflessione. In base alla proposizione (4.11),  $\overline{G}$  è un gruppo diedrale. D'altra parte, si vede facilmente che le uniche rotazioni non banali nel gruppo  $G$  delle simmetrie sono quelle di un angolo  $\pi$ . Pertanto  $\overline{G} = D_2 = \{1, \rho_\pi, r, \rho_\pi r\}$ .



(4.16)



Esempi di disegni per i 17 gruppi cristallografici del piano.

Il gruppo puntuale  $\bar{G}$  e il gruppo delle traslazioni  $L_G$  non caratterizzano completamente il gruppo  $G$ . La situazione è complicata dal fatto che una riflessione in  $\bar{G}$  non è necessariamente l'immagine di una riflessione in  $G$ ; infatti, essa può essere rappresentata in  $G$  soltanto da glissoriflessioni, come accade nel disegno a mattoni esaminato in precedenza.

Per illustrare, con un esempio, i metodi richiesti per classificare i gruppi cristallografici piani, descriviamo quei gruppi il cui gruppo puntuale contiene una rotazione  $\rho$  di un angolo  $\pi/2$ . In base alla proposizione (4.11), il gruppo puntuale sarà  $C_4$  oppure  $D_4$ . Poiché un qualsiasi elemento di  $G$  che rappresenta  $\rho$  è anche una rotazione di  $\pi/2$  intorno a qualche punto  $p$ , possiamo supporre che  $p$  sia l'origine. Allora anche  $\rho$  può essere considerato come un elemento di  $G$ .

**(4.17) PROPOSIZIONE** *Sia  $G$  un gruppo cristallogрафico tale che il suo gruppo puntuale contenga una rotazione  $\rho$  di un angolo  $\pi/2$ . Scegliamo le coordinate in modo tale che l'origine sia il centro di una rotazione di  $\pi/2$  in  $G$ . Sia  $a$  un vettore di lunghezza minima in  $L = L_G$ , e poniamo:  $b = \rho(a)$ ,  $c = \frac{1}{2}(a + b)$ . Denotiamo con  $r$  la riflessione intorno alla retta generata da  $a$ . Allora  $G$  è generato da uno dei seguenti insiemi:  $\{t_a, \rho\}$ ,  $\{t_a, \rho, r\}$ ,  $\{t_a, \rho, t_{cr}\}$ . Dunque esistono tre gruppi di questo tipo.*

**Dimostrazione.** Osserviamo innanzitutto che  $L$  è un reticolo quadrato, generato da  $a$  e  $b$ . Infatti,  $a$  appartiene a  $L$  per ipotesi, e la proposizione (4.10) afferma che anche  $b = \rho(a)$  appartiene a  $L$ . Questi due vettori generano un sottoreticolo quadrato  $L'$  di  $L$ . Se  $L \neq L'$ , allora in base al lemma (4.14), esiste un elemento  $w \in L$  nel quadrato i cui vertici sono  $0, a, b, a + b$  e distinto dai vertici. Ma un qualsiasi vettore siffatto avrebbe distanza minore di  $|a|$  da almeno uno dei vertici  $v$ , e il vettore differenza  $w - v$  risulterebbe un vettore di  $L$  più corto di  $a$ , il che contraddice la scelta fatta per  $a$ . Dunque  $L = L'$ , come affermato all'inizio.

Ora gli elementi  $t_a$  e  $\rho$  appartengono a  $G$ , e  $\rho t_a \rho^{-1} = t_b$  [cfr. (2.5)]. Pertanto il sottogruppo  $H$  di  $G$  generato dall'insieme  $\{t_a, \rho\}$  contiene  $t_a$  e  $t_b$ . Ne segue che esso contiene  $t_w$ , per ogni  $w \in L$ . Gli elementi di questo gruppo sono i prodotti  $t_w \rho^i$ :

$$H = \{t_w \rho^i \mid w \in L, 0 \leq i \leq 3\}.$$

Esso è uno dei gruppi in questione. Consideriamo ora gli eventuali altri elementi che  $G$  può contenere.

**Caso 1:** Ogni elemento di  $G$  conserva l'orientazione. In tal caso, il gruppo puntuale è  $C_4$ . Ogni elemento di  $G$  ha la forma  $m = t_u \rho_\theta$ , e se un tale elemento appartiene a  $G$ , allora  $\rho_\theta$  appartiene al gruppo puntuale. Quindi  $\rho_\theta = \rho^i$  per qualche  $i$ , e  $t_u \rho^i = t_u$  appartiene anch'esso a  $G$ . Ne segue che  $u \in L$ , e  $m \in H$ . Dunque in questo caso  $G = H$ .

**Caso 2:**  $G$  contiene un movimento che inverte l'orientazione. In tal caso il gruppo puntuale è  $D_4$ , e contiene la riflessione intorno alla retta generata da  $a$ . Scegiamo le coordinate in modo che questa riflessione diventi la riflessione standard  $r$ . Allora  $r$  sarà rappresentata in  $G$  da un elemento della forma  $m = t_u r$ . Ci sono due casi possibili.

(a) L'elemento  $u$  appartiene a  $L$ , ossia  $t_u \in G$ . Allora anche  $r$  appartiene a  $G$ , sicché  $G$  contiene il suo gruppo puntuale  $\overline{G} = D_4$ . Se  $m' = t_w \rho_0$  oppure  $m' = t_w \rho_0 r$  è un elemento arbitrario di  $G$ , allora  $\rho_0 r$  appartiene anch'esso a  $G$ ; ne segue che  $t_w \in G$  e  $w \in L$ . Allora  $G$  è il gruppo generato dall'insieme  $\{t_a, \rho, r\}$ .

(b) L'elemento  $u$  non appartiene a  $L$ . Questo è il caso difficile da trattare.

(4.18) LEMMA *Sia  $U$  l'insieme dei vettori  $u$  tali che  $t_{ur} \in G$ . Allora:*

- (a)  $L + U = U$ .
- (b)  $\rho U = U$ .
- (c)  $U + rU \subset L$ .

*Dimostrazione.* Se  $v \in L$  e  $u \in U$ , allora  $t_v$  e  $t_{ur}$  appartengono a  $G$ ; ne segue che  $t_v t_{ur} = t_{v+ur} \in G$ . Ciò mostra che  $v + u \in U$  e quindi prova (a). Supponiamo ora che  $u \in U$ . Allora  $\rho t_{ur} \rho = t_{\rho u} \rho r \rho = t_{\rho u r} \in G$ . Ciò mostra che  $\rho u \in U$  e quindi prova (b). Infine, se  $u, v \in U$ , allora  $t_{ur} t_{rv} = t_{u+r v} \in G$ ; ne segue che  $u + rv \in L$ , ciò che prova (c). ■

La parte (a) del lemma ci permette di scegliere un vettore  $u \in U$  giacente nel quadrato di vertici  $0, a, b, a+b$  e non contenuto nei segmenti  $[a, a+b]$  e  $[b, a+b]$ . Esprimiamo  $u$  mediante la base  $(a, b)$ , nella forma  $u = xa + yb$ , dove  $0 \leq x, y < 1$ . Allora  $u + ru = 2xa$ . Poiché  $u + ru \in L$  in virtù di (4.18c), i valori possibili per  $x$  sono  $0, \frac{1}{2}$ . Inoltre, anche  $\rho u + a = (1-y)a + xb$  giace nel quadrato, e la stessa argomentazione prova che  $y$  è 0 oppure  $\frac{1}{2}$ . Dunque i tre valori possibili per  $u$  sono  $\frac{1}{2}a, \frac{1}{2}b$  e  $\frac{1}{2}(a+b) = c$ . Ma, se  $u = \frac{1}{2}a$ , allora  $\rho u = \frac{1}{2}b$  e  $ru = u = \frac{1}{2}a$  e quindi  $c = \frac{1}{2}(a+b) \in L$  (4.18b,c). Ciò è impossibile, poiché  $c$  è più corto di  $a$ . Analogamente, il caso  $u = \frac{1}{2}b$  è impossibile. Pertanto l'unico caso restante è  $u = c$ , che significa che il gruppo  $G$  è generato da  $\{t_a, \rho, t_c r\}$ . ■

## 5 Simmetria astratta: azioni di un gruppo

Il concetto di simmetria può essere applicato a oggetti diversi dalle figure geometriche. Per esempio, il coniugio  $(a+bi) \mapsto (a-bi)$  può essere interpretato

come una simmetria dei numeri complessi. Esso è quasi completamente compatibile con la struttura di  $\mathbb{C}$ : se  $\bar{\alpha}$  denota il complesso coniugato di  $\alpha$ , allora  $\bar{\alpha} + \bar{\beta} = \bar{\alpha} + \bar{\beta}$  e  $\bar{\alpha}\bar{\beta} = \bar{\alpha}\bar{\beta}$ . Essendo compatibile con l'addizione e la moltiplicazione, il coniugio è chiamato un *automorfismo* del campo  $\mathbb{C}$ . Naturalmente, tale simmetria è proprio la simmetria "bilaterale" del piano complesso rispetto all'asse reale, ma l'affermazione che essa è un automorfismo si riferisce alla sua struttura algebrica.

Un altro esempio di simmetria "bilaterale" astratta è dato da un gruppo ciclico  $H$  di ordine 3. Abbiamo visto (cap. 3, § 2) che questo gruppo ha un automorfismo  $\varphi$  che scambia tra loro i due elementi diversi dall'identità.

L'insieme degli automorfismi di un gruppo  $H$  (o di una qualsiasi altra struttura matematica  $H$ ) costituisce un gruppo  $\text{Aut } H$ , in cui la legge di composizione è la composizione di applicazioni. Ogni automorfismo dovrebbe essere considerato come una simmetria di  $H$ , nel senso che è una permutazione degli elementi di  $H$  compatibile con la struttura di  $H$ . Ma, anziché essere una figura geometrica con una forma rigida, la struttura in questo caso è la legge di gruppo. Il gruppo degli automorfismi del gruppo ciclico di ordine 3 contiene due elementi: l'applicazione identica e l'applicazione  $\varphi$ .

Quindi i termini *automorfismo* e *simmetria* sono più o meno sinonimi, con l'unica differenza che il primo designa una permutazione di un insieme che conserva qualche struttura algebrica, mentre il secondo spesso si riferisce ad una permutazione che conserva una struttura geometrica.

Questi esempi sono casi particolari di una nozione più generale, quella di azione di un gruppo su un insieme. Supponiamo che siano dati un gruppo  $G$  e un insieme  $S$ . Un'azione di  $G$  su  $S$  è una legge che associa ad elementi  $g \in G$  e  $s \in S$  un elemento  $gs$  di  $S$ . In altre parole, è una legge di composizione, ossia un'applicazione  $G \times S \rightarrow S$ , che scriviamo in generale come una moltiplicazione:

$$g, s \mapsto gs.$$

Si richiede inoltre che tale legge soddisfi i seguenti assiomi:

- (5.1) (a)  $1s = s$ , per ogni  $s$  (1 è l'identità di  $G$ ).  
(b) Proprietà associativa:  $(gg')s = g(g's)$ , per ogni  $g, g' \in G$  e  $s \in S$ .

Un insieme  $S$ , con un'azione di  $G$ , è chiamato spesso un *G-insieme*. Tale azione in realtà dovrebbe essere chiamata un'azione a sinistra, poiché la moltiplicazione per gli elementi di  $G$  si effettua a sinistra.

Esempi di tale nozione si possono trovare in molti contesti. Per esempio, sia  $G = M$  il gruppo di tutti i movimenti rigidi del piano. Allora  $M$  agisce sull'insieme dei punti del piano, sull'insieme delle rette del piano, sull'insieme dei triangoli del piano, e così via. Oppure, sia  $G$  il gruppo ciclico  $\{1, r\}$  di ordine 2, con  $r^2 = 1$ .

Allora  $G$  agisce sull'insieme  $S$  dei numeri complessi, mediante la legge  $r_\alpha = \bar{\alpha}$ . Negli esempi concreti gli assiomi (5.1) sono di solito banalmente verificati.

Il motivo per cui una legge di composizione siffatta è chiamata un'azione è che, se fissiamo un elemento  $g$  di  $G$ , ma lasciamo variare  $s$  in  $S$ , allora la *moltiplicazione a sinistra per  $g$*  definisce un'applicazione di  $S$  in sé; denotiamo tale applicazione con  $m_g$ . Dunque

$$(5.2) \quad m_g : S \rightarrow S$$

è definita da:

$$m_g(s) = gs.$$

Questa applicazione descrive il modo in cui l'elemento  $g$  opera su  $S$ . Si noti che  $m_g$  è una *permutazione* di  $S$ , ossia, è un'applicazione biiettiva, infatti gli assiomi provano che essa ha l'inversa destra e sinistra:

$$m_{g^{-1}} = \text{moltiplicazione per } g^{-1}.$$

Si ha:  $m_{g^{-1}}(m_g(s)) = g^{-1}(gs) = (g^{-1}g)s = 1s = s$ , e scambiando i ruoli di  $g$  e  $g^{-1}$ , si ottiene anche:  $m_g(m_{g^{-1}}(s)) = s$ .

La cosa più importante che possiamo fare per studiare un insieme  $S$  su cui agisce un gruppo  $G$  è decomporre l'insieme in orbite. Sia  $s$  un elemento di  $S$ . L'*orbita* di  $s$  in  $S$  è l'insieme:

$$(5.3) \quad O_s = \{s' \in S \mid s' = gs \text{ per qualche } g \in G\}.$$

L'orbita è un sottoinsieme di  $S$ , e si scrive spesso nella forma:  $O_s = \{gs \mid g \in G\}$ , in analogia con la notazione usata per le classi laterali [cap. 2, (6.1)]. Noi non useremo tale notazione, poiché  $O_s$  somiglia troppo alla notazione relativa allo stabilizzatore, che introdurremo tra breve. Se pensiamo che gli elementi di  $G$  operano su  $S$  mediante permutazioni, allora  $O_s$  è l'insieme delle immagini di  $s$  rispetto alle varie permutazioni  $m_g$ . Così, ad esempio, se  $G = M$  è il gruppo dei movimenti e  $S$  è l'insieme dei triangoli del piano, l'orbita  $O_\Delta$  di un triangolo  $\Delta$  assegnato è l'insieme di tutti i triangoli congruenti a  $\Delta$ . Un altro esempio di orbita è stato introdotto quando abbiamo dimostrato l'esistenza di un punto fisso per l'azione di un gruppo finito sul piano (3.1).

Le orbite relative all'azione di un gruppo sono classi di equivalenza rispetto alla relazione:

$$(5.4) \quad s \sim s', \text{ se } s' = gs \text{ per qualche } g \in G.$$

La dimostrazione che questa è una relazione di equivalenza è facile, e pertanto verrà omessa; abbiamo effettuato una verifica simile quando abbiamo introdotto le

classi laterali (cap. 2, § 6). Essendo classi di equivalenza, le orbite costituiscono una partizione dell'insieme  $S$ :

$$(5.5) \quad S \text{ è un'unione di orbite disgiunte.}$$

Il gruppo  $G$  agisce su  $S$  operando indipendentemente su ciascuna orbita. In altre parole, un elemento  $g \in G$  permuta gli elementi di ciascuna orbita e non porta elementi di un'orbita in un'altra orbita. Per esempio, l'insieme dei triangoli del piano può essere ripartito in classi di congruenza, date dalle orbite relative all'azione di  $M$ . Un movimento  $m$  permuta separatamente ciascuna classe di congruenza. Si noti che le orbite di  $s$  e di  $gs$  sono uguali.

Se  $S$  consiste di una sola orbita, si dice che  $G$  agisce *transitivamente* su  $G$ . Ciò significa che ogni elemento di  $S$  viene portato in un qualsiasi altro elemento di  $S$  da qualche elemento del gruppo. Così, ad esempio, il gruppo delle simmetrie della figura (1.7) agisce transitivamente sull'insieme delle gambe. Il gruppo  $M$  dei movimenti rigidi del piano agisce transitivamente sull'insieme dei punti, e agisce transitivamente sull'insieme delle rette del piano. Non agisce transitivamente sull'insieme dei triangoli del piano.

Lo *stabilizzatore* di un elemento  $s \in S$  è il sottogruppo  $G_s$  di  $G$  costituito dagli elementi che lasciano fisso  $s$ :

$$(5.6) \quad G_s = \{g \in G \mid gs = s\}.$$

È chiaro che  $G_s$  è un sottogruppo. Così come il nucleo di un omomorfismo di gruppi  $\varphi : G \rightarrow G'$  ci dice quando due elementi  $x, y \in G$  hanno la stessa immagine, ossia, se  $x^{-1}y \in \ker \varphi$  [cap. 2, (5.13)], analogamente possiamo descrivere quando due elementi  $x, y \in G$  agiscono allo stesso modo su un elemento  $s \in S$ , mediante lo stabilizzatore  $G_s$ :

$$(5.7) \quad xs = ys \text{ se e soltanto se } x^{-1}y \in G_s.$$

Infatti  $xs = ys$  implica  $s = x^{-1}ys$ , e viceversa.

Come esempio di stabilizzatore non banale, consideriamo l'azione del gruppo  $M$  dei movimenti rigidi sull'insieme dei punti del piano. Lo stabilizzatore dell'origine è il sottogruppo  $\mathbf{O}$  degli operatori ortogonali.

Oppure, se  $S$  è l'insieme dei triangoli del piano e  $\Delta$  è un particolare triangolo equilatero, allora lo stabilizzatore di  $\Delta$  è il suo gruppo delle simmetrie, ossia, un sottogruppo di  $M$  isomorfo a  $D_3$  (cfr. (3.4)). Conviene notare che, quando si dice che un movimento  $m$  stabilizza un triangolo  $\Delta$ , non si intende dire che  $m$  lascia fissi i punti di  $\Delta$ . (L'unico movimento che lascia fisso ogni punto di un triangolo è l'identità.) Si intende invece che, permutando l'insieme dei triangoli, il movimento porta  $\Delta$  in sé. È importante che tale distinzione sia ben chiara.

## 6 L'azione sulle classi laterali

Sia  $H$  un sottogruppo di un gruppo  $G$ . Abbiamo visto che le classi laterali sinistre  $aH = \{ah \mid h \in H\}$  formano una partizione del gruppo [cap. 2, (6.3)]. Chiameremo *spazio delle classi laterali* l'insieme delle classi laterali sinistre e lo denoteremo spesso con  $G/H$ , usando la stessa notazione introdotta per il gruppo quoziante rispetto ad un sottogruppo normale.

L'osservazione fondamentale da fare è che, sebbene  $G/H$  non sia un gruppo, a meno che il sottogruppo  $H$  non sia normale,  $G$  agisce sullo spazio delle classi laterali  $G/H$  in modo naturale. L'azione è del tutto ovvia: se  $g$  è un elemento del gruppo e  $C$  è una classe laterale, allora  $gC$  è per definizione la classe laterale:

$$(6.1) \quad gC = \{gc \mid c \in C\}.$$

Dunque, se  $C = aH$ , allora  $gC$  è la classe  $gaH$ . È chiaro che gli assiomi (5.1) sono soddisfatti.

Si noti che il gruppo  $G$  agisce transitivamente su  $G/H$ , poiché  $G/H$  è l'orbita della classe laterale  $1H = H$ . Lo stabilizzatore della classe laterale  $1H$  è il sottogruppo  $H \subset G$ . Si noti ancora la distinzione: la moltiplicazione per un elemento  $h \in H$  non opera in modo banale sugli elementi della classe laterale  $1H$ , tuttavia essa manda quella classe in sé.

Per comprendere l'azione sulle classi laterali, può essere utile riflettere sull'esempio seguente. Sia  $G$  il gruppo  $D_3$  delle simmetrie di un triangolo equilatero. Come in (3.6),  $G$  può essere descritto da due generatori  $x, y$  soddisfacenti alle relazioni:  $x^3 = 1, y^2 = 1, yx = x^2y$ . Allora  $H = \{1, y\}$  è un sottogruppo di ordine 2 e le sue classi laterali sono:

$$(6.2) \quad C_1 = H = \{1, y\}, \quad C_2 = \{x, xy\}, \quad C_3 = \{x^2, x^2y\},$$

e  $G$  agisce su  $G/H = \{C_1, C_2, C_3\}$ . Pertanto, come in (5.2), ogni elemento  $g$  di  $G$  determina una permutazione  $m_g$  di  $\{C_1, C_2, C_3\}$ . Gli elementi  $x, y$  agiscono nel modo seguente:

$$(6.3) \quad m_x: \begin{matrix} 1 & 2 \\ \curvearrowright & \curvearrowleft \end{matrix} \quad \text{e} \quad m_y: \begin{matrix} 1 & 2 & 3 \\ \curvearrowright & \curvearrowleft & \curvearrowright \end{matrix}.$$

Infatti, i sei elementi di  $G$  forniscono tutte e sei le permutazioni di tre elementi e pertanto l'applicazione:

$$G \rightarrow S_3 \approx \text{Perm}(G/H)$$

$$g \mapsto m_g$$

è un isomorfismo. Dunque il gruppo diedrale  $G = D_3$  è isomorfo al gruppo simmetrico  $S_3$ , cosa che già sapevamo.

La proposizione seguente collega un'azione qualsiasi di un gruppo con l'azione sullo spazio delle classi laterali:

(6.4) PROPOSIZIONE Sia  $S$  un  $G$ -insieme, e sia  $s$  un elemento di  $S$ . Sia  $H$  lo stabilizzatore di  $s$ , e sia  $O_s$  l'orbita di  $s$ . Allora esiste un'applicazione biiettiva naturale:

$$G/H \xrightarrow{\varphi} O_s$$

definita da:

$$aH \mapsto as.$$

Tale applicazione è compatibile con l'azione di  $G$ , nel senso che  $\varphi(gC) = g\varphi(C)$ , per ogni classe laterale  $C$  e per ogni elemento  $g \in G$ .

La proposizione ci dice che ogni azione di un gruppo può essere descritta mediante le azioni sulle classi laterali. Per esempio, sia  $S = \{v_1, v_2, v_3\}$  l'insieme dei vertici di un triangolo equilatero, e sia  $G$  il suo gruppo delle simmetrie, presentato come sopra. L'elemento  $y$  è una riflessione che stabilizza uno dei vertici del triangolo, diciamo  $v_1$ . Lo stabilizzatore di tale vertice è  $H = \{1, y\}$ , e la sua orbita è  $S$ . Utilizzando opportunamente gli indici, l'insieme (6.2) delle classi laterali viene mandato in  $S$  mediante l'applicazione  $C_i \mapsto v_i$ .

*Dimostrazione della proposizione (6.4).* È chiaro che l'applicazione  $\varphi$ , se esiste, è compatibile con l'azione del gruppo. Ciò che non è chiaro, a priori, è che la legge  $gH \mapsto gs$  definisce un'applicazione. Poiché una stessa classe laterale può essere scritta in molti modi nella forma  $gH$ , dobbiamo dimostrare che, se  $a$  e  $b$  sono elementi del gruppo, e se  $aH = bH$ , allora si ha anche:  $as = bs$ . Ciò è vero, poiché sappiamo che  $aH = bH$  se e solo se  $b = ah$  per qualche  $h$  in  $H$  [cap. 2, (6.5)], e d'altra parte, se  $b = ah$ , allora  $bs = ahs = as$ , poiché  $h$  fissa  $s$ . Inoltre, l'orbita di  $s$  è costituita dagli elementi  $gs$ , e  $\varphi$  manda  $gH$  in  $gs$ . Dunque  $\varphi$  manda  $G/H$  su  $O_s$ , e  $\varphi$  è suriettiva. Infine, dimostriamo che  $\varphi$  è iniettiva. Supponiamo che  $aH$  e  $bH$  abbiano la stessa immagine:  $as = bs$ . Allora  $s = a^{-1}bs$ , e dato che  $H$  è, per definizione, lo stabilizzatore di  $s$ , ciò implica che  $a^{-1}b = h \in H$ . Pertanto  $b = ah \in aH$ , e quindi  $aH = bH$ . Ciò completa la dimostrazione. ■

(6.5) PROPOSIZIONE Sia  $S$  un  $G$ -insieme, e consideriamo un elemento  $s \in S$ . Sia  $s'$  un elemento dell'orbita di  $s$ , diciamo  $s' = as$ . Allora:

(a) L'insieme degli elementi  $g$  di  $G$  tali che  $gs = s'$  è la classe laterale sinistra:

$$aG_s = \{g \in G \mid g = ah \text{ per qualche } h \in G_s\}.$$

(b) Lo stabilizzatore di  $s'$  è un sottogruppo coniugato dello stabilizzatore di  $s$ :

$$G_{s'} = aG_s a^{-1} = \{g \in G \mid g = aha^{-1} \text{ per qualche } h \in G_s\}.$$

Proseguiamo la dimostrazione. ■

Come esempio, rideterminiamo lo stabilizzatore di un punto  $p$  del piano, rispetto all'azione del gruppo dei movimenti. Abbiamo già fatto questo calcolo in (2.11b). Si ha:  $p = t_p(0)$ , e lo stabilizzatore dell'origine è il gruppo ortogonale  $\mathbf{O}$ . Dunque, in base a (6.5b):

$$G_p = t_p \mathbf{O} t_p^{-1} = t_p \mathbf{O} t_{-p} = \{m \in M \mid m = t_p \rho_\theta t_{-p} \text{ oppure } m = t_p \rho_\theta r_{t_{-p}}\}.$$

D'altra parte, sappiamo che  $G_p$  è formato da rotazioni e riflessioni intorno al punto  $p$ . Esse sono i movimenti che lasciano fisso  $p$ . Pertanto  $t_p \mathbf{O} t_p^{-1}$  è costituito da tali elementi. Ciò è in accordo con (2.11).

## 7 La formula delle classi

Sia  $H$  un sottogruppo di  $G$ . Come sappiamo dal capitolo 2 (6.9), tutte le classi laterali di  $H$  in  $G$  hanno lo stesso numero di elementi:  $|H| = |aH|$ . Poiché  $G$  è un'unione di classi laterali disgiunte e il numero delle classi laterali è l'indice, denotato con  $[G : H]$  oppure  $|G/H|$ , otteniamo la formula fondamentale per l'ordine  $|G|$  del gruppo  $G$  [cfr. cap. 2 (6.10)]:

$$(7.1) \quad |G| = |H| |G/H|.$$

Sia ora  $S$  un  $G$ -insieme. Allora, combinando la proposizione (6.4) con (7.1), si ottiene il seguente risultato:

(7.2) PROPOSIZIONE (Formula delle classi) *Sia  $s \in S$ . Allora si ha:*

*(ordine di  $G$ ) = (ordine dello stabilizzatore) (ordine dell'orbita)*

$$|G| = |G_s| |O_s|.$$

In modo equivalente, l'ordine dell'orbita è uguale all'indice dello stabilizzatore:

$$|O_s| = [G : G_s]$$

per ogni  $s \in S$ . Di conseguenza, l'ordine di ogni orbita divide l'ordine del gruppo.

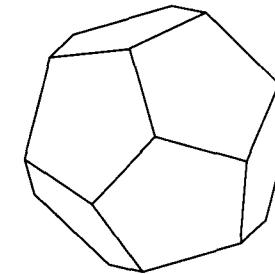
Una formula più elementare utilizza la partizione di  $S$  in orbite per contare i suoi elementi. Denotiamo le varie orbite che costituiscono  $S$ , con  $O_1, \dots, O_k$ . Allora:

$$(7.3) \quad |S| = |O_1| + |O_2| + \dots + |O_k|.$$

Queste semplici formule hanno un gran numero di applicazioni.

### 7.4) Esempio

Consideriamo il gruppo  $G$  delle simmetrie di un dodecaedro regolare  $D$  che conservano l'orientazione. Dalla discussione del capitolo 4 (§ 8) è chiaro che sono tutte rotazioni. È problematico contare senza fare errori. Consideriamo l'azione di  $G$  sull'insieme  $S$  delle facce di  $D$ . Lo stabilizzatore di una faccia  $s$  è il gruppo delle rotazioni di multipli di  $2\pi/5$  intorno a una retta perpendicolare passante per il centro di  $s$ , quindi l'ordine di  $G_s$  è 5. Vi sono 12 facce, e  $G$  agisce transitivamente su di esse, dunque  $|G| = 5 \cdot 12 = 60$ . Oppure:  $G$  agisce transitivamente sui vertici  $v$  di  $D$ . Ci sono tre rotazioni, inclusa l'identità 1, che lasciamo fisso un vertice, sicché  $|G_v| = 3$ , e ci sono 20 vertici: ne segue che  $|G| = 3 \cdot 20 = 60$ , che costituisce una verifica. Un calcolo simile si può fare per gli spigoli. Se  $e$  è uno spigolo, allora  $|G_e| = 2$ , e quindi poiché  $60 = 2 \cdot 30$ , il dodecaedro ha 30 spigoli.



Seguendo un principio generale, dovremmo studiare la restrizione di un'azione di un gruppo  $G$  a un sottogruppo. Supponiamo che  $G$  agisca su un insieme  $S$ , e sia  $H$  un sottogruppo di  $G$ . Possiamo restringere l'azione, per ottenere un'azione di  $H$  su  $S$ . Così facendo, si ottengono altre relazioni numeriche.

Chiaramente, l' $H$ -orbita di un elemento  $s$  sarà contenuta nella sua  $G$ -orbita. Pertanto possiamo considerare una sola  $G$ -orbita e scomporla in  $H$ -orbite; contiamo poi gli ordini di queste  $H$ -orbite, ottenendo una nuova formula. Per esempio, sia  $S$  l'insieme delle 12 facce del dodecaedro, e sia  $H$  lo stabilizzatore di una faccia  $s$  assegnata. Allora  $H$  lascia fissa anche la faccia opposta a  $s$ , e pertanto vi sono due  $H$ -orbite di ordine 1. Le facce rimanenti costituiscono due orbite di ordine 5. In questo caso, la relazione (7.3) diventa:

$$12 = 1 + 1 + 5 + 5.$$

Oppure, sia  $S$  l'insieme delle facce, e sia  $K$  lo stabilizzatore di un vertice. Allora  $K$  non lascia fissa nessuna faccia, e pertanto ogni  $K$ -orbita ha ordine 3:

$$12 = 3 + 3 + 3 + 3.$$

Le relazioni ci permettono di collegare diversi sottogruppi di un gruppo.

Terminiamo il paragrafo con una semplice applicazione di questo procedimento al caso in cui il  $G$ -insieme è lo spazio delle classi laterali di un sottogruppo:

(7.5) PROPOSIZIONE *Siano  $H$  e  $K$  sottogruppi di un gruppo  $G$ . Allora l'indice di  $H \cap K$  in  $H$  è al più uguale all'indice di  $K$  in  $G$ :*

$$[H : H \cap K] \leq [G : K].$$

*Dimostrazione.* Per evitare confusione, denotiamo lo spazio delle classi laterali  $G/K$  con  $S$ , e la classe  $1K$  con  $s$ . Dunque  $|S| = [G : K]$ . Come abbiamo già osservato, lo stabilizzatore di  $s$  è il sottogruppo  $K$ . Restringiamo ora l'azione di  $G$  al sottogruppo  $H$  e decomponiamo  $S$  in  $H$ -orbite. Lo stabilizzatore di  $s$  rispetto a tale azione ristretta è ovviamente  $H \cap K$ . Non sappiamo molto sull' $H$ -orbita  $O$  di  $s$ , tranne che essa è un sottoinsieme di  $S$ . Applichiamo ora la proposizione (7.2), la quale ci dice che  $|O| = [H : H \cap K]$ . Pertanto  $[H : H \cap K] = |O| \leq |S| = [G : K]$ , come richiesto. ■

## 8 Rappresentazioni mediante permutazioni

Per definizione, il gruppo simmetrico  $S_n$  agisce sull'insieme  $S = \{1, \dots, n\}$ . Una *rappresentazione mediante permutazioni* di un gruppo  $G$  è un omomorfismo

$$(8.1) \quad \varphi : G \rightarrow S_n.$$

Data una tale rappresentazione, otteniamo un'azione di  $G$  su  $S = \{1, \dots, n\}$ , indicando con  $m_g$  (5.2) la permutazione  $\varphi(g)$ . Infatti, le azioni di un gruppo  $G$  su  $\{1, \dots, n\}$  corrispondono in modo biunivoco alle rappresentazioni.

Più in generale, sia  $S$  un insieme arbitrario e sia  $\text{Perm}(S)$  il gruppo delle sue permutazioni. Sia  $G$  un gruppo.

(8.2) PROPOSIZIONE *Esiste una corrispondenza biunivoca:*

$$\{\text{azioni di } G \text{ su } S\} \longleftrightarrow \{\text{omomorfismi } G \rightarrow \text{Perm}(S)\}$$

*definita nel modo seguente: data un'azione, definiamo  $\varphi : G \rightarrow \text{Perm}(S)$  mediante la legge:  $\varphi(g) = m_g$ , dove  $m_g$  è la moltiplicazione per  $g$  (5.2).*

Facciamo vedere che  $\varphi$  è un omomorfismo, lasciando il resto della dimostrazione di (8.2) come esercizio. Abbiamo già osservato (§5) che  $m_g$  è una permutazione per quanto definito sopra,  $\varphi(g) \in \text{Perm}(S)$ . Le proprietà da verificare quindi è  $\varphi(xy) = \varphi(x)\varphi(y)$ , oppure  $m_{xy} = m_x m_y$ , dove la moltiplicazione è la composizione di permutazioni. Pertanto dobbiamo dimostrare che  $m_{xy}(s) = m_x(m_y(s))$  per ogni  $s \in S$ . In base alla definizione (5.2),  $m_{xy}(s) = (xy)s$  e  $m_x(m_y(s)) = x(y^s)$ . La

proprietà associativa (5.1b) relativa all'azione di un gruppo prova che  $(xy)s = x(y^s)$ , come richiesto. ■

L'isomorfismo  $D_3 \rightarrow S_3$  ottenuto nel paragrafo 6 mediante l'azione di  $D_3$  sulle classi laterali di  $H$  (6.2) è un esempio particolare di rappresentazione mediante permutazioni. In generale un omomorfismo non è necessariamente iniettivo o suriettivo; se  $\varphi : G \rightarrow \text{Perm}(S)$  è iniettivo, si dice che l'azione corrispondente è **fedele**. Per essere fedele, quindi, l'azione deve avere la proprietà che  $m_g \neq$  identità, a meno che  $g = 1$ , oppure:

$$\text{se } gs = s \text{ per ogni } s \in S, \text{ allora } g = 1.$$

L'azione del gruppo dei movimenti  $M$  sull'insieme  $S$  dei triangoli equilateri del piano è fedele, poiché l'identità è l'unico movimento che lascia fissi tutti i triangoli.

Il resto del paragrafo contiene alcune applicazioni delle rappresentazioni mediante permutazioni.

(8.3) PROPOSIZIONE *Il gruppo  $GL_2(\mathbb{F}_2)$  delle matrici invertibili a coefficienti in  $\mathbb{F}_2$  è isomorfo al gruppo simmetrico  $S_3$ .*

*Dimostrazione.* Denotiamo il campo  $\mathbb{F}_2$  con  $F$ , e il gruppo  $GL_2(\mathbb{F}_2)$  con  $G$ . Abbiamo già elencato in precedenza [cap. 3 (2.10)] i sei elementi di  $G$ . Sia  $V = F^2$  lo spazio vettoriale dei vettori colonna; esso è costituito dai quattro vettori  $0, e_1, e_2, e_1 + e_2$ . Il gruppo  $G$  agisce su  $V$  e lascia fisso  $0$ , e quindi agisce sull'insieme dei tre vettori non nulli, i quali formano una sola orbita. Ciò fornisce una rappresentazione  $\varphi : G \rightarrow S_3$ . Ora l'immagine di  $e_1$  mediante la moltiplicazione per una matrice  $P \in G$  è la prima colonna di  $P$ , e l'immagine di  $e_2$  è la seconda colonna di  $P$ . Pertanto  $P$  non può agire in modo banale su questi due elementi, a meno che non sia l'identità. Ciò prova che l'azione di  $G$  è fedele, e quindi che l'applicazione  $\varphi$  è iniettiva. Poiché entrambi i gruppi hanno ordine 6,  $\varphi$  è un isomorfismo. ■

(8.4) PROPOSIZIONE *Indichiamo con  $c_g$  il coniugio mediante  $g$ , ossia l'applicazione  $c_g(x) = gxg^{-1}$ . L'applicazione  $f : S_3 \rightarrow \text{Aut}(S_3)$  dal gruppo simmetrico al suo gruppo degli automorfismi, definita dalla legge  $g \mapsto c_g$  è biiettiva.*

*Dimostrazione.* Sia  $A$  il gruppo degli automorfismi di  $S_3$ . Sappiamo dal capitolo 2 (3.4) che  $c_g$  è un automorfismo. Inoltre,  $c_{gh} = c_g c_h$ , poiché  $c_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = c_g(c_h(x))$  per ogni  $x$ . Ciò prova che  $f$  è un omomorfismo. Ora, il coniugio mediante  $g$  è l'identità, se e soltanto se,  $g$  appartiene al centro del gruppo. Il centro di  $S_3$  è banale, e pertanto  $f$  è iniettiva. Per dimostrare la suriettività di  $f$ , consideriamo una rappresentazione mediante permutazioni di  $A$ . Il gruppo  $A$  agisce sull'insieme  $S_3$  in modo ovvio; precisamente,

se  $\alpha$  è un automorfismo e  $s \in S_3$ , allora  $\alpha s = \alpha(s)$ . Elementi di  $S_3$  di ordini diversi apparterranno ad orbite distinte rispetto a tale azione; quindi  $A$  agisce, in particolare, sul sottoinsieme di  $S_3$  costituito dagli elementi di ordine 2, cioè l'insieme  $\{y, xy, x^2y\}$ . Se un automorfismo  $\alpha$  lascia fissi sia  $xy$  che  $y$ , allora lascia fisso anche il loro prodotto  $xyy = x$ . Poiché  $x$  e  $y$  generano  $S_3$ , l'unico automorfismo di questo tipo è l'identità. Ciò prova che l'azione di  $A$  su  $\{y, xy, x^2y\}$  è fedele e che la rappresentazione associata  $A \rightarrow \text{Perm}\{y, xy, x^2y\}$  è iniettiva. Pertanto l'ordine di  $A$  è al più 6, ma dato che  $f$  è iniettiva e l'ordine di  $S_3$  è 6, ne segue che  $f$  è biettiva. ■

(8.5) PROPOSIZIONE *Il gruppo degli automorfismi di un gruppo ciclico di ordine  $p$ , con  $p$  primo, è isomorfo al gruppo moltiplicativo  $\mathbb{F}_p^*$  degli elementi non nulli di  $\mathbb{F}_p$ .*

*Dimostrazione.* Usiamo il gruppo additivo  $\mathbb{F}_p$  come modello per un gruppo ciclico di ordine  $p$ . Esso è generato dall'elemento 1. Denotiamo il gruppo moltiplicativo  $\mathbb{F}_p^*$  con  $G$ . Allora  $G$  agisce su  $\mathbb{F}_p$  mediante la moltiplicazione a sinistra, e tale azione definisce un omomorfismo iniettivo  $\varphi : G \rightarrow \text{Perm}(\mathbb{F}_p)$  nel gruppo delle permutazioni dell'insieme  $\mathbb{F}_p$  di  $p$  elementi.

Inoltre, il gruppo di automorfismi  $A = \text{Aut}(\mathbb{F}_p)$  è un sottogruppo di  $\text{Perm}(\mathbb{F}_p)$ . La proprietà distributiva prova che la moltiplicazione per un elemento  $a \in \mathbb{F}_p^*$  è un automorfismo di  $\mathbb{F}_p$ . Infatti, essa è un'applicazione biettiva, e  $a(x+y) = ax+ay$ ; quindi l'immagine di  $\varphi : G \rightarrow \text{Perm}(\mathbb{F}_p)$  è contenuta nel sottogruppo  $A$ . Infine, un automorfismo di  $\mathbb{F}_p$  è determinato dall'immagine del generatore 1, e tale immagine non può essere zero. Usando l'azione di  $G$ , possiamo mandare 1 in qualsiasi elemento non nullo. Pertanto  $\varphi$  è un'applicazione suriettiva di  $G$  su  $A$ . Essendo iniettivo e suriettivo,  $\varphi$  è un isomorfismo. ■

## 9 Sottogruppi finiti del gruppo delle rotazioni

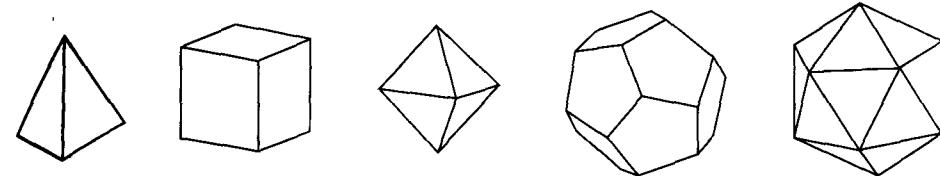
In questo paragrafo utilizzeremo la formula delle classi per classificare i sottogruppi finiti del gruppo delle rotazioni  $SO_3$ , che è stato definito nel capitolo 4 (5.4). Come accade per i gruppi finiti di movimenti del piano, esistono in realtà pochi sottogruppi finiti di  $SO_3$ , e sono tutti gruppi di simmetrie di figure ben note.

(9.1) TEOREMA *Ogni sottogruppo finito  $G$  di  $SO_3$  è uno dei seguenti gruppi:*

- $C_k$ : gruppo ciclico delle rotazioni di multipli di  $2\pi/k$  intorno a una retta;
- $D_k$ : gruppo diedrale (3.4) delle simmetrie di un poligono regolare di  $k$  lati;
- $T$ : gruppo tetraedrale delle 12 rotazioni che portano un tetraedro regolare in sé stesso;

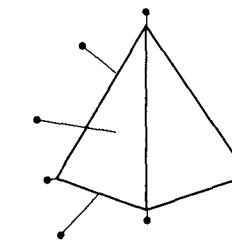
**O:** gruppo ottaedrale di ordine 24 delle rotazioni di un cubo, oppure di un ottaedro regolare;

**I:** gruppo icosaedrale delle 60 rotazioni di un dodecaedro regolare, oppure di un icosaedro regolare:



Non cercheremo di classificare i sottogruppi infiniti.

*Dimostrazione.* Sia  $G$  un sottogruppo finito di  $SO_3$ , e sia  $N$  il suo ordine. Ogni elemento  $g$  di  $G$  diverso dall'identità è una rotazione intorno a una retta  $\ell$ , e tale retta è ovviamente unica. Pertanto  $g$  lascia fissi esattamente due punti della sfera unitaria  $S$  di  $\mathbb{R}^3$ , precisamente i due punti di intersezione  $\ell \cap S$ . Chiamiamo tali punti i *poli* di  $g$ . Dunque un polo è un punto  $p$  sulla sfera unitaria tale che  $gp = p$  per qualche elemento  $g \neq 1$  di  $G$ . Per esempio, se  $G$  è il gruppo delle simmetrie di rotazione di un tetraedro  $\Delta$ , allora i poli saranno i punti di  $S$  situati sopra i vertici, i centri delle facce e i centri degli spigoli di  $\Delta$ .



Denotiamo con  $P$  l'insieme dei poli.

(9.2) LEMMA *L'insieme  $P$  è portato in sé dall'azione di  $G$  sulla sfera. Quindi  $G$  agisce su  $P$ .*

*Dimostrazione.* Sia  $p$  un polo, diciamo il polo di  $g \in G$ . Sia  $x$  un elemento arbitrario di  $G$ . Dobbiamo dimostrare che  $xp$  è un polo, ossia che  $xp$  è lasciato fisso da qualche elemento  $g'$  di  $G$  diverso dall'identità. L'elemento cercato è  $xgx^{-1}$ , infatti  $xgx^{-1}(xp) = xgp = xp$ , e  $xgx^{-1} \neq 1$  poiché  $g \neq 1$ . ■

Cerchiamo ora di ricavare informazioni sul gruppo, contando i poli. Poiché un elemento di  $G$  diverso da 1 ha due poli, si potrebbe pensare che vi siano

in tutto  $2N - 2$  poli. Ciò non è del tutto corretto, poiché uno stesso punto  $p$  può essere un polo per più elementi del gruppo.

Lo stabilizzatore  $G_p$  di un polo  $p$  è il gruppo di tutte le rotazioni intorno alla retta  $\ell = (0, p)$  che appartengono a  $G$ . Tale gruppo è ciclico ed è generato dalla rotazione di angolo minimo  $\theta$  in  $G$  [cfr. dimostrazione del teorema (3.4a)]. Se l'ordine dello stabilizzatore è  $r_p$ , allora  $\theta = 2\pi/r_p$ .

Sappiamo che  $r_p > 1$  poiché, essendo  $p$  un polo, lo stabilizzatore  $G_p$  contiene un elemento diverso da 1. In base alla formula delle classi (7.2), si ha:

$$|G_p| \cdot |O_p| = |G|.$$

Scriviamo questa equazione nella forma:

$$(9.3) \quad r_p n_p = N,$$

dove  $n_p$  è il numero dei poli nell'orbita  $O_p$  di  $p$ .

L'insieme degli elementi di  $G$  con un polo  $p$  assegnato è lo stabilizzatore  $G_p$ , privato dell'identità. Pertanto vi sono  $(r_p - 1)$  elementi del gruppo aventi  $p$  come polo. D'altra parte, ogni elemento  $g$  del gruppo, diverso da 1, ha due poli. Dovendo sottrarre 1 dappertutto può esserci un po' di confusione, tuttavia la relazione corretta è:

$$(9.4) \quad \sum_{p \in P} (r_p - 1) = 2N - 2.$$

Ora, se  $p$  e  $p'$  appartengono a una stessa orbita, gli stabilizzatori  $G_p$  e  $G_{p'}$  hanno lo stesso ordine. Ciò accade poiché  $O_p = O_{p'}$  e  $|G| = |G_p| \cdot |O_p| = |G_{p'}| \cdot |O_{p'}|$ . Pertanto possiamo raccogliere insieme nel membro a sinistra di (9.4) i termini che corrispondono ai poli in un'orbita  $O_p$  assegnata. Vi sono  $n_p$  termini siffatti, sicché il numero dei poli raccolti insieme è  $n_p(r_p - 1)$ . Denotiamo le orbite con  $O_1, O_2, \dots$ . Allora:

$$\sum_i n_i(r_i - 1) = 2N - 2,$$

dove  $n_i = |O_i|$  e  $r_i = |G_{O_i}|$  per qualsiasi  $p \in O_i$ . Poiché  $N = n_i r_i$ , possiamo dividere per  $N$  entrambi i membri e poi scambiarli tra loro, in modo da ottenere la celebre formula:

$$(9.5) \quad 2 - \frac{2}{N} = \sum_i \left(1 - \frac{1}{r_i}\right).$$

Questa formula può non apparire molto promettente a prima vista, ma fornisce una grande quantità di informazioni. Il membro a sinistra è minore di 2, mentre ciascun termine a destra è almeno  $\frac{1}{2}$ . Ne segue che non ci possono essere più di tre orbite!

Il resto della classificazione si fa elencando i vari casi possibili:

**Una sola orbita:**  $2 - \frac{2}{N} = 1 - \frac{1}{r}$ . Ciò è impossibile, poiché

$$2 - \frac{2}{N} \geq 1, \text{ mentre } 1 - \frac{1}{r} < 1.$$

**Due orbite:**  $2 - \frac{2}{N} = \left(1 - \frac{1}{r_1}\right) + \left(1 - \frac{1}{r_2}\right)$ , ossia,  $\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2}$ .

Sappiamo che  $r_i \leq N$ , poiché  $r_i$  divide  $N$ . Tale equazione può valere soltanto se  $r_1 = r_2 = N$ . (Quindi  $n_1 = n_2 = 1$ .) Vi sono due poli  $p, p'$ , entrambi lasciati fissi da ogni elemento del gruppo. Ovviamente,  $G$  è il gruppo ciclico  $C_N$  delle rotazioni intorno alla retta  $\ell$  passante per  $p$  e  $p'$ .

**Tre orbite:** Questo è il caso più importante: la formula (9.5) si riduce a

$$\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1.$$

Scriviamo gli  $r_i$  in ordine crescente. Allora  $r_1 = 2$ . Infatti, se tutti gli  $r_i$  valessero almeno 3, allora il membro a destra sarebbe  $\leq 0$ , che è impossibile.

**Caso 1.** Almeno due degli ordini  $r_i$  valgono 2:  $r_1 = r_2 = 2$ . Il terzo ordine  $r_3 = r$  può essere arbitrario, e  $N = 2r$ . Allora  $n_3 = 2$ , ossia esiste una coppia di poli  $\{p, p'\}$  che forma l'orbita  $O_3$ . Ogni elemento  $g$  lascia fissi  $p$  e  $p'$  oppure li scambia tra loro. Pertanto gli elementi di  $G$  sono rotazioni intorno alla retta  $\ell = (p, p')$ , oppure sono rotazioni di  $\pi$  intorno a una retta  $\ell'$  perpendicolare a  $\ell$ . Si vede facilmente che  $G$  è il gruppo delle rotazioni che lasciano fisso un poligono regolare di  $r$  lati  $\Delta$ , ossia il gruppo diedrale  $D_r$ . Il poligono  $\Delta$  giace nel piano perpendicolare a  $\ell$ , con i vertici e i centri dei lati corrispondenti ai poli rimanenti. Le simmetrie (di riflessione) bilaterali del poligono in  $\mathbb{R}^2$  sono diventate rotazioni di un angolo  $\pi$ , dopo aver posto  $\Delta$  in  $\mathbb{R}^3$ .

**Caso 2.** Uno solo degli  $r_i$  è uguale a 2. Le terne  $r_1 = 2, r_2 \geq 4, r_3 \geq 4$  non sono ammissibili, poiché  $1/2 + 1/4 + 1/4 - 1 = 0$ . Analogamente, le terne  $r_1 = 2, r_2 = 3, r_3 \geq 6$  non sono ammissibili, poiché  $1/2 + 1/3 + 1/6 - 1 = 0$ . Restano soltanto tre casi possibili:

- (9.6)    (i)  $r_i = (2, 3, 3)$ ,  $N = 12$ ;  
(ii)  $r_i = (2, 3, 4)$ ,  $N = 24$ ;  
(iii)  $r_i = (2, 3, 5)$ ,  $N = 60$ .

Ci restano da analizzare questi tre casi. Illustriamo brevemente le configurazioni corrispondenti:

- (9.7) (i)  $n_i = (6, 4, 4)$ . I poli nell'orbita  $O_2$  sono i vertici di un tetraedro regolare  $\Delta$ , e  $G$  è il gruppo delle rotazioni che lo lasciano fisso:  $G = T$ . Qui  $n_1$  è il numero degli spigoli di  $\Delta$ , e  $n_2, n_3$  sono, rispettivamente, il numero dei vertici e il numero delle facce di  $\Delta$ .
- (ii)  $n_i = (12, 8, 6)$ . I poli in  $O_2$  sono i vertici di un cubo, e i poli in  $O_3$  sono i vertici di un ottaedro regolare.  $G = O$  è il gruppo delle loro rotazioni. Gli interi  $n_i$  sono, rispettivamente, i numeri degli spigoli, dei vertici e delle facce di un cubo.
- (iii)  $n_i = (30, 20, 12)$ . I poli in  $O_2$  sono i vertici di un dodecaedro regolare, e quelli in  $O_3$  sono i vertici di un icosaedro regolare:  $G = I$ .

C'è ancora un po' di lavoro da fare per dimostrare le affermazioni di (9.7). Intuitivamente, i poli in un'orbita dovrebbero essere i vertici di un poliedro regolare, perché formano un'orbita e pertanto sono disposti in modo uniforme sulla sfera. Tuttavia, ciò non è del tutto corretto, poiché i centri degli spigoli di un cubo, per esempio, formano un'orbita, ma non generano un poliedro regolare. (La figura che essi generano è chiamata un poliedro *troncato*.)

Ad esempio, consideriamo (9.7iii). Sia  $p$  uno dei 12 poli in  $O_3$ , e sia  $q$  uno dei poli di  $O_2$  più vicini a  $p$ . Poiché lo stabilizzatore di  $p$  è di ordine 5 e agisce su  $O_2$  (giacché altrettanto fa  $G$ ), le immagini di  $q$  forniscono un insieme di cinque poli, tra i più vicini a  $p$ , ottenuti da  $q$  mediante le cinque rotazioni intorno a  $p$  in  $G$ . Pertanto il numero dei poli di  $O_2$  più vicini a  $p$  è un multiplo di 5, e si vede facilmente che 5 è l'unica possibilità. Dunque questi cinque poli sono i vertici di un pentagono regolare. I 12 pentagoni così definiti formano un dodecaedro regolare. ■

Chiudiamo il capitolo osservando che, per il gruppo  $M_3$  dei movimenti rigidi dello spazio a 3 dimensioni, esiste una trattazione analoga a quella dei movimenti del piano da noi sviluppata. In particolare, si può definire la nozione di *gruppo cristallografico spaziale*, che è un sottogruppo discreto il cui gruppo di traslazioni è un reticolo  $L$  di dimensione tre. Dire che  $L$  è un reticolo equivale a dire che vi sono tre vettori linearmente indipendenti  $a, b, c$  in  $\mathbb{R}^3$  tali che  $t_a, t_b, t_c \in G$ . Tali gruppi cristallografici sono analoghi ai gruppi cristallografici in  $M = M_2$ , e i cristalli forniscono esempi di configurazioni di dimensione tre aventi tali gruppi come gruppi di simmetrie. Immaginiamo che i cristalli siano infinitamente grandi. Allora il fatto che le molecole sono disposte con regolarità implica che esse formano una configurazione avente tre simmetrie di traslazione indipendenti. È stato dimostrato che esistono 230 tipi di gruppi cristallografici spaziali, analoghi ai 17 gruppi cristallografici piani (4.15). Si tratta di una lista troppo lunga per essere davvero utile, e pertanto i cristalli sono stati classificati sommariamente

*gruppi puntuali* corrispondenti, basta consultare un libro di cristallografia.

Una buona eredità è meglio del più bel problema di geometria, perché rimpiazza un metodo generale e serve a risolvere di un gran numero di problemi.

Gottfried Wilhelm Leibniz

## Esercizi

### 1 Simmetria delle figure piane

1. Dimostrare che l'insieme delle simmetrie di una figura  $F$  nel piano costituisce un gruppo.
2. Elencare tutte le simmetrie di (a) un quadrato e (b) un pentagono regolare.
3. Elencare tutte le simmetrie delle seguenti figure:  
 (a) (1.4) (b) (1.5) (c) (1.6) (d) (1.7).
4. Sia  $G$  un gruppo finito di rotazioni del piano intorno all'origine. Dimostrare che  $G$  è ciclico.

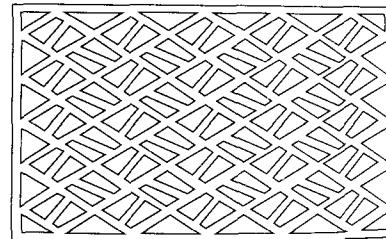
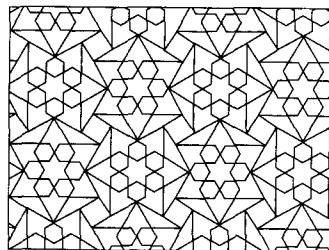
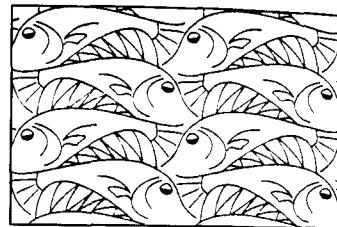
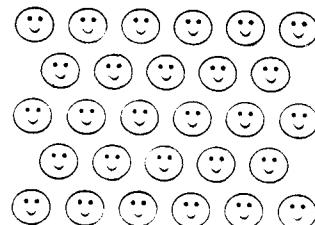
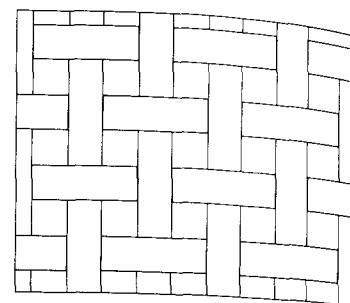
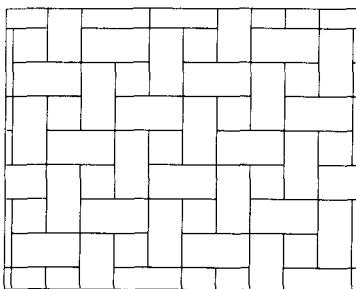
### 2 Il gruppo dei movimenti del piano

1. Calcolare algebricamente il punto fisso di  $t_a\rho_\theta$ .
2. Verificare le regole (2.5) mediante calcoli esplicativi, utilizzando le definizioni (2.3).
3. Dimostrare che  $\mathbf{O}$  non è un sottogruppo normale di  $M$ .
4. Sia  $m$  un movimento che inverte l'orientazione. Dimostrare che  $m^2$  è una traslazione.
5. Si denoti con  $SM$  il sottoinsieme dei movimenti del piano che conservano l'orientazione. Dimostrare che  $SM$  è un sottogruppo normale di  $M$ , e determinare il suo indice in  $M$ .
6. Dimostrare che un operatore lineare su  $\mathbb{R}^2$  è una riflessione se e solo se i suoi autovalori sono 1 e  $-1$ , e i suoi autovettori sono ortogonali.
7. Dimostrare che un coniugato di una riflessione o di una glissoriflessione è un movimento dello stesso tipo, e che se  $m$  è una glissoriflessione, allora i vettori di spostamento di  $m$  e dei suoi coniugati hanno la stessa lunghezza.
8. Dimostrare che l'applicazione (2.12) è un omomorfismo.
9. Dimostrare che l'applicazione  $M \rightarrow \{1, r\}$  definita da:  $t_a\rho_\theta \mapsto 1$ ,  $t_a\rho_\theta r \mapsto r$  è un omomorfismo.
10. Calcolare l'effetto della rotazione degli assi di un angolo  $\eta$  sulle espressioni  $t_a\rho_\theta$  e  $t_a\rho_\theta r$  di un movimento.
11. (a) Calcolare gli autovalori e gli autovettori dell'operatore lineare  $m = \rho_\theta r$ .  
 (b) Dimostrare algebricamente che  $m$  è una riflessione intorno a una retta passante per l'origine e formante un angolo di ampiezza  $\frac{1}{2}\theta$  con l'asse  $x$ .  
 (c) Dimostrare geometricamente il risultato enunciato in (b).

- 12.** Calcolare il vettore di spostamento della glissoriflessione  $t_a \rho_{\theta T}$  in termini di  $a$  e  $\theta$ .
- 13.** (a) Sia  $m$  una glissoriflessione rispetto a una retta  $\ell$ . Dimostrare geometricamente che un punto  $x$  appartiene a  $\ell$  se e solo se i punti  $x$ ,  $m(x)$ ,  $m^2(x)$  sono allineati.  
(b) Viceversa, dimostrare che se  $m$  è un movimento che inverte l'orientazione e c'è un punto tale che  $x$ ,  $m(x)$ ,  $m^2(x)$  sono punti distinti su una retta  $\ell$ , allora  $m$  è una glissoriflessione rispetto a  $\ell$ .
- 14.** Trovare un isomorfismo dal gruppo  $SM$  al sottogruppo di  $GL_2(\mathbb{C})$  delle matrici della forma:  $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ , con  $|a| = 1$ .
- 15.** (a) Scrivere le formule per i movimenti (2.3), utilizzando la variabile complessa  $z = x + iy$ .
- (b) Dimostrare che ogni movimento ha la forma  $m(z) = \alpha z + \beta$  oppure  $m(z) = \alpha \bar{z} + \beta$ , dove  $|\alpha| = 1$  e  $\beta$  è un numero complesso arbitrario.

- 3. Gruppi finiti di movimenti**
- Si denoti con  $D_n$  il gruppo diedrale (3.6). Esprimere il prodotto  $x^2 y x^{-1} y^{-1} x^3 y^3$  nella forma  $x^i y^j$  in  $D_n$ .
  - Elencare tutti i sottogruppi del gruppo  $D_4$ , trovando quelli normali.
  - Trovare tutti i sottogruppi normali propri e determinare i gruppi quoziante dei gruppi  $D_{13}$  e  $D_{15}$ .
  - (a) Calcolare esplicitamente le classi laterali del sottogruppo  $H = \{1, x^5\}$  nel gruppo diedrale  $D_{10}$ .  
(b) Dimostrare che  $D_{10}/H$  è isomorfo a  $D_5$ .  
(c) È vero che  $D_{10}$  è isomorfo a  $D_5 \times H$ ?
  - Elencare i sottogruppi di  $G = D_6$  che non contengono  $N = \{1, x^3\}$ .
  - Dimostrare che ogni sottogruppo finito di  $M$  è un sottogruppo coniugato di uno dei sottogruppi standard elencati nel corollario (3.5).
- 4 Gruppi discreti di movimenti**
- Dimostrare che un gruppo discreto  $G$  costituito da rotazioni intorno all'origine è ciclico ed è generato da  $\rho_\theta$ , dove  $\theta$  è il più piccolo angolo (positivo) di rotazione in  $G$ .  
Dimostrare algebricamente che  $G$  contiene una traslazione.
  - Sia  $G$  un sottogruppo di  $M$  che contiene rotazioni intorno a due punti distinti. Determinare il gruppo puntuale di  $G$ .
  - Sia  $(a, b)$  una base di un reticolo  $L$  in  $\mathbb{R}^2$ . Dimostrare che ogni altra base di  $L$  ha la forma  $(a', b') = (a, b)P$ , dove  $P$  è una matrice  $2 \times 2$  ad elementi interi, con determinante  $\pm 1$ .
  - Determinare il gruppo puntuale per ciascuno dei disegni illustrati nella figura (4.16).
- 5.** (a) Sia  $B$  un quadrato di lato  $a$ , e sia  $\epsilon > 0$  fissato. Sia  $S$  un sottoinsieme di  $B$  tale che la distanza tra due punti arbitrari di  $S$  sia  $\geq \epsilon$ . Trovare esplicitamente un maggiorante per il numero degli elementi di  $S$ .  
(b) Fare la stessa cosa per un ipercubo  $B$  in  $\mathbb{R}^n$ .
- 6.** Dimostrare che il sottogruppo di  $\mathbf{R}$  generato da 1 e  $\sqrt{2}$  è denso in  $\mathbf{R}$ .
- 7.** Dimostrare che ogni sottogruppo discreto di  $\mathbf{O}$  è finito.
- 8.** Sia  $G$  un sottogruppo discreto di  $M$ . Dimostrare che esiste un punto  $p_0$  nel piano che non è lasciato fisso da nessun elemento di  $G$  diverso dall'identità.
- 9.** Dimostrare che il gruppo delle simmetrie del seguente disegno di un fregio:
- ... E E E E E E E E ...
- è isomorfo al prodotto diretto  $C_2 \times C_\infty$  di un gruppo ciclico di ordine 2 e di un gruppo ciclico infinito.
- 10.** Sia  $G$  il gruppo delle simmetrie del seguente disegno di un fregio:
- ... L L L L L L L L ...
- Determinare il gruppo puntuale  $\overline{G}$  di  $G$ .
  - Per ciascun elemento  $\bar{g} \in \overline{G}$ , e ciascun elemento  $g \in G$  che rappresenta  $\bar{g}$ , descrivere geometricamente l'azione di  $g$ .
  - Sia  $H$  il sottogruppo delle traslazioni di  $G$ . Determinare  $[G : H]$ .
- 11.** Sia  $G$  il gruppo delle simmetrie del disegno:
- 
- 12.** Sia  $G$  il gruppo delle simmetrie di un reticolo triangolare equilatero  $L$ . Determinare l'indice in  $G$  del sottogruppo  $T \cap G$ .
- 13.** Sia  $G$  un gruppo discreto in cui ogni elemento conserva l'orientazione. Dimostrare che il gruppo puntuale  $\overline{G}$  è un gruppo ciclico di rotazioni e che esiste un punto  $p$  nel piano tale che l'insieme degli elementi del gruppo che lasciano fisso  $p$  è isomorfo a  $\overline{G}$ .

- 14.** Per ciascuno dei disegni seguenti, trovare un disegno in (4.16) con lo stesso tipo di simmetria:



- 15.** Sia  $N$  il gruppo dei movimenti rigidi della retta  $\ell = \mathbb{R}^1$ . Alcuni elementi di  $N$  sono:

$$t_a : x \mapsto x + a, \quad a \in \mathbb{R}, \quad s : x \mapsto -x.$$

- (a) Dimostrare che gli elementi di  $N$  sono della forma  $t_a$  oppure  $t_a s$ , e descrivere geometricamente la loro azione su  $\ell$ .
- (b) Calcolare i prodotti  $t_a t_b$ ,  $s t_a$ ,  $s s$ .
- (c) Trovare tutti i sottogruppi discreti di  $N$  che contengono una traslazione. (Converrà scegliere l'origine e l'unità di misura con riferimento al sottogruppo particolare.) Dimostrare che la lista ottenuta è completa.

- \*16.** Sia  $N'$  il gruppo dei movimenti della striscia infinita:

$$R = \{(x, y) \mid -1 \leq y \leq 1\}.$$

Esso può essere considerato come un sottogruppo del gruppo  $M$ . I seguenti elementi appartengono a  $N'$ :

$$t_a : (x, y) \mapsto (x + a, y)$$

$$s : (x, y) \mapsto (-x, y)$$

$$r : (x, y) \mapsto (x, -y)$$

$$\rho : (x, y) \mapsto (-x, -y).$$

- (a) Dimostrare che questi elementi generano  $N'$ , e descrivere gli elementi di  $N'$  come prodotti.

- (b) Enunciare e dimostrare le regole analoghe alle (2.5) per tali movimenti.

- (c) Un disegno di un fregio è un qualsiasi disegno sulla striscia che sia periodico e non degenere, nel senso che il suo gruppo delle simmetrie è discreto. Data la periodicità, il suo gruppo delle simmetrie conterrà una traslazione. Alcuni esempi di disegni di fregio sono illustrati nel testo (1.3, 1.4, 1.6, 1.7). Classificare i gruppi delle simmetrie corrispondenti, identificando quelli che differiscono tra loro soltanto per la scelta dell'origine e dell'unità di misura sulla striscia. Si suggerisce di cominciare provando a fare disegni con vari tipi di simmetrie. Fare un'analisi accurata dei singoli casi nella dimostrazione dei risultati. Si potrebbe procedere nel modo seguente:

Sia  $G$  un sottogruppo discreto contenente una traslazione.

Caso 1: Ogni elemento di  $G$  è una traslazione. Allora ...

Caso 2:  $G$  contiene la rotazione  $\rho$  ma non contiene nessuna simmetria che inverte l'orientazione. Allora ...

e così via.

- \*17.** Sia  $L$  un reticolo di  $\mathbb{R}^2$ , e siano  $a, b$  vettori linearmente indipendenti in  $L$ . Dimostrare che il sottogruppo  $L' = \{ma + nb \mid m, n \in \mathbb{Z}\}$  di  $L$  generato da  $a, b$  ha indice finito, e che l'indice è il numero dei punti del reticolo contenuti nel parallelogramma di vertici  $0, a, b, a + b$  e non appartenenti ai "lati lontani"  $[a, a + b]$  e  $[b, a + b]$ . (Pertanto,  $0$  è incluso, e così pure i punti che giacciono sui lati  $[0, a], [0, b]$ , fatta eccezione per i punti  $a, b$ .)

- 18.** (a) Trovare un sottoinsieme  $F$  del piano che non è lasciato fisso da nessun movimento  $m \in M$ .

- (b) Sia  $G$  un gruppo discreto di movimenti. Dimostrare che l'unione  $S$  di tutte le immagini di  $F$  mediante gli elementi di  $G$  è un sottoinsieme il cui gruppo delle simmetrie  $G'$  contiene  $G$ .

- (c) Provare con un esempio che  $G'$  può essere più grande di  $G$ .

- \*19.** Dimostrare che esiste un sottoinsieme  $F$  tale che  $G' = G$ .

- \*19.** Sia  $G$  un gruppo cristalografico tale che nessun elemento  $g \neq 1$  lascia fisso alcun punto del piano. Dimostrare che  $G$  è generato da due traslazioni, oppure da una traslazione e una glissoriflessione.

- \*20. Sia  $G$  un gruppo cristalografico il cui gruppo dei punti è  $D_1 = \{1, r\}$ .
- Dimostrare che le rette delle glissoriflessioni e le rette delle riflessioni di  $r$  sono tutte parallele.
  - Si ponga  $L = L_G$ . Provare che  $L$  contiene vettori non nulli  $a = (a_1, 0)^t$ ,  $b = (0, b_2)^t$ .
  - Denotiamo con  $a$  e  $b$  i vettori più piccoli del tipo indicato in (b). Allora una base del reticolo  $L$  è data da  $(a, b)$  oppure  $(a, c)$ , dove  $c = \frac{1}{2}(a + b)$ .
  - Dimostrare che, se le coordinate nel piano sono scelte in modo tale che l'asse  $x$  sia una retta di glissoriflessione, allora  $G$  contiene uno degli elementi  $g = r$  oppure  $g = t_{\frac{1}{2}a}r$ . In entrambi i casi, provare che  $G = L \cup Lg$ .
  - Esistono quattro casi possibili descritti dalle alternative (c) e (d). Provare che vi sono soltanto tre tipi distinti di gruppi.
21. Dimostrare che se il gruppo puntuale di un gruppo cristalografico  $G$  è  $C_6$ ,  $L = L_G$  è un reticolo triangolare equilatero, e  $G$  è il gruppo di tutte le simmetrie di rotazione di  $L$  intorno all'origine.
22. Dimostrare che se il gruppo puntuale di un gruppo cristalografico  $G$  è  $D_6$ ,  $L = L_G$  è un reticolo triangolare equilatero, e  $G$  è il gruppo di tutte le simmetrie di  $L$ .
- \*23. Dimostrare che i gruppi delle simmetrie dei disegni illustrati nella figura (4.16) esauriscono i casi possibili.
- 5 Simmetria astratta: azione di un gruppo*
- Determinare il gruppo degli automorfismi dei seguenti gruppi:
    - $C_4$ ;  $C_6$ ;  $C_2 \times C_2$ .
  - Dimostrare che la relazione (5.4) è una relazione di equivalenza.
  - Sia  $S$  un insieme su cui agisce  $G$ . Dimostrare che la relazione  $s \sim s'$  se  $s' = gs$  per qualche  $g \in G$ , è una relazione di equivalenza.
  - Sia  $\varphi : G \rightarrow G'$  un omomorfismo, e sia  $S$  un insieme su cui agisce  $G'$ . Dimostrare che è possibile definire un'azione di  $G$  su  $S$ , utilizzando l'omomorfismo  $\varphi$ .
  - Sia  $G = D_4$  il gruppo diedrale delle simmetrie del quadrato.
    - Qual è lo stabilizzatore di un vertice? e di un lato?
    - $G$  agisce sull'insieme di due elementi costituito dalle diagonali. Qual è lo stabilizzatore di una diagonale?
  - In ciascuna delle figure illustrate nell'esercizio 14 del paragrafo 4, trovare i punti che hanno stabilizzatori non banali, e determinare tali stabilizzatori.
  - \*7. Sia  $G$  un sottogruppo discreto di  $M$ .
    - Dimostrare che lo stabilizzatore  $G_p$  di un punto  $p$  è finito.
    - Dimostrare che l'orbita  $O_p$  di un punto  $p$  è un insieme discreto, ossia che esiste un numero reale  $\epsilon > 0$  tale che la distanza tra due punti distinti dell'orbita è almeno  $\epsilon$ .

- Siano  $B, B'$  due regioni limitate del piano. Dimostrare che esiste soltanto un numero finito di elementi  $g \in G$  tali che l'intersezione  $gB \cap B'$  è non vuota.
  - Si consideri l'azione di  $G = GL_n(\mathbb{R})$  sull'insieme  $S = \mathbb{R}^n$  mediante la moltiplicazione a sinistra.
    - Descrivere la decomposizione di  $S$  nelle orbite rispetto a tale azione.
    - Qual è lo stabilizzatore di  $e_1$ ?
  - Decomporre l'insieme  $\mathbb{C}^{2 \times 2}$  delle matrici complesse  $2 \times 2$  rispetto alle seguenti azioni di  $GL_2(\mathbb{C})$ :
    - moltiplicazione a sinistra;
    - coniugio.
  - (a) Sia  $S = \mathbb{R}^{m \times n}$  l'insieme delle matrici reali  $m \times n$ , e sia  $G = GL_m(\mathbb{R}) \times GL_n(\mathbb{R})$ . Dimostrare che la legge:  $(P, Q), A \mapsto PAQ^{-1}$  definisce un'azione di  $G$  su  $S$ .
    - Descrivere la decomposizione di  $S$  in  $G$ -orbite.
    - Sia  $m \leq n$ . Qual è lo stabilizzatore della matrice  $[I \mid O]$ ?
  - (a) Descrivere l'orbita e lo stabilizzatore della matrice  $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$  rispetto al coniugio in  $GL_2(\mathbb{R})$ .
    - Interpretare la matrice in  $GL_2(\mathbb{F}_3)$  e determinare l'ordine (ossia il numero degli elementi) dell'orbita.
  - (a) Definire un automorfismo di un campo.
    - Dimostrare che il campo  $\mathbb{Q}$  dei numeri razionali non possiede automorfismi diversi dall'identità.
    - Determinare  $\text{Aut } F$ , dove  $F = \mathbb{Q}[\sqrt{2}]$  (cfr. 000).
- 6 L'azione sulle classi laterali*
- Qual è lo stabilizzatore della classe laterale  $aH$  rispetto all'azione di  $G$  su  $G/H$ ?
  - Sia  $G$  un gruppo, e sia  $H$  il sottogruppo ciclico generato da un elemento  $x$  di  $G$ . Dimostrare che se la moltiplicazione a sinistra per  $x$  lascia fissa ogni classe laterale di  $H$  in  $G$ , allora  $H$  è un sottogruppo normale.
  - (a) Descrivere esplicitamente l'applicazione biettiva (6.4), nel caso in cui  $G$  è il gruppo diedrale  $D_4$  e  $S$  è l'insieme dei vertici di un quadrato.
    - Fare la stessa cosa per  $D_n$  e per i vertici di un poligono regolare di  $n$  lati.
  - (a) Descrivere esplicitamente lo stabilizzatore  $H$  dell'indice 1 rispetto all'azione del gruppo simmetrico  $G = S_n$  su  $\{1, \dots, n\}$ .
    - Descrivere esplicitamente l'azione di  $G$  sulle classi laterali di  $H$  in  $G$ .
    - Descrivere esplicitamente l'applicazione (6.4).
  - Descrivere tutti i modi possibili in cui  $S_3$  può agire su un insieme di quattro elementi.
  - Dimostrare la proposizione (6.5).

7. Un'applicazione  $S \rightarrow S'$  di  $G$ -insiemi è un *omomorfismo* di  $G$ -insiemi se  $\varphi(gs) = g\varphi(s)$  per ogni  $s \in S$  e per ogni  $g \in G$ . Sia  $\varphi$  un omomorfismo siffatto. Dimostrare che:
- Lo stabilizzatore  $G_{\varphi(s)}$  contiene lo stabilizzatore  $G_s$ .
  - L'orbita di un elemento  $s \in S$  viene mandata sull'orbita di  $\varphi(s)$ .

### 7 La formula delle classi

- Utilizzare la formula delle classi per determinare gli ordini del gruppo delle simmetrie di rotazione di un cubo e del gruppo delle simmetrie di rotazione di un tetraedro.
- Sia  $G$  il gruppo delle simmetrie di rotazione di un cubo  $C$ . Due tetraedri regolari  $\Delta, \Delta'$  possono essere inscritti in  $C$ , ciascuno utilizzando metà dei vertici. Qual è l'ordine dello stabilizzatore di  $\Delta$ ?
- Calcolare l'ordine del gruppo delle simmetrie di un dodecaedro, includendo sia le rotazioni che le simmetrie che invertono l'orientazione, quali le riflessioni rispetto a piani. Fare la stessa cosa per le simmetrie di un cubo e di un tetraedro.
- Sia  $G$  il gruppo delle simmetrie di rotazione di un cubo, siano  $S_v, S_s, S_f$  gli insiemi dei vertici, degli spigoli e delle facce del cubo, e siano  $H_v, H_s, H_f$  gli stabilizzatori di un vertice, di uno spigolo e di una faccia. Determinare le formule che descrivono la decomposizione di ciascuno dei tre insiemi in orbite per ciascuno dei sottogruppi.
- Siano  $G \supset H \supset K$  gruppi. Dimostrare la formula:  $[G : K] = [G : H][H : K]$  senza l'ipotesi che  $G$  sia finito.
- (a) Dimostrare che se  $H$  e  $K$  sono sottogruppi di indice finito di un gruppo  $G$ , anche l'intersezione  $H \cap K$  è di indice finito.  
(b) Provare con un esempio che l'indice  $[H : H \cap K]$  non divide necessariamente  $[G : K]$ .

### 8 Rappresentazioni mediante permutazioni

- Determinare tutti i modi in cui il gruppo tetraedrale  $T$  (cfr. (9.1)) può agire su un insieme di due elementi.
- Sia  $S$  un insieme sul quale agisce un gruppo  $G$ , e si ponga  $H = \{g \in G \mid gs = s \text{ per ogni } s \in S\}$ . Dimostrare che  $H$  è un sottogruppo normale di  $G$ .
- Sia  $G$  il gruppo diedrale delle simmetrie di un quadrato. Stabilire se l'azione di  $G$  sui vertici o sulle diagonali è fedele.
- Supponiamo che esistano due orbite per l'azione di un gruppo  $G$  su un insieme  $S$ , e che esse abbiano ordini  $m, n$ , rispettivamente. Utilizzare l'azione per definire un omomorfismo da  $G$  al prodotto di gruppi simmetrici  $S_m \times S_n$ .
- Un gruppo  $G$  agisce fedelmente su un insieme  $S$  di cinque elementi, e vi sono due orbite: una di ordine 3 e una di ordine 2. Quali sono i casi possibili per  $G$ ?
- Completare la dimostrazione della proposizione (8.2).
- Sia  $F = \mathbb{F}_3$ . Descrivere i quattro sottospazi di dimensione uno dello spazio dei vettori colonna  $F^2$ . La moltiplicazione a sinistra per una matrice invertibile permuta questi

- sottospazi.** Dimostrare che tale azione definisce un omomorfismo  $\varphi : GL_2(F) \rightarrow S_4$ . Determinare il nucleo e l'immagine di  $\varphi$ .
- Per ciascuno dei gruppi seguenti, trovare il più piccolo intero  $n$  tale che il gruppo abbia un'azione fedele su un insieme con  $n$  elementi:
- il gruppo dei quaternioni  $H$ ;
  - $D_4$ ;
  - $D_6$ .

### 9 Sottogruppi finiti del gruppo delle rotazioni

- Descrivere le orbite dei poli per il gruppo delle rotazioni di un ottaedro e di un icosaedro.
- Determinare il gruppo delle simmetrie di una palla da baseball, tenendo conto delle cuciture e considerando anche le simmetrie che invertono l'orientazione.
- Sia  $O$  il gruppo delle rotazioni di un cubo. Determinare lo stabilizzatore di una diagonale che congiunge due vertici opposti.
- Sia  $G = O$  il gruppo delle rotazioni di un cubo, e sia  $H$  il sottogruppo che porta uno dei due tetraedri inscritti in sé (si veda l'esercizio 2 del §7). Provare che  $H = T$ .
- Dimostrare che il gruppo icosaedrale ha un sottogruppo di ordine 10.
- Determinare tutti i sottogruppi dei seguenti gruppi:
  - $T$ ;
  - $I$ .
- Spiegare perché i gruppi delle simmetrie del cubo e dell'ottaedro, e del dodecaedro e dell'icosaedro, sono uguali.
- (a) I 12 punti  $(\pm 1, \pm \alpha, 0), (0, \pm 1, \pm \alpha), (\pm \alpha, 0, \pm 1)$  formano i vertici di un icosaedro regolare, se  $\alpha$  è scelto in modo opportuno. Verificare ciò, e determinare  $\alpha$ .  
(b) Determinare la matrice della rotazione di  $2\pi/5$  intorno all'origine in  $\mathbb{R}^2$ .  
(c) Determinare la matrice della rotazione di  $\mathbb{R}^3$  di  $2\pi/5$  intorno all'asse che contiene il punto  $(1, \alpha, 0)$ .
- Dimostrare la restrizione cristallografica per i gruppi cristallografici spaziali: una simmetria di rotazione di un cristallo ha ordine 2, 3, 4 o 6.

### Esercizi vari

- Descrivere completamente i seguenti gruppi:
  - $\text{Aut } D_4$ ;
  - $\text{Aut } H$ , dove  $H$  è il gruppo dei quaternioni.
- (a) Dimostrare che l'insieme  $\text{Aut } G$  degli automorfismi di un gruppo  $G$  costituisce un gruppo.  
(b) Dimostrare che l'applicazione  $\varphi : G \rightarrow \text{Aut } G$  definita da:  $g \mapsto (\text{coniugio mediante } g)$  è un omomorfismo, e determinarne il nucleo.  
(c) Un automorfismo dato dal coniugio mediante un elemento del gruppo si chiama un *automorfismo interno*. Dimostrare che l'insieme degli automorfismi interni, ossia l'immagine di  $\varphi$ , è un sottogruppo normale di  $\text{Aut } G$ , che si denota con  $\text{Int } G$ .

3. Dato il gruppo dei quaternioni  $H$ , determinare il gruppo quoziante  $\text{Aut } H / \text{Int } H$ .

\*4. Sia  $G$  un gruppo cristallografico piano. Un *dominio fondamentale*  $D$  per  $G$  è una regione limitata del piano il cui bordo è costituito da curve lisce a tratti, tale che gli insiemi  $gD$ , al variare di  $g$  in  $G$ , ricoprono il piano senza sovrapposizioni, fatta eccezione per il bordo. Supponiamo che  $D$  abbia un numero finito di componenti connesse.

(a) Trovare domini fondamentali per i gruppi delle simmetrie dei disegni illustrati nell'esercizio 14 del paragrafo 4.

(b) Provare che due domini fondamentali arbitrari  $D, D'$  per  $G$  possono essere tagliati in un numero finito di pezzi congruenti della forma:  $gD \cap D'$  oppure  $D \cap gD'$  (si veda l'esercizio 7 del §5).

(c) Concludere che  $D$  e  $D'$  hanno la stessa area. (Può accadere che le curve del bordo si intersechino infinite volte, e ciò solleva qualche problema intorno alla definizione di area. Si suggerisce di mettere da parte tali considerazioni, nella soluzione.)

\*5. Sia  $G$  un gruppo cristallografico piano e sia  $p_0$  un punto del piano che non sia lasciato fisso da nessun elemento di  $G$ . Sia  $S = \{gp_0 \mid g \in G\}$  l'orbita di  $p_0$ . Il piano può essere diviso in poligoni, ciascuno dei quali contenente un solo punto di  $S$ . Precisamente, il poligono  $\Delta_p$  contenente  $p$  è l'insieme dei punti  $q$  la cui distanza da  $p$  è la minima distanza da un punto arbitrario di  $S$ :

$$\Delta_p = \{q \in \mathbb{R}^2 \mid \text{dist}(q, p) \leq \text{dist}(q, p') \text{ per ogni } p' \in S\}.$$

(a) Dimostrare che  $\Delta_p$  è un poligono.

(b) Dimostrare che  $\Delta_p$  è un dominio fondamentale per  $G$ .

(c) Provare che questo metodo vale per tutti i sottogruppi discreti di  $M$ , tranne il fatto che il dominio  $\Delta_p$  che viene costruito non è necessariamente un insieme limitato.

(d) Dimostrare che  $\Delta_p$  è limitato se e solo se il gruppo è un gruppo cristallografico piano.

\*6. (a) Siano  $G' \subset G$  due gruppi di reticolo. Sia  $D$  un dominio fondamentale per  $G$ . Dimostrare che un dominio fondamentale  $D'$  per  $G'$  può essere costruito a partire da un numero finito di insiemi della forma  $gD$  ( $g \in G$ ).

(b) Dimostrare che  $[G : G'] < \infty$  e che  $[G : G'] = \text{area}(D')/\text{area}(D)$ .

(c) Calcolare l'indice  $[G : L_G]$  per ciascuno dei motivi (4.16).

\*7. Sia  $G$  un gruppo finito che agisce su un insieme finito  $S$ . Per ogni elemento  $g \in G$ , denotiamo con  $S^g$  il sottoinsieme degli elementi di  $S$  lasciati fissi da  $g$ :  $S^g = \{s \in S \mid gs = s\}$ .

(a) Possiamo immaginare una tabella di verità per l'affermazione che  $gs = s$ , diciamo con le righe aventi per indici gli elementi di  $G$  e le colonne aventi per indici gli elementi di  $S$ . Costruire una tavola siffatta per l'azione del gruppo diedrale  $D_3$  sui vertici di un triangolo equilatero.

(b) Dimostrare la formula:  $\sum_{s \in S} |G_s| = \sum_{g \in G} |S^g|$ .

(c) Dimostrare la *formula di Burnside*:

$$|G| \cdot (\text{numero delle orbite}) = \sum_{g \in G} |S^g|.$$

8. Vi sono  $70 = \binom{8}{4}$  modi di colorare i lati di un ottagono, ottenendo quattro lati neri e quattro lati bianchi. Il gruppo  $D_8$  agisce su questo insieme di 70 elementi, e le orbite rappresentano colorazioni equivalenti. Utilizzare la formula di Burnside per contare il numero delle classi di equivalenza.

9. Sia  $G$  un gruppo di ordine  $n$  che agisce in modo non banale su un insieme di  $r$  elementi. Dimostrare che se  $n > r!$   $G$  possiede un sottogruppo normale proprio.

## Capitolo 6

### Ulteriori proprietà dei gruppi

Più c'è da fare o da dimostrare più è facile fare o dimostrare.

James Joseph Sylvester

#### 1 Le azioni di un gruppo su se stesso

Quando si parla di azione di un gruppo  $G$  su se stesso, si intende che, nella definizione dell'azione,  $G$  svolge il ruolo sia del gruppo che dell'insieme sul quale esso agisce. Ogni gruppo agisce su se stesso in vari modi, due dei quali verranno esaminati ora. Il primo è la *moltiplicazione a sinistra*:

$$(1.1) \quad \begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gx. \end{aligned}$$

Si tratta ovviamente di un'azione transitiva di  $G$  su  $G$ , ossia  $G$  forma un'unica orbita, e lo stabilizzatore di un elemento arbitrario è il sottogruppo  $\{1\}$  costituito dal solo elemento neutro. Pertanto l'azione è fedele, e l'omomorfismo

$$(1.2) \quad \begin{aligned} G &\longrightarrow \text{Perm}(G) \\ g &\longmapsto m_g = \text{moltiplicazione a sinistra per } g \end{aligned}$$

definito nel capitolo 5 (§ 8) è iniettivo.

(1.3) **TEOREMA DI CAYLEY** *Ogni gruppo finito  $G$  è isomorfo a un sottogruppo di un gruppo di permutazioni. Se  $G$  ha ordine  $n$ , allora  $G$  è isomorfo a un sottogruppo del gruppo simmetrico  $S_n$ .*

*Dimostrazione.* Poiché l'azione mediante la moltiplicazione a sinistra è fedele,  $G$  è isomorfo alla sua immagine in  $\text{Perm}(G)$ . Se  $G$  ha ordine  $n$ , allora  $\text{Perm}(G)$  è isomorfo a  $S_n$ . ■

Sebbene il teorema di Cayley sia interessante di per sé, non è particolarmente utile per i calcoli, perché  $S_n$ , avendo ordine  $n!$ , è troppo grande rispetto a  $n$ .

La seconda azione che considereremo è più riposta. Si tratta del *coniugio*, l'applicazione  $G \times G \rightarrow G$  definita da:

$$(1.4) \quad (g, x) \mapsto g x g^{-1}.$$

Per ovvie ragioni, non useremo per essa la notazione moltiplicativa. Occorre verificare gli assiomi (5.1) dati nel capitolo 5 con una notazione provvisoria, ad esempio  $g * x$ , per indicare il coniugato  $g x g^{-1}$ .

Lo stabilizzatore di un elemento  $x \in G$  rispetto al coniugio ha un nome particolare: è chiamato il *centralizzante* di  $x$  e si denota con  $Z(x)$ :

$$(1.5) \quad Z(x) = \{g \in G \mid g x g^{-1} = x\} = \{g \in G \mid g x = x g\}.$$

Il centralizzante è l'insieme degli elementi del gruppo che commutano con  $x$ . Si noti che  $x \in Z(x)$ , poiché  $x$  commuta con se stesso.

L'orbita di  $x$  rispetto all'azione data dal coniugio è chiamata la *classe di coniugio* di  $x$ . Essa è costituita da tutti gli elementi coniugati  $g x g^{-1}$ . Scriviamo spesso la classe di coniugio nella forma

$$(1.6) \quad C_x = \{x' \in G \mid x' = g x g^{-1} \text{ per qualche } g \in G\}.$$

In virtù della formula delle classi [cap. 5 (7.2)], si ha:  $|G| = |C_x| |Z(x)|$ .

Poiché le classi di coniugio sono orbite rispetto all'azione di un gruppo, esse formano una partizione di  $G$ . Ciò fornisce la cosiddetta *equazione delle classi* per un gruppo finito [cfr. cap. 5 (7.3)]:

$$(1.7) \quad |G| = \sum_{\substack{\text{classi di} \\ \text{coniugio } C}} |C|.$$

Se denotiamo le classi di coniugio con  $C_i$ ,  $i = 1, \dots, k$ , la (1.7) si scrive

$$|G| = |C_1| + \dots + |C_k|.$$

Tuttavia vi è qualche pericolo di confusione, poiché la  $i$  in  $C_i$  è un indice, mentre il simbolo  $C_x$  in (1.6) sta a indicare la classe di coniugio contenente l'elemento  $x$  di  $G$ . In particolare,  $C_1$  ha due significati. Forse sarà meglio mettere per prima, nella lista, la classe di coniugio dell'identità 1 di  $G$ . In tal modo le due interpretazioni di  $C_1$  coincidono.

Si noti che l'identità è lasciata fissa da tutti gli elementi  $g \in G$ . Pertanto  $C_1$  è costituito soltanto dall'elemento 1. Inoltre ciascun termine nel secondo membro di (1.7), essendo l'ordine di un'orbita, divide il primo membro. Ciò costituisce una forte restrizione sulle combinazioni di interi che possono comparire nell'equazione (1.7).

- (1.8) I numeri nel secondo membro dell'equazione delle classi dividono l'ordine del gruppo, e almeno uno di essi è uguale a 1.

Per esempio, le classi di coniugio nel gruppo diedrale  $D_3$ , descritto nel capitolo 5 (3.6), sono i tre sottoinsiemi seguenti:

$$\{1\}, \{x, x^2\}, \{y, xy, x^2y\}.$$

Le due rotazioni  $x$  e  $x^2$  sono coniugate tra loro e così pure le tre riflessioni. L'equazione delle classi per  $D_3$  è

$$(1.9) \quad 6 = 1 + 2 + 3.$$

Ricordiamo [cfr. cap. 2 (4.10)] che il centro di un gruppo  $G$  è l'insieme  $Z$  degli elementi che commutano con tutti gli elementi del gruppo:

$$Z = \{g \in G \mid gx = xg \text{ per ogni } x \in G\}.$$

Ora la classe di coniugio di un elemento  $x$  è costituita soltanto da  $x$  se e soltanto se  $x = gxg^{-1}$  per ogni  $g \in G$ , cioè se  $x$  sta nel centro. Dunque nel secondo membro dell'equazione delle classi gli elementi del centro sono rappresentati da 1.

La proposizione seguente discende direttamente dalle definizioni.

- (1.10) PROPOSIZIONE Un elemento  $x$  appartiene al centro di un gruppo  $G$  se e soltanto se il suo centralizzante  $Z(x)$  è l'intero gruppo. ■

L'equazione delle classi (1.7) è utile in particolare quando l'ordine di  $G$  è una potenza positiva di un numero primo  $p$ . Un gruppo di questo tipo è chiamato  $p$ -gruppo. Vediamo ora alcune applicazioni dell'equazione delle classi ai  $p$ -gruppi.

- (1.11) PROPOSIZIONE Il centro di un  $p$ -gruppo  $G$  ha ordine  $> 1$ .

*Dimostrazione.* Il primo membro della (1.7) è una potenza di  $p$ , diciamo  $p^e$ . Inoltre, ogni termine a secondo membro è anch'esso una potenza di  $p$ , poiché divide  $p^e$ . Vogliamo provare che qualche elemento  $x \neq 1$  del gruppo sta nel centro, cioè che almeno due termini di secondo membro della (1.7) sono uguali a 1. Ora i termini diversi da 1, essendo potenze positive di  $p$ , sono divisibili per  $p$ . Se la classe  $C_1$  fosse l'unica a dare un contributo di 1 nell'espressione a secondo membro, l'equazione si scriverebbe nella forma:

$$p^e = 1 + \sum (\text{multipli di } p),$$

che è impossibile, a meno che  $e = 0$ . ■

Il precedente ragionamento può essere rovesciato e generalizzato per stabilire il seguente importante teorema del punto fisso, relativo alle azioni di  $p$ -gruppi:

- (1.12) PROPOSIZIONE Sia  $G$  un  $p$ -gruppo, e sia  $S$  un insieme finito sul quale  $G$  agisce. Supponiamo che l'ordine di  $S$  non sia divisibile per  $p$ . Allora esiste un punto fisso per l'azione di  $G$  su  $S$ , ossia un elemento  $s \in S$  il cui stabilizzatore è l'intero gruppo.

- (1.13) PROPOSIZIONE Ogni gruppo di ordine  $p^2$ , con  $p$  primo, è abeliano.

*Dimostrazione.* Sia  $G$  un gruppo di ordine  $p^2$ . Proveremo che, per ogni  $x \in G$ , il centralizzante  $Z(x)$  è l'intero gruppo. Allora, in base alla proposizione (1.10), la dimostrazione sarà terminata. Sia dunque  $x \in G$ . Se  $x$  sta nel centro  $Z$ , allora ovviamente  $Z(x) = G$ . Se  $x \notin Z$ , allora  $Z(x)$  è strettamente più grande di  $Z$ , poiché contiene  $Z$  e l'elemento  $x$ . Ora gli ordini di  $Z$  e  $Z(x)$  dividono  $|G| = p^2$ , e la proposizione (1.11) ci dice che  $|Z|$  è almeno  $p$ . L'unica possibilità è che  $|Z(x)| = p^2$ . Pertanto  $Z(x) = G$ . ■

Esistono gruppi non abeliani di ordine  $p^3$ . Il gruppo diedrale  $D_4$ , per esempio, ha ordine 8.

Utilizziamo la proposizione (1.13) per classificare i gruppi di ordine  $p^2$ .

- (1.14) COROLLARIO Ogni gruppo di ordine  $p^2$ , con  $p$  primo, è di uno dei tipi seguenti:

- (a) un gruppo ciclico di ordine  $p^2$ ;
- (b) il prodotto di due gruppi ciclici di ordine  $p$ .

*Dimostrazione.* Poiché l'ordine di un elemento divide  $p^2$ , vi sono due casi da considerare:

*Caso 1:*  $G$  contiene un elemento di ordine  $p^2$  ed è pertanto un gruppo ciclico.

*Caso 2:* Ogni elemento  $x$  di  $G$  diverso dall'identità ha ordine  $p$ . Siano  $x, y$  due elementi diversi da 1, e siano  $H_1, H_2$  i gruppi ciclici di ordine  $p$  generati, rispettivamente, da  $x$  e  $y$ . Possiamo scegliere  $y$  in modo tale che non sia una potenza di  $x$ . Allora, poiché  $y \notin H_1$ ,  $H_1 \cap H_2$  è più piccolo di  $H_2$ , che ha ordine  $p$ . Pertanto  $H_1 \cap H_2 = \{1\}$ . Inoltre, i sottogruppi  $H_i$  sono normali, essendo  $G$  abeliano. Poiché  $y \notin H_1$ , il gruppo  $H_1 H_2$  è strettamente più grande di  $H_1$ , e il suo ordine divide  $p^2$ . Dunque  $H_1 H_2 = G$ . In base alla proposizione (8.6) del capitolo 2,  $G \cong H_1 \times H_2$ . ■

Il numero dei casi possibili per i gruppi di ordine  $p^n$  cresce rapidamente con  $n$ . Vi sono cinque classi di isomorfismo di gruppi di ordine 8 e 14 classi di isomorfismo di gruppi di ordine 16.

## 2 L'equazione delle classi del gruppo icosaedrale

In questo paragrafo determineremo le classi di coniugio nel gruppo icosaedrale  $I$  delle simmetrie di rotazione di un dodecaedro, e le useremo per studiare questo interessantissimo gruppo. Come abbiamo visto, l'ordine del gruppo icosaedrale è 60. Esso contiene rotazioni di multipli di  $2\pi/5$  intorno ai centri delle facce del dodecaedro, di multipli di  $2\pi/3$  intorno ai vertici, e di  $\pi$  intorno ai centri degli spigoli. Ciascuno dei 20 vertici ha uno stabilizzatore di ordine 3, e vertici opposti hanno lo stesso stabilizzatore; quindi vi sono 10 sottogruppi di ordine 3: gli stabilizzatori dei vertici. Ciascun sottogruppo di ordine 3 contiene due elementi di ordine 3, e l'intersezione di due qualunque di questi sottogruppi è costituita soltanto dall'identità. Pertanto  $I$  contiene  $10 \times 2 = 20$  elementi di ordine 3. Analogamente, le facce hanno stabilizzatori di ordine 5: ce ne sono sei, i quali forniscono  $6 \times 4 = 24$  elementi di ordine 5. Vi sono 15 stabilizzatori relativi agli spigoli, i quali hanno ordine 2; quindi esistono 15 elementi di ordine 2. Infine, vi è un elemento di ordine 1. Dato che

$$(2.1) \quad 60 = 1 + 15 + 20 + 24,$$

abbiamo elencato tutti gli elementi del gruppo.

La (2.1) si ottiene mediante una partizione del gruppo secondo gli ordini degli elementi. Essa è strettamente collegata con l'equazione delle classi, ma si può vedere che non è esattamente la stessa equazione, perché 24, che compare a secondo membro, non divide 60. D'altra parte, sappiamo che elementi coniugati hanno lo stesso ordine; quindi l'equazione delle classi si ottiene suddividendo ulteriormente questa partizione di  $G$ . Inoltre, si noti che i sottogruppi di ordine 3 sono tutti coniugati. Questa è una proprietà generale delle azioni di gruppi, poiché essi sono gli stabilizzatori dei vertici, i quali formano un'unica orbita [cap. 5 (6.5)]. La stessa proprietà vale per i sottogruppi di ordine 5 e per quelli di ordine 2.

È chiaro che i 15 elementi di ordine 2, essendo gli elementi non banali di sottogruppi coniugati di ordine 2, formano una classe di coniugio. Cosa si può dire per gli elementi di ordine 3? Sia  $x$  una rotazione di  $2\pi/3$  in senso antiorario intorno a un vertice  $v$ . Sebbene  $x$  sia coniugato a una rotazione dello stesso angolo intorno a qualsiasi altro vertice [cap. 5 (6.5)], non è tanto chiaro se  $x$  è o non è coniugato a  $x^2$ . Forse la prima congettura sarebbe che  $x$  e  $x^2$  non sono coniugati.

Sia  $v'$  il vertice opposto a  $v$ , e sia  $x'$  la rotazione di  $2\pi/3$  in senso antiorario intorno a  $v'$ . Pertanto  $x$  e  $x'$  sono elementi coniugati del gruppo. Si noti che la rotazione  $x$  in senso antiorario intorno a  $v$  è lo stesso movimento dato dalla rotazione in senso orario di  $2\pi/3$  intorno al vertice opposto  $v'$ . Dunque  $x^2 = x'$ , e ciò prova che in effetti  $x$  e  $x^2$  sono coniugati. Ne segue che tutti gli elementi di ordine 3 sono coniugati. Analogamente, le 12 rotazioni di  $2\pi/5$  e  $-2\pi/5$  sono coniugate. Esse non sono coniugate alle rimanenti 12 rotazioni di  $4\pi/5$  e  $-4\pi/5$  di ordine 5. (Un motivo, come abbiamo già osservato, è che l'ordine di una classe di coniugio divide l'ordine del gruppo, e 24 non divide 60.) Pertanto vi sono due classi di coniugio di elementi di ordine 5, e l'equazione delle classi è:

$$(2.2) \quad 60 = 1 + 15 + 20 + 12 + 12.$$

Utilizzeremo ora l'equazione delle classi per dimostrare il teorema seguente:

(2.3) TEOREMA *Il gruppo icosaedrale  $I$  non ha sottogruppi normali propri.*

Un gruppo  $G$  si dice *semplice* se non è il gruppo banale e se non contiene sottogruppi normali propri (ossia, sottogruppi normali diversi da  $\{1\}$  e  $G$ ). Pertanto il teorema può essere rienunciato nella forma seguente:

(2.4) *Il gruppo icosaedrale è un gruppo semplice.*

I gruppi ciclici di ordine primo non contengono sottogruppi propri e pertanto sono gruppi semplici. Tutti gli altri gruppi, tranne il gruppo banale, contengono sottogruppi propri, sebbene non necessariamente normali. È opportuno sottolineare che in questo contesto il termine *semplice* non indica “non complicato”, ma significa grosso modo “non composto”.

*Dimostrazione del teorema (2.3).* La dimostrazione del lemma seguente si effettua direttamente:

### (2.5) LEMMA

- (a) *Se un sottogruppo normale  $N$  di un gruppo  $G$  contiene un elemento  $x$ , allora contiene la classe di coniugio  $C_x$  di  $x$  in  $G$ . In altre parole, un sottogruppo normale è un'unione di classi di coniugio.*
- (b) *L'ordine di un sottogruppo normale  $N$  di  $G$  è la somma degli ordini delle classi di coniugio che esso contiene. ■*

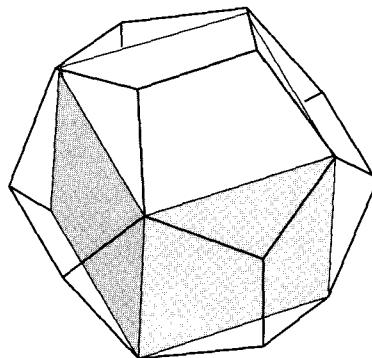
Applichiamo ora questo lemma. L'ordine di un sottogruppo normale proprio del gruppo icosaedrale è un divisore proprio di 60 ed è anche la somma di alcuni dei termini che compaiono nel membro a destra dell'equazione delle classi (2.2),

compreso il termine 1. Dato che nessun numero intero verifica queste condizioni, il teorema è dimostrato. ■

(2.6) TEOREMA *Il gruppo icosaedrale è isomorfo al gruppo alterno  $A_5$ .*

*Dimostrazione.* Per descrivere questo isomorfismo, dobbiamo trovare un insieme  $S$  di cinque elementi sul quale  $I$  agisce. Un insieme siffatto è costituito dai cinque cubi che possono essere inscritti in un dodecaedro, uno dei quali è illustrato qui sotto:

(2.7)



Uno dei cubi inscritti in un dodecaedro.

Il gruppo  $I$  agisce su questo insieme di cubi  $S$ , e tale azione definisce un omomorfismo  $\varphi : I \rightarrow S_5$ , ossia la rappresentazione mediante permutazioni associata. L'applicazione  $\varphi$  è l'isomorfismo cercato da  $I$  alla sua immagine  $A_5$ . Per dimostrare che è un isomorfismo useremo il fatto che  $I$  è un gruppo semplice, ma avremo bisogno di pochissime informazioni sull'azione in sé.

Poiché il nucleo di  $\varphi$  è un sottogruppo normale di  $I$ , che è un gruppo semplice, si ha  $\ker \varphi = \{1\}$  oppure  $\ker \varphi = I$ . Se fosse  $\ker \varphi = I$  avremmo che l'azione di  $I$  sull'insieme dei cinque cubi è l'azione banale, che è chiaramente falso. Pertanto  $\ker \varphi = \{1\}$  e  $\varphi$  è iniettivo, definendo così un isomorfismo di  $I$  sulla sua immagine in  $S_5$ .

Denotiamo l'immagine in  $S_5$  anch'essa con  $I$ . Restringiamo l'omomorfismo dato dal segno:  $S_5 \rightarrow \{\pm 1\}$  a  $I$ , ottenendo un omomorfismo  $I \rightarrow \{\pm 1\}$ . Se questo omomorfismo fosse suriettivo, il suo nucleo sarebbe un sottogruppo normale di  $I$  di ordine 30 [cap. 2 (6.15)]. Ciò è impossibile, poiché  $I$  è semplice. Pertanto la restrizione è l'omomorfismo banale, il che significa proprio che  $I$  è contenuto nel nucleo  $A_5$  dell'omomorfismo  $S_5 \rightarrow \{\pm 1\}$ . Poiché entrambi i gruppi hanno ordine 60,  $I = A_5$ . ■

Ogni volta che un gruppo  $G$  agisce su un insieme  $S$ , vi è anche un'azione sui sottoinsiemi. Se  $U \subset S$  è un sottoinsieme, allora

$$(3.1) \quad gU = \{gu \mid u \in U\}$$

è un altro sottoinsieme di  $S$ . Gli assiomi di un'azione sono chiaramente verificati e quindi  $G$  agisce sull'insieme dei sottoinsiemi di  $S$ . Possiamo considerare l'azione sui sottoinsiemi di un dato ordine, se vogliamo. Poiché la moltiplicazione per  $g$  è una permutazione di  $S$ , i sottoinsiemi  $U$  e  $gU$  hanno lo stesso ordine.

Per esempio, sia  $O$  il gruppo ottaedrale delle 24 rotazioni di un cubo, e sia  $S$  l'insieme dei vertici del cubo. Consideriamo l'azione di  $O$  sui sottoinsiemi di ordine 2 di  $S$ , ossia sulle 28 coppie non ordinate di vertici, che formano tre orbite per il gruppo:

- (i) {coppie di vertici su uno spigolo};
- (ii) {coppie di vertici opposti su una faccia del cubo};
- (iii) {coppie di vertici opposti sul cubo}.

Queste orbite hanno, rispettivamente, ordine 12, 12 e 4:  $28 = 12 + 12 + 4$ .

Lo stabilizzatore di un sottoinsieme  $U$  è l'insieme degli elementi  $g$  del gruppo tali che  $gU = U$ . Lo stabilizzatore di una coppia di vertici opposti su una faccia contiene quindi due elementi: l'identità e la rotazione di  $\pi$  intorno alla faccia. Ciò è in accordo con la formula delle classi:  $24 = 2 \cdot 12$ .

Conviene sottolineare ancora una volta questo punto importante: l'uguaglianza  $gU = U$  non significa che  $g$  lascia fissi gli elementi di  $U$ , ma invece che  $g$  permuta gli elementi in  $U$ , ossia, che  $gu \in U$  per ogni  $u \in U$ .

(3.2) PROPOSIZIONE *Sia  $H$  un gruppo che agisce su un insieme  $S$ , e sia  $U$  un sottoinsieme di  $S$ . Allora  $H$  stabilizza  $U$  se e solo se  $U$  è un'unione di  $H$ -orbite.*

Questa proposizione rientra semplicemente il fatto che l' $H$ -orbita di un elemento  $u \in U$  è l'insieme di tutti gli elementi  $hu$ . Se  $H$  stabilizza  $U$ , allora  $U$  contiene l' $H$ -orbita di qualsiasi suo elemento. ■

Consideriamo il caso in cui  $G$  agisce mediante la moltiplicazione a sinistra sui sottoinsiemi di  $G$ . Ogni sottogruppo  $H$  di  $G$  è un sottoinsieme, e la sua orbita è costituita dalle classi laterali sinistre. Questa azione di  $G$  sulle classi laterali è stata definita nel capitolo 5 (6.1). Tuttavia qualunque sottoinsieme di  $G$  ha un'orbita.

## (3.3) Esempio

Sia  $G = D_3$  il gruppo diedrale delle simmetrie di un triangolo equilatero, presentato come al solito nella forma:

$$G = \{x^i y^j \mid 0 \leq i \leq 2, 0 \leq j \leq 1, x^3 = 1, y^2 = 1, yx = x^2y\}.$$

Questo gruppo contiene 15 sottoinsiemi di ordine 2, e possiamo decomporre tale insieme di 15 sottoinsiemi in orbite rispetto alla moltiplicazione a sinistra. Vi sono tre sottogruppi di ordine 2:

$$(3.4) \quad H_1 = \{1, y\}, \quad H_2 = \{1, xy\}, \quad H_3 = \{1, x^2y\}.$$

Le loro classi laterali formano tre orbite di ordine 3. Gli altri sei sottoinsiemi di ordine 2 formano un'unica orbita:  $15 = 3 + 3 + 3 + 6$ . Tale orbita è costituita da:

$$(3.5) \quad \{1, x\}, \{x, x^2\}, \{x^2, 1\}, \{y, x^2y\}, \{xy, y\}, \{x^2y, xy\}. \blacksquare$$

(3.6) PROPOSIZIONE *Sia  $U$  un sottoinsieme di un gruppo  $G$ . L'ordine dello stabilizzatore  $\text{Stab}(U)$  di  $U$  rispetto all'azione data dalla moltiplicazione a sinistra divide l'ordine di  $U$ .*

*Dimostrazione.* Denotiamo con  $H$  lo stabilizzatore di  $U$ . La proposizione (3.2) afferma che  $U$  è un'unione di orbite rispetto all'azione di  $H$  su  $G$ . Queste  $H$ -orbite sono classi laterali destre  $H_g$ . Dunque  $U$  è un'unione di classi laterali destre. Pertanto l'ordine di  $U$  è un multiplo di  $|H|$ . ■

Naturalmente, poiché lo stabilizzatore è un sottogruppo di  $G$ , il suo ordine divide anche  $|G|$ . Pertanto, se  $|U|$  e  $|G|$  non hanno fattori comuni, allora  $\text{Stab}(U)$  è il sottogruppo banale  $\{1\}$ .

Anche l'azione mediante il coniugio sui sottoinsiemi di  $G$  è interessante. Per esempio, possiamo ripartire i 15 sottoinsiemi di  $D_3$  di ordine 2 in orbite rispetto al coniugio. L'insieme  $\{H_1, H_2, H_3\}$  di sottogruppi coniugati è un'orbita, e l'insieme  $\{x, x^2\}$  forma un'orbita da solo. Le altre orbite hanno ordine 2, 3 e 6:  $15 = 1 + 2 + 3 + 3 + 6$ .

Ciò che è importante, per i nostri scopi, è l'orbita rispetto al coniugio di un sottogruppo  $H \subset G$ . Tale orbita è l'insieme dei sottogruppi coniugati:

$$\{gHg^{-1} \mid g \in G\}.$$

Il sottogruppo  $H$  è normale se e soltanto se la sua orbita è costituita soltanto da  $H$ , ossia,  $gHg^{-1} = H$  per ogni  $g \in G$ .

Lo stabilizzatore di un sottogruppo  $H$  rispetto al coniugio è chiamato il *normalizzante* di  $H$  e si denota con

$$(3.7) \quad N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

La formula delle classi diventa

$$(3.8) \quad |G| = |N(H)| \cdot |\{\text{sottogruppi coniugati}\}|.$$

Pertanto il numero dei sottogruppi coniugati è uguale all'indice  $[G : N(H)]$ .

Si noti che il normalizzante contiene sempre il sottogruppo stesso:

$$(3.9) \quad N(H) \supset H,$$

perché  $hHh^{-1} = H$ , se  $h \in H$ . Pertanto, per il teorema di Lagrange,  $|H|$  divide  $|N(H)|$ , e  $|N(H)|$  divide  $|G|$ .

Nell'esempio (3.3), i sottogruppi  $H_1, H_2, H_3$  sono tutti coniugati, e quindi  $|N(H_i)| = 2$ ; pertanto  $N(H_i) = H_i$ .

La definizione del normalizzante  $N(H)$  mostra che  $H$  è un sottogruppo normale di  $N(H)$ , e infatti  $N(H)$  è il più grande sottogruppo di  $G$  che contiene  $H$  come sottogruppo normale. In particolare,  $N(H) = G$  se e soltanto se  $H$  è un sottogruppo normale di  $G$ .

## 4 I teoremi di Sylow

I teoremi di Sylow, che dimostreremo in questo paragrafo, descrivono i sottogruppi di un gruppo finito arbitrario aventi come ordine una potenza di un numero primo.

Sia  $G$  un gruppo di ordine  $n = |G|$ , e sia  $p$  un numero primo che divide  $n$ . Indicheremo con  $p^e$  la più grande potenza di  $p$  che divide  $n$ , sicché

$$(4.1) \quad n = p^e m$$

con  $m$  intero, e  $p$  non divide  $m$ .

(4.2) TEOREMA (Primo teorema di Sylow) *Esiste un sottogruppo di  $G$  di ordine  $p^e$ .*

Le dimostrazioni dei teoremi di Sylow si trovano alla fine del paragrafo (p. 246).

(4.3) COROLLARIO *Se un primo  $p$  divide l'ordine di un gruppo finito  $G$ , allora  $G$  contiene un elemento di ordine  $p$ .*

Infatti, sia  $H$  un sottogruppo di ordine  $p^e$ , e sia  $x$  un elemento di  $H$  diverso da 1. L'ordine di  $x$  divide  $p^e$ , sicché è uguale a  $p^r$ , per qualche  $r$  intero,  $0 < r \leq e$ . Allora  $x^{p^{r-1}}$  ha ordine  $p$ . ■

Senza il teorema di Sylow, questo corollario non è ovvio. Noi già sappiamo che l'ordine di qualsiasi elemento divide  $|G|$ , ma potremmo immaginare, per esempio, un gruppo di ordine 6 costituito dall'identità 1 e da cinque elementi di ordine 2. Un gruppo siffatto non esiste. In base a (4.3), un gruppo di ordine 6 deve contenere un elemento di ordine 3 e un elemento di ordine 2.

(4.4) COROLLARIO *Vi sono esattamente due classi di isomorfismo di gruppi di ordine 6: la classe del gruppo ciclico  $C_6$  e quella del gruppo diedrale  $D_3$ .*

*Dimostrazione.* Sia  $G$  un gruppo di ordine 6, e siano  $x$  e  $y$  elementi di  $G$  di ordine rispettivamente 3 e 2. Si vede facilmente che i sei prodotti  $x^i y^j$ ,  $0 \leq i \leq 2$ ,  $0 \leq j \leq 1$ , sono elementi distinti del gruppo. Infatti possiamo riscrivere un'equazione  $x^i y^j = x^r y^s$  nella forma  $x^{i-r} = y^{s-j}$ . Ogni potenza di  $x$  diversa dall'identità ha ordine 3, e ogni potenza di  $y$  diversa dall'identità ha ordine 2. Pertanto  $x^{i-r} = y^{s-j} = 1$ , e ciò mostra che  $r = i$  e  $s = j$ . Poiché  $G$  ha ordine 6, i sei elementi  $1, x, x^2, y, xy, x^2y$  descrivono l'intero gruppo. In particolare,  $yx$  deve essere uno di essi. Non è possibile che  $yx = y$ , poiché ciò implicherebbe  $x = 1$ . Per analoghe ragioni,  $yx \neq 1, x, x^2$ . Quindi in  $G$  deve valere una delle due relazioni:

$$yx = xy \quad \text{oppure} \quad yx = x^2y.$$

Ciascuna di tali relazioni, insieme con  $x^3 = 1$  e  $y^2 = 1$ , permette di determinare la tabella di moltiplicazione del gruppo. Ne segue che vi sono al più due classi di isomorfismo di gruppi di ordine 6; dato che già conosciamo due, cioè le classi del gruppo ciclico  $C_6$  e del gruppo diedrale  $D_3$ , esse sono le uniche classi. ■

(4.5) DEFINIZIONE *Sia  $G$  un gruppo di ordine  $n = p^e m$ , dove  $p$  è un primo che non divide  $m$  ed  $e \geq 1$ . I sottogruppi  $H$  di  $G$  di ordine  $p^e$  sono chiamati  $p$ -sottogruppi, o semplicemente sottogruppi, di Sylow di  $G$ .*

Dunque un  $p$ -sottogruppo di Sylow è un  $p$ -sottogruppo il cui indice nel gruppo non è divisibile per  $p$ . In base al teorema (4.2), un gruppo finito  $G$  possiede sempre un  $p$ -sottogruppo di Sylow, se  $p$  divide l'ordine di  $G$ . I rimanenti teoremi di Sylow (4.6) e (4.8) danno maggiori informazioni su di essi.

(4.6) TEOREMA (Secondo teorema di Sylow) *Sia  $K$  un sottogruppo di  $G$  il cui ordine è divisibile per  $p$  e sia  $H$  un  $p$ -sottogruppo di Sylow di  $G$ . Allora esiste un sottogruppo coniugato  $H' = gHg^{-1}$  tale che  $K \cap H'$  è un sottogruppo di Sylow di  $K$ .*

#### 4.7) COROLLARIO

- (a) *Se  $K$  è un qualsiasi sottogruppo di  $G$  che sia un  $p$ -gruppo, allora  $K$  è contenuto in un  $p$ -sottogruppo di Sylow di  $G$ .*
- (b) *I  $p$ -sottogruppi di Sylow di  $G$  sono tutti coniugati.*

È chiaro che un coniugato di un sottogruppo di Sylow è anch'esso un sottogruppo di Sylow. Pertanto, per ottenere la prima parte del corollario, dobbiamo soltanto osservare che il sottogruppo di Sylow di un  $p$ -gruppo  $K$  è il gruppo  $K$  stesso. Ne segue che, se  $H$  è un sottogruppo di Sylow e  $K$  è un  $p$ -gruppo, esiste un coniugato  $H'$  tale che  $K \cap H' = K$ , che equivale a dire che  $H'$  contiene  $K$ . Per la parte (b), siano  $K$  e  $H$  sottogruppi di Sylow. Allora esiste un coniugato  $H'$  di  $H$  che contiene  $K$ . Poiché i loro ordini sono uguali,  $K = H'$ . Dunque  $K$  e  $H$  sono coniugati. ■

(4.8) TEOREMA (Terzo teorema di Sylow) *Sia  $|G| = n$ , con  $n = p^e m$  come in (4.1). Sia  $s$  il numero dei  $p$ -sottogruppi di Sylow. Allora  $s$  divide  $m$  ed è congruo a 1 modulo  $p$ :  $s|m$ ,  $s = ap + 1$  per qualche intero  $a \geq 0$ .*

Prima di dimostrare questi teoremi, li utilizzeremo per determinare i gruppi di ordine 15 e di ordine 21. Tali esempi mostrano la potenza dei teoremi di Sylow, ma non è il caso di farsi troppe illusioni. La classificazione dei gruppi di ordine  $n$  non è facile quando  $n$  ha molti fattori primi. Ci sono semplicemente troppi casi possibili.

#### 4.9) PROPOSIZIONE

- (a) *Ogni gruppo di ordine 15 è ciclico.*
- (b) *Esistono due classi di isomorfismo di gruppi di ordine 21: la classe del gruppo ciclico  $C_{21}$  e la classe del gruppo  $G$  avente due generatori  $x, y$  che soddisfano le relazioni:  $x^7 = 1$ ,  $y^3 = 1$ ,  $yx = x^2y$ .*

#### *Dimostrazione*

- (a) Sia  $G$  un gruppo di ordine 15. In base a (4.8), il numero dei suoi 3-sottogruppi di Sylow divide 5 ed è congruo a 1 modulo 3. L'unico intero che verifica queste condizioni è 1. Pertanto esiste un unico 3-sottogruppo di Sylow  $H$ , e quindi è un sottogruppo normale. Analogamente, esiste un unico 5-sottogruppo di Sylow  $K$ , anch'esso normale. È chiaro che  $K \cap H = \{1\}$ , poiché l'ordine di  $K \cap H$  divide sia 5 che 3. Inoltre  $KH$  è un sottogruppo di ordine  $> 5$ , e quindi  $KH = G$ . In virtù della proposizione (8.6) del cap. 2,  $G$  è isomorfo al gruppo prodotto  $H \times K$ . Dunque ogni gruppo di ordine 15 è isomorfo a un prodotto diretto di gruppi ciclici di ordine 3 e 5, e quindi tutti i gruppi di ordine 15 sono isomorfi tra loro. Poiché il gruppo ciclico  $C_{15}$  è uno di essi, ogni gruppo di ordine 15 è ciclico.

(b) Sia  $G$  un gruppo di ordine 21. Allora il teorema (4.8) prova che il 7-sottogruppo di Sylow  $K$  deve essere normale. Tuttavia la possibilità che esistano sette 3-sottogruppi di Sylow coniugati  $H$  non è esclusa dal teorema, e in effetti tale caso si verifica. Denotiamo con  $x$  un generatore di  $K$  e con  $y$  un generatore di uno dei 3-sottogruppi di Sylow  $H$ . Allora  $x^7 = 1$ ,  $y^3 = 1$  e, poiché  $K$  è normale,  $yxy^{-1} = x^i$  per qualche  $i < 7$ .

Possiamo limitare i valori degli esponenti possibili  $i$  utilizzando la relazione  $y^3 = 1$ . Essa implica che

$$x = y^3xy^{-3} = y^2x^iy^{-2} = yx^{i^2}y^{-1} = x^{i^3}.$$

Pertanto  $i^3 \equiv 1 \pmod{7}$ . Ciò significa che  $i$  può assumere i valori 1, 2, 4.

*Caso 1:*  $yxy^{-1} = x$ . Il gruppo è abeliano e, in base alla proposizione (8.6) del capitolo 2, è isomorfo a un prodotto diretto di gruppi ciclici di ordine 3 e 7. Un gruppo siffatto è ciclico [cfr. cap. 2 (8.4)].

*Caso 2:*  $yxy^{-1} = x^2$ . La moltiplicazione in  $G$  può essere eseguita usando le regole:  $x^7 = 1$ ,  $y^3 = 1$ ,  $yx = x^2y$ , per ridurre ogni prodotto degli elementi  $x, y$  ad uno della forma  $x^i y^j$  con  $0 \leq i < 7$  e  $0 \leq j < 3$ . Lasciamo per esercizio il compito di dimostrare che tale gruppo effettivamente esiste.

*Caso 3:*  $yxy^{-1} = x^4$ . In tal caso, sostituiamo  $y$  con  $y^2$ , che è anch'esso un generatore di  $H$ , per ridurci al caso precedente:  $y^2xy^{-2} = yx^4y^{-1} = x^{16} = x^2$ . Dunque esistono due classi di isomorfismo di gruppi di ordine 21, come affermato. ■

Passiamo ora alla dimostrazione dei teoremi di Sylow.

*Dimostrazione del primo teorema di Sylow.* Sia  $S$  l'insieme di tutti i sottoinsiemi di  $G$  di ordine  $p^e$ . Uno di tali sottoinsiemi è il sottogruppo che stiamo cercando, ma invece di trovarlo direttamente, proveremo che uno di questi sottoinsiemi ha uno stabilizzatore di ordine  $p^e$ . Lo stabilizzatore sarà il sottogruppo cercato.

(4.10) **LEMMA** *Il numero dei sottoinsiemi di ordine  $p^e$  in un insieme di  $n = p^em$  elementi (con  $p$  che non divide  $m$ ) è il coefficiente binomiale:*

$$N = \binom{n}{p^e} = \frac{n(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}.$$

Inoltre,  $N$  non è divisibile per  $p$ .

*Dimostrazione.* È ben noto che il numero dei sottoinsiemi di ordine  $p^e$  è dato dal coefficiente binomiale  $N$ . Per dimostrare che  $N$  non è divisibile per  $p$ , basta osservare che ogni volta che  $p$  divide un termine  $(n-k)$  del numeratore di  $N$ ,  $p$  divide anche il termine  $(p^e-k)$  del denominatore, ed esattamente lo stesso numero di volte. Infatti, se scriviamo  $k$  nella forma  $k = p^i l$ , con  $p$  che non divide  $l$ , allora  $i < e$ . Pertanto  $(n-k)$  e  $(p^e-k)$  sono entrambi divisibili per  $p^i$ , ma non per  $p^{i+1}$ . ■

Decomponiamo l'insieme  $S$  in orbite rispetto all'azione data dalla moltiplicazione a sinistra, ottenendo la formula:

$$N = |S| = \sum_{\text{orbite } O} |O|.$$

Poiché  $p$  non divide  $N$ , qualche orbita ha un ordine che non è divisibile per  $p$ , e sia ad esempio l'orbita del sottoinsieme  $U$ . Applichiamo ora la proposizione (3.6) e concludiamo che  $|\text{Stab}(U)|$  è una potenza di  $p$ . Poiché

$$(4.11) \quad |\text{Stab}(U)| \cdot |O_U| = |G| = p^em$$

in base alla formula delle classi, e poiché  $|O_U|$  non è divisibile per  $p$ , ne segue che  $|\text{Stab}(U)| = p^e$ . Questo stabilizzatore è il sottogruppo cercato. ■

*Dimostrazione del secondo teorema di Sylow.* Sono dati in  $G$  un sottogruppo  $K$  il cui ordine è divisibile per  $p$  e un sottogruppo di Sylow  $H$ . Dobbiamo far vedere che, per qualche sottogruppo coniugato  $H'$  di  $H$ , l'intersezione  $K \cap H'$  è un sottogruppo di Sylow di  $K$ .

Denotiamo con  $S$  l'insieme delle classi laterali sinistre  $G/H$ . Le proprietà di  $S$  di cui abbiamo bisogno sono che  $G$  agisce transitivamente, ossia che l'insieme  $S$  forma una sola orbita, e inoltre che  $H$  è lo stabilizzatore di uno dei suoi elementi, precisamente di  $s = 1H$ . Pertanto lo stabilizzatore di  $as$  è il sottogruppo coniugato  $aHa^{-1}$  [cfr. cap. 5 (6.5b)].

Restringiamo l'azione di  $G$  a  $K$  e decomponiamo  $S$  in  $K$ -orbite. Poiché  $H$  è un sottogruppo di Sylow, l'ordine di  $S$  è primo con  $p$ . Pertanto esiste qualche  $K$ -orbita  $O$  il cui ordine è primo con  $p$ . Sia ad esempio  $O$  la  $K$ -orbita dell'elemento  $as$ , e sia  $H'$  lo stabilizzatore  $aHa^{-1}$  di  $as$  rispetto all'azione di  $G$ . Allora lo stabilizzatore di  $as$  per l'azione ristretta di  $K$  è ovviamente  $H' \cap K$ , e l'indice  $[K : H' \cap K]$  è  $|O|$ , che è primo con  $p$ . Inoltre, essendo un coniugato di  $H$ ,  $H'$  è un  $p$ -gruppo. Pertanto  $H' \cap K$  è un  $p$ -gruppo, e quindi  $H' \cap K$  è un sottogruppo di Sylow di  $K$ . ■

*Dimostrazione del terzo teorema di Sylow.* In base al corollario (4.7), i sottogruppi di Sylow di  $G$  sono tutti coniugati di un sottogruppo assegnato, diciamo di  $H$ . Pertanto il numero dei sottogruppi di Sylow è  $s = [G : N]$ , dove  $N$  è il normalizzante di  $H$ . Poiché  $H \subset N$ ,  $[G : N]$  divide  $[G : H] = m$ . Per dimostrare

che  $s \equiv 1$  (modulo  $p$ ), decomponiamo l'insieme  $\{H_1, \dots, H_s\}$  dei sottogruppi di Sylow in orbite per l'azione di coniugio mediante  $H = H_1$ . Un'orbita è costituita da un solo sottogruppo  $H_i$  se e soltanto se  $H$  è contenuto nel normalizzante  $N$  di  $H_i$ . In tal caso,  $H$  e  $H_i$  sono entrambi sottogruppi di Sylow di  $N_i$ , e  $H_i$  è normale in  $N_i$ . Il corollario (4.7b) prova che  $H = H_i$ . Pertanto esiste un'unica  $H$ -orbita di ordine 1, precisamente  $\{H\}$ . Le altre orbite hanno un ordine divisibile per  $p$ , poiché i loro ordini dividono  $|H|$ , in virtù della formula delle classi. Ciò prova che  $s \equiv 1$  (modulo  $p$ ). ■

## 5 I gruppi di ordine 12

In questo paragrafo useremo i teoremi di Sylow per classificare i gruppi di ordine 12.

(5.1) TEOREMA *Esistono cinque classi di isomorfismo di gruppi di ordine 12, rappresentate da:*

- (i) *il prodotto di gruppi ciclici  $C_3 \times C_4$ ;*
- (ii) *il prodotto di gruppi ciclici  $C_2 \times C_2 \times C_3$ ;*
- (iii) *il gruppo alterno  $A_4$ ;*
- (iv) *il gruppo diedrale  $D_6$ ;*
- (v) *il gruppo generato da  $x, y$ , con le relazioni:  $x^4 = 1$ ,  $y^3 = 1$ ,  $xy = y^2x$ .*

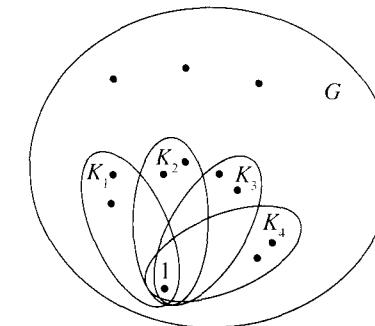
Si noti che  $C_3 \times C_4$  è isomorfo a  $C_{12}$  e che  $C_2 \times C_2 \times C_3$  è isomorfo a  $C_2 \times C_6$  [cfr. cap. 2 (8.4)].

*Dimostrazione.* Sia  $G$  un gruppo di ordine 12. Denotiamo con  $H$  un 2-sottogruppo di Sylow di  $G$ , che ha ordine 4, e con  $K$  un 3-sottogruppo di Sylow, di ordine 3. Dal teorema (4.8) segue che il numero dei 2-sottogruppi di Sylow è 1 o 3, e che il numero dei 3-sottogruppi di Sylow è 1 o 4. Inoltre,  $H$  è un gruppo di ordine 4 ed è pertanto o un gruppo ciclico oppure il gruppo quadrinomio di Klein  $V$ , ossia un prodotto di due gruppi ciclici di ordine 2:

$$(5.2) \quad H \approx C_4 \quad \text{oppure} \quad H \approx V.$$

(5.3) LEMMA *Almeno uno dei due sottogruppi  $H, K$  è normale.*

*Dimostrazione.* Supponiamo che  $K$  non sia normale. Allora  $K$  ha quattro sottogruppi coniugati  $K = K_1, \dots, K_4$ . Poiché  $|K_i| = 3$ , l'intersezione di due qualsiasi di questi sottogruppi deve essere l'identità. Contando gli elementi, si ha che vi sono soltanto tre elementi di  $G$  che non appartengono ad alcuno dei gruppi  $K_i$ .



Ogni 2-sottogruppo di Sylow  $H$  ha ordine 4, e  $H \cap K_i = \{1\}$ ; quindi  $H$  è costituito da questi tre elementi e da 1. Abbiamo così la descrizione di  $H$  e ciò mostra che esiste un unico 2-sottogruppo di Sylow, che perciò è normale. ■

Poiché  $H \cap K = \{1\}$ , ogni elemento di  $HK$  si scrive in modo unico come un prodotto  $hk$  [cap. 2 (8.6)], e poiché  $|G| = 12$ ,  $HK = G$ . Se  $H$  è normale, allora  $K$  agisce su  $H$  mediante il coniugio; dimostreremo che tale azione, insieme con la struttura di  $H$  e  $K$ , determina la struttura di  $G$ . Analogamente, se  $K$  è normale, allora  $H$  agisce su  $K$ , e tale azione determina  $G$ .

*Caso 1:*  $H$  e  $K$  sono entrambi normali. Allora, in virtù della (8.6) del capitolo 2,  $G$  è isomorfo al gruppo prodotto  $H \times K$ . In base a (5.2), vi sono due casi possibili:

$$(5.4) \quad G \approx C_4 \times C_3 \quad \text{oppure} \quad G \approx V \times C_3.$$

Questi sono i gruppi abeliani di ordine 12.

*Caso 2:*  $H$  è normale, ma  $K$  non lo è. Allora vi sono quattro 3-sottogruppi di Sylow coniugati  $\{K_1, \dots, K_4\}$ , e  $G$  agisce mediante il coniugio su questo insieme  $S$  di quattro sottogruppi. Tale azione determina una rappresentazione:

$$(5.5) \quad G \xrightarrow{\varphi} S_4.$$

*Dimostriamo* che in questo caso  $\varphi$  manda, mediante un isomorfismo,  $G$  nel gruppo alterno  $A_4$ .

Lo stabilizzatore di  $K_i$  per l'azione di coniugio è il normalizzante  $N(K_i)$ , che contiene  $K_i$ . La formula delle classi prova che  $|N(K_i)| = 3$ , e quindi che  $N(K_i) = K_i$ . Poiché l'unico elemento comune ai sottogruppi  $K_i$  è l'identità, soltanto l'identità stabilizza tutti questi sottogruppi. Pertanto  $\varphi$  è iniettiva e  $G$  è isomorfo alla sua immagine in  $S_4$ .

Poiché  $G$  ha quattro sottogruppi di ordine 3, esso contiene otto elementi di ordine 3, e questi elementi certamente generano il gruppo. Se  $x$  ha ordine 3, allora  $\varphi(x)$  è una permutazione di ordine 3 in  $S_4$ . Le permutazioni di ordine 3 sono pari, e quindi  $\text{im } \varphi \subset A_4$ . Poiché  $|G| = |A_4|$ , i due gruppi sono uguali.

Come corollario, osserviamo che, se  $H$  è normale e  $K$  non lo è, allora  $H$  è il gruppo quadrinomio di Klein  $V$ , poiché il 2-sottogruppo di Sylow di  $A_4$  è  $V$ .

**Caso 3:**  $K$  è normale, ma  $H$  non lo è. In questo caso,  $H$  agisce su  $K$  mediante il coniugio e il coniugio mediante un elemento di  $H$  è un automorfismo di  $K$ . Denotiamo con  $y$  un generatore del gruppo ciclico  $K$ :  $y^3 = 1$ . Vi sono soltanto due automorfismi di  $K$ : l'identità e l'automorfismo che scambia tra loro  $y$  e  $y^2$ .

Supponiamo che  $H$  sia ciclico di ordine 4, e sia  $x$  un generatore di  $H$ :  $x^4 = 1$ . Allora, poiché  $G$  non è abeliano,  $xy \neq yx$ , e pertanto la coniugazione mediante  $x$  non è l'automorfismo banale di  $K$ . Ne segue che  $xyx^{-1} = y^2$ . L'algoritmo di Todd-Coxeter (cfr. §9) offre un modo per dimostrare che queste relazioni definiscono un gruppo di ordine 12:

$$(5.6) \quad x^4 = 1, \quad y^3 = 1, \quad xyx^{-1} = y^2.$$

L'ultima possibilità è che  $H$  sia isomorfo al gruppo quadrinomio di Klein. Poiché vi sono soltanto due automorfismi di  $K$ , esiste un elemento  $w \in H$  diverso dall'identità che agisce banalmente, ossia:  $wyw^{-1} = y$ . Poiché  $G$  non è abeliano, esiste anche un elemento  $v$  che agisce in modo non banale:  $v y v^{-1} = y^2$ . Allora gli elementi di  $H$  sono  $\{1, v, w, vw\}$ , e le relazioni  $v^2 = w^2 = 1$ ,  $vw = wv$  valgono in  $H$ . L'elemento  $x = wy$  ha ordine 6, e  $v x v^{-1} = v w y v^{-1} = w y^2 = y^2 w = x^{-1}$ . Le relazioni  $x^6 = 1$ ,  $v^2 = 1$ ,  $v x v^{-1} = x^{-1}$  definiscono il gruppo  $D_6$ , e quindi  $G$  è il gruppo diedrale in questo caso. ■

## 6 Calcoli nel gruppo simmetrico

Vogliamo richiamare l'attenzione su due punti relativi al calcolo con le permutazioni. Il primo riguarda l'ordine di moltiplicazione. Per avere una convenzione uniforme, abbiamo usato la notazione funzionale  $p(x)$  per tutte le applicazioni  $p$ , incluse le permutazioni. Ciò comporta che un prodotto  $pq$  deve essere interpretato come l'operazione composta  $p \circ q$ , ossia "applicare prima  $q$ , poi  $p$ ". Quando si moltiplicano le permutazioni, più comunemente si legge  $pq$  come "applicare prima  $p$ , poi  $q$ ", e useremo qui questa seconda convenzione. Una notazione compatibile con l'azione di una permutazione  $p$  su un indice  $i$  richiede di scrivere la permutazione a destra dell'indice:

(i)p.

Applicando prima  $p$  e poi  $q$  a un indice  $i$ , otteniamo: ((i)p)q = (i)pq, come richiesto. In realtà, questa notazione sembra un po' bizzarra, quindi di solito elimineremo le parentesi:

$$(i)p = ip.$$

Ciò che è importante è che  $p$  deve comparire a destra.

Per rendere la nostra convenzione per la moltiplicazione compatibile con la moltiplicazione tra matrici, dobbiamo sostituire la matrice  $P$  associata ad una permutazione  $p$  [cfr. cap. 1 (4.6)] con la sua trasposta  $P^t$ , e usare questa per moltiplicare a destra per un vettore riga.

Il secondo punto è che non conviene fare i calcoli con le matrici di permutazione, poiché le matrici sono oggetti grandi in rapporto alla quantità di informazioni che contengono. È necessaria una notazione migliore. Un modo per descrivere una permutazione è per mezzo di una tabella. Possiamo considerare la configurazione:

$$(6.1) \quad p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 5 & 2 & 1 & 7 \end{bmatrix}$$

come una notazione per la permutazione definita da

$$1p = 4, \quad 2p = 6, \dots$$

È facile calcolare i prodotti usando questa notazione. Se, per esempio

$$q = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \end{bmatrix},$$

allora possiamo calcolare  $pq$  (prima  $p$ , poi  $q$ ), leggendo le due tabelle in successione:

$$pq = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 6 & 1 & 4 & 2 & 5 \end{bmatrix}.$$

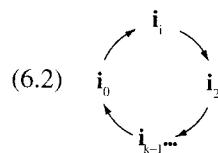
La notazione (6.1) è ancora troppo pesante, e naturalmente la riga in alto è sempre la stessa. Potremmo in teoria eliminarla, dimezzando il lavoro di scrittura, ciò renderebbe difficile trovare il posto giusto nella riga in basso, se stessimo mutando ad esempio 18 numeri.

Comunemente viene usata un'altra notazione, chiamata *notazione in cicli*. Essa descrive una permutazione di  $n$  elementi mediante al più  $n$  simboli e si basa sulla partizione degli indici in orbite rispetto all'azione di una permutazione. Sia  $p$  una permutazione, e sia  $H$  il sottogruppo ciclico generato da  $p$ . Decomponiamo l'insieme  $\{1, \dots, n\}$  in  $H$ -orbite e le chiamiamo  $p$ -orbite. Le  $p$ -orbite formano una partizione dell'insieme degli indici, chiamata la *decomposizione in cicli* associata alla permutazione  $p$ .

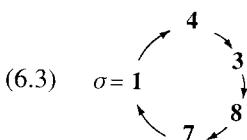
Se un indice  $i$  appartiene a un'orbita di  $k$  elementi, gli elementi dell'orbita saranno

$$O = \{i, ip, ip^2, \dots, ip^{k-1}\}.$$

Denotiamo  $ip^r$  con  $i_r$ , sicché  $O = \{i_0, i_1, \dots, i_{k-1}\}$ . Allora  $p$  agisce su tale orbita nel modo seguente:



Una permutazione che agisce in questo modo su un sottoinsieme  $\{i_0, i_1, \dots, i_{k-1}\}$  degli indici e lascia fissi i rimanenti indici è chiamata *permutazione ciclica*. Così, ad esempio,



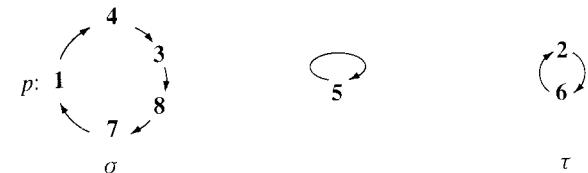
definisce una permutazione ciclica di ordine 5 di  $\{1, \dots, 8\}$ , coll'intesa che gli indici **2, 5, 6** che non compaiono sono lasciati fissi, ossia, ciascuno di essi forma una  $\sigma$ -orbita di un solo elemento. Quando parliamo degli *indici sui quali agisce una permutazione*, intendiamo quegli indici che non sono lasciati fissi: in questo caso **1, 3, 4, 7, 8**.

Un'altra permutazione ciclica di  $\{1, \dots, 8\}$  è

$$(6.4) \quad \tau = \begin{pmatrix} 2 \\ 6 \end{pmatrix}.$$

Una tale permutazione ciclica di ordine 2 è chiamata *trasposizione*. Una trasposizione è una permutazione che agisce su due indici.

La permutazione  $p$  definita in (6.1) non è ciclica, poiché vi sono 3  $p$ -orbite:



È chiaro che

$$p = \sigma\tau = \tau\sigma,$$

dove  $\sigma\tau$  è la permutazione prodotto.

(6.5) PROPOSIZIONE Siano  $\sigma, \tau$  permutazioni che agiscono su insiemi disgiunti di indici. Allora  $\sigma\tau = \tau\sigma$ .

*Dimostrazione.* Se né  $\sigma$  né  $\tau$  agiscono su un indice  $i$ , allora  $i\sigma\tau = i\tau\sigma = i$ . Se  $\sigma$  manda  $i$  in  $j \neq i$ , allora  $\tau$  lascia fissi sia  $i$  che  $j$ . In tal caso,  $i\sigma\tau = j\tau = j$  e  $i\tau\sigma = i\sigma = j$ . Allo stesso modo si tratta il caso in cui  $\tau$  agisce su  $i$ . ■

Si noti tuttavia che quando moltiplichiamo permutazioni che agiscono su insiemi non disgiunti di indici, le operazioni non commutano necessariamente. Il gruppo simmetrico  $S_n$  non è un gruppo commutativo, se  $n > 2$ . Per esempio, se  $\tau'$  è la trasposizione che scambia tra loro **3** e **6** e se  $\sigma$  è come sopra, allora  $\sigma\tau' \neq \tau'\sigma$ .

(6.6) PROPOSIZIONE Ogni permutazione  $p$  diversa dall'identità è un prodotto di permutazioni cicliche che agiscono su insiemi disgiunti di indici  $p = \sigma_1\sigma_2 \cdots \sigma_k$ , e tali permutazioni cicliche  $\sigma_r$  sono determinate univocamente da  $p$ .

*Dimostrazione.* Sappiamo che  $p$  agisce come una permutazione ciclica, qualora venga ristretta ad una sola orbita. Per ciascuna  $p$ -orbita, possiamo definire una permutazione ciclica  $\sigma_r$  che permuta tale orbita allo stesso modo di  $p$  e che lascia fissi gli altri indici. Chiaramente,  $p$  è il prodotto di queste permutazioni cicliche. Viceversa, supponiamo che  $p$  sia scritta come un prodotto  $\sigma_1\sigma_2 \cdots \sigma_k$  di permutazioni cicliche che agiscono su insiemi distinti  $O_1, \dots, O_k$  di indici. In base alla proposizione (6.5), l'ordine non ha importanza. Si noti che  $\sigma_2, \dots, \sigma_k$  lasciano fissi gli elementi di  $O_1$ ; ne segue che  $p$  e  $\sigma_1$  agiscono nello stesso modo su  $O_1$ . Pertanto  $O_1$  è una  $p$ -orbita. Lo stesso discorso vale per le altre permutazioni cicliche. Dunque  $O_1, \dots, O_k$  sono le  $p$ -orbite che contengono più di un elemento, e le permutazioni  $\sigma_i$  sono quelle costruite all'inizio della dimostrazione. ■

Una *notazione ciclica* per la permutazione ciclica (6.2) è

$$(6.7) \quad (\mathbf{i}_0 \mathbf{i}_1 \cdots \mathbf{i}_{k-1}).$$

Dunque, in particolare, la nostra permutazione  $\sigma$  ha la notazione ciclica  $(1 \ 4 \ 3 \ 8 \ 7)$ . La notazione non è completamente determinata dalla permutazione, poiché possiamo cominciare la lista con uno qualsiasi degli indici  $\mathbf{i}_0, \dots, \mathbf{i}_{k-1}$ . Vi sono cinque notazioni equivalenti per  $\sigma$ :

$$\sigma = (4 \ 3 \ 8 \ 7 \ 1) = (3 \ 8 \ 7 \ 1 \ 4) = \dots$$

Una qualsiasi di queste notazioni può essere usata.

Una *notazione in cicli* per una permutazione arbitraria  $p$  si ottiene scrivendo la permutazione come un prodotto di permutazioni cicliche che agiscono su insiemi di indici disgiunti, e scrivendo poi le notazioni cicliche per ciascuna di tali permutazioni, in successione. L'ordine è irrilevante. Così, ad esempio, due delle possibili notazioni in cicli per la permutazione  $p$  sopra descritta sono

$$(1 \ 4 \ 3 \ 8 \ 7)(2 \ 6) \text{ e } (6 \ 2)(8 \ 7 \ 1 \ 4 \ 3).$$

Se vogliamo, possiamo includere l'“uno-ciclo”  $(5)$ , per rappresentare l'elemento fisso  $5$ , presentando in tal modo tutti gli indici della lista ma di solito non si fa.

Con tale notazione, ogni permutazione può essere espressa mediante una successione di al più  $n$  interi, opportunamente racchiusi in parentesi. I prodotti possono essere ancora descritti mediante giustapposizione. Una notazione in cicli per la permutazione  $q$  considerata sopra è  $q = (1 \ 2 \ 4 \ 8 \ 7 \ 5)(3 \ 6)$ . Si ha allora

$$(6.8) \quad \begin{array}{cccc} \sigma & \tau & \sigma' & \tau' \\ pq = (1 \ 4 \ 3 \ 8 \ 7)(2 \ 6)(1 \ 2 \ 4 \ 8 \ 7 \ 5)(3 \ 6) & = \sigma \tau \sigma' \tau' \end{array}$$

Questa successione di cicli rappresenta la permutazione  $pq$ . Per calcolare il prodotto su un indice, basta seguire l'indice attraverso i quattro fattori:

$$1 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 4 \xrightarrow{\sigma'} 8 \xrightarrow{\tau'} 8, \text{ e così via.}$$

Tuttavia, l'espressione (6.8) non mostra la decomposizione di  $pq$  in cicli disgiunti, poiché gli indici compaiono più di una volta. Calcolando la permutazione  $pq$  come sopra, si ottiene la decomposizione in cicli

$$pq = (185)(237)(46) = \begin{array}{c} 8 \\ \curvearrowright \\ 1 \\ \curvearrowright \\ 5 \end{array} \quad \begin{array}{c} 3 \\ \curvearrowright \\ 2 \\ \curvearrowright \\ 7 \end{array} \quad \begin{array}{c} 4 \\ \curvearrowright \\ 6 \end{array}.$$

A conclusione dei calcoli, ogni indice compare al più una volta.

Come ulteriore esempio, consideriamo  $\rho = (5 \ 4 \ 8)$ . Allora

$$\sigma\rho = (1 \ 4 \ 3 \ 8 \ 7)(5 \ 4 \ 8) = (1 \ 8 \ 7)(3 \ 5 \ 4)$$

$$(6.9) \quad \rho\sigma = (5 \ 4 \ 8)(1 \ 4 \ 3 \ 8 \ 7) = (1 \ 4 \ 7)(3 \ 8 \ 5).$$

Calcoliamo ora la coniugata di una permutazione  $p$ . Poiché  $p$  è un prodotto di cicli disgiunti, sarà sufficiente descrivere la coniugata  $q^{-1}\sigma q$  di una permutazione ciclica  $\sigma = (\mathbf{i}_1 \dots \mathbf{i}_k)$ . (Il fatto che abbiamo cambiato l'ordine della moltiplicazione rende l'espressione per il coniugio mediante  $q^{-1}$  un po' più semplice di quella per il coniugio mediante  $q$ .)

#### (6.10) PROPOSIZIONE

- (a) Denotiamo con  $\sigma$  la permutazione ciclica  $(\mathbf{i}_1 \mathbf{i}_2 \cdots \mathbf{i}_k)$ , e sia  $q$  una permutazione arbitraria. Denotiamo l'indice  $\mathbf{i}_r q$  con  $\mathbf{j}_r$ . Allora la permutazione coniugata  $q^{-1}\sigma q$  è la permutazione ciclica  $(\mathbf{j}_1 \mathbf{j}_2 \cdots \mathbf{j}_k)$ .
- (b) Se una permutazione arbitraria  $p$  è scritta come un prodotto di cicli disgiunti  $\sigma$ , allora  $q^{-1}pq$  è il prodotto di cicli disgiunti  $q^{-1}\sigma q$ .
- (c) Due permutazioni  $p, p'$  sono elementi coniugati del gruppo simmetrico se e soltanto se le loro decomposizioni in cicli hanno gli stessi ordini.

*Dimostrazione.* La dimostrazione di (a) si riduce al calcolo seguente:

$$\mathbf{j}_r q^{-1}\sigma q = \mathbf{i}_r \sigma q = \mathbf{i}_{r+1} q = \mathbf{j}_{r+1},$$

in cui gli indici vanno letti modulo  $k$ . La parte (b) segue facilmente. Inoltre, il fatto che permutazioni coniugate hanno decomposizioni in cicli con gli stessi ordini segue da (b). Viceversa, supponiamo che  $p$  e  $p'$  abbiano decomposizioni in cicli con gli stessi ordini; che sia, ad esempio,  $p = (\mathbf{i}_1 \dots \mathbf{i}_r)(\mathbf{i}'_1 \dots \mathbf{i}'_s) \dots$  e  $p' = (\mathbf{j}_1 \dots \mathbf{j}_r)(\mathbf{j}'_1 \dots \mathbf{j}'_s) \dots$ . Definiamo  $q$  come la permutazione  $i_\nu \mapsto j_\nu$ ,  $i'_\nu \mapsto j'_\nu$ , e così via. Allora  $p' = q^{-1}pq$ . ■

Determiniamo l'equazione delle classi per il gruppo simmetrico  $S_4$ , come esempio. Tale gruppo contiene sei trasposizioni:

$$(1 \ 2), \quad (1 \ 3), \quad (1 \ 4), \quad (2 \ 3), \quad (2 \ 4), \quad (3 \ 4),$$

tre prodotti di trasposizioni disgiunte:

$$(1 \ 2)(3 \ 4), \quad (1 \ 3)(2 \ 4), \quad (1 \ 4)(2 \ 3),$$

otto 3-cicli, e sei 4-cicli. In base alla proposizione (6.10), ciascuno di questi insiemi forma una classe di coniugio. Pertanto l'equazione delle classi di  $S_4$  è:

$$24 = 1 + 3 + 6 + 6 + 8.$$

Descriveremo ora i sottogruppi  $G$  del gruppo simmetrico  $S_p$ , il cui ordine sia divisibile per  $p$  e il cui  $p$ -sottogruppo di Sylow sia normale. Supponiamo che  $p$  sia un numero primo. Poiché  $p$  divide  $p! = |S_p|$  una volta sola,  $p$  divide anche  $|G|$  una volta sola, e pertanto il  $p$ -sottogruppo di Sylow di  $G$  è un gruppo ciclico.

Risulta che tali sottogruppi si descrivono in modo molto semplice ed elegante mediante il campo finito  $\mathbb{F}_p$ . Per ottenere questa descrizione usiamo gli elementi  $\{\mathbf{0}, \mathbf{1}, \dots, \mathbf{p-1}\}$  del campo finito come indici. Alcune permutazioni di questo insieme sono date dalle stesse operazioni del campo. Precisamente, abbiamo le operazioni (aggiungere l'elemento  $a$ ) e (moltiplicare per l'elemento  $c$ ), per ogni  $a, c \in \mathbb{F}_p$ , con  $c \neq 0$ . Essendo invertibili sono permutazioni di  $\mathbb{F}_p^*$ , quindi rappresentano elementi del gruppo simmetrico. Per esempio, (aggiungere 1) è il  $p$ -ciclo:

$$(6.11) \quad (\text{aggiungere } 1) = (\mathbf{0} \ 1 \ 2 \ \dots \ (\mathbf{p-1})).$$

L'operatore (moltiplicare per  $c$ ) lascia sempre fisso l'indice  $\mathbf{0}$ , ma la sua decomposizione in cicli dipende dall'ordine dell'elemento  $c$  in  $\mathbb{F}_p^*$ . Per esempio,

$$(6.12) \quad \begin{aligned} (\text{moltiplicare per } 2) &= (\mathbf{1} \ 2 \ 4 \ 3) && \text{se } p = 5 \\ &= (\mathbf{1} \ 2 \ 4)(\mathbf{3} \ 6 \ 5) && \text{se } p = 7. \end{aligned}$$

Combinando le operazioni di addizione e moltiplicazione si ottengono tutti gli operatori su  $\mathbb{F}_p$  della forma

$$(6.13) \quad x \mapsto cx + a.$$

L'insieme di questi operatori forma un sottogruppo  $G$  di ordine  $p(p-1)$  del gruppo simmetrico.

Il gruppo degli operatori (6.13) può essere rappresentato in modo espressivo come l'insieme delle matrici  $2 \times 2$  a elementi nel campo  $\mathbb{F}_p$  della forma:

$$(6.14) \quad \begin{bmatrix} 1 & a \\ & c \end{bmatrix}.$$

Questa matrice agisce con la moltiplicazione a destra sul vettore  $(1, x)$  mandandolo in  $(1, cx+a)$ . Pertanto possiamo riottenere l'azione di  $G$  su  $\mathbb{F}_p$  moltiplicando a destra per la matrice corrispondente. (Usiamo la moltiplicazione a destra in conseguenza dell'ordine scelto per le operazioni.) Le operazioni (aggiungere  $a$ ) e (moltiplicare per  $c$ ) sono rappresentate dalle matrici elementari

$$\begin{bmatrix} 1 & a \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & c \end{bmatrix}.$$

(6.15) TEOREMA Sia  $p$  un numero primo, e sia  $H$  un sottogruppo del gruppo simmetrico  $S_p$  il cui ordine sia divisibile per  $p$ . Se il  $p$ -sottogruppo di Sylow di  $H$  è normale, allora, con un'opportuna rinumerazione degli indici,  $H$  è contenuto nel gruppo degli operatori della forma (6.13).

Per esempio, il gruppo diedrale  $D_p$  agisce fedelmente sui vertici di un poligono regolare di  $p$  lati, e quindi può essere descritto come un sottogruppo del gruppo simmetrico  $S_p$ . È il sottogruppo di (6.14) costituito dalle matrici in cui  $c = \pm 1$ .

**Dimostrazione.** Gli unici elementi di ordine  $p$  di  $S_p$  sono i  $p$ -cicli. Pertanto  $H$  contiene un  $p$ -ciclo, diciamo  $\sigma$ . Possiamo rinumerare gli indici in modo tale che  $\sigma$  diventi il  $p$ -ciclo standard (aggiungere 1) = ( $\mathbf{0} \ 1 \ \dots \ (\mathbf{p-1})$ ). Allora questa permutazione genera il  $p$ -sottogruppo di Sylow di  $H$ .

Sia  $\tau_1$  un altro elemento di  $H$ . Dobbiamo provare che  $\tau_1$  corrisponde ad un operatore della forma (6.13). Supponiamo ad esempio che  $\tau_1$  mandi l'indice  $\mathbf{0}$  in  $\mathbf{i}$ . Poiché anche  $\sigma^i$  manda  $\mathbf{0}$  in  $\mathbf{i}$ , il prodotto  $\tau = \sigma^{-i} \tau_1$  lascia fisso  $\mathbf{0}$ . Basta provare che  $\tau$  ha la forma (6.13); per questo faremo vedere che  $\tau$  è uno degli operatori (moltiplicare per  $c$ ).

Per ipotesi,  $K = \{1, \sigma, \dots, \sigma^{p-1}\}$  è un sottogruppo normale di  $H$ . Pertanto si ha:

$$(6.16) \quad \tau^{-1} \sigma \tau = \sigma^k$$

per qualche  $k$  compreso tra 1 e  $p-1$ . Determiniamo ora  $\tau$ , calcolando entrambi i membri di quest'equazione. In base alla proposizione (6.10), il membro a sinistra è il  $p$ -ciclo

$$\tau^{-1} \sigma \tau = (\mathbf{0} \tau \ 1 \tau \ \dots \ (\mathbf{p-1}) \tau),$$

mentre il calcolo diretto del membro a destra dà

$$\sigma^k = (\mathbf{0} \ k \ 2k \ \dots \ (\mathbf{p-1})k)$$

$$(\mathbf{0} \tau \ 1 \tau \ \dots \ (\mathbf{p-1}) \tau) = (\mathbf{0} \ k \ 2k \ \dots \ (\mathbf{p-1})k).$$

Dobbiamo fare attenzione nell'interpretare l'uguaglianza di questi due cicli, poiché la notazione in cicli non è unica. Occorre sapere che il primo indice nel ciclo a sinistra è lo stesso che compare come primo indice nel ciclo a destra, altrimenti dovremmo identificare degli indici uguali nei due cicli e cominciare con questi. Ecco perché abbiamo normalizzato all'inizio, per avere  $\mathbf{0}\tau = \mathbf{0}$ . Sapendo ciò, le due liste coincidono, e concludiamo che

$$1\tau = k, \quad 2\tau = 2k, \quad \dots$$

Questo è l'operatore (moltiplicare per  $k$ ), come affermato. ■

Ritorniamo ora per un momento al problema dell'ordine delle operazioni. Se vogliamo usare la notazione  $p(\mathbf{i})$  per le permutazioni in questo paragrafo, come facciamo altrove per le funzioni, dobbiamo modificare il modo di effettuare i calcoli con i cicli, per tener conto di ciò. Il modo più sistematico di procedere è quello di leggere *ogni cosa*, inclusi i cicli, da destra a sinistra. In altre parole, dovremmo leggere il ciclo  $(1 \ 4 \ 3 \ 8 \ 7)$  nel modo seguente:

$$1 \leftarrow 4 \leftarrow 3 \leftarrow 8 \leftarrow 7 \leftarrow 1.$$

Si tratta dell'inversa della permutazione (6.3). Possiamo allora interpretare il prodotto  $(1 \ 4 \ 3 \ 8 \ 7)(5 \ 4 \ 8)$  come la composizione: "Applicare prima  $(5 \ 4 \ 8)$ , poi  $(1 \ 4 \ 3 \ 8 \ 7)$ ". Il calcolo di tale prodotto dà:

$$1 \leftarrow 8 \leftarrow 7 \leftarrow 1, \quad 3 \leftarrow 5 \leftarrow 4 \leftarrow 3,$$

che scriveremmo come  $(1 \ 8 \ 7)(3 \ 5 \ 4)$ . Si noti che questa è la stessa successione di simboli ottenuta in (6.9). Miracolosamente, leggendo ogni cosa all'indietro, si ottiene lo stesso risultato quando moltiplichiamo le permutazioni. Ma naturalmente, la notazione  $(1 \ 8 \ 7)(3 \ 5 \ 4)$  ora sta a indicare l'inversa della permutazione (6.9). Il fatto che le notazioni si moltiplicano coerentemente nei due modi di leggere le permutazioni mitiga il "reato" che abbiamo commesso passando da sinistra a destra.

## 7 Il gruppo libero

Abbiamo visto alcuni gruppi, quali il gruppo simmetrico  $S_3$ , i gruppi diedrali  $D_n$ , e il gruppo  $M$  dei movimenti rigidi del piano, in cui i calcoli possono essere eseguiti facilmente utilizzando una lista di generatori e una lista di relazioni per lavorare con essi. Il resto del capitolo è dedicato allo studio degli aspetti teorici relativi a tali metodi. In questo paragrafo consideriamo i gruppi che hanno un insieme di generatori soddisfacenti *unicamente* alle relazioni che sono conseguenza degli assiomi di gruppo [quale, ad esempio,  $x(yz) = (xy)z$ ]. Un insieme  $S$  di elementi di un gruppo che non soddisfano a nessun'altra relazione all'infuori di quelle che derivano dagli assiomi si dice *libero*, e un gruppo che possiede un insieme libero di generatori è detto *gruppo libero*. Descriveremo ora i gruppi liberi.

Partiamo da un insieme arbitrario di simboli, diciamo  $S = \{a, b, c, \dots\}$ , che può essere finito o infinito, e definiamo una *parola* come una successione finita di simboli di  $S$ , in cui sono ammesse ripetizioni. Per esempio,  $a, aa, ba, aaba$  sono parole. Due parole possono essere composte mediante giustapposizione:

$$aa, ba \mapsto aaba;$$

In questo modo l'insieme  $W$  di tutte le parole ha una legge di composizione associativa. Per di più, la "parola vuota" può essere introdotta come elemento neutro rispetto a tale legge. Ci servirà un simbolo per indicarla; useremo  $1$ . L'insieme  $W$  chiamato il *semigruppo libero* sull'insieme di simboli  $S$ . Purtroppo non è un gruppo, poiché mancano gli inversi, e l'introduzione degli inversi complica le cose.

Sia  $S'$  l'insieme costituito dai simboli di  $S$  e in più dai simboli  $a^{-1}$  per ogni  $a \in S$ :

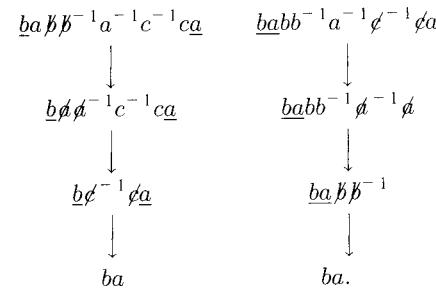
$$(7.1) \quad S' = \{a, a^{-1}, b, b^{-1}, c, c^{-1}, \dots\}.$$

Sia  $W'$  l'insieme delle parole formate con i simboli di  $S'$ . Se una parola  $w \in W'$  è della forma

$$\dots \underline{xx}^{-1} \dots \quad \text{oppure} \quad \dots \underline{x}^{-1}x \dots$$

per qualche  $x \in S$ , possiamo convenire di ridurne la lunghezza cancellando  $x$  e  $x^{-1}$ . La parola è *ridotta* se non è possibile effettuare cancellazioni. A partire da ogni  $w$ , possiamo eseguire un numero finito di cancellazioni, ottenendo infine una parola ridotta  $w_0$  (eventualmente la parola vuota 1) che prende il nome di *forma ridotta* di  $w$ .

Spesso è possibile operare le cancellazioni in più modi. Per esempio, partendo da  $w = babb^{-1}a^{-1}c^{-1}ca$ , possiamo seguire due vie:



La parola ridotta è la stessa, sebbene le lettere provengano da posti diversi nella parola originaria (le lettere che sopravvivono alle cancellazioni sono state sottolineate). Questa è la situazione generale.

**(7.2) PROPOSIZIONE** Esiste un'unica forma ridotta di una parola assegnata  $w$ .

*Dimostrazione.* Procediamo per induzione sulla lunghezza di  $w$ . Se  $w$  è ridotta, non vi è nulla da dimostrare. Altrimenti, deve esistere qualche coppia di lettere che possono essere cancellate, diciamo la coppia sottolineata:

$$w = \dots \underline{xx}^{-1} \dots$$

(Denotiamo con  $x$  un generico elemento di  $S'$ , con la convenzione ovvia che, se  $x = a^{-1}$ , allora  $x^{-1} = a$ .) Se faremo vedere che possiamo ottenere ogni forma ridotta  $w_0$  di  $w$  cancellando per prima la coppia  $\underline{xx}^{-1}$ , allora la proposizione seguirà per induzione sulla parola accorciata  $\dots \cancel{x}^{-1} \dots$  così ottenuta.

Sia  $w_0$  una forma ridotta di  $w$ . Sappiamo che  $w_0$  è ottenuta da  $w$  mediante una successione di cancellazioni. La prima possibilità è che la coppia  $\underline{xx}^{-1}$  venga cancellata in qualche passo di questa successione. Allora potremmo anche riordinare le operazioni e cancellare  $\underline{xx}^{-1}$  per prima. Dunque questo caso è risolto. D'altra parte, la coppia  $\underline{xx}^{-1}$  non può restare in  $w_0$ , poiché  $w_0$  è ridotta. A un certo punto, quindi, almeno uno dei due simboli deve venire cancellato. Se la coppia stessa non è cancellata, allora la prima cancellazione che riguarda la coppia deve essere del tipo

$$\dots \cancel{x}^{-1} \cancel{x} \dots \text{ oppure } \dots \underline{x} \cancel{x}^{-1} \cancel{x} \dots$$

Si noti che la parola ottenuta mediante questa cancellazione è la stessa che si ottiene cancellando la coppia originaria  $\underline{xx}^{-1}$ . A questo punto, quindi, possiamo cancellare invece la coppia originaria. Ci ritroviamo così nel primo caso, e la proposizione è dimostrata. ■

Due parole  $w, w'$  di  $W'$  sono *equivalenti*, e scriviamo  $w \sim w'$ , se hanno la stessa forma ridotta. Questa è una relazione di equivalenza.

**(7.3) PROPOSIZIONE** *I prodotti di parole equivalenti sono equivalenti: se  $w \sim w'$  e  $v \sim v'$ , allora  $wv \sim w'v'$ .*

*Dimostrazione.* Per ottenere la parola ridotta equivalente al prodotto  $wv$ , possiamo cancellare innanzitutto quanto più è possibile in  $w$  e in  $v$ , per ridurre  $w$  a  $w_0$  e  $v$  a  $v_0$ . Allora  $wv$  è ridotta a  $w_0v_0$ . Ora continuiamo a cancellare in  $w_0v_0$ , se possibile. Poiché  $w' \sim w$  e  $v' \sim v$ , lo stesso procedimento, applicato a  $w'v'$ , porta anch'esso a  $w_0v_0$  e quindi fornisce la stessa parola ridotta. ■

Da questa proposizione segue che le classi di equivalenza di parole possono essere moltiplicate tra loro, ossia, che esiste una legge di composizione ben definita sull'insieme delle classi di equivalenza di parole.

**(7.4) PROPOSIZIONE** *Denotiamo con  $F$  l'insieme delle classi di equivalenza di parole in  $W'$ . Allora  $F$  è un gruppo rispetto alla legge di composizione indotta da  $W'$ .*

*Dimostrazione.* L'associatività della moltiplicazione e il fatto che la classe della parola vuota 1 è un'identità discendono dalle proprietà corrispondenti in  $W'$ . Resta da verificare che tutti gli elementi di  $F$  sono invertibili. Ma è chiaro che, se  $w = xy \dots z$ , allora la classe di  $z^{-1} \dots y^{-1} x^{-1}$  è l'inversa della classe di  $w$ . ■

**(7.5) DEFINIZIONE** *Il gruppo  $F$  delle classi di equivalenza di parole è il gruppo libero sull'insieme  $S$ .*

Per la proposizione (7.2) un elemento del gruppo libero  $F$  corrisponde ad un'unica parola ridotta di  $W'$ . Per moltiplicare parole ridotte, basta unire e cancellare:

$$(abc^{-1})(cb) \rightarrow abc^{-1}cb = abb.$$

Per le parole ridotte si può introdurre anche la notazione esponenziale:  $aaab^{-1}b^{-1} = a^3b^{-2}$ .

Il gruppo libero sull'insieme  $S = \{a\}$  costituito da un solo elemento coincide con l'insieme di tutte le potenze di  $a$ :  $F = \{a^n\}$  ed è un gruppo ciclico infinito. Invece, il gruppo libero su un insieme  $S = \{a, b\}$  di due elementi è molto complicato.

## 8 Generatori e relazioni

Dopo aver descritto i gruppi liberi, consideriamo ora il caso più frequente in cui un insieme di generatori di un gruppo non è libero, ossia esistono alcune relazioni non banali tra di essi. La nostra trattazione è basata sulle proprietà di rappresentazione del gruppo libero e dei gruppi quoziente.

**(8.1) PROPOSIZIONE** (Proprietà di rappresentazione del gruppo libero) *Sia  $F$  il gruppo libero su un insieme  $S = \{a, b, \dots\}$ , e sia  $G$  un gruppo. Ogni applicazione tra insiemi  $f : S \rightarrow G$  si estende in modo unico ad un omomorfismo di gruppi  $\varphi : F \rightarrow G$ . Se denotiamo l'immagine  $f(x)$  di un elemento  $x \in S$  con  $\tilde{x}$ , allora  $\varphi$  manda una parola di  $S' = \{a, a^{-1}, b, b^{-1}, \dots\}$  nel prodotto corrispondente degli elementi  $\{\tilde{a}, \tilde{a}^{-1}, \tilde{b}, \tilde{b}^{-1}, \dots\}$  in  $G$ .*

*Dimostrazione.* Questa legge definisce un'applicazione sull'insieme delle parole in  $S'$ . Dobbiamo provare che parole equivalenti vengono mandate nello stesso prodotto in  $G$ . Ciò è evidente perché la cancellazione in una parola non cambia il prodotto corrispondente in  $G$ . Inoltre, poiché la moltiplicazione in  $F$  è definita mediante giustapposizione, l'applicazione  $\varphi$  così definita è un omomorfismo. Essa rappresenta l'unico modo di estendere  $f$  ad un omomorfismo. ■

Se  $S$  è un sottoinsieme di un gruppo  $G$ , la proprietà di rappresentazione del gruppo libero definisce un omomorfismo  $\varphi : F \rightarrow G$  dal gruppo libero su  $S$  a  $G$ . Ciò traduce il fatto che gli elementi di  $S$  non soddisfano alcuna relazione in  $F$ , tranne quelle che discendono dagli assiomi di gruppo, e spiega l'uso dell'aggettivo "libero".

Si dice che un insieme di elementi  $S$  genera un gruppo  $G$  se l'applicazione  $\varphi$  dal gruppo libero su  $S$  a  $G$  è suriettiva. Ciò equivale a dire che ogni elemento di  $G$  è un prodotto di una successione di elementi di  $S'$ , sicché è in accordo con la terminologia introdotta nel capitolo 2 (§ 2). In ogni caso, sia che  $S$  generi o non generi  $G$ , l'immagine dell'omomorfismo  $\varphi$  della proposizione (8.1) è un sottogruppo chiamato il *sottogruppo generato da S*. Tale sottogruppo è costituito precisamente da tutti i prodotti degli elementi di  $S'$ .

Supponiamo che  $S$  generi  $G$ . Allora gli elementi di  $S$  vengono chiamati *generatori*. Poiché  $\varphi$  è un omomorfismo suriettivo, il primo teorema di isomorfismo [cap. 2 (10.9)] ci dice che  $G$  è isomorfo al gruppo quoziante  $F/N$ , dove  $N = \ker \varphi$ . Gli elementi di  $N$  prendono il nome di *relazioni* tra i generatori. Essi sono classi di equivalenza di parole  $w$  con la proprietà che il prodotto corrispondente in  $G$  è 1:

$$\varphi(w) = 1 \quad \text{o} \quad w = 1 \text{ in } G.$$

In particolare, se  $N = \{1\}$ ,  $\varphi$  è un isomorfismo. In questo caso, anche  $G$  è chiamato gruppo libero.

Se conosciamo un insieme di generatori e anche tutte le relazioni, possiamo effettuare calcoli nel gruppo isomorfo  $F/N$  e quindi nel gruppo  $G$ . Ma il sottogruppo  $N$  sarà infinito, a meno che  $G$  non sia libero, sicché non possiamo elencare tutti i suoi elementi. Diremo piuttosto che un insieme di parole

$$R = \{r_1, r_2, \dots\}$$

è un insieme di *relazioni* che definiscono  $G$  se  $R \subset N$  e se  $N$  è il più piccolo sottogruppo normale contenente  $R$ . Ciò significa che  $N$  è generato dal sottoinsieme costituito da tutte le parole in  $R$  e anche da tutte le loro coniugate.

Potrebbe sembrare più opportuno richiedere che le relazioni che definiscono  $G$  siano generatori del gruppo  $N$ . Ma conviene ricordare che il nucleo dell'omomorfismo  $F \rightarrow G$  definito mediante un insieme di generatori è sempre un sottogruppo normale, sicché non è necessario considerare una lista più lunga di relazioni che definiscono  $G$ . Se sappiamo che qualche relazione  $r = 1$  vale in  $G$ , allora possiamo concludere che anche la relazione  $xrx^{-1} = 1$  vale in  $G$ , semplicemente moltiplicando ambo i membri dell'equazione a sinistra e a destra, rispettivamente, per  $x$  e  $x^{-1}$ .

Conosciamo già esempi di generatori e relazioni, tra cui il gruppo diedrale  $D_n$  [cap. 5 (3.6), (3.7)], generato da due elementi  $x, y$ , con le relazioni

$$(8.2) \quad x^n = 1, \quad y^2 = 1, \quad xyxy = 1.$$

(8.3) PROPOSIZIONE Gli elementi  $x^n, y^2, xyxy$  formano un insieme di relazioni che definiscono il gruppo diedrale.

Questa proposizione è stata sostanzialmente verificata [cfr. cap. 5 (3.6)]. Ma per dimostrarla formalmente, e per lavorare liberamente utilizzando generatori e relazioni, avremo bisogno della cosiddetta "proprietà di rappresentazione dei gruppi quoziante". È una generalizzazione del primo teorema di isomorfismo:

(8.4) PROPOSIZIONE (Proprietà di rappresentazione dei gruppi quoziante) *Dato un sottogruppo normale  $N$  di  $G$ , poniamo  $\bar{G} = G/N$  e denotiamo con  $\pi$  l'applicazione canonica  $\pi: G \rightarrow \bar{G}$  definita da  $\pi(a) = \bar{a} = aN$ . Sia  $\varphi: G \rightarrow G'$  un omomorfismo il cui nucleo contenga  $N$ . Allora esiste un unico omomorfismo  $\bar{\varphi}: \bar{G} \rightarrow G'$  tale che  $\bar{\varphi}\pi = \varphi$ :*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \searrow & \nearrow \bar{\varphi} & \\ \bar{G} & & \end{array} .$$

Tale applicazione è definita dalla legge  $\bar{\varphi}(\bar{a}) = \varphi(a)$ .

*Dimostrazione.* Per definire un'applicazione  $\bar{\varphi}: \bar{G} \rightarrow G'$ , dobbiamo definire  $\bar{\varphi}(\alpha)$  per ogni elemento  $\alpha$  di  $\bar{G}$ . Per fare ciò, rappresentiamo  $\alpha$  mediante un elemento  $a \in G$ , scegliendo  $a$  in modo tale che  $\alpha = \pi(a)$ . Ciò significa che  $\alpha = \bar{a}$ . Ora, poiché vogliamo che l'applicazione  $\bar{\varphi}$  soddisfi la relazione  $\bar{\varphi}(\pi(a)) = \varphi(a)$ , non vi è altra scelta che definire  $\bar{\varphi}$  mediante la legge  $\bar{\varphi}(\alpha) = \varphi(a)$ , come asserito nella proposizione. Per dimostrare che ciò è lecito, dobbiamo far vedere che il valore che si ottiene per  $\bar{\varphi}(\alpha)$ , ossia  $\varphi(a)$ , dipende soltanto da  $\alpha$  e non dalla scelta del rappresentante  $a$ . Spesso ciò si esprime dicendo che occorre verificare che l'applicazione  $\bar{\varphi}$  è "ben definita".

Siano  $a$  e  $a'$  due elementi di  $G$  tali che  $\bar{a} = \bar{a}' = \alpha$ . L'uguaglianza  $\bar{a} = \bar{a}'$  significa che  $aN = a'N$ , oppure [cap. 2 (5.13)] che  $a' \in aN$ . Pertanto  $a' = an$  per qualche  $n \in N$ . Poiché  $N \subset \ker \varphi$  per ipotesi,  $\varphi(n) = 1$ . Dunque  $\varphi(a') = \varphi(a)\varphi(n) = \varphi(a)$ , come richiesto.

Infine, l'applicazione  $\bar{\varphi}$  è un omomorfismo, poiché  $\bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b}) = \varphi(a)\varphi(b) = \varphi(ab) = \bar{\varphi}(\bar{ab})$ . ■

*Dimostrazione della proposizione (8.3).* Abbiamo dimostrato nel capitolo 5 (3.6) che  $D_n$  è generato dagli elementi  $x, y$  che soddisfano (8.2). Pertanto, indicando con  $F$  il gruppo libero su  $x, y$ , esiste un'applicazione suriettiva  $\varphi: F \rightarrow D_n$ , e  $R = \{x^n, y^2, xyxy\}$  è contenuto in  $\ker \varphi$ . Sia  $N$  il più piccolo sottogruppo normale di  $F$  contenente  $R$ . Allora, poiché  $\ker \varphi$  è un sottogruppo normale che contiene  $R$ ,  $N \subset \ker \varphi$ . La proprietà di rappresentazione dei gruppi quoziante fornisce un omomorfismo  $\bar{\varphi}: F/N \rightarrow D_n$ . Se proviamo che  $\bar{\varphi}$  è un'applicazione biiettiva, la proposizione sarà dimostrata.

Osserviamo che, poiché  $\varphi$  è suriettiva, anche  $\bar{\varphi}$  è suriettiva. Inoltre, in  $F/N$  valgono le relazioni  $\bar{x}^n = 1$ ,  $\bar{y}^2 = 1$ ,  $\bar{x}\bar{y}\bar{x}\bar{y} = 1$ . Usando tali relazioni, possiamo esprimere ogni parola in  $\bar{x}, \bar{y}$  nella forma:  $\bar{x}^i\bar{y}^j$ , con  $0 \leq i \leq n-1$  e  $0 \leq j \leq 1$ .

Ciò prova che  $F/N$  ha al più  $2n$  elementi. Poiché  $|D_n| = 2n$ , ne segue che  $\varphi$  è biettiva, come richiesto. ■

Useremo la notazione

$$(8.5) \quad \langle x_1, \dots, x_m; r_1, \dots, r_k \rangle$$

per indicare il gruppo generato dagli elementi  $x_1, \dots, x_m$ , con le relazioni (che lo definiscono)  $r_1, \dots, r_k$ . In particolare:

$$(8.6) \quad D_n = \langle x, y; x^n, y^2, xyxy \rangle.$$

Come nuovo esempio, consideriamo il gruppo generato da  $x, y$ , con l'unica relazione  $xyx^{-1}y^{-1} = 1$ . In generale, se  $x, y$  sono elementi di un gruppo, l'elemento

$$(8.7) \quad xyx^{-1}y^{-1}$$

è chiamato il loro *commutatore*. Esso gode dell'importante proprietà di essere uguale a 1 se e solo se  $x$  e  $y$  commutano tra loro (come si può vedere moltiplicando ambo i membri dell'equazione  $xyx^{-1}y^{-1} = 1$  a destra per  $yx$ .) Se quindi imponiamo la relazione  $xyx^{-1}y^{-1} = 1$  sul gruppo libero, otteniamo un gruppo in cui  $x$  e  $y$  commutano tra loro. Dunque, se  $N$  è il più piccolo sottogruppo normale contenente il commutatore  $xyx^{-1}y^{-1}$  e se  $G = F/N$ , allora le classi resto di  $x$  e  $y$  sono elementi che commutano in  $G$ . Ne segue che due elementi qualunque di  $G$  commutano tra loro.

(8.8) PROPOSIZIONE *Sia  $F$  il gruppo libero su  $x, y$  e sia  $N$  il più piccolo sottogruppo normale generato dal commutatore  $xyx^{-1}y^{-1}$ . Allora il gruppo quoziante  $G = F/N$  è abeliano.*

*Dimostrazione.* Denotiamo le classi resto dei generatori  $x, y$  in  $G$  con le stesse lettere. Poiché il commutatore appartiene a  $N$ , gli elementi  $x, y$  commutano in  $G$ . Allora  $xyx^{-1} = xyy^{-1} = x$ , il che implica  $xy^{-1} = y^{-1}x$ , cioè  $x$  commuta anche con  $y^{-1}$ . Inoltre,  $x$  commuta ovviamente con  $x$  e con  $x^{-1}$ . Pertanto  $x$  commuta con qualsiasi parola in  $S' = \{x, x^{-1}, y, y^{-1}\}$ , e così pure  $y$ . Ne segue per induzione che due parole qualsiasi in  $S'$  commutano tra loro. Poiché  $x, y$  generano il gruppo,  $G$  è commutativo. ■

Come conseguenza, si ha che il commutatore  $uvu^{-1}v^{-1}$  di due parole  $u, v \in S'$  appartiene al sottogruppo normale generato dal solo commutatore  $xyx^{-1}y^{-1}$ : poiché, dato che  $u, v$  commutano in  $G$ , il loro commutatore rappresenta l'elemento neutro in  $G$ .

Il gruppo  $G$  costruito ora è chiamato il *gruppo abeliano libero* sull'insieme  $\{x, y\}$ , poiché gli elementi  $x, y$  non soddisfano alcuna relazione all'infuori di quelle che sono conseguenze degli assiomi di gruppo e della proprietà commutativa.

Negli esempi che abbiamo visto, la conoscenza delle relazioni ci ha permesso di effettuare facilmente i calcoli nel gruppo. Ciò tuttavia può trarre in inganno, poiché i calcoli con un insieme arbitrario di relazioni spesso non sono affatto facili. Per esempio, supponiamo di cambiare leggermente le relazioni (8.6) che definiscono il gruppo diedrale, sostituendo  $y^2$  con  $y^3$ :

$$(8.9) \quad G = \langle x, y; x^n, y^3, xyxy \rangle.$$

Questo gruppo è molto più complicato. Per  $n > 5$ , è un gruppo infinito.

La situazione diventa molto difficile quando le relazioni sono abbastanza complicate. Supponiamo di avere un insieme  $R$  di parole, e sia  $N$  il più piccolo sottogruppo normale contenente  $R$ . Siano  $w, w'$  due parole qualsiasi. Allora possiamo chiederci se  $w$  e  $w'$  rappresentano o no lo stesso elemento di  $F/N$ . Questo è chiamato il *problema della parola per i gruppi*, ed è stato dimostrato che non esiste alcun procedimento generale per giungere alla sua soluzione in un intervallo di tempo predeterminato. Tuttavia, generatori e relazioni consentono di eseguire calcoli in modo efficiente in molti casi, e quindi risultano uno strumento utile. Nel prossimo paragrafo, esamineremo un importante metodo di calcolo: l'algoritmo di Todd-Coxeter.

Ricapitolando, quando parliamo di un gruppo definito da generatori  $S$  e relazioni  $R$ , intendiamo il gruppo quoziante  $F/N$ , dove  $F$  è il gruppo libero su  $S$  e  $N$  è il più piccolo sottogruppo normale di  $F$  contenente  $R$ . Si noti che qualsiasi insieme di relazioni  $R$  definisce un gruppo, poiché  $F/N$  è sempre definito. Più grande è  $R$ , più grande diventa  $N$  e più grande è la contrazione che ha luogo nell'omomorfismo  $\pi : F \rightarrow F/N$ . Se  $R$  diventa "troppo grande", il peggio che può accadere è che  $N = F$ , e quindi che  $F/N$  è il gruppo banale. Dunque non esiste, per così dire, un insieme contraddittorio di relazioni. Gli unici problemi che possono sorgere si presentano quando  $F/N$  diventa troppo piccolo, e ciò accade quando le relazioni danno luogo ad una contrazione maggiore di quella prevista.

## 9 L'algoritmo di Todd-Coxeter

Sia  $H$  un sottogruppo di un gruppo finito  $G$ . L'algoritmo di Todd-Coxeter, che viene descritto in questo paragrafo, è un metodo diretto, alquanto sorprendente, per contare le classi laterali di  $H$  in  $G$  e per determinare l'azione di  $G$  sull'insieme delle classi laterali. Poiché sappiamo che ogni azione su un'orbita somiglia ad un'azione sulle classi laterali [cap. 5 (6.3)], l'algoritmo è in realtà un metodo per descrivere un'azione qualsiasi di un gruppo.

Per poter effettuare esplicitamente i calcoli, sia il gruppo  $G$  che il sottogruppo  $H$  devono essere assegnati in modo esplicito. Consideriamo pertanto un gruppo:

$$(9.1) \quad G = \langle x_1, \dots, x_m; r_1, \dots, r_k \rangle$$

presentato mediante generatori  $x_1, \dots, x_m$  e relazioni  $r_1, \dots, r_k$  date esplicitamente, come nel paragrafo precedente. Dunque  $G$  è realizzato come il gruppo quoziente  $F/N$ , dove  $F$  è il gruppo libero sull'insieme  $\{x_1, \dots, x_m\}$  e  $N$  è il più piccolo sottogruppo normale contenente  $\{r_1, \dots, r_k\}$ . Supponiamo inoltre che il sottogruppo  $H$  di  $G$  sia dato esplicitamente mediante un insieme di parole:

$$(9.2) \quad \{h_1, \dots, h_s\}$$

nel gruppo libero  $F$ , le cui immagini in  $G$  generano  $H$ .

Per cominciare, analizziamo un esempio in dettaglio. Consideriamo il gruppo  $G$  generato da tre elementi  $x, y, z$ , con le relazioni  $x^3, y^2, z^2, xyz$ , e il sottogruppo ciclico  $H$  generato da  $z$ :

$$(9.3) \quad G = \langle x, y, z; x^3, y^2, z^2, xyz \rangle, \quad H = \{z\}.$$

Poiché vogliamo determinare l'azione sulle classi laterali, che è una rappresentazione mediante permutazioni [cap. 5 (8.1)], dobbiamo decidere come scrivere le permutazioni. Useremo la notazione in cicli del § 6. Ciò ci obbliga a lavorare con le *classi laterali destre*  $Hg$ , piuttosto che con le classi laterali sinistre, poiché vogliamo che  $G$  agisca a destra. Denotiamo con  $\mathcal{C}$  l'insieme delle classi laterali destre di  $H$  in  $G$ . Dobbiamo decidere inoltre come descrivere esplicitamente l'azione del gruppo, e il modo più semplice è quello di ritornare di nuovo al gruppo libero, ossia di descrivere le permutazioni associate ai generatori  $x, y, z$  assegnati.

Le azioni dei generatori sull'insieme delle classi laterali soddisferanno alle seguenti regole:

#### (9.4) REGOLE

1. L'azione di ciascun generatore ( $x, y, z$  nell'esempio) è una permutazione.
2. Le relazioni ( $x^3, y^2, z^2, xyz$  nell'esempio) agiscono in modo banale.
3. I generatori di  $H$  ( $z$  nell'esempio) lasciano fissa la classe laterale  $H1$ .
4. L'azione sulle classi laterali è transitiva.

La prima regola è una proprietà generale delle azioni di gruppi. Essa segue dal fatto che gli elementi di un gruppo sono invertibili, e la inseriamo nell'elenco invece di menzionare esplicitamente gli inversi dei generatori. La seconda regola vale poiché le relazioni rappresentano 1 in  $G$ , ed è il gruppo  $G$  che agisce. Le regole 3 e 4 sono proprietà particolari dell'azione sulle classi laterali.

Determiniamo ora l'azione sulle classi laterali, applicando soltanto queste regole. Usiamo gli indici  $1, 2, 3, \dots$  per denotare le classi laterali, con  $1$  che sta a indicare la classe laterale  $H1$ . Poiché non sappiamo quante classi laterali ci sono,

non sappiamo di quanti indici abbiamo bisogno. Ne aggiungeremo di nuovi, se necessario.

Innanzitutto, la regola 3 ci dice che  $z$  manda  $1$  in se stesso:  $1z = 1$ . Ciò esaurisce le informazioni contenute nella regola 3, sicché restano le regole 1 e 2. La regola 4 comparirà soltanto in modo implicito.

Non sappiamo in che modo  $x$  agisce sull'indice  $1$ . Supponiamo che  $1x \neq 1$  e assegnamo un nuovo indice, diciamo  $1x = 2$ . Continuando con il generatore  $x$ , non conosciamo  $2x$ , e pertanto assegnamo un terzo indice:  $1x^2 = 2x = 3$ . La regola 2 ora entra in gioco. Essa ci dice che  $x^3$  lascia fisso ogni indice. Pertanto  $1x^3 = 3x = 1$ . Queste informazioni vengono riassunte di solito in una tabella:

$x$	$x$	$x$	
1	2	3	1

che descrive l'azione di  $x$  sui tre indici. La relazione  $xxx$  compare in alto, e la regola 2 si riflette nel fatto che lo stesso indice  $1$  compare alle due estremità. A questo punto, abbiamo determinato l'azione di  $x$  sui tre indici  $1, 2, 3$ , con l'eccezione di un solo fatto: non sappiamo ancora che questi indici rappresentano classi laterali distinte.

Consideriamo ora l'azione di  $y$  sull'indice  $1$ . Di nuovo, non la conosciamo, sicché assegnamo un nuovo indice, diciamo  $1y = 4$ . Applichiamo ancora la regola 2. Poiché  $y^2$  agisce in modo banale, sappiamo che  $1y^2 = 4y = 1$ :

$y$	$y$	
1	4	1

Infine resta la relazione  $xyz$ . Sappiamo che  $1x = 2$ , ma non conosciamo ancora  $2y$ . Pertanto poniamo  $1xy = 2y = 5$ . La regola 2 ci dice allora che  $1xyz = 5z = 1$ :

$x$	$y$	$z$	
1	2	5	1

Applichiamo ora la regola 1, secondo cui l'azione di ciascun elemento del gruppo è una permutazione degli indici. Abbiamo stabilito che  $1z = 1$  e inoltre che  $5z = 1$ . Ne segue che  $5 = 1$ . Eliminiamo l'indice  $5$ , sostituendolo con  $1$ . Ciò, a sua volta, ci dice che  $2y = 1$ . D'altra parte, abbiamo già stabilito che  $4y = 1$ . Pertanto  $4 = 2$  in base alla regola 1, e quindi eliminiamo  $4$ .

Gli elementi nella tabella qui sotto sono stati ora determinati:

$x$	$x$	$x$	$y$	$y$	$z$	$z$	$x$	$y$	$z$
1	2	3	1	2	1	1	1	2	1
2	3	1	2	1	2	2	3	2	2
3	1	2	3		3	3	1	2	3

e  $H = G$ . Pertanto  $x$  è una potenza di  $y$ . La terza relazione prova che  $x^2 = 1$ . Combinando questo fatto con la prima relazione, otteniamo  $x = 1$ . Dunque  $G$  è un gruppo ciclico di ordine 3. Questo esempio illustra il modo in cui le relazioni possono contrarre il gruppo. ■

Negli esempi precedenti, abbiamo considerato un sottogruppo  $H$  generato da uno dei generatori scelti per  $G$ , ma potremmo anche fare i calcoli con un sottogruppo  $H$  generato da un insieme arbitrario di parole. Esse vanno fatte intervenire nei calcoli, usando la regola 3.

Questo metodo può essere usato anche nel caso in cui  $G$  è infinito, purché l'indice  $[G : H]$  sia finito. Se vi sono infinite classi laterali non ci si può aspettare che il procedimento abbia termine.

Ci poniamo ora il problema di stabilire perché il procedimento che abbiamo descritto fornisce l'azione sulle classi laterali. Una dimostrazione formale di questo fatto non è possibile senza definire prima l'algoritmo rigorosamente, e ciò non è stato fatto. Pertanto tratteremo il problema in modo informale, cominciando a descrivere il procedimento seguito. A un dato stadio del processo di calcolo, avremo un certo insieme  $I$  di indici, e l'azione di alcuni generatori del gruppo su alcuni indici sarà stata determinata. Chiamiamo tale azione un'*azione parziale* su  $I$ . Un'azione parziale non deve essere necessariamente coerente con le regole 1, 2 e 3, ma dovrebbe essere transitiva, ossia tutti gli indici dovrebbero appartenere all'*"orbita parziale"* di  $\mathbf{1}$ . A questo punto entra in gioco la regola 4. Essa ci dice di non introdurre alcun indice di cui non abbiamo bisogno.

La posizione iniziale è  $I = \{\mathbf{1}\}$ , senza alcuna azione assegnata. Ad ogni stadio ci sono due possibilità per il passo successivo:

- (9.9) (i) possiamo uguagliare due indici  $\mathbf{i}, \mathbf{j} \in I$  come conseguenza di una delle prime tre regole, oppure
- (ii) possiamo scegliere un generatore  $x$  e un indice  $\mathbf{i}$  tali che  $\mathbf{i}x$  non sia stato ancora determinato e definire  $\mathbf{i}x = \mathbf{j}$ , dove  $\mathbf{j}$  è un nuovo indice.

Il procedimento termina quando resta determinata un'azione che sia coerente con le regole, ossia, quando otteniamo una tabella completa e coerente, e valgono le regole.

A questo punto, sorgono due problemi. In primo luogo, tale procedimento avrà termine? In secondo luogo, se esso ha termine, l'azione ottenuta è quella giusta? La risposta ad entrambi i problemi è positiva. Si può dimostrare che il procedimento ha sempre termine, purché il gruppo sia finito e venga data preferenza al passo (i). Ciò non verrà dimostrato. Il fatto più importante per le applicazioni è che, se il procedimento ha termine, la rappresentazione mediante permutazioni che si ottiene è quella giusta.

(9.10) TEOREMA Supponiamo che mediante un numero finito di passi (i) e (ii) venga ottenuta una tabella coerente. Allora la tabella definisce una rappresentazione mediante permutazioni che può venire identificata, con un'opportuna rinumerazione degli indici, con la rappresentazione sulle classi laterali.

*Abbozzo di dimostrazione.* Denotiamo con  $I^*$  l'insieme finale degli indici, con la sua azione. Dimostreremo il risultato definendo un'applicazione biettiva  $\varphi^* : I^* \rightarrow \mathcal{C}$  da tale insieme all'insieme delle classi laterali che è compatibile con le due azioni. Definiamo  $\varphi^*$  induttivamente, definendo ad ogni stadio un'applicazione  $\varphi : I \rightarrow \mathcal{C}$  dall'insieme degli indici determinati a quello stadio a  $\mathcal{C}$ , tale che  $\varphi$  sia compatibile con l'azione parziale su  $I$ . All'inizio,  $\{\mathbf{1}\} \rightarrow \mathcal{C}$  manda  $\mathbf{1} \mapsto H\mathbf{1}$ . Supponiamo ora che  $\varphi : I \rightarrow \mathcal{C}$  sia stata definita, e sia  $I'$  il risultato dell'applicazione  $\varphi$  a  $I$  di uno dei passi (9.9). Nel caso di un passo (ii), non è difficile estendere  $\varphi$  ad un'applicazione  $\varphi' : I' \rightarrow \mathcal{C}$ . Basta definire  $\varphi'(\mathbf{k}) = \varphi(\mathbf{k})$  se  $\mathbf{k} \neq \mathbf{j}$ , e  $\varphi'(\mathbf{j}) = \varphi(\mathbf{i})x$ . Supponiamo poi di usare un passo (i) per uguagliare due indici, diciamo  $\mathbf{i}, \mathbf{j}$ , sicché  $I$  si contrae per formare il nuovo insieme di indici  $I'$ . Allora il lemma seguente ci permette di definire l'applicazione  $\varphi' : I' \rightarrow \mathcal{C}$ :

(9.11) LEMMA Supponiamo che sia data un'applicazione  $\varphi : I \rightarrow \mathcal{C}$  compatibile con un'azione parziale su  $I$ . Consideriamo  $\mathbf{i}, \mathbf{j} \in I$ , e supponiamo che una delle regole 1, 2, 3 implichi che  $\mathbf{i} = \mathbf{j}$ . Allora  $\varphi(\mathbf{i}) = \varphi(\mathbf{j})$ .

*Dimostrazione.* Ciò è vero poiché, come abbiamo già osservato, l'azione sulle classi laterali soddisfa tutte le regole (9.4). Pertanto, se le regole implicano che  $\mathbf{i} = \mathbf{j}$ , esse implicano anche che  $\varphi(\mathbf{i}) = \varphi(\mathbf{j})$ . ■

Resta da dimostrare che l'applicazione  $\varphi^* : I^* \rightarrow \mathcal{C}$  è biettiva, cosa che vedremo costruendo l'applicazione inversa  $\psi^* : \mathcal{C} \rightarrow I^*$  mediante il lemma seguente:

(9.12) LEMMA Sia  $S$  un insieme su cui agisce  $G$ , e sia  $s \in S$  un elemento stabilizzato da  $H$ . Allora esiste una e una sola applicazione  $\psi : \mathcal{C} \rightarrow S$  che è compatibile con le azioni sui due insiemi e che manda  $H\mathbf{1}$  in  $s$ .

*Dimostrazione.* Questa dimostrazione ripete quella della proposizione (6.4) del capitolo 5, con la differenza che siamo passati alle azioni a destra. Poiché  $g$  manda  $H$  in  $Hg$  e poiché vogliamo che  $\psi(Hg) = \psi(H)g$ , dobbiamo cercare di porre:  $\psi(Hg) = sg$ . Ciò dimostra l'unicità dell'applicazione  $\psi$ . Per provare l'esistenza, verifichiamo innanzitutto che la legge  $\psi(Hg) = sg$  è ben definita. Infatti, se  $Ha = Hb$ , allora  $ba^{-1} \in H$ ; per ipotesi,  $ba^{-1}$  stabilizza  $s$ , e pertanto  $sa = sb$ . Infine,  $\psi$  è compatibile con le azioni di  $G$  poiché  $\psi(Hga) = sga = (sg)a = \psi(Hg)a$ . ■

Ora, per dimostrare che  $\varphi^*$  è biettiva, utilizziamo il lemma per costruire un'applicazione  $\psi^* : \mathcal{C} \rightarrow I^*$ . Consideriamo l'applicazione composta  $\varphi^* \psi^* : \mathcal{C} \rightarrow \mathcal{C}$ ,

L'angolo in basso a destra mostra che  $2z = 3$ . Ciò permette di determinare il resto della tabella. Vi sono tre indici, e l'azione è descritta da

$$x = (1 \ 2 \ 3), \quad y = (1 \ 2), \quad z = (2 \ 3).$$

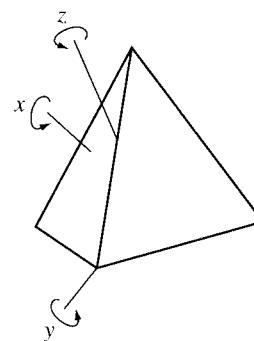
Poiché vi sono tre indici, concludiamo che vi sono tre classi laterali e che l'indice di  $H$  in  $G$  è 3. Concludiamo inoltre che l'ordine di  $H$  è 2, e quindi che  $G$  ha ordine 6. Infatti  $z^2 = 1$  è una delle relazioni; pertanto  $z$  ha ordine 1 o 2, e poiché  $z$  non agisce in modo banale sugli indici,  $z \neq 1$ . Le tre permutazioni sopra elencate generano il gruppo simmetrico, e pertanto la rappresentazione mediante permutazioni è un isomorfismo di  $G$  su  $S_3$ .

Naturalmente, queste conclusioni dipendono dal fatto che sappiamo che la rappresentazione che abbiamo costruito è quella giusta, cosa che dimostreremo alla fine del paragrafo. Prima, calcoliamo ancora alcuni esempi.

### (9.5) Esempio

Consideriamo il gruppo tetraedrale  $T$  delle 12 simmetrie di rotazione di un tetraedro regolare (cfr. cap. 5, § 9). Se denotiamo con  $y$  e  $x$  le rotazioni in senso antiorario di  $2\pi/3$  intorno a un vertice e al centro di una faccia, come illustrato qui sotto, allora  $yx = z$  è la rotazione di  $\pi$  intorno a uno spigolo. Pertanto in  $T$  valgono le relazioni

$$(9.6) \quad x^3 = 1, \quad y^3 = 1, \quad yxyx = 1.$$



Dimostriamo che (9.6) è un insieme completo di relazioni di  $T$ . Consideriamo il gruppo  $G = \langle y, x; y^3, x^3, yxyx \rangle$  definito da queste relazioni. Poiché le relazioni (9.6) valgono in  $T$ , la proprietà di rappresentazione dei gruppi quoziente fornisce un omomorfismo  $\varphi : G \rightarrow T$ . Questa applicazione è suriettiva, poiché, come si vede facilmente,  $y$  e  $x$  generano  $T$ . Dobbiamo dimostrare soltanto che  $\varphi$  è iniettiva. Lo faremo mostrando che l'ordine del gruppo  $G$  è 12.

È possibile analizzare direttamente le relazioni, ma esse non sono particolarmente facili da trattare. Potremmo anche calcolare l'ordine di  $G$  contando le classi laterali del sottogruppo banale  $H = \{1\}$ , ma neanche questo metodo è efficiente.

È meglio usare un sottogruppo non banale  $H$  di  $G$ : ad esempio, quello generato da  $y$ , che ha ordine al più 3, poiché  $y^3 = 1$ . Se dimostriamo che il suo ordine è 3 e che il suo indice in  $G$  è 4, ne seguirà che  $G$  ha ordine 12, da cui la tesi.

Si ottiene la seguente tabella (provi il lettore a ricavarla per esercizio)

$x$	$x$	$x$	$y$	$y$	$y$	$y$	$x$	$y$	$x$
1	2	3	1	1	1	1	1	2	3
2	3	1	2	3	4	2	3	1	1
3	1	2	3	4	2	3	4	4	2
4	4	4	4	2	3	4	2	3	4

Pertanto la rappresentazione mediante permutazioni è

$$(9.7) \quad x = (1 \ 2 \ 3), \quad y = (2 \ 3 \ 4).$$

Poiché vi sono quattro indici, l'indice di  $H$  è 4. Inoltre, osserviamo che  $y$  ha precisamente ordine 3. Infatti, essendo  $y^3 = 1$ , l'ordine è al più 3, e poiché la permutazione  $(2 \ 3 \ 4)$  associata a  $y$  ha ordine 3, esso è almeno 3. Pertanto l'ordine del gruppo è 12, come annunciato. Aggiungiamo, per inciso, che possiamo concludere che  $T$  è isomorfo al gruppo alterno  $A_4$ , verificando che le permutazioni (9.7) generano quel gruppo. ■

### (9.8) Esempio

Modifichiamo leggermente le relazioni (9.6). Supponiamo che  $G$  sia generato da  $x, y$ , con le relazioni:

$$x^3 = 1, \quad y^3 = 1, \quad yxy^2x = 1,$$

e sia  $H$  il sottogruppo generato da  $y$ . Cominciamo a costruire una tabella. Poiché  $y^3 = 1$ , accorciamo l'ultima relazione sostituendo  $y^2$  con  $y^{-1}$ . Chiaramente  $y^{-1}$  agisce come l'inversa della permutazione associata a  $y$ . Gli elementi nell'ultima riga della tabella sono stati determinati procedendo da destra.

$x$	$x$	$x$	$y$	$y$	$y$	$y$	$x$	$y^{-1}$	$x$
1	2	3	1	1	1	1	1	2	3

Riscriviamo la relazione  $2y^{-1} = 3$  nella forma  $3y = 2$ . Poiché anche  $2y = 3$ , ne segue che  $3y^2 = 3$  e che  $3y^3 = 2$ . Ma  $y^3 = 1$ , sicché  $3 = 2$ , che a sua volta implica  $1 = 2 = 3$ . Poiché i generatori  $x, y$  lasciano fisso 1, vi è un'unica classe laterale,

che manda  $H_1$  in  $H_1$ . Applichiamo di nuovo il lemma, sostituendo  $S$  con  $\varphi^*\psi^*$ . L'asserzione del lemma relativa all'unicità ci dice che  $\varphi^*\psi^*$  è l'applicazione identica. D'altra parte, poiché l'azione su  $I^*$  è transitiva e poiché  $\psi^*$  è compatibile con le azioni,  $\psi^*$  deve essere suriettiva. Ne segue che  $\varphi^*$  e  $\psi^*$  sono biettive.

Rispetto a un onesto lavoro, il metodo assiomatico ha molti vantaggi.

Bertrand Russell

### Esercizi

#### 1 Le azioni di un gruppo su se stesso

1. È vero che la regola  $(g, x) \mapsto xg^{-1}$  definisce un'azione di  $G$  su se stesso?
2. Sia  $H$  un sottogruppo di un gruppo  $G$ . Allora  $H$  agisce su  $G$  mediante la moltiplicazione a sinistra. Descrivere le orbite rispetto a tale azione.
3. Dimostrare la formula:  $|G| = |Z| + \sum |C|$ , dove la somma è estesa alle classi di coniugio contenenti più di un elemento e  $Z$  è il centro di  $G$ .
4. Dimostrare il teorema del punto fisso (1.12).
5. Determinare le classi di coniugio nel gruppo  $M$  dei movimenti del piano.
6. Determinare, tra le espressioni seguenti, quelle che possono essere interpretate come equazioni delle classi per un gruppo di ordine 10:

$$1+1+1+2+5, \quad 1+2+2+5, \quad 1+2+3+4, \quad 1+1+2+2+2+2.$$

7. Determinare l'ordine della classe di coniugio di  $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}$  in  $GL_2(\mathbb{F}_5)$ .

8. Determinare l'equazione delle classi per ciascuno dei seguenti gruppi
  - (a) il gruppo dei quaternioni;
  - (b) il gruppo quadrinomio di Klein;
  - (c) il gruppo diedrale  $D_5$ ;
  - (d)  $D_6$ ;
  - (e)  $D_n$ ;
  - (f) il gruppo delle matrici triangolari superiori in  $GL_2(\mathbb{F}_3)$ ;
  - (g)  $SL_2(\mathbb{F}_3)$ .

9. Sia  $G$  un gruppo di ordine  $n$ , e sia  $F$  un campo. Dimostrare che  $G$  è isomorfo ad un sottogruppo di  $GL_n(F)$ .

10. Determinare il centralizzante in  $GL_3(\mathbb{R})$  di ciascuna delle seguenti matrici:

$$(a) \begin{bmatrix} 1 & & \\ & 2 & \\ & & 3 \end{bmatrix}; \quad (b) \begin{bmatrix} 1 & & \\ & 1 & \\ & & 2 \end{bmatrix}; \quad (c) \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix};$$

### Esercizi

$$(d) \begin{bmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{bmatrix}; \quad (e) \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}; \quad (f) \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}.$$

- \*11. Determinare tutti i gruppi finiti che contengono al più tre classi di coniugio.

12. Sia  $N$  un sottogruppo normale di un gruppo  $G$ , con  $|N| = 5$  e  $|G|$  dispari. Dimostrare che  $N$  è contenuto nel centro di  $G$ .

- \*13. (a) Determinare le possibili equazioni delle classi per i gruppi di ordine 8.

- (b) Classificare i gruppi di ordine 8.

14. Sia  $Z$  il centro di un gruppo  $G$ . Dimostrare che se  $G/Z$  è un gruppo ciclico  $G$  è abeliano e quindi  $G = Z$ .

- \*15. Sia  $G$  un gruppo di ordine 35.

- (a) Supponiamo che  $G$  agisca in modo non banale su un insieme di cinque elementi. Dimostrare che  $G$  ha un sottogruppo normale di ordine 7.

- (b) Dimostrare che ogni gruppo di ordine 35 è ciclico.

#### 2 L'equazione delle classi del gruppo icosaedrale

1. Determinare l'intersezione  $I \cap O$  (essendo  $O$  il gruppo ottaedrale), immaginando il dodecaedro e il cubo situati nello spazio come illustrato nella figura (2.7).

2. Due tetraedri possono essere inscritti in un cubo  $C$ , ciascuno utilizzando metà dei vertici. Collegare ciò con l'inclusione:  $A_4 \subset S_4$ .

3. È vero che  $I$  contiene come sottogruppo  $T$ , oppure  $D_6$ , oppure  $D_3$ ?

4. Dimostrare che il gruppo icosaedrale non possiede sottogruppi di ordine 30.

5. È vero che  $A_5$  è l'unico sottogruppo normale proprio di  $S_5$ ?

6. Dimostrare che nessun gruppo di ordine  $p^e$  (con  $p$  primo ed  $e > 1$ ) è semplice.

7. È vero che un gruppo abeliano è semplice se e soltanto se ha ordine primo?

8. (a) Determinare l'equazione delle classi per il gruppo  $T$  delle rotazioni di un tetraedro.

- (b) Qual è il centro di  $T$ ?

- (c) Dimostrare che  $T$  ha un unico sottogruppo di ordine 4.

- (d) Dimostrare che  $T$  non ha sottogruppi di ordine 6.

9. (a) Terminare l'equazione delle classi per il gruppo ottaedrale  $O$ .

- (b) Esistono esattamente due sottogruppi normali propri di  $O$ . Determinarli, dimostrare che sono normali, e provare che non ve ne sono altri.

10. Dimostrare che il gruppo tetraedrale  $T$  è isomorfo al gruppo alterno  $A_4$ , e che il gruppo ottaedrale  $O$  è isomorfo al gruppo simmetrico  $S_4$ . (Suggerimento: trovare insiemi di quattro elementi sui quali agiscono tali gruppi.)

11. È vero che il gruppo icosaedrale non è un sottogruppo del gruppo delle matrici  $2 \times 2$  reali triangolari superiori?
- \*12. È vero che un gruppo semplice non abeliano non può agire in modo non banale su un insieme contenente meno di cinque elementi?

## 3 Azioni sui sottoinsiemi

1. Sia  $S$  l'insieme dei sottoinsiemi di ordine 2 del gruppo diedrale  $D_3$ . Determinare le orbite rispetto all'azione di  $D_3$  su  $S$  mediante il coniugio.
2. Determinare le orbite rispetto alla moltiplicazione a sinistra e rispetto al coniugio sull'insieme dei sottoinsiemi di ordine 3 di  $D_3$ .
3. Elenicare tutti i sottogruppi del gruppo diedrale  $D_4$ , e ripartirli in classi di coniugio.
4. Sia  $H$  un sottogruppo di un gruppo  $G$ . Dimostrare che l'orbita della classe laterale sinistra  $gH$  rispetto all'azione data dal coniugio contiene la classe laterale destra  $Hg$ .
5. Sia  $U$  un sottoinsieme di un gruppo finito  $G$ , e supponiamo che  $|U|$  e  $|G|$  non abbiano fattori comuni. È vero che lo stabilizzatore di  $U$  è banale rispetto all'azione data dal coniugio?
6. Si consideri l'azione data dalla moltiplicazione a sinistra per  $G$  sull'insieme dei suoi sottoinsiemi. Sia  $U$  un sottoinsieme tale che la sua orbita  $\{gU\}$  costituisce una partizione di  $G$ . Sia  $H$  l'unico sottoinsieme in tale orbita che contiene 1. Dimostrare che  $H$  è un sottogruppo di  $G$  e che gli insiemi  $gU$  sono le sue classi laterali sinistre.
7. Sia  $H$  un sottogruppo di un gruppo  $G$ . È vero che il normalizzante  $N(H)$  è un sottogruppo normale del gruppo  $G$ ?
8. Siano  $H \subset K \subset G$  grupperi. Dimostrare che  $H$  è normale in  $K$  se e soltanto se  $K \subset N(H)$ .
9. Dimostrare che il sottogruppo  $B$  delle matrici triangolari superiori in  $GL_n(\mathbb{R})$  è coniugato al sottogruppo  $L$  delle matrici triangolari inferiori.
10. Sia  $B$  il sottogruppo di  $G = GL_n(\mathbb{C})$  delle matrici triangolari superiori, e sia  $U \subset B$  l'insieme delle matrici triangolari superiori con gli elementi diagonali uguali a 1. Dimostrare che  $B = N(U)$  e che  $B = N(B)$ .
- \*11. Si denoti con  $S_n$  il sottogruppo di  $GL_n(\mathbb{R})$  costituito dalle matrici di permutazione. Determinare il normalizzante di  $S_n$  in  $GL_n(\mathbb{R})$ .
12. Sia  $S$  un insieme finito su cui agisce transitivamente un gruppo  $G$ , e sia  $U$  un sottoinsieme di  $S$ . Dimostrare che i sottoinsiemi  $gU$  ricoprono uniformemente  $S$ , ossia che ogni elemento di  $S$  appartiene a uno stesso numero di insiemi  $gU$ .
13. (a) Sia  $H$  un sottogruppo normale di  $G$  di ordine 2. Dimostrare che  $H$  è contenuto nel centro di  $G$ .  
 (b) Sia  $H$  un sottogruppo normale di ordine primo  $p$  di un gruppo finito  $G$ . Supponiamo che  $p$  sia il più piccolo primo che divide  $|G|$ . Dimostrare che  $H$  è contenuto nel centro  $Z(G)$ .

## Esercizi

- \*14. Sia  $H$  un sottogruppo proprio di un gruppo finito  $G$ . Dimostrare che l'unione dei coniugati di  $H$  non è l'intero gruppo  $G$ .
15. Sia  $K$  un sottogruppo normale di ordine 2 di un gruppo  $G$ , e sia  $\bar{G} = G/K$ . Sia  $\bar{C}$  una classe di coniugio in  $\bar{G}$ . Sia  $S$  la controimmagine di  $\bar{C}$  in  $G$ . Dimostrare che si verifica uno dei due casi seguenti:
- (a)  $S = C$  è una classe di coniugio e  $|C| = 2|\bar{C}|$ .
  - (b)  $S = C_1 \cup C_2$  è costituita da due classi di coniugio e  $|C_1| = |C_2| = |\bar{C}|$ .
16. Calcolare le classi laterali doppie  $HgH$  del sottogruppo  $H = \{1, y\}$  nel gruppo diedrale  $D_n$ . Dimostrare che ogni classe laterale doppia ha due oppure quattro elementi.
17. Siano  $H, K$  sottogruppi di  $G$ , e sia  $H'$  un sottogruppo coniugato di  $H$ . Mettere in relazione tra loro le classi laterali doppie  $H'gK$  e  $HgK$ .
18. Cosa si può dire sull'ordine di una classe laterale doppia  $HgK$ ?
- #### 4 I teoremi di Sylow
1. Quanti elementi di ordine 5 sono contenuti in un gruppo di ordine 20?
  2. Dimostrare che nessun gruppo di ordine  $pq$ , con  $p$  e  $q$  primi, è semplice.
  3. Dimostrare che nessun gruppo di ordine  $p^2q$ , con  $p$  e  $q$  primi, è semplice.
  4. Dimostrare che l'insieme delle matrici  $\begin{bmatrix} 1 & a \\ 0 & c \end{bmatrix}$ , con  $a, c \in \mathbb{F}_7$  e  $c = 1, 2, 4$ , costituisce un gruppo del tipo descritto in (4.9b) (e che pertanto un tale gruppo esiste).
  5. Trovare i 2-sottogruppi di Sylow nei seguenti casi:
    - (a)  $D_{10}$ ; (b)  $T$ ; (c)  $O$ ; (d)  $I$ .
  6. Trovare un  $p$ -sottogruppo di Sylow di  $GL_2(\mathbb{F}_p)$ .
  - \*7. (a) Sia  $H$  un sottogruppo di  $G$  di indice primo  $p$ . Quali sono i numeri possibili dei sottogruppi coniugati di  $H$ ?  
 (b) Supponiamo che  $p$  sia il più piccolo primo che divide  $|G|$ . Dimostrare che  $H$  è un sottogruppo normale.
  - \*8. Sia  $H$  un  $p$ -sottogruppo di Sylow di  $G$  e si ponga  $K = N(H)$ . È vero che  $K = N(K)$ ?
  9. Sia  $G$  un gruppo di ordine  $p^em$ . Dimostrare che  $G$  contiene un sottogruppo di ordine  $p^r$ , per ogni intero  $r \leq e$ .
  10. Sia  $n = pm$  un intero divisibile una sola volta per  $p$ , e sia  $G$  un gruppo di ordine  $n$ . Sia  $H$  un  $p$ -sottogruppo di Sylow di  $G$ , e sia  $S$  l'insieme di tutti i  $p$ -sottogruppi di Sylow. Come si decompone  $S$  in  $H$ -orbite?
  - \*11. (a) Calcolare l'ordine di  $GL_n(\mathbb{F}_p)$ .  
 (b) Trovare un  $p$ -sottogruppo di Sylow di  $GL_n(\mathbb{F}_p)$ .  
 (c) Calcolare il numero dei  $p$ -sottogruppi di Sylow.  
 (d) Utilizzare il secondo teorema di Sylow per dare un'altra dimostrazione del primo teorema di Sylow.

- \*12. Dimostrare che nessun gruppo di ordine 224 è semplice.
13. Dimostrare che, se  $G$  ha ordine  $n = p^e a$ , dove  $1 \leq a < p$  ed  $e \geq 1$ , allora  $G$  possiede un sottogruppo normale proprio.
14. Dimostrare che gli unici gruppi semplici di ordine  $< 60$  sono i gruppi di ordine primo.
15. Classificare i gruppi di ordine 33.
16. Classificare i gruppi di ordine 18.
17. Dimostrare che esistono al più cinque classi di isomorfismo di gruppi di ordine 20.
- \*18. Sia  $G$  un gruppo semplice di ordine 60.
- (a) Dimostrare che  $G$  contiene sei 5-sottogruppi di Sylow, dieci 3-sottogruppi di Sylow, e cinque 2-sottogruppi di Sylow.
  - (b) Dimostrare che  $G$  è isomorfo al gruppo alterno  $A_5$ .

### 5 I gruppi di ordine 12

1. Determinare le equazioni delle classi dei gruppi di ordine 12.
2. Dimostrare che un gruppo di ordine  $n = 2p$ , con  $p$  primo, è un gruppo ciclico oppure un gruppo diedrale.
- \*3. Sia  $G$  un gruppo di ordine 30.

  - (a) Dimostrare che il 5-sottogruppo di Sylow  $K$  o il 3-sottogruppo di Sylow  $H$  è normale.
  - (b) Dimostrare che  $HK$  è un sottogruppo ciclico di  $G$ .
  - (c) Classificare i gruppi di ordine 30.

4. Sia  $G$  un gruppo di ordine 55.

  - (a) Dimostrare che  $G$  è generato da due elementi  $x, y$ , soddisfacenti alle relazioni:  $x^{11} = 1$ ,  $y^5 = 1$ ,  $xy^{-1} = x^r$ , per qualche  $r$ , con  $1 \leq r < 11$ .
  - (b) Dimostrare che  $r$  non può assumere i seguenti valori: 2, 6, 7, 8, 10.
  - (c) Dimostrare che  $r$  può assumere i valori rimanenti, e che esistono due classi di isomorfismo di gruppi di ordine 55.

### 6 Calcoli nel gruppo simmetrico

1. Verificare i prodotti (6.9).
2. Dimostrare esplicitamente che la permutazione  $(1\ 2\ 3)(4\ 5)$  è coniugata a  $(2\ 4\ 1)(3\ 5)$ .
3. Siano  $p, q$  due permutazioni. Dimostrare che i prodotti  $pq$  e  $qp$  hanno cicli di uguale lunghezza.
4. (a) È vero che il gruppo simmetrico  $S_7$  contiene un elemento di ordine 5, o un elemento di ordine 10, o un elemento di ordine 15?
- (b) Qual è l'ordine più grande possibile di un elemento di  $S_7$ ?

- Mostrare come sia possibile stabilire se una permutazione è pari o dispari, se essa è scritta come un prodotto di cicli.
- È vero che l'ordine di una permutazione è il minimo comune multiplo degli ordini dei cicli che la compongono?
- È vero che il sottogruppo ciclico  $H$  di  $S_n$  generato dal ciclo  $(1\ 2\ 3\ 4\ 5)$  è un sottogruppo normale?
- Calcolare il numero delle permutazioni in  $S_n$  che non lasciano fisso alcun indice.
- Determinare la decomposizione in cicli della permutazione:  $i \mapsto n - i$ .
10. (a) Dimostrare che ogni permutazione  $p$  è un prodotto di trasposizioni.
  - (b) Quante trasposizioni occorrono per scrivere il ciclo  $(1\ 2\ 3\ \dots\ n)$ ?
  - (c) Supponiamo che una permutazione sia scritta in due modi come un prodotto di trasposizioni, diciamo  $p = \tau_1 \tau_2 \dots \tau_m$  e  $p = \tau'_1 \tau'_2 \dots \tau'_n$ . Dimostrare che  $m$  ed  $n$  sono entrambi pari o entrambi dispari.
  11. Qual è il centralizzante dell'elemento  $(1\ 2)$  di  $S_4$ ?
  12. Trovare tutti i sottogruppi di ordine 4 del gruppo simmetrico  $S_4$ . Quali tra di essi sono normali?
  13. Determinare l'equazione delle classi di  $A_4$ .
  14. (a) Determinare il numero delle classi di coniugio e l'equazione delle classi per il gruppo  $S_5$ .
  - (b) Elencare le classi di coniugio in  $A_5$ , e confrontare tale lista con la lista delle classi di coniugio nel gruppo icosaedrale [cfr. (2.2)].
  15. Dimostrare che le trasposizioni  $(1\ 2), (2\ 3), \dots, (n-1, n)$  generano il gruppo simmetrico  $S_n$ .
  16. Dimostrare che il gruppo simmetrico  $S_n$  è generato dai cicli  $(1\ 2 \dots n)$  e  $(1\ 2)$ .
  17. (a) Dimostrare che il prodotto di due trasposizioni  $(i\ j)(k\ l)$  può essere sempre scritto come un prodotto di 3-cicli. Esaminare anche il caso in cui alcuni indici sono uguali tra loro.
  - (b) Dimostrare che il gruppo alterno  $A_n$  è generato da 3-cicli, se  $n \geq 3$ .
  18. Dimostrare che se un sottogruppo normale proprio di  $S_n$  contiene un 3-ciclo, allora esso è  $A_n$ .
  - \*19. Dimostrare che  $A_n$  è semplice per ogni  $n \geq 5$ .
  - \*20. Dimostrare che  $A_n$  è l'unico sottogruppo di  $S_n$  di indice 2.
  21. Spiegare la coincidenza miracolosa alla fine del paragrafo, utilizzando il gruppo opposto (cap. 2, § 1, esercizio 12).
- 7 Il gruppo libero
1. È vero che il gruppo libero con due generatori è isomorfo al prodotto di due gruppi ciclici infiniti?

2. (a) Sia  $F$  il gruppo libero su  $x, y$ . Dimostrare che i due elementi  $u = x^2$  e  $v = y^3$  generano un sottogruppo di  $F$  che è isomorfo al gruppo libero su  $u, v$ .  
 (b) Dimostrare che i tre elementi:  $u = x^2$ ,  $v = y^2$ ,  $z = xy$  generano un sottogruppo isomorfo al gruppo libero su  $u, v, z$ .

3. È possibile definire una *parola chiusa* in  $S'$  come il cappio orientato ottenuto congiungendo i simboli alle estremità di una parola. Così, ad esempio, il cappio:

$$\begin{array}{ccccc} & ca^{-1} & & & \\ b & & b^{-1} & & \\ a & & & b & \\ & a & c & & \\ & bbd & & & \end{array}$$

rappresenta una parola chiusa, se lo leggiamo in senso orario. Stabilire una corrispondenza biunivoca tra le parole chiuse ridotte e le classi di coniugio nel gruppo libero.

4. Sia  $p$  un numero primo, e sia  $N$  il numero delle parole di lunghezza  $p$  in un insieme finito  $S$ . Dimostrare che  $N$  è divisibile per  $p$ .

### 8 Generatori e relazioni

- Dimostrare che due elementi  $a, b$  di un gruppo generano lo stesso sottogruppo generato da  $bab^2, bab^3$ .
- Dimostrare che il più piccolo sottogruppo normale di un gruppo  $G$  contenente un sottoinsieme  $S$  è generato come sottogruppo dall'insieme  $\{gsg^{-1} \mid g \in G, s \in S\}$ .
- È vero che  $y^2x^2$  appartiene al sottogruppo normale generato da  $xy$  e dai suoi coniugati?
- Dimostrare che il gruppo generato da  $x, y, z$  con l'unica relazione  $yxyz^{-2} = 1$  è in realtà un gruppo libero.
- Sia  $S$  un insieme di elementi di un gruppo  $G$  e siano  $\{r_i\}$  alcune relazioni che valgono tra gli elementi di  $S$  in  $G$ . Sia  $F$  il gruppo libero su  $S$ . Dimostrare che l'applicazione  $F \rightarrow G$  (8.1) si fattorizza attraverso  $F/N$ , dove  $N$  è il sottogruppo normale generato da  $\{r_i\}$ .
- Sia  $G$  un gruppo con un sottogruppo normale  $N$ . Supponiamo che  $G$  e  $G/N$  siano entrambi gruppi ciclici. Dimostrare che  $G$  può essere generato da due elementi.
- Un sottogruppo  $H$  di un gruppo  $G$  è chiamato *caratteristico*, se è mandato in se stesso da tutti gli automorfismi di  $G$ .
  - Dimostrare che ogni sottogruppo caratteristico è normale.
  - Dimostrare che il centro  $Z$  di un gruppo  $G$  è un sottogruppo caratteristico.
  - Dimostrare che il sottogruppo  $H$  generato da tutti gli elementi di  $G$  di ordine  $n$  è caratteristico.
- Determinare i sottogruppi normali e i sottogruppi caratteristici del gruppo dei quaternioni.
- Il sottogruppo commutatore  $C$  di un gruppo  $G$  è il più piccolo sottogruppo contenente tutti i commutatori.

### Esercizi

- Dimostrare che il sottogruppo commutatore è un sottogruppo caratteristico.
  - Dimostrare che  $G/C$  è un gruppo abeliano.
  - Determinare il sottogruppo commutatore del gruppo  $M$  dei movimenti del piano.
  - Dimostrare, mediante un calcolo esplicito, che il commutatore  $x(yz)x^{-1}(yz)^{-1}$  appartiene al sottogruppo normale generato dai due commutatori  $xyx^{-1}y^{-1}$  e  $xzx^{-1}z^{-1}$  e dai loro coniugati.
  - Si denoti con  $G$  il gruppo abeliano libero  $\langle x, y; xyx^{-1}y^{-1} \rangle$  definito in (8.8). Dimostrare la proprietà universale di tale gruppo, ossia che, se  $u, v$  sono elementi di un gruppo abeliano  $A$ , esiste uno ed un solo omomorfismo  $\varphi : G \rightarrow A$  tale che  $\varphi(x) = u$ ,  $\varphi(y) = v$ .
  - Dimostrare che il sottogruppo normale del gruppo libero  $\langle x, y \rangle$  che è generato dal commutatore  $xyx^{-1}y^{-1}$  è il sottogruppo commutatore.
  - Sia  $N$  un sottogruppo normale di un gruppo  $G$ . Dimostrare che  $G/N$  è abeliano se e solo se  $N$  contiene il sottogruppo commutatore di  $G$ .
  - Sia  $\varphi : G \rightarrow G'$  un omomorfismo suriettivo di gruppi. Sia  $S$  un sottoinsieme di  $G$  tale che  $\varphi(S)$  genera  $G'$ , e sia  $T$  un insieme di generatori di  $\ker \varphi$ . Dimostrare che  $S \cup T$  genera  $G$ .
  - È vero che ogni gruppo finito  $G$  può essere presentato mediante un insieme finito di generatori e un insieme finito di relazioni?
  - Sia  $G$  il gruppo generato da  $x, y, z$  con certe relazioni  $\{r_i\}$ . Supponiamo che una delle relazioni abbia la forma:  $wx$ , dove  $w$  è una parola in  $y, z$ . Sia  $r'_i$  la relazione ottenuta sostituendo  $x$  con  $w^{-1}$  in  $r_i$ , e sia  $G'$  il gruppo generato da  $y, z$ , con le relazioni  $\{r'_i\}$ . Dimostrare che  $G$  e  $G'$  sono isomorfi.
- ### 9 L'algoritmo di Todd-Coxeter
- Dimostrare che gli elementi  $x, y$  di (9.5) generano  $T$ , e che le permutazioni (9.7) generano  $A_4$ .
  - Utilizzare l'algoritmo di Todd-Coxeter per descrivere il gruppo generato da due elementi  $x, y$ , con le seguenti relazioni:
    - $x^2 = y^2 = 1, xyx = yxy;$
    - $x^2 = y^3 = 1, xyx = yxy;$
    - $x^3 = y^3 = 1, xyx = yxy;$
    - $x^4 = y^2 = 1, xyx = yxy;$
    - $x^4 = y^4 = x^2y^2 = 1.$
  - Utilizzare l'algoritmo di Todd-Coxeter per determinare l'ordine del gruppo generato da  $x, y$ , con le seguenti relazioni:
    - $x^4 = 1, y^3 = 1, xy = y^2x \quad (b) x^7 = 1, y^3 = 1, yx = x^2y.$
  - Descrivere il gruppo  $G$  generato dagli elementi  $x, y, z$ , con le relazioni  $x^4 = y^4 = z^3 = x^2z^2 = 1$  e  $z = xy$ .

5. Analizzare il gruppo  $G$  generato da  $x, y$ , con le relazioni  $x^4 = 1, y^4 = 1, x^2 = y^2, xy = y^3x$ .
- \*6. Analizzare il gruppo generato dagli elementi  $x, y$ , con le relazioni  $x^{-1}yx = y^{-1}, y^{-1}xy = x^{-1}$ .
7. Sia  $G$  il gruppo generato dagli elementi  $x, y$ , con le relazioni  $x^4 = 1, y^3 = 1, x^2 = yxy$ . Dimostrare che tale gruppo è banale, nei due modi seguenti:
  - (a) utilizzando l'algoritmo di Todd-Coxeter;
  - (b) lavorando direttamente con le relazioni.
8. Descrivere il gruppo  $G$  generato da due elementi  $x, y$ , con le relazioni:  $x^3 = y^3 = yxyxy = 1$ .
9. Siano  $p \leq q \leq r$  interi  $> 1$ . Il gruppo triangolare  $G^{pqr}$  è definito mediante i generatori nel modo seguente:  $G^{pqr} = \langle x, y, z; x^p, y^q, z^r, xyz \rangle$ . In ciascuno dei casi sottoelencati, dimostrare che il gruppo triangolare è isomorfo al gruppo corrispondente, e precisamente:
  - (a) al gruppo diedrale  $D_n$ , se  $(p, q, r) = (2, 2, n)$ ;
  - (b) al gruppo tetraedrale, se  $(p, q, r) = (2, 3, 3)$ ;
  - (c) al gruppo ottaedrale, se  $(p, q, r) = (2, 3, 4)$ ;
  - (d) al gruppo icosaedrale, se  $(p, q, r) = (2, 3, 5)$ .
10. Si denoti con  $\Delta$  un triangolo rettangolo isoscele, e si denotino con  $a, b, c$  le riflessioni del piano intorno ai tre lati di  $\Delta$ . Posto  $x = ab, y = bc, z = ca$ , dimostrare che  $x, y, z$  generano un gruppo triangolare.
11. (a) Dimostrare che il gruppo  $G$  generato dagli elementi  $x, y, z$  con le relazioni  $x^2 = y^3 = z^5 = 1, xyz = 1$  ha ordine 60.  
 (b) Sia  $H$  il sottogruppo generato da  $x$  e  $xyz^{-1}$ . Determinare la rappresentazione mediante permutazioni di  $G$  su  $G/H$ , e descrivere  $H$ .  
 (c) Dimostrare che  $G$  è isomorfo al gruppo alterno  $A_5$ .  
 (d) Sia  $K$  il sottogruppo di  $G$  generato da  $x$  e  $yxz$ . Determinare la rappresentazione mediante permutazioni di  $G$  su  $G/K$ , e descrivere  $K$ .

## Esercizi vari

1. (a) Dimostrare che il sottogruppo  $T'$  di  $O_3$ , costituito da tutte le simmetrie di un tetraedro regolare, incluse le simmetrie che invertono l'orientazione, ha ordine 24.  
 (b) È vero che  $T'$  è isomorfo al gruppo simmetrico  $S_4$ ?  
 (c) Enunciare e dimostrare risultati analoghi per il gruppo delle simmetrie di un dodecaedro.
2. (a) Sia  $U = \{1, x\}$  un sottoinsieme di ordine 2 di un gruppo  $G$ . Si consideri il grafo avente un vertice per ciascun elemento di  $G$  e un lato congiungente i vertici  $g$  e  $gx$ , per ogni  $g \in G$ . Dimostrare che i vertici collegati col vertice 1 sono gli elementi del gruppo ciclico generato da  $x$ .  
 (b) Procedere in modo analogo per l'insieme  $U = \{1, x, y\}$ .

- \*3. (a) Supponiamo che un gruppo  $G$  agisca transitivamente su un insieme  $S$ , e che  $H$  sia lo stabilizzatore di un elemento  $s_0 \in S$ . Si consideri l'azione di  $G$  su  $S \times S$  definita da  $g(s_1, s_2) = (gs_1, gs_2)$ . Stabilire una corrispondenza biunivoca tra le classi laterali doppie di  $H$  in  $G$  e le  $G$ -orbite in  $S \times S$ .  
 (b) Descrivere esplicitamente tale corrispondenza nel caso in cui  $G$  è il gruppo diedrale  $D_5$  e  $S$  è l'insieme dei vertici di un pentagono regolare.  
 (c) Descrivere tale corrispondenza nel caso in cui  $G = T$  e  $S$  è l'insieme degli spigoli di un tetraedro.
- \*4. Supponiamo che  $H \subset K \subset G$  siano sottogruppi, che  $H$  sia normale in  $K$ , e che  $K$  sia normale in  $G$ . È vero che  $H$  è normale in  $G$ ?
- \*5. Dimostrare la decomposizione di Bruhat, ossia, che  $GL_n(\mathbb{R})$  è l'unione delle classi laterali doppie  $BPB$ , dove  $B$  è il gruppo delle matrici triangolari superiori e  $P$  è una matrice di permutazione.
6. (a) Dimostrare che il gruppo  $G$  generato da  $x, y$  con le relazioni  $x^2, y^2$  è un gruppo infinito, procedendo in due modi:
  - (i) È chiaro che ogni parola può essere ridotta, utilizzando tali relazioni, nella forma  $\cdots xyxy \cdots$ . Dimostrare che ogni elemento di  $G$  è rappresentato da una e una sola parola siffatta.
  - (ii) Descrivere  $G$  come il gruppo generato dalle riflessioni  $r, r'$  intorno a due rette  $\ell, \ell'$ , il cui angolo di intersezione non è un multiplo razionale di  $2\pi$ .
- (b) Sia  $N$  un sottogruppo normale proprio arbitrario di  $G$ . Dimostrare che  $G/N$  è un gruppo diedrale.
7. Siano  $H, N$  sottogruppi di un gruppo  $G$ , e supponiamo che  $N$  sia un sottogruppo normale.
  - (a) Determinare i nuclei delle restrizioni dell'omomorfismo canonico  $\pi : G \rightarrow G/N$  ai sottogruppi  $H$  e  $HN$ .
  - (b) Applicare il primo teorema di isomorfismo a tali restrizioni per dimostrare il secondo teorema di isomorfismo:  $H/(H \cap N)$  è isomorfo a  $(HN)/N$ .
8. Siano  $H, N$  sottogruppi normali di un gruppo  $G$  tali che  $H \supset N$ , e si ponga  $\overline{H} = H/N$ ,  $\overline{G} = G/N$ .
  - (a) Dimostrare che  $\overline{H}$  è un sottogruppo normale di  $\overline{G}$ .
  - (b) Utilizzare l'omomorfismo composto  $G \rightarrow \overline{G} \rightarrow \overline{G}/\overline{H}$  per dimostrare il terzo teorema di isomorfismo:  $G/H$  è isomorfo a  $\overline{G}/\overline{H}$ .

per ogni  $v, w, v_i, w_i \in V$  e per ogni  $c \in F$ . Spesso si usa una notazione simile a quella del prodotto scalare. Useremo frequentemente la notazione:

$$(1.4) \quad \langle v, w \rangle$$

per indicare il valore  $f(v, w)$  della forma. Dunque  $\langle v, w \rangle$  è uno scalare, ossia un elemento di  $F$ .

Una forma bilineare  $\langle \cdot, \cdot \rangle$  si dice *simmetrica* se

$$(1.5) \quad \langle v, w \rangle = \langle w, v \rangle$$

e *antisimmetrica* se

$$(1.6) \quad \langle v, w \rangle = -\langle w, v \rangle,$$

per ogni  $v, w \in V$ . (A rigore, se il campo  $F$  ha caratteristica 2, ossia  $1 + 1 = 0$  in  $F$ , questa definizione di antisimmetria non è corretta; cfr. § 8.)

Se la forma  $f$  è simmetrica o antisimmetrica, la linearità nella seconda variabile segue dalla linearità nella prima variabile.

Gli esempi più importanti di forme bilineari sono le forme sullo spazio  $F^n$  dei vettori colonna, ottenute a partire da una matrice  $A$   $n \times n$  a elementi in  $F$ , ponendo:

$$(1.7) \quad \langle X, Y \rangle = X^t A Y.$$

Si noti che tale prodotto è una matrice  $1 \times 1$ , ossia uno scalare, e che è una forma bilineare. Nel caso in cui  $A = I$  si ottiene il prodotto scalare ordinario.

Una matrice  $A$  si dice *simmetrica*, se

$$(1.8) \quad A^t = A, \quad \text{ossia, } a_{ij} = a_{ji} \quad \text{per ogni } i, j.$$

(1.9) PROPOSIZIONE *La forma (1.7) è simmetrica se e soltanto se la matrice  $A$  è simmetrica.*

*Dimostrazione.* Supponiamo che  $A$  sia simmetrica. Poiché  $Y^t A X$  è una matrice  $1 \times 1$ , essa è uguale alla propria trasposta:  $Y^t A X = (Y^t A X)^t = X^t A^t Y = X^t A Y$ . Pertanto  $\langle Y, X \rangle = \langle X, Y \rangle$ . L'altra implicazione si ottiene ponendo  $X = e_i$  e  $Y = e_j$ . Ne segue che  $\langle e_i, e_j \rangle = e_i^t A e_j = a_{ij}$ , mentre  $\langle e_j, e_i \rangle = a_{ji}$ . Se la forma è simmetrica, allora  $a_{ij} = a_{ji}$  e quindi  $A$  è simmetrica. ■

Sia  $\langle \cdot, \cdot \rangle$  una forma bilineare su uno spazio vettoriale  $V$ , e sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di  $V$ . Possiamo mettere in relazione la forma con un prodotto  $X^t A Y$

Presumo che al non iniziato le formule appariranno fredde e squalide.  
Benjamin Pierce

## 1 Definizione di forma bilineare

Il modello per le forme bilineari è il prodotto scalare di vettori in  $\mathbb{R}^n$ :

$$(1.1) \quad (X \cdot Y) = X^t Y = x_1 y_1 + \dots + x_n y_n,$$

che è stato descritto nel capitolo 4 (§ 5). Il simbolo  $(X \cdot Y)$  ha varie proprietà, le più importanti delle quali sono le seguenti:

$$(1.2) \quad \begin{aligned} \text{Bilinearità:} \quad & ((X_1 + X_2) \cdot Y) = (X_1 \cdot Y) + (X_2 \cdot Y) \\ & (X \cdot (Y_1 + Y_2)) = (X \cdot Y_1) + (X \cdot Y_2) \\ & (cX \cdot Y) = c(X \cdot Y) = (X \cdot cY) \\ \text{Simmetria:} \quad & (X \cdot Y) = (Y \cdot X) \\ \text{Positività:} \quad & (X \cdot X) > 0, \quad \text{se } X \neq 0. \end{aligned}$$

Si noti che la bilinearità dice che, se si fissa una variabile, la funzione dell'altra variabile che così si ottiene è un'applicazione lineare  $\mathbb{R}^n \rightarrow \mathbb{R}$ .

In questo capitolo studieremo il prodotto scalare e i suoi analoghi. È chiaro come si possano estendere la bilinearità e la simmetria al caso di uno spazio vettoriale su un campo arbitrario, mentre la positività, a priori, può essere definita soltanto quando il campo degli scalari è  $\mathbb{R}$ . Estenderemo anche il concetto di positività agli spazi vettoriali complessi nel paragrafo 4.

Sia  $V$  uno spazio vettoriale su un campo  $F$ . Una *forma bilineare* su  $V$  è una funzione di due variabili su  $V$  a valori nel campo:  $V \times V \xrightarrow{f} F$ , che soddisfa i seguenti assiomi:

$$(1.3) \quad \begin{aligned} f(v_1 + v_2, w) &= f(v_1, w) + f(v_2, w) \\ f(cv, w) &= cf(v, w) \\ f(v, w_1 + w_2) &= f(v, w_1) + f(v, w_2) \\ f(v, cw) &= cf(v, w) \end{aligned}$$

mediante la *matrice della forma* rispetto alla base. Per definizione, essa è la matrice  $A = (a_{ij})$ , dove:

$$(1.10) \quad a_{ij} = \langle v_i, v_j \rangle.$$

Si noti che  $A$  è una matrice simmetrica se e solo se la forma  $\langle \cdot, \cdot \rangle$  è simmetrica, e inoltre la simmetria della forma bilineare non dipende dalla base. Pertanto, se la matrice della forma rispetto a una certa base è simmetrica, allora la sua matrice rispetto a qualsiasi altra base sarà anch'essa simmetrica.

La matrice  $A$  permette di calcolare il valore della forma su due vettori  $v, w \in V$ . Siano  $X, Y$  i loro vettori delle coordinate (definiti nel cap. 3, § 4), sicché  $v = BX$ ,  $w = BY$ . Allora risulta:

$$\langle v, w \rangle = \left\langle \sum_i v_i x_i, \sum_j v_j y_j \right\rangle,$$

che, utilizzando la bilinearità, si sviluppa in  $\sum_{i,j} x_i y_j \langle v_i, v_j \rangle = \sum_{i,j} x_i a_{ij} y_j = X^t A Y$ , da cui:

$$(1.11) \quad \langle v, w \rangle = X^t A Y.$$

Pertanto, se identifichiamo  $F^n$  con  $V$  usando la base  $\mathbf{B}$ , come si è visto nel cap. 3 (4.14), la forma bilineare  $\langle \cdot, \cdot \rangle$  corrisponde a  $X^t A Y$ .

Come avviene nello studio degli operatori lineari, un problema fondamentale è quello di descrivere l'effetto di un cambiamento di base su un prodotto come questo. Per esempio, vorremmo sapere cosa accade al prodotto scalare quando si cambia la base di  $\mathbb{R}^n$ . L'effetto di un cambiamento di base  $\mathbf{B} = \mathbf{B}'P$  [cap. 3 (4.16)] sulla matrice della forma può essere determinato facilmente utilizzando le regole:  $X' = PX$ ,  $Y' = PY$ . Precisamente, se  $A'$  è la matrice della forma rispetto a una nuova base  $\mathbf{B}'$ , allora, per definizione di  $A'$ , si ha:  $\langle v, w \rangle = X'^t A' Y' = X^t P^t A' P Y$ . Ma si ha anche  $\langle v, w \rangle = X^t A Y$ . Pertanto risulta:

$$(1.12) \quad P^t A' P = A.$$

Poniamo  $Q = (P^{-1})^t$ . Poiché  $P$  può essere una matrice invertibile arbitraria, anche  $Q$  è arbitraria.

(1.13) COROLLARIO *Sia  $A$  la matrice di una forma bilineare rispetto a una base. Le matrici  $A'$  che rappresentano la stessa forma rispetto a basi diverse sono le matrici  $A' = Q A Q^t$ , dove  $Q$  è una matrice arbitraria in  $GL_n(F)$ .* ■

Applichiamo ora la formula (1.12) all'esempio iniziale del prodotto scalare su  $\mathbb{R}^n$ . La matrice del prodotto scalare rispetto alla base canonica è la matrice

**Teorica:**  $(X \cdot Y) = X^t I Y$ . Pertanto la formula (1.12) dice che, se si cambia la base, la matrice della forma si trasforma in

$$(1.14) \quad A' = (P^{-1})^t I (P^{-1}) = (P^{-1})^t (P^{-1}),$$

dove  $P$  è la matrice del cambiamento di base, come prima. Se la matrice  $P$  è **ortogonale**, ossia tale che  $P^t P = I$ , allora  $A' = I$ , e il prodotto scalare si trasforma nel prodotto scalare:  $(X \cdot Y) = (PX \cdot PY) = (X' \cdot Y')$ , come si è visto nel cap. 4 (5.13). Ma rispetto a un cambiamento di base generico, la formula per il prodotto scalare diventa  $X'^t A' Y'$ , dove  $A'$  è data da (1.14). Per esempio, sia  $n = 2$ , e sia  $\mathbf{B}'$  la base:

$$v'_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad v'_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Allora:

$$(1.15) \quad P^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{e} \quad A' = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

La matrice  $A'$  rappresenta il prodotto scalare su  $\mathbb{R}^2$  rispetto alla base  $\mathbf{B}'$ .

Possiamo anche procedere in modo inverso. Supponiamo di avere una forma bilineare  $\langle \cdot, \cdot \rangle$  su uno spazio vettoriale reale  $V$ . Ci chiediamo se sia possibile, scegliendo una base opportuna, far diventare questa forma il prodotto scalare. Partiamo da una base  $\mathbf{B}$  arbitraria, sicché abbiamo una matrice  $A$  con cui lavorare. Allora il problema è quello di cambiare questa base in modo tale che la nuova matrice sia l'identità, se è possibile. In base alla formula (1.12), ciò equivale a risolvere l'equazione matriciale  $I = (P^{-1})^t A (P^{-1})$ , ossia:

$$(1.16) \quad A = P^t P.$$

(1.17) COROLLARIO *Le matrici  $A$  che rappresentano una forma equivalente al prodotto scalare sono le matrici  $A = P^t P$ , dove  $P$  è una matrice invertibile.* ■

Questo corollario fornisce una risposta teorica al problema di determinare le forme bilineari equivalenti al prodotto scalare, ma non è molto soddisfacente, poiché non abbiamo ancora un metodo pratico per stabilire quali matrici possono essere scritte come un prodotto  $P^t P$ , e tantomeno un metodo pratico per trovare  $P$ .

Possiamo ricavare alcune condizioni sulla matrice  $A$  dalle proprietà del prodotto scalare elencate in (1.2). La bilinearità non impone nessuna condizione su  $A$ , poiché il simbolo  $X^t A Y$  è sempre bilineare. Tuttavia, la simmetria e la positività

impongono delle restrizioni. La proprietà più facile da verificare è la simmetria: affinché rappresenti il prodotto scalare, la matrice  $A$  deve essere simmetrica. Anche la positività costituisce una forte restrizione: affinché rappresenti il prodotto scalare, la matrice  $A$  deve avere la proprietà che

$$(1.18) \quad X^t A X > 0, \quad \text{per ogni } X \neq 0.$$

Una matrice reale simmetrica con questa proprietà si dice *definita positiva*.

(1.19) TEOREMA *Le seguenti proprietà di una matrice  $n \times n$  reale  $A$  sono equivalenti:*

- (i)  *$A$  rappresenta il prodotto scalare, rispetto a una base di  $\mathbb{R}^n$ .*
- (ii) *Esiste una matrice invertibile  $P \in GL_n(\mathbb{R})$  tale che  $A = P^t P$ .*
- (iii)  *$A$  è simmetrica e definita positiva.*

Abbiamo visto che (i) e (ii) sono equivalenti [corollario (1.17)] e che (i) implica (iii). Resta da dimostrare che (iii) implica (i). Sarà più conveniente riformulare tale implicazione nel contesto degli spazi vettoriali.

Una forma bilineare simmetrica  $\langle , \rangle$  su uno spazio vettoriale reale di dimensione finita  $V$  si dice *definita positiva*, se

$$(1.20) \quad \langle v, v \rangle > 0$$

per ogni vettore non nullo  $v \in V$ . Pertanto una matrice reale simmetrica  $A$  è definita positiva se e soltanto se la forma  $\langle X, Y \rangle = X^t A Y$  che essa definisce su  $\mathbb{R}^n$  è definita positiva. Inoltre, la forma  $\langle , \rangle$  è definita positiva se e soltanto se la sua matrice  $A$  rispetto a qualsiasi base è una matrice definita positiva. Questo è chiaro, poiché se  $X$  è il vettore delle coordinate di un vettore  $v$ , allora  $\langle v, v \rangle = X^t A X$  (1.11).

Due vettori  $v, w$  si dicono *ortogonali* rispetto a una forma simmetrica se  $\langle v, w \rangle = 0$ . L'ortogonalità tra due vettori si denota spesso con

$$(1.21) \quad v \perp w.$$

Tale definizione estende il concetto di ortogonalità che abbiamo già visto nel caso in cui la forma è il prodotto scalare su  $\mathbb{R}^n$  [cap. 4 (5.12)]. Una base  $\mathbf{B} = (v_1, \dots, v_n)$  di  $V$  è chiamata una *base ortonormale* rispetto alla forma, se

$$\langle v_i, v_j \rangle = 0 \quad \text{per ogni } i \neq j, \quad \text{e} \quad \langle v_i, v_i \rangle = 1 \quad \text{per ogni } i.$$

Dalla definizione segue direttamente che una base  $\mathbf{B}$  è ortonormale se e solo se la matrice della forma rispetto a  $\mathbf{B}$  è l'identità.

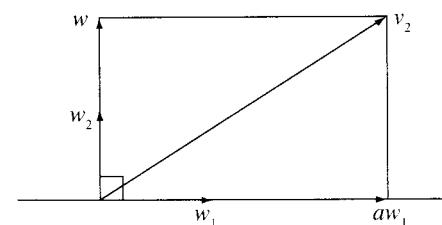
(1.22) TEOREMA *Sia  $\langle , \rangle$  una forma simmetrica definita positiva su uno spazio vettoriale reale di dimensione finita  $V$ . Allora esiste una base ortonormale in  $V$ .*

*Dimostrazione.* Descriveremo un metodo, chiamato il *procedimento di Gram-Schmidt*, per costruire una base ortonormale a partire da una base arbitraria  $\mathbf{B} = (v_1, \dots, v_n)$ . Il primo passo è normalizzare  $v_1$ , sicché  $\langle v_1, v_1 \rangle = 1$ . Per fare ciò, osserviamo che

$$(1.23) \quad \langle cv, cv \rangle = c^2 \langle v, v \rangle.$$

Poiché la forma è definita positiva, si ha  $\langle v_1, v_1 \rangle > 0$ . Poniamo  $c = \langle v_1, v_1 \rangle^{-\frac{1}{2}}$ , e sostituiamo  $v_1$  con  $w_1 = cv_1$ .

Ora cerchiamo una combinazione lineare di  $w_1$  e  $v_2$  che sia ortogonale a  $w_1$ . Una combinazione lineare siffatta è  $w = v_2 - aw_1$ , dove  $a = \langle v_2, w_1 \rangle$ . Si ha infatti  $\langle w, w_1 \rangle = \langle v_2, w_1 \rangle - a \langle w_1, w_1 \rangle = \langle v_2, w_1 \rangle - a = 0$ . Normalizziamo tale vettore  $w$  in modo che abbia lunghezza 1, ottenendo un vettore  $w_2$  che sostituiamo a  $v_2$ . L'interpretazione geometrica di questa operazione è illustrata qui sotto nel caso in cui la forma è il prodotto scalare. Il vettore  $aw_1$  è la proiezione ortogonale di  $v_2$  sul sottospazio (la retta) generato da  $w_1$ .



Questo è il procedimento generale. Supponiamo che i  $k-1$  vettori  $w_1, \dots, w_{k-1}$  siano ortonormali e che  $(w_1, \dots, w_{k-1}, v_k, \dots, v_n)$  sia una base. Allora, per modificare  $v_k$ , procediamo nel modo seguente. Poniamo  $a_i = \langle v_k, w_i \rangle$  e

$$(1.24) \quad w = v_k - a_1 w_1 - a_2 w_2 - \cdots - a_{k-1} w_{k-1}.$$

Allora  $w$  è ortogonale a  $w_i$ , per  $i = 1, \dots, k-1$ , perché:

$$\langle w, w_i \rangle = \langle v_k, w_i \rangle - a_1 \langle w_1, w_i \rangle - a_2 \langle w_2, w_i \rangle - \cdots - a_{k-1} \langle w_{k-1}, w_i \rangle.$$

Dato che  $w_1, \dots, w_{k-1}$  sono ortonormali, tutti i termini  $\langle w_j, w_i \rangle$ , con  $1 \leq j \leq k-1$ , sono nulli, tranne il termine  $\langle w_i, w_i \rangle$ , che è uguale a 1. Pertanto la somma si riduce a

$$\langle w, w_i \rangle = \langle v_k, w_i \rangle - a_i \langle w_i, w_i \rangle = \langle v_k, w_i \rangle - a_i = 0.$$

Normalizziamo  $w$  in modo che abbia lunghezza 1, ottenendo un vettore  $w_k$  che sostituiamo a  $v_k$ , come prima. Allora i vettori  $w_1, \dots, w_k$  sono ortonormali. Poiché  $v_k$  appartiene al sottospazio generato da  $(w_1, \dots, w_k; v_{k+1}, \dots, v_n)$ , questo insieme è una base. L'esistenza di una base ortonormale segue per induzione su  $k$ . ■

*Fine della dimostrazione del teorema (1.19).* Che la parte (iii) del teorema (1.19) implica (i) segue dal teorema (1.22). Infatti, se  $A$  è simmetrica e definita positiva, allora anche la forma  $\langle X, Y \rangle = X^t A Y$ , che essa definisce su  $\mathbb{R}^n$ , è simmetrica e definita positiva. In tal caso, il teorema (1.22) assicura che esiste una base  $\mathbf{B}'$  di  $\mathbb{R}^n$  che è ortonormale rispetto alla forma  $\langle X, Y \rangle = X^t A Y$ . (Ma la base probabilmente non sarà ortonormale rispetto al prodotto scalare ordinario su  $\mathbb{R}^n$ .) Ora la matrice  $A'$  della forma  $\langle X, Y \rangle$  rispetto alla nuova base  $\mathbf{B}'$  soddisfa la relazione (1.12):  $P^t A' P = A$ ; d'altro canto poiché  $\mathbf{B}'$  è ortonormale,  $A' = I$ . Pertanto  $A = P^t P$ . Ciò dimostra (ii), e poiché già sappiamo che (i) e (ii) sono equivalenti, dimostra anche (i). ■

Purtroppo, non esiste nessun modo davvero semplice per dimostrare che una matrice è definita positiva. Uno dei criteri più comodi è quello che ora illustreremo. Indichiamo con  $A_i$  la sottomatrice  $i \times i$  di  $A$  nell'angolo in alto a sinistra, sicché

$$A_1 = [a_{11}], \quad A_2 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad A_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \dots, A_n = A.$$

(1.25) TEOREMA Una matrice reale simmetrica  $n \times n$   $A$  è definita positiva se e soltanto se il determinante  $\det A_i$  è positivo per ciascun  $i = 1, \dots, n$ .

Per esempio, la matrice  $2 \times 2$

$$(1.26) \quad A = \begin{bmatrix} a & b \\ b & d \end{bmatrix}$$

è definita positiva se e soltanto se  $a > 0$  e  $ad - b^2 > 0$ . Utilizzando questo criterio, possiamo verificare immediatamente che la matrice  $A'$  di (1.15) è definita positiva, ciò che è in accordo col fatto che essa rappresenta il prodotto scalare.

La dimostrazione del teorema (1.25) si trova alla fine del prossimo paragrafo (p. 293).

## 2 Forme simmetriche: ortogonalità

In questo paragrafo consideriamo uno spazio vettoriale reale di dimensione finita  $V$ , sul quale è definita una forma bilineare simmetrica  $\langle \cdot, \cdot \rangle$ , ma togliamo l'ipotesi, fatta nel paragrafo precedente, che la forma sia definita positiva. Una

forma tale che  $\langle v, v \rangle$  assume sia valori positivi che negativi si dice *indefinita*. La forma di Lorentz

$$X^t A Y = x_1 y_1 + x_2 y_2 + x_3 y_3 - c^2 x_4 y_4$$

della fisica è un esempio tipico di forma indefinita sullo "spazio-tempo"  $\mathbb{R}^4$ . Il coefficiente  $c$  che rappresenta la velocità della luce può essere normalizzato e sostituito da 1, e allora la matrice della forma rispetto alla base assegnata diventa

$$(2.1) \quad \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

Ci poniamo ora il problema di descrivere tutte le forme simmetriche su uno spazio vettoriale reale di dimensione finita. La nozione fondamentale che si utilizza nello studio delle forme simmetriche è ancora quella di ortogonalità. Ma se una forma non è definita positiva può accadere che un vettore non nullo  $v$  sia ortogonale a se stesso:  $\langle v, v \rangle = 0$ . È il caso, ad esempio, del vettore  $(1, 0, 0, 1)^t \in \mathbb{R}^4$ , con la forma definita da (2.1). Dobbiamo quindi rivedere la nostra intuizione geometrica. In realtà, la cosa non è preoccupante, perché abbiamo a disposizione abbastanza vettori che non sono ortogonali a se stessi.

(2.2) PROPOSIZIONE Supponiamo che la forma simmetrica  $\langle \cdot, \cdot \rangle$  non sia identicamente nulla. Allora esiste un vettore  $v \in V$  che non è ortogonale a se stesso, tale cioè che  $\langle v, v \rangle \neq 0$ .

*Dimostrazione.* Il fatto che la forma  $\langle \cdot, \cdot \rangle$  non è identicamente nulla significa che esiste una coppia di vettori  $v, w \in V$  tali che  $\langle v, w \rangle \neq 0$ . Prendiamo in esame questi vettori. Se  $\langle v, v \rangle \neq 0$ , oppure se  $\langle w, w \rangle \neq 0$ , allora la proposizione è dimostrata. Supponiamo che  $\langle v, v \rangle = \langle w, w \rangle = 0$ . Consideriamo il vettore  $u = v+w$ , e calcoliamo  $\langle u, u \rangle$ , utilizzando la bilinearità:

$$\langle u, u \rangle = \langle v+w, v+w \rangle = \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle = 0 + 2\langle v, w \rangle + 0.$$

Poiché  $\langle v, w \rangle \neq 0$ , ne segue che  $\langle u, u \rangle \neq 0$ . ■

Se  $W$  è un sottospazio di  $V$ , denoteremo con  $W^\perp$  l'insieme di tutti i vettori  $v \in V$  che sono ortogonali ad ogni vettore  $w \in W$ :

$$(2.3) \quad W^\perp = \{v \in V \mid \langle v, w \rangle = 0\}.$$

Esso è un sottospazio di  $V$ , chiamato il *complemento ortogonale* di  $W$ .

(2.4) PROPOSIZIONE Sia  $w \in V$  un vettore tale che  $\langle w, w \rangle \neq 0$ , e sia  $W = \{cw\}$  il sottospazio generato da  $w$ . Allora  $V$  è la somma diretta di  $W$  e del suo complemento ortogonale:

$$V = W \oplus W^\perp.$$

*Dimostrazione.* In base ai risultati (6.4), (6.5) del capitolo 3, dobbiamo dimostrare due cose:

- (a)  $W \cap W^\perp = \{0\}$ . Ciò è chiaro. Il vettore  $cw$  non è ortogonale a  $w$ , a meno che  $c = 0$ , poiché  $\langle cw, w \rangle = c\langle w, w \rangle$  e  $\langle w, w \rangle \neq 0$ .
- (b)  $W$  e  $W^\perp$  generano  $V$ , ossia, ogni vettore  $v \in V$  può essere scritto nella forma  $v = aw + v'$ , dove  $v' \in W^\perp$ . Per dimostrarlo, risolviamo l'equazione  $\langle v - aw, w \rangle = 0$  rispetto ad  $a$ , ossia  $\langle v - aw, w \rangle = \langle v, w \rangle - a\langle w, w \rangle = 0$ . La soluzione è  $a = \frac{\langle v, w \rangle}{\langle w, w \rangle}$ . Poniamo allora  $v' = v - aw$ . ■

Altri due concetti di cui avremo bisogno sono quelli di spazio annullatore di una forma simmetrica e di forma non degenere. Un vettore  $v \in V$  è chiamato un *vettore annullatore* per la forma assegnata se  $\langle v, w \rangle = 0$  per ogni  $w \in V$ , cioè se  $v$  è ortogonale all'intero spazio  $V$ . Lo *spazio annullatore* della forma è l'insieme di tutti i vettori annullatori:

$$(2.5) \quad N = \{v \mid \langle v, V \rangle = 0\} = V^\perp.$$

Una forma simmetrica è *non degenere* se lo spazio annullatore è  $\{0\}$ .

(2.6) PROPOSIZIONE Sia  $A$  la matrice di una forma simmetrica rispetto a una base.

- (a) Lo spazio annullatore della forma è l'insieme dei vettori  $v$  tali che il vettore delle coordinate  $X$  di  $v$  è soluzione dell'equazione omogenea  $AX = 0$ .
- (b) La forma è non degenere se e solo se la matrice  $A$  è non singolare.

*Dimostrazione.* Fissata la base, la forma corrisponde al prodotto  $X^t A Y$  [cfr. (1.11)]. Potremmo lavorare anche con questo prodotto. Se  $Y$  è un vettore tale che  $AY = 0$ , allora  $X^t A Y = 0$  per ogni  $X$ ; pertanto  $Y$  appartiene allo spazio annullatore. Viceversa, supponiamo che  $AY \neq 0$ . Allora  $AY$  ha almeno una coordinata non nulla. La  $i$ -esima coordinata di  $AY$  è  $e_i^t A Y$ . Pertanto uno dei prodotti  $e_i^t A Y$  è diverso da zero. Ne segue che  $Y$  non è un vettore annullatore per la forma, il che dimostra (a). La parte (b) della proposizione segue da (a). ■

<sup>1</sup> [Tale sottospazio di  $V$  è chiamato anche il *radicale* di  $V$  rispetto alla forma assegnata, oppure il *nucleo* della forma.]

Enunciamo ora una versione generalizzata di (2.4):

(2.7) PROPOSIZIONE Sia  $W$  un sottospazio di  $V$ , e consideriamo la restrizione a  $W$  di una forma simmetrica  $\langle \cdot, \cdot \rangle$ , non degenere su  $W$ . Allora  $V = W \oplus W^\perp$ .

Omettiamo la dimostrazione, che segue da vicino quella di (2.4). ■

(2.8) DEFINIZIONE Una base ortogonale  $\mathbf{B} = (v_1, \dots, v_n)$  di  $V$  rispetto a una forma simmetrica  $\langle \cdot, \cdot \rangle$  è una base tale che  $v_i \perp v_j$  per ogni  $i \neq j$ .

Poiché la matrice  $A$  di una forma è definita da  $a_{ij} = \langle v_i, v_j \rangle$ , la base  $\mathbf{B}$  è ortogonale se e soltanto se  $A$  è una matrice *diagonale*. Si noti che, se la forma simmetrica  $\langle \cdot, \cdot \rangle$  è non degenere e la base  $\mathbf{B} = (v_1, \dots, v_n)$  è ortogonale, allora  $\langle v_i, v_i \rangle \neq 0$  per ogni  $i$ , ossia gli elementi diagonali di  $A$  sono diversi da zero.

(2.9) TEOREMA Sia  $\langle \cdot, \cdot \rangle$  una forma simmetrica su uno spazio vettoriale reale  $V$ .

- (a) Esiste una base ortogonale in  $V$ . Più precisamente, esiste una base  $\mathbf{B} = (v_1, \dots, v_n)$  tale che  $\langle v_i, v_j \rangle = 0$  per  $i \neq j$  e tale che per ciascun indice  $i$ ,  $\langle v_i, v_i \rangle$  è uguale a 1, -1, o 0.
- (b) (Matrici) Sia  $A$  una matrice reale simmetrica  $n \times n$ . Esiste una matrice  $Q \in GL_n(\mathbb{R})$  tale che  $Q A Q^t$  è una matrice diagonale avente come elementi diagonali 1, -1, o 0.

La parte (b) del teorema segue da (a) e (1.13), tenendo conto del fatto che ogni matrice simmetrica  $A$  è la matrice di una forma simmetrica. ■

Possiamo riordinare la base  $\mathbf{B}$  in modo che gli indici con  $\langle v_i, v_i \rangle = 1$  siano i primi, e così via. Allora la matrice  $A$  della forma sarà

$$(2.10) \quad A = \begin{bmatrix} I_p & & \\ & -I_m & \\ & & 0_z \end{bmatrix},$$

dove  $p, m, z$  sono, rispettivamente, i numeri degli elementi uguali a 1, -1, 0, sicché  $p + m + z = n$ . Tali numeri sono determinati univocamente dalla forma o dalla matrice  $A$ :

(2.11) TEOREMA (Legge di Sylvester) I numeri  $p, m, z$  che compaiono in (2.10) sono determinati univocamente dalla forma, non dipendono cioè dalla scelta della base ortogonale  $\mathbf{B}$  tale che  $\langle v_i, v_i \rangle = \pm 1$  oppure 0.

La coppia di interi  $(p, m)$  è chiamata la *segnatura* della forma.

*Dimostrazione del teorema (2.9).* Se la forma è identicamente nulla, allora la matrice  $A$  rispetto a qualsiasi base sarà la matrice nulla, che è una matrice diagonale. Supponiamo che la forma non sia identicamente nulla. Allora, in base alla proposizione (2.2), esiste un vettore  $v = v_1$  con  $\langle v_1, v_1 \rangle \neq 0$ . Sia  $W$  il sottospazio generato da  $v_1$ . Dalla proposizione (2.4) segue che  $V = W \oplus W^\perp$ , e pertanto una base per  $V$  si ottiene unendo la base  $(v_1)$  di  $W$  con una base arbitraria  $(v_2, \dots, v_n)$  e definisce una forma su  $W^\perp$ . Procedendo per induzione sulla dimensione, si conclude che  $W^\perp$  ha una base ortogonale  $(v_2, \dots, v_n)$ . Allora  $(v_1, v_2, \dots, v_n)$  è una base ortogonale di  $V$ . Infatti,  $\langle v_1, v_i \rangle = 0$  se  $i > 1$ , poiché  $v_i \in W^\perp$ , e  $\langle v_i, v_j \rangle = 0$  se  $i, j > 1$  e  $i \neq j$ , poiché  $(v_2, \dots, v_n)$  è una base ortogonale.

Resta da normalizzare la base ortogonale appena costruita. Se  $\langle v_i, v_i \rangle \neq 0$ , risolviamo l'equazione  $c^{-2} = \pm \langle v_i, v_i \rangle$  e sostituiamolo il vettore  $v_i$  della base con  $c v_i$ . Allora risulta  $\langle v_i, v_i \rangle = \pm 1$ . Ciò completa la dimostrazione. ■

*Dimostrazione del teorema (2.11).* Poniamo  $r = p + m$  ( $r$  è il rango della matrice  $A$ ). Sia  $(v_1, \dots, v_n)$  una base ortogonale di  $V$  del tipo in esame, ossia tale che la matrice corrispondente sia la matrice (2.10). Dimostreremo innanzitutto che il numero  $z$  è ben determinato, provando che i vettori  $v_{r+1}, \dots, v_n$  formano una base per lo spazio annullatore  $N = V^\perp$ . Ciò proverà che  $z = \dim N$ , e quindi che  $z$  non dipende dalla scelta di una base.

Un vettore  $w \in V$  è un vettore annullatore per la forma se e soltanto se è ortogonale ad ogni elemento  $v_i$  della base. Scriviamo  $w$  come una combinazione lineare dei vettori della base:  $w = c_1 v_1 + \dots + c_n v_n$ . Allora, poiché  $\langle v_i, v_j \rangle = 0$  se  $i \neq j$ , otteniamo  $\langle w, v_i \rangle = c_i \langle v_i, v_i \rangle$ . Ora  $\langle v_i, v_i \rangle = 0$  se e soltanto se  $i > r$ . Pertanto, affinché  $w$  sia ortogonale ad ogni vettore  $v_i$ , i coefficienti  $c_i$  devono essere tutti nulli per  $i \leq r$ . Ciò dimostra che  $(v_{r+1}, \dots, v_n)$  genera  $N$ , ed essendo un insieme linearmente indipendente, esso è una base per  $N$ .

L'equazione  $p+m+z=n$  mostra che anche  $p+m$  è determinato. Ci resta ancora da dimostrare che uno dei due interi rimanenti  $p, m$  è determinato. (Ciò non è così semplice, in realtà; per esempio, non è vero che il sottospazio generato da  $(v_1, \dots, v_p)$  è determinato univocamente dalla forma.)

Supponiamo che sia data una seconda base  $(v'_1, \dots, v'_n)$  del tipo in esame e che, in corrispondenza di essa, si ottengano gli interi  $p', m'$  (con  $z' = z$ ). Proveremo che i  $p + (n - p')$  vettori

$$(2.12) \quad v_1, \dots, v_p; v'_{p'+1}, \dots, v'_n$$

sono linearmente indipendenti. Allora, poiché  $V$  ha dimensione  $n$ , ne seguirà che  $p + (n - p') \leq n$ , sicché  $p \leq p'$ , e, scambiando i ruoli di  $p$  e  $p'$ , che  $p = p'$ .

Sia data una relazione lineare tra i vettori (2.12), che possiamo scrivere nella forma

$$(2.13) \quad b_1 v_1 + \dots + b_p v_p = c_{p'+1} v'_{p'+1} + \dots + c_n v'_n.$$

Denotiamo con  $v$  il vettore definito da una di queste due espressioni. Calcoliamo  $\langle v, v \rangle$  in due modi. Utilizzando l'espressione a sinistra, si ottiene

$$\langle v, v \rangle = b_1^2 \langle v_1, v_1 \rangle + \dots + b_p^2 \langle v_p, v_p \rangle = b_1^2 + \dots + b_p^2 \geq 0,$$

mentre, utilizzando l'espressione a destra, si ha

$$\langle v, v \rangle = c_{p'+1}^2 \langle v'_{p'+1}, v'_{p'+1} \rangle + \dots + c_n^2 \langle v'_n, v'_n \rangle = -c_{p'+1}^2 - \dots - c_n^2 \leq 0.$$

Ne segue che  $b_1^2 + \dots + b_p^2 = 0$ , e quindi  $b_1 = \dots = b_p = 0$ . Ma allora, tenendo presente che  $(v'_1, \dots, v'_n)$  è una base, segue dalla relazione (2.13) che  $c_{p'+1} = \dots = c_n = 0$ . Pertanto tale relazione è banale, come richiesto. ■

Per trattare le forme indefinite, spesso si usa la notazione  $I_{p,m}$  per indicare la matrice diagonale:

$$(2.14) \quad I_{p,m} = \begin{bmatrix} I_p & \\ & -I_m \end{bmatrix}.$$

Con tale notazione, la matrice che rappresenta la forma di Lorentz (2.1) è  $I_{3,1}$ .

Dimostreremo ora il teorema (1.25), il quale afferma che una matrice  $A$  è definita positiva se e soltanto se  $\det A_i > 0$  per ogni  $i$ .

*Dimostrazione del teorema (1.25).* Supponiamo che la forma  $X^T A Y$  sia definita positiva. Un cambiamento di base in  $\mathbb{R}^n$  trasforma la matrice  $A$  in  $A' = Q A Q^T$ , e di conseguenza

$$\det A' = (\det Q)(\det A)(\det Q^T) = (\det Q)^2(\det A).$$

Poiché i determinanti differiscono per il fattore  $(\det Q)^2$ , si ha che  $\det A'$  è positivo se e solo se  $\det A$  è positivo. In base a (1.19) possiamo scegliere una matrice  $Q$  tale che  $A' = I$ , e poiché  $I$  ha determinante 1, si ha  $\det A > 0$ .

La matrice  $A_i$  rappresenta la restrizione della forma al sottospazio  $V_i$  generato da  $(v_1, \dots, v_i)$ , e naturalmente la forma è definita positiva su  $V_i$ . Pertanto  $\det A_i > 0$  per lo stesso motivo per cui  $\det A > 0$ .

Viceversa, supponiamo che  $\det A_i$  sia positivo per ogni  $i$ . Procedendo per induzione su  $n$ , possiamo supporre che la forma sia definita positiva su  $V_{n-1}$ . Pertanto esiste una matrice  $Q' \in GL_{n-1}$  tale che  $Q' A_{n-1} Q'^T = I_{n-1}$ . Sia  $Q$  la matrice

$$Q = \begin{bmatrix} Q' & \\ & 1 \end{bmatrix}.$$

Allora

$$QAQ^t = \begin{bmatrix} I & * \\ * & \ddots \\ * & \cdots & * \end{bmatrix}.$$

Semplifichiamo ora l'ultima riga di questa matrice, tranne l'elemento di indice  $(n,n)$ , mediante operazioni elementari sulle righe  $E_1, \dots, E_{n-1}$ . Poniamo  $P = E_{n-1} \cdots E_1 Q$ . Allora:

$$A' = PAP^t = \begin{bmatrix} I & & 0 \\ & \vdots & \\ 0 & \cdots & 0 & c \end{bmatrix}, \quad \text{per qualche } c.$$

Anche l'ultima colonna è stata semplificata, poiché  $A' = PAP^t$  è simmetrica. Poiché  $\det A > 0$ , si ha anche  $\det A' = (\det A)(\det P)^2 > 0$ , e ciò implica che  $c > 0$ . Pertanto la matrice  $A'$  rappresenta una forma definita positiva. Essa rappresenta inoltre la stessa forma rappresentata da  $A$ , quindi  $A$  è definita positiva. ■

### 3 La geometria associata a una forma positiva

In questo paragrafo consideriamo ancora una volta una forma bilineare definita positiva  $\langle \cdot, \cdot \rangle$  su uno spazio vettoriale reale  $V$  di dimensione  $n$ . Uno spazio vettoriale reale insieme con una forma definita positiva spesso viene chiamato uno *spazio euclideo*.

È naturale definire la *lunghezza* di un vettore  $v$  mediante la regola

$$(3.1) \quad |v| = \sqrt{\langle v, v \rangle},$$

in analogia con la lunghezza di un vettore in  $\mathbb{R}^n$  [cap. 4 (5.10)]. Una conseguenza importante del fatto che la forma è definita positiva è che possiamo stabilire se un vettore  $v$  è nullo calcolando la sua lunghezza:

$$(3.2) \quad v = 0 \quad \text{se e soltanto se} \quad \langle v, v \rangle = 0.$$

Come si è visto nel paragrafo 1, esiste in  $V$  una base ortonormale  $\mathbf{B} = (v_1, \dots, v_n)$ , e perciò la forma corrisponde al prodotto scalare su  $\mathbb{R}^n$ :

$$\langle v, w \rangle = X^t Y,$$

se  $v = \mathbf{B}X$  e  $w = \mathbf{B}Y$ . Utilizzando tale corrispondenza, possiamo trasferire la geometria di  $\mathbb{R}^n$  su  $V$ . Ogni volta che abbiamo un problema su uno spazio euclideo  $V$ , un modo naturale di procedere sarà quello di scegliere una base

ortonormale opportuna, riducendo in tal modo il problema al caso familiare del prodotto scalare su  $\mathbb{R}^n$ .

Dato un sottospazio  $W$  di  $V$ , possiamo effettuare due operazioni. La prima consiste nel *restringere* la forma  $\langle \cdot, \cdot \rangle$  al sottospazio, semplicemente definendo il valore della forma su una coppia  $w_1, w_2$  di vettori di  $W$  come  $\langle w_1, w_2 \rangle$ . La restrizione di una forma bilineare ad un sottospazio  $W$  è una forma bilineare su  $W$ , e inoltre, se la forma è simmetrica oppure è simmetrica e definita positiva, tale risulta la restrizione.

La restrizione della forma può essere usata per definire l'*angolo* non orientato tra due vettori  $v, w$ . Se i vettori sono linearmente dipendenti, l'angolo è zero; in caso contrario  $(v, w)$  è una base di un sottospazio di dimensione due  $W$  di  $V$ . La restrizione della forma a  $W$  è ancora definita positiva, e pertanto esiste una base ortonormale  $(w_1, w_2)$  di  $W$ . Mediante tale base, i vettori  $v, w$  corrispondono ai rispettivi vettori delle coordinate  $X, Y$  in  $\mathbb{R}^2$ . Ciò permette di interpretare le proprietà geometriche dei vettori  $v, w$  in termini di proprietà di  $X, Y$ .

Poiché la base  $(w_1, w_2)$  è ortonormale, la forma corrisponde al prodotto scalare su  $\mathbb{R}^2$ :  $\langle v, w \rangle = X^t Y$ . Pertanto

$$|v| = |X|, \quad |w| = |Y|, \quad \text{e} \quad \langle v, w \rangle = (X \cdot Y).$$

Definendo l'angolo  $\theta$  tra  $v$  e  $w$  come l'angolo tra  $X$  e  $Y$  si ha:

$$(3.3) \quad \langle v, w \rangle = |v| |w| \cos \theta,$$

come conseguenza della formula analoga [cap. 4 (5.11)] per il prodotto scalare in  $\mathbb{R}^2$ . Tale formula permette di esprimere  $\cos \theta$  mediante gli altri simboli, e  $\cos \theta$  determina  $\theta$  a meno di un fattore  $\pm 1$ . Pertanto l'angolo tra  $v$  e  $w$  è determinato, a meno del segno, soltanto dalla forma. Questo è il migliore risultato che si può ottenere, anche in  $\mathbb{R}^3$ .

In uno spazio euclideo valgono risultati standard, quali la *diseguaglianza di Schwarz*:

$$(3.4) \quad |\langle v, w \rangle| \leq |v| |w|,$$

e la *diseguaglianza triangolare*:

$$(3.5) \quad |v + w| \leq |v| + |w|,$$

che possono essere dimostrati mediante la restrizione a un sottospazio di dimensione due.

La seconda operazione che possiamo effettuare su un sottospazio assegnato  $W$  consiste nel proiettare  $V$  su  $W$ . Poiché la restrizione della forma a  $W$  è definita positiva, è non degenere. Pertanto  $V = W \oplus W^\perp$ , in base a (2.7), e quindi ogni vettore  $v \in V$  si scrive in modo unico nella forma:

$$(3.6) \quad v = w + w', \quad \text{con} \quad w \in W \quad \text{e} \quad \langle w, w' \rangle = 0.$$

La proiezione ortogonale  $\pi : V \rightarrow W$  viene definita come l'applicazione lineare

$$(3.7) \quad v \mapsto \pi(v) = w,$$

dove  $w$  è dato dalla (3.6).

Il vettore  $\pi(v)$  può essere calcolato facilmente mediante una base ortonormale  $(w_1, \dots, w_r)$  di  $W$ , come mostra il seguente notevole risultato:

(3.8) PROPOSIZIONE Sia  $(w_1, \dots, w_r)$  una base ortonormale di un sottospazio  $W$ , e sia  $v \in V$ . La proiezione ortogonale  $\pi(v)$  di  $v$  su  $W$  è il vettore

$$\pi(v) = \langle v, w_1 \rangle w_1 + \dots + \langle v, w_r \rangle w_r.$$

Pertanto, se  $\pi$  è definita dalla (3.7), allora  $v - \pi(v)$  è ortogonale a  $W$ . Ciò spiega il significato geometrico del procedimento di Gram-Schmidt descritto nel §1.

*Dimostrazione.* Denotiamo con  $\tilde{w}$  il secondo membro della relazione in esame. Allora  $\langle \tilde{w}, w_i \rangle = \langle v, w_i \rangle \langle w_i, w_i \rangle = \langle v, w_i \rangle$  per  $i = 1, \dots, r$ , da cui  $v - \tilde{w} \in W^\perp$ . Poiché l'espressione (3.6) per  $v$  è unica, si ha  $w = \tilde{w}$  e  $w' = v - \tilde{w}$ . ■

Anche il caso in cui  $W = V$  è importante. In tal caso,  $\pi$  è l'applicazione identica.

(3.9) COROLLARIO Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base ortonormale di uno spazio euclideo  $V$ . Allora:

$$v = \langle v, v_1 \rangle v_1 + \dots + \langle v, v_n \rangle v_n.$$

In altre parole, il vettore delle coordinate di  $v$  rispetto alla base ortonormale  $\mathbf{B}$  è:

$$X = (\langle v, v_1 \rangle, \dots, \langle v, v_n \rangle)^t. ■$$

#### 4 Forme hermitiane

In questo paragrafo supponiamo che il campo degli scalari sia il campo  $\mathbb{C}$  dei numeri complessi. Quando si lavora con gli spazi vettoriali complessi, si desidera avere un concetto analogo a quello di lunghezza di un vettore, e naturalmente è possibile definire la lunghezza in  $\mathbb{C}^n$ , identificando tale spazio con  $\mathbb{R}^{2n}$ . Se  $X = (x_1, \dots, x_n)^t$  è un vettore complesso e se  $x_r = a_r + b_r i$ , allora la lunghezza di  $X$  è

$$(4.1) \quad |X| = \sqrt{a_1^2 + b_1^2 + \dots + a_n^2 + b_n^2} = \sqrt{\bar{x}_1 x_1 + \dots + \bar{x}_n x_n},$$

dove la sopralineatura denota l'operazione di coniugio, cioè  $\bar{x} = a - bi$  se  $x = a + bi$ . Tale formula suggerisce che il prodotto scalare "non va bene" per i vettori complessi e che dovremmo definire un prodotto mediante la formula

$$(4.2) \quad \langle X, Y \rangle = \bar{X}^t Y = \bar{x}_1 y_1 + \dots + \bar{x}_n y_n.$$

Il prodotto così definito possiede la proprietà di *positività*:

$$(4.3) \quad \text{Se } X \neq 0, \quad \langle X, X \rangle \text{ è un numero reale positivo}$$

e inoltre, nel caso di vettori reali coincide col prodotto scalare.

Il prodotto (4.2) è chiamato il *prodotto hermitiano standard*, o anche il *prodotto scalare hermitiano*. Esso ha le seguenti proprietà:

(4.4) *Linearità nella seconda variabile:*

$$\langle X, cY \rangle = c \langle X, Y \rangle \quad \text{e} \quad \langle X, Y_1 + Y_2 \rangle = \langle X, Y_1 \rangle + \langle X, Y_2 \rangle;$$

*Antilinearità nella prima variabile:*

$$\langle cX, Y \rangle = \bar{c} \langle X, Y \rangle \quad \text{e} \quad \langle X_1 + X_2, Y \rangle = \langle X_1, Y \rangle + \langle X_2, Y \rangle;$$

*Simmetria hermitiana:*

$$\langle Y, X \rangle = \overline{\langle X, Y \rangle}.$$

Pertanto possiamo avere un prodotto definito positivo, con qualche piccola rinuncia riguardante la linearità e la simmetria.

Quando c'è da lavorare con nozioni che riguardano la lunghezza, conviene utilizzare il prodotto hermitiano, sebbene le forme bilineari simmetriche sugli spazi vettoriali complessi intervengano anch'esse nelle applicazioni.

Se  $V$  è uno spazio vettoriale complesso, una *forma hermitiana* su  $V$  è una qualsiasi funzione di due variabili:

$$(4.5) \quad \begin{aligned} V \times V &\longrightarrow \mathbb{C} \\ (v, w) &\longmapsto \langle v, w \rangle \end{aligned}$$

che soddisfi alle relazioni (4.4). Sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di  $V$ . Allora la *matrice* della forma si definisce in modo analogo a quello già visto per la matrice di una forma bilineare:

$$A = (a_{ij}), \quad \text{dove} \quad a_{ij} = \langle v_i, v_j \rangle.$$

La formula per la forma ora diventa:

$$(4.6) \quad \langle v, w \rangle = \bar{X}^t A Y,$$

se  $v = BX$  e  $w = BY$ .

La matrice  $A$  non è arbitraria, poiché la simmetria hermitiana implica che

$$a_{ij} = \langle v_i, v_j \rangle = \overline{\langle v_j, v_i \rangle} = \bar{a}_{ji},$$

ossia che  $A = \bar{A}^t$ . Introduciamo ora l'*aggiunta* di una matrice  $A$  [diversa da quella definita nel cap. 1 (5.4)] data da:

$$(4.7) \quad A^* = \bar{A}^t.$$

Essa soddisfa alle seguenti proprietà:

$$(A + B)^* = A^* + B^*$$

$$(AB)^* = B^* A^*$$

$$(A^*)^{-1} = (A^{-1})^*$$

$$A^{**} = A.$$

Tali proprietà si verificano facilmente. La formula (4.6) può essere riscritta ora nella forma:

$$(4.8) \quad \langle v, w \rangle = X^* A Y,$$

e il prodotto hermitiano standard su  $\mathbb{C}^n$  diventa:  $\langle X, Y \rangle = X^* Y$ .

Una matrice  $A$  è chiamata *hermitiana* o *autoaggiunta* se

$$(4.9) \quad A = A^*,$$

ed è chiaro che le matrici delle forme hermitiane sono matrici hermitiane. I loro elementi soddisfano alla relazione:  $a_{ji} = \bar{a}_{ij}$ . Ciò implica che gli elementi diagonali sono numeri reali e che gli elementi al di sotto della diagonale sono numeri complessi, coniugati di quelli al di sopra di essa:

$$A = \begin{bmatrix} r_1 & a_{1j} \\ & \ddots \\ \bar{a}_{ij} & r_n \end{bmatrix}, \quad r_i \in \mathbb{R}, \quad a_{ij} \in \mathbb{C}.$$

Per esempio,  $\begin{bmatrix} 2 & i \\ -i & 1 \end{bmatrix}$  è una matrice hermitiana.

Si noti che la condizione affinché una matrice reale sia hermitiana è:  $a_{ji} = a_{ij}$ . Dunque:

(4.10) *Le matrici hermitiane reali sono le matrici simmetriche reali.*

La discussione relativa al cambiamento di base nei §§ 1 e 2 può essere sviluppata in modo analogo per le forme hermitiane. Precisamente, data una forma hermitiana, un cambiamento di base mediante una matrice  $P$  porta, come in (1.12), a:

$$X'^* A' Y' = (PX)^* A' PY = X^* (P^* A' P) Y.$$

Pertanto la nuova matrice  $A'$  soddisfa alla relazione:

$$(4.11) \quad A = P^* A' P \quad \text{oppure} \quad A' = (P^*)^{-1} A P^{-1}.$$

Poiché  $P$  è arbitraria, possiamo sostituirla con  $Q = (P^*)^{-1}$ , ottenendo così la descrizione seguente analoga a (1.13):

(4.12) COROLLARIO *Sia  $A$  la matrice di una forma hermitiana rispetto a una base. Le matrici che rappresentano la stessa forma hermitiana rispetto a basi diverse sono quelle della forma  $A' = QAQ^*$ , essendo  $Q \in GL_n(\mathbb{C})$  una matrice invertibile arbitraria. ■*

Per le forme hermitiane, le matrici analoghe alle matrici ortogonali sono le matrici unitarie. Una matrice  $P$  è chiamata *unitaria*, se soddisfa alla condizione:

$$(4.13) \quad P^* P = I \quad \text{oppure} \quad P^* = P^{-1}.$$

Per esempio,  $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$  è una matrice unitaria.

Si noti che per una matrice reale  $P$ , tale condizione diventa:  $P^t P = I$ . Dunque:

(4.14) *Le matrici unitarie reali sono le matrici ortogonali reali.*

Le matrici unitarie formano un gruppo, precisamente il *gruppo unitario  $U_n$* :

$$(4.15) \quad U_n = \{P \mid P^* P = I\}.$$

La formula (4.11) dice che le matrici unitarie rappresentano cambiamenti di base che lasciano invariato il prodotto hermitiano standard  $X^* Y$ :

(4.16) COROLLARIO *Un cambiamento di base conserva il prodotto hermitiano standard, ossia  $X^* Y = X'^* Y'$ , se e soltanto se la sua matrice  $P$  è unitaria. ■*

Tuttavia il corollario (4.12) afferma che, in generale, un cambiamento di base trasforma il prodotto hermitiano standard  $X^* Y$  in  $X'^* A' Y'$ , dove  $A' = QAQ^*$  e  $Q \in GL_n(\mathbb{C})$ .

La nozione di ortogonalità per le forme hermitiane si definisce esattamente come per le forme bilineari simmetriche: un vettore  $v$  si dice *ortogonale* a un vettore  $w$  se  $\langle v, w \rangle = 0$ . Poiché  $\overline{\langle v, w \rangle} = \langle w, v \rangle$ , l'ortogonalità è ancora una relazione simmetrica. Possiamo ora ripetere per le forme hermitiane, senza variazioni essenziali, la trattazione sviluppata nei paragrafi 1 e 2, e la legge di Sylvester (2.11) per le forme simmetriche reali vale anche nel caso hermitiano. In particolare, possiamo parlare di forme *definite positive*, ossia aventi la proprietà:

$$(4.17) \quad \langle v, v \rangle \text{ è un numero reale positivo, se } v \neq 0,$$

e di basi ortonormali  $\mathbf{B} = (v_1, \dots, v_n)$ , ossia tali che:

$$(4.18) \quad \langle v_i, v_i \rangle = 1 \quad \text{e} \quad \langle v_i, v_j \rangle = 0, \quad \text{se } i \neq j.$$

(4.19) **TEOREMA** *Sia  $\langle , \rangle$  una forma hermitiana su uno spazio vettoriale complesso  $V$ . Allora esiste una base ortonormale in  $V$  se e soltanto se la forma è definita positiva.*

(4.20) **PROPOSIZIONE** *Sia  $\langle , \rangle$  una forma hermitiana su uno spazio vettoriale complesso  $V$ , e sia  $W$  un sottospazio di  $V$ . Allora, se la restrizione della forma a  $W$  è non degenera, si ha:  $V = W \oplus W^\perp$ .*

Le dimostrazioni di questi risultati sono lasciate per esercizio. ■

## 5 Il teorema spettrale

In questo paragrafo studieremo uno spazio vettoriale complesso  $V$  di dimensione  $n$  e una forma hermitiana definita positiva  $\langle , \rangle$  su  $V$ . Uno spazio vettoriale complesso su cui è data una forma hermitiana definita positiva è chiamato spesso uno *spazio hermitiano*. Se si vuole, si può pensare che  $V$  sia  $\mathbb{C}^n$ , con il prodotto hermitiano standard  $X^*Y$ . La scelta di una base ortonormale in  $V$  permette tale identificazione.

Poiché la forma  $\langle , \rangle$  è assegnata, non sceglieremo una base arbitraria in  $V$  per effettuare i calcoli. È naturale lavorare esclusivamente con basi ortonormali, il che porta dei cambiamenti in tutti i calcoli precedenti. In particolare, non sarà più vero che la matrice  $P$  di un cambiamento di base è una qualunque matrice invertibile. Infatti, se  $\mathbf{B} = (v_1, \dots, v_n)$ ,  $\mathbf{B}' = (v'_1, \dots, v'_n)$  sono due basi ortonormali, allora la matrice  $P$  che le collega sarà unitaria. Il fatto che le basi sono ortonormali significa che la matrice della forma  $\langle , \rangle$  rispetto a ciascuna base è l'identità  $I$ , e pertanto la (4.11) diventa  $I = P^*IP$ , ossia  $P^*P = I$ .

Passiamo ora a studiare un operatore lineare

$$(5.1) \quad T : V \rightarrow V,$$

su uno spazio hermitiano  $V$ . Sia  $\mathbf{B}$  una base ortonormale, e sia  $M$  la matrice associata a  $T$ . Un cambiamento di base ortonormale trasforma  $M$  in  $M' = PMP^{-1}$  [cap. 4 (3.4)], dove  $P$  è una matrice unitaria; ne segue che:

$$(5.2) \quad M' = PMP^*.$$

(5.3) **PROPOSIZIONE** *Sia  $T$  un operatore lineare su uno spazio hermitiano  $V$ , e sia  $M$  la matrice associata a  $T$  rispetto a una base ortonormale  $\mathbf{B}$ .*

- (a) *La matrice  $M$  è hermitiana se e soltanto se  $\langle v, Tw \rangle = \langle Tv, w \rangle$  per ogni  $v, w \in V$ . In tal caso,  $T$  è chiamato operatore hermitiano.*
- (b) *La matrice  $M$  è unitaria se e soltanto se  $\langle v, w \rangle = \langle Tv, Tw \rangle$  per ogni  $v, w \in V$ . In tal caso,  $T$  è chiamato operatore unitario.*

**Dimostrazione.** Siano  $X, Y$  i vettori delle coordinate di  $v, w$ :  $v = \mathbf{B}X$ ,  $w = \mathbf{B}Y$ , sicché  $\langle v, w \rangle = X^*Y$  e  $Tv = \mathbf{B}MX$ . Allora  $\langle v, Tw \rangle = X^*MY$ , e  $\langle Tv, w \rangle = X^*M^*Y$ . Pertanto, se  $M = M^*$ , allora  $\langle v, Tw \rangle = \langle Tv, w \rangle$  per ogni  $v, w$ , ossia  $T$  è hermitiano. Viceversa, se  $T$  è hermitiano, poniamo:  $v = e_i$ ,  $w = e_j$  come nella dimostrazione di (1.9) e otteniamo:  $b_{ij} = e_i^*(Me_j) = (e_i^*M^*)e_j = \bar{b}_{ji}$ . Dunque  $M = M^*$ . Analogamente,  $\langle v, w \rangle = X^*Y$  e  $\langle Tv, Tw \rangle = X^*M^*MY$ ; pertanto  $\langle v, w \rangle = \langle Tv, Tw \rangle$  per ogni  $v, w$  se e soltanto se  $M^*M = I$ . ■

## (5.4) TEOREMA SPETTRALE

- (a) *Sia  $T$  un operatore hermitiano su uno spazio vettoriale hermitiano  $V$ . Allora esiste una base ortonormale di  $V$  costituita da autovettori di  $T$ .*
- (b) *(Matrici) Sia  $M$  una matrice hermitiana. Allora esiste una matrice unitaria  $P$  tale che  $PMP^*$  è una matrice diagonale reale.*

**Dimostrazione.** Scegliamo un autovettore  $v = v_1$  e normalizziamolo in modo che abbia lunghezza 1, ossia  $\langle v, v \rangle = 1$ . Estendiamo  $\{v_1\}$  ad una base ortonormale di  $V$ . Allora la matrice associata a  $T$  diventa:

$$M = \begin{bmatrix} a & * & \cdots & * \\ 0 & \left[ \begin{array}{c} \vdots \\ N \end{array} \right] \\ \vdots & & & \\ 0 & & & \end{bmatrix}.$$

Poiché  $T$  è hermitiano, tale risulta la matrice  $M$  (5.3). Ciò implica che  $* \cdots * = 0 \cdots 0$  e che  $N$  è hermitiana. A questo punto si procede per induzione. ■

Per diagonalizzare una matrice hermitiana  $M$  mediante una matrice unitaria  $P$ , si può procedere determinando gli autovettori. Se gli autovalori sono distinti, gli autovettori corrispondenti saranno ortogonali. (Ciò segue dal teorema spettrale.) Sia  $\mathbf{B}'$  la base ortonormale ottenuta normalizzando le lunghezze degli autovettori. Allora  $P = [\mathbf{B}']^{-1}$  [cap. 3 (4.20)].

Per esempio, consideriamo la matrice

$$M = \begin{bmatrix} 2 & i \\ -i & 2 \end{bmatrix}.$$

Gli autovalori di tale matrice sono 3, 1, e i vettori:

$$v'_1 = \begin{bmatrix} 1 \\ -i \end{bmatrix}, \quad v'_2 = \begin{bmatrix} 1 \\ i \end{bmatrix}$$

sono autovettori associati a questi autovalori. Normalizziamo le loro lunghezze mediante il fattore  $\frac{1}{\sqrt{2}}$ . Allora:

$$P = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}^* = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \quad \text{e} \quad PMP^* = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}.$$

Ma il teorema spettrale afferma che una matrice hermitiana può essere diagonalizzata anche se i suoi autovalori non sono distinti. Questo enunciato diventa particolarmente semplice per le matrici  $2 \times 2$ . Precisamente, se il polinomio caratteristico di una matrice hermitiana  $2 \times 2$   $M$  ha una radice doppia, allora esiste una matrice unitaria  $P$  tale che  $PMP^* = aI$ . Ne segue che  $M = P^*aIP = aP^*P = aI$ . Pertanto dal teorema spettrale si ottiene che  $M = aI$ , ossia, le uniche matrici hermitiane  $2 \times 2$  il cui polinomio caratteristico ha una radice doppia sono le matrici  $aI$ , dove  $a$  è un numero reale. Possiamo verificare questo fatto direttamente, a partire dalla definizione. Scriviamo:  $M = \begin{bmatrix} a & \beta \\ \bar{\beta} & d \end{bmatrix}$ , dove  $a, d$  sono numeri reali e  $\beta$  è un numero complesso. Allora il polinomio caratteristico della matrice  $M$  è  $t^2 - (a+d)t + (ad - \beta\bar{\beta})$ , e questo polinomio ha una radice doppia se e soltanto se il suo discriminante si annulla, ossia:

$$(a+d)^2 - 4(ad - \beta\bar{\beta}) = (a-d)^2 + 4\beta\bar{\beta} = 0.$$

Entrambi i termini  $(a-d)^2$  e  $\beta\bar{\beta}$  sono numeri reali non negativi, quindi, se il discriminante si annulla, si ha  $a=d$  e  $\beta=0$ . In questo caso risulta  $M = aI$ , come annunciato.

Vediamo ora una conseguenza interessante del teorema spettrale, che si dimostra direttamente:

**(5.5) PROPOSIZIONE** *Gli autovalori di un operatore hermitiano  $T$  sono numeri reali.*

*Dimostrazione.* Sia  $a$  un autovalore, e sia  $v$  un autovettore di  $T$  associato ad  $a$ , sicché  $T(v) = av$ . Allora, in virtù di (5.3), si ha  $\langle Tv, v \rangle = \langle v, Tv \rangle$ , ossia  $\langle av, v \rangle = \langle v, av \rangle$ . Per la linearità coniugata (4.4), si ha:

$$\bar{a}\langle v, v \rangle = \langle av, v \rangle = \langle v, av \rangle = a\langle v, v \rangle,$$

e d'altra parte,  $\langle v, v \rangle \neq 0$  poiché la forma  $\langle \cdot, \cdot \rangle$  è definita positiva. Pertanto  $a = \bar{a}$ . Ciò prova che  $a$  è un numero reale. ■

Per le matrici reali simmetriche valgono risultati analoghi a quelli che abbiamo dimostrato per le matrici hermitiane. Sia  $V$  uno spazio vettoriale reale con una forma bilineare definita positiva  $\langle \cdot, \cdot \rangle$ . Sia  $T$  un operatore lineare su  $V$ .

**(5.6) PROPOSIZIONE** *Sia  $M$  la matrice di  $T$  rispetto ad una base ortonormale.*

- (a) *La matrice  $M$  è simmetrica se e soltanto se  $\langle v, Tw \rangle = \langle Tv, w \rangle$  per ogni  $v, w \in V$ . In tal caso,  $T$  è chiamato operatore simmetrico.*
- (b) *La matrice  $M$  è ortogonale se e soltanto se  $\langle v, w \rangle = \langle Tv, Tw \rangle$  per ogni  $v, w \in V$ . In tal caso,  $T$  è chiamato operatore ortogonale.* ■

**(5.7) PROPOSIZIONE** *Gli autovalori di una matrice simmetrica reale sono reali.*

*Dimostrazione.* Una matrice simmetrica reale è hermitiana. Pertanto si tratta di un caso particolare di (5.5). ■

**(5.8) TEOREMA SPETTRALE (caso reale)**

- (a) *Sia  $T$  un operatore simmetrico su uno spazio vettoriale reale  $V$  con una forma bilineare definita positiva. Allora esiste una base ortonormale di autovettori di  $T$ .*
- (b) *(Matrici) Sia  $M$  una matrice simmetrica reale  $n \times n$ . Allora esiste una matrice ortogonale  $P \in O_n(\mathbb{R})$  tale che  $PMP^T$  è diagonale.*

*Dimostrazione.* Poiché sappiamo che gli autovalori di un operatore simmetrico sono reali, possiamo copiare la dimostrazione di (5.4). ■

## 6 Coniche e quadriche

Una conica è il luogo dei punti del piano  $\mathbb{R}^2$  definito da un'equazione di secondo grado in due variabili, della forma:

$$(6.1) \quad f(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + b_1x_1 + b_2x_2 + c = 0.$$

Più precisamente, il luogo (6.1) è un'ellisse, un'iperbole, o una parabola; negli altri casi la conica è detta *degenera*. Una conica degenera può essere una coppia di rette, una sola retta, un punto, oppure l'insieme vuoto, a seconda della particolare equazione. Il termine *quadrica* viene usato per indicare l'analogo luogo di punti in  $\mathbb{R}^n$ , con  $n \geq 3$ .

La parte quadratica di  $f(x_1, x_2)$  è chiamata *forma quadratica*:

$$(6.2) \quad q(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2.$$

In generale, una *forma quadratica* in  $n$  variabili  $x_1, \dots, x_n$  è un polinomio avente tutti i termini di grado 2 nelle variabili.

Conviene esprimere la forma  $q(x_1, x_2)$  con la notazione matriciale. A tale scopo, introduciamo la matrice simmetrica:

$$(6.3) \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix}.$$

Allora  $q(x_1, x_2) = X^t AX$ , dove  $X$  denota il vettore colonna  $(x_1, x_2)^t$ . Introduciamo inoltre il vettore riga  $B = (b_1, b_2)$ . Allora l'equazione (6.1) può essere scritta nella forma matriciale:

$$(6.4) \quad X^t AX + BX + c = 0.$$

Nelle formule (6.1) e (6.2) abbiamo messo il coefficiente 2 per evitare alcuni coefficienti  $\frac{1}{2}$  nella matrice (6.3). Un altro modo di scrivere la forma quadratica è il seguente:

$$q(x_1, x_2) = a_{11}x_1^2 + a_{12}x_1x_2 + a_{12}x_2x_1 + a_{22}x_2^2.$$

Ci proponiamo di descrivere le classi di congruenza delle coniche, come figure geometriche, ossia le loro orbite rispetto all'azione del gruppo  $M$  dei movimenti rigidi del piano. Un movimento rigido produrrà un cambiamento di variabili nell'equazione (6.1).

(6.5) TEOREMA *Ogni conica non degenera è congruente ad una delle coniche seguenti:*

*Ellisse:*  $a_{11}x_1^2 + a_{22}x_2^2 - 1 = 0,$

*Iperbole:*  $a_{11}x_1^2 - a_{22}x_2^2 - 1 = 0,$

*Parabola:*  $a_{11}x_1^2 - x_2 = 0,$

con  $a_{11}, a_{22} > 0$ .

**Dimostrazione.** Semplificheremo l'equazione (6.1) in due passaggi, dapprima applicando una trasformazione ortogonale (una rotazione o una riflessione) per diagonalizzare  $A$  e successivamente applicando una traslazione per eliminare, quanto più possibile, i termini lineare e costante  $BX + c$ .

In virtù del teorema spettrale (5.8), esiste una matrice ortogonale  $P$  tale che  $PAP^t$  è diagonale. Effettuiamo il cambiamento di variabili  $X' = PX$ , ossia  $X = P^t X'$ . Sostituendo nell'equazione (6.4), si ottiene:

$$(6.6) \quad X'^t (PAP^t) X' + (BP^t) X' + c = 0.$$

Pertanto esiste un cambiamento ortogonale di variabili tale che la forma quadratica diventa diagonale, ossia il coefficiente  $a_{12}$  di  $x_1x_2$  è zero.

Supponiamo che  $A$  sia diagonale. Allora  $f$  è della forma

$$f(x_1, x_2) = a_{11}x_1^2 + a_{22}x_2^2 + b_1x_1 + b_2x_2 + c = 0.$$

Eliminiamo  $b_i$  completando i quadrati, mediante la sostituzione

$$(6.7) \quad x_i = x'_i - \frac{b_i}{2a_{ii}}.$$

Tale sostituzione dà luogo a

$$(6.8) \quad f(x_1, x_2) = a_{11}x_1'^2 + a_{22}x_2'^2 + c'.$$

Questa sostituzione corrisponde ad una traslazione mediante il vettore  $(b_1/2a_{11}, b_2/2a_{22})^t$ , e può essere effettuata purché  $a_{11}$  e  $a_{22}$  siano diversi da zero.

Se  $a_{ii} = 0$ , ma  $b_i \neq 0$ , possiamo utilizzare la sostituzione

$$(6.9) \quad x_i = x'_i - c/b_i$$

per eliminare invece il termine costante. Possiamo normalizzare un coefficiente in modo da renderlo uguale a  $-1$ . Così facendo e lasciando da parte le coniche degeneri, restano i tre casi elencati nel teorema. Non è difficile provare che un cambiamento dei coefficienti  $a_{11}, a_{22}$  dà luogo a una diversa classe di congruenza (ad eccezione dello scambio di  $a_{11}, a_{22}$  nell'equazione di un'ellisse.) ■

Il metodo usato sopra può essere applicato nel caso di un numero qualsiasi di variabili per classificare le quadriche in dimensione  $n$ . L'equazione generale di secondo grado ha la forma

$$(6.10) \quad f(x_1, \dots, x_n) = \sum_i a_{ii}x_i^2 + \sum_{i < j} 2a_{ij}x_i x_j + \sum_i b_i x_i + c = 0,$$

che si può anche scrivere in modo più compatto, come

$$(6.11) \quad f(x_1, \dots, x_n) = \sum_{i,j} a_{ij}x_i x_j + \sum_i b_i x_i + c = 0,$$

dove la prima somma è estesa a tutte le coppie di indici, e abbiamo posto  $a_{ji} = a_{ij}$ .

Definiamo le matrici  $A, B$  nel modo seguente:

$$A = \begin{bmatrix} a_{11}a_{12} & \cdots & a_{1n} \\ a_{12} & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nn} \end{bmatrix}, \quad B = (b_1, \dots, b_n).$$

Allora la forma quadratica è:

$$(6.12) \quad q(x_1, \dots, x_n) = X^t AX,$$

e risulta:

$$(6.13) \quad f(x_1, \dots, x_n) = X^t AX + BX + c.$$

Mediante un'opportuna trasformazione ortogonale  $P$ , la quadrica viene portata nella forma (6.6), dove  $PAP^t$  è diagonale. Quando  $A$  è diagonale, i termini lineari vengono eliminati mediante la traslazione (6.7), altrimenti si utilizza la sostituzione (6.9).

Enunciamo ora la classificazione delle quadriche in  $\mathbb{R}^3$ .

(6.14) TEOREMA *Le classi di congruenza delle quadriche non degeneri in  $\mathbb{R}^3$  sono rappresentate da:*

*Ellissoidi:*

$$a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 - 1 = 0,$$

*Iperboloidi a una falda:*<sup>2</sup>

$$a_{11}x_1^2 + a_{22}x_2^2 - a_{33}x_3^2 - 1 = 0,$$

*Iperboloidi a due falde:*<sup>3</sup>

$$a_{11}x_1^2 - a_{22}x_2^2 - a_{33}x_3^2 - 1 = 0,$$

*Paraboloidi ellittici:*

$$a_{11}x_1^2 + a_{22}x_2^2 + x_3 = 0,$$

*Paraboloidi iperbolici:*

$$a_{11}x_1^2 - a_{22}x_2^2 - x_3 = 0,$$

con  $a_{11}, a_{22}, a_{33} > 0$ . ■

Data un'equazione di secondo grado  $f(x_1, x_2) = 0$ , possiamo determinare più facilmente il tipo di conica che essa rappresenta utilizzando cambiamenti di coordinate non ortogonali. Per esempio, se la forma quadratica associata  $q$  è definita positiva, allora la conica è un'ellisse, oppure è degenere (nel qual caso, è costituita da un unico punto oppure è l'insieme vuoto). Per distinguere tali casi, possiamo servirci di cambiamenti di coordinate arbitrari. Un cambiamento di coordinate non ortogonale distorcerà la conica, ma non trasformerà un'ellisse in un'iperbole o in una conica degenere.

<sup>2</sup> Detti anche iperboloidi iperbolici.

<sup>3</sup> Detti anche iperboloidi ellittici.

Consideriamo, ad esempio, la conica di equazione

$$(6.15) \quad x_1^2 + x_1x_2 + x_2^2 + 4x_1 + 3x_2 + 4 = 0.$$

La matrice associata è

$$A = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix},$$

la quale è definita positiva, in virtù di (1.25). Se diagonalizziamo  $A$  mediante la sostituzione non ortogonale  $X' = PX$ , dove

$$P = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}, \quad PAP^t = \begin{bmatrix} 1 & 3 \\ 3 & 4 \end{bmatrix}, \quad BP^t = (4, 1),$$

otteniamo

$$x_1'^2 + \frac{3}{4}x_2'^2 + 4x_1' + x_2' + 4 = 0.$$

Completando i quadrati, si ha:

$$x_1''^2 + \frac{3}{4}x_2''^2 - \frac{1}{3} = 0,$$

ossia un'ellisse. Pertanto anche l'equazione (6.15) rappresenta un'ellisse. D'altra parte, se nella (6.15) poniamo il termine costante uguale a 5, il luogo da essa definito in  $\mathbb{R}^2$  diventa l'insieme vuoto.

## 7 Il teorema spettrale per gli operatori normali

Il teorema spettrale (5.4) afferma che ogni matrice hermitiana  $M$  può essere trasformata in una matrice diagonale reale  $D$  mediante una matrice unitaria  $P$ :  $D = PMP^*$ . Consideriamo ora le matrici  $M$  che possono essere trasformate allo stesso modo in una matrice diagonale  $D$ , ma senza richiedere che  $D$  sia reale. Come vedremo, per tali matrici esiste una caratterizzazione semplice ed elegante.

(7.1) DEFINIZIONE *Una matrice  $M$  si dice normale se commuta con la propria aggiunta, ossia se  $MM^* = M^*M$ .*

(7.2) LEMMA *Se  $M$  è normale e  $P$  è unitaria, allora  $M' = PMP^*$  è anch'essa normale, e viceversa.*

*Dimostrazione.* Supponiamo che  $M$  sia normale. Allora

$$\begin{aligned} M'M'^* &= PMP^*(PMP^*)^* = PMM^*P^* = \\ &= PM^*MP^* = (PMP^*)^*(PMP^*) = M'^*M'. \end{aligned}$$

Pertanto  $PMP^*$  è normale. Il viceversa si dimostra sostituendo  $P$  con  $P^*$ . ■

Questo lemma ci permette di definire un *operatore normale*  $T : V \rightarrow V$  su uno spazio hermitiano  $V$  come un operatore lineare tale che la matrice  $M$  ad esso associata rispetto ad una qualsiasi base ortonormale sia una matrice normale.

(7.3) TEOREMA Una matrice complessa  $M$  è normale se e soltanto se esiste una matrice unitaria  $P$  tale che  $PMP^*$  sia diagonale.

Le matrici normali più importanti, a parte le matrici hermitiane, sono le matrici unitarie. Infatti, se  $M$  è unitaria, si ha  $M^* = M^{-1}$ , da cui:  $MM^* = M^*M = I$ , ciò prova che  $M$  è normale.

(7.4) COROLLARIO Ogni classe di equivalenza di matrici simili nel gruppo unitario contiene una matrice diagonale. ■

*Dimostrazione del teorema (7.3).* Osserviamo innanzitutto che due matrici diagonali commutano tra loro; pertanto ogni matrice diagonale è normale:  $DD^* = D^*D$ . Il lemma assicura che, se  $PMP^* = D$ , allora  $M$  è normale. Viceversa, supponiamo che  $M$  sia normale. Sceglio un autovettore  $v = v_1$  di  $M$  e lo normalizziamo in modo che  $\langle v, v \rangle = 1$ , come nella dimostrazione di (5.4). Estendiamo poi  $\{v_1\}$  ad una base ortonormale. Allora  $M$  sarà trasformata in una matrice:

$$M_1 = PMP^* = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & \begin{bmatrix} N \end{bmatrix} \\ \vdots & & & \\ 0 & & & \end{bmatrix}, \quad \text{e} \quad M_1^* = PM^*P^* = \begin{bmatrix} \bar{a}_{11} & 0 & \cdots & 0 \\ \bar{a}_{12} & \begin{bmatrix} N^* \end{bmatrix} \\ \vdots & & & \\ \bar{a}_{1n} & & & \end{bmatrix}.$$

L'elemento nell'angolo in alto a sinistra di  $M_1^*M_1$  è  $a_{11}\bar{a}_{11}$ , mentre l'elemento di ugual posto in  $M_1M_1^*$  è  $a_{11}\bar{a}_{11} + a_{12}\bar{a}_{12} + \cdots + a_{1n}\bar{a}_{1n}$ . Poiché  $M$  è normale, tale risulta  $M_1$ , ossia,  $M_1^*M_1 = M_1M_1^*$ . Ne segue che  $a_{12}\bar{a}_{12} + \cdots + a_{1n}\bar{a}_{1n} = 0$ . Poiché  $a_{1j}\bar{a}_{1j} \geq 0$ , ciò prova che gli elementi  $a_{1j}$  con  $j > 1$  sono nulli e che

$$M_1 = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & \begin{bmatrix} N \end{bmatrix} \\ \vdots & & & \\ 0 & & & \end{bmatrix}.$$

A questo punto, si continua lavorando su  $N$ , e il teorema si dimostra per induzione. ■

## 8 Forme antisimmetriche

La teoria delle forme antisimmetriche è indipendente dal campo degli scalari. Ci si potrebbe aspettare qualche difficoltà con i campi di caratteristica 2, in cui  $1+1=0$ . In questi campi  $a = -a$  per ogni  $a$ , sicché le condizioni per la simmetria (1.5) e per l'antisimmetria (1.6) risultano le stesse. Come vedremo, i campi di caratteristica 2 non danno luogo a difficoltà con le forme antisimmetriche, se la definizione di antisimmetria viene opportunamente modificata. La definizione che vale per tutti i campi è la seguente:

(8.1) DEFINIZIONE Una forma bilineare  $\langle , \rangle$  su uno spazio vettoriale  $V$  si dice antisimmetrica se

$$\langle v, v \rangle = 0$$

per ogni  $v \in V$ .

Con tale definizione la regola

$$(8.2) \quad \langle v, w \rangle = -\langle w, v \rangle$$

per ogni  $v, w \in V$  continua a valere. Essa si dimostra considerando lo sviluppo

$$\langle v+w, v+w \rangle = \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle,$$

e utilizzando il fatto che  $\langle v, v \rangle = \langle w, w \rangle = \langle v+w, v+w \rangle = 0$ . Se la caratteristica del campo degli scalari è diversa da 2, allora (8.1) e (8.2) sono equivalenti. Infatti, se (8.2) vale per ogni  $v, w$ , allora, ponendo  $w = v$ , si ottiene:  $\langle v, v \rangle = -\langle v, v \rangle$ . Ciò implica che  $2\langle v, v \rangle = 0$ , da cui  $\langle v, v \rangle = 0$ , a meno che  $2 = 0$  nel campo.

Si noti che, se  $F$  ha caratteristica 2, allora  $1 = -1$  in  $F$ , e quindi (8.2) prova che la forma è effettivamente simmetrica. Ma la maggior parte delle forme simmetriche non soddisfano alla (8.1).

La matrice  $A$  di una forma antisimmetrica rispetto a una base arbitraria è caratterizzata dalle proprietà:

$$(8.3) \quad a_{ii} = 0 \quad \text{e} \quad a_{ij} = -a_{ji}, \quad \text{se } i \neq j.$$

Assumiamo queste proprietà come definizione di una *matrice antisimmetrica*. Se la caratteristica del campo è diversa da 2, allora le (8.3) sono equivalenti alla condizione:

$$(8.4) \quad A^t = -A.$$

## (8.5) TEOREMA

- (a) Sia  $V$  uno spazio vettoriale di dimensione  $m$  sopra un campo  $F$ , e sia  $\beta$  una forma antisimmetrica non degenera su  $V$ . Allora  $m$  è un intero pari, ed esiste una base  $\mathbf{B}$  di  $V$  tale che rispetto ad essa la matrice  $A$  della forma è

$$J_{2n} = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},$$

dove  $0, I$  denotano matrici  $n \times n$  e  $n = \frac{1}{2}m$ .

- (b) (Matrici) Sia  $A$  una matrice  $m \times m$  antisimmetrica non singolare. Allora  $m$  è pari, ed esiste una matrice  $Q \in GL_m(F)$  tale che  $QAQ^t$  è la matrice  $J_{2n}$ .

Una base  $\mathbf{B}$  del tipo descritto in (8.5a) è una *base simplettica standard*. Si noti che, riscrivendo la base simplettica standard nell'ordine:  $(v_1, v_{n+1}, v_2, v_{n+2}, \dots, v_n, v_{2n})$ , la matrice  $J_{2n}$  viene trasformata in una matrice costituita da blocchi  $2 \times 2$  del tipo:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

lungo la diagonale. Questa è la forma più conveniente per dimostrare il teorema. La dimostrazione è lasciata come esercizio. ■

## 9 Sommario dei risultati, in notazione matriciale

**NUMERI REALI:** Una matrice quadrata  $A$  è simmetrica se  $A^t = A$ ; ortogonale se  $A^t = A^{-1}$ .

- (1) (Teorema spettrale) Se  $A$  è una matrice simmetrica reale, esiste una matrice ortogonale  $P$  tale che  $PAP^t (= PAP^{-1})$  è diagonale.
- (2) Se  $A$  è una matrice simmetrica reale, esiste una matrice reale invertibile  $P$  tale che:

$$PAP^t = \begin{bmatrix} I_p & & \\ & -I_m & \\ & & 0_z \end{bmatrix},$$

con  $p, m, z$  interi.

- (3) (Legge di Sylvester) I numeri  $p, m, z$  sono determinati dalla matrice  $A$ .

**NUMERI COMPLESSI:** Una matrice quadrata complessa  $A$  è hermitiana se  $A^* = A$ ; unitaria se  $A^* = A^{-1}$ ; normale se  $AA^* = A^*A$ .

- (1) (Teorema spettrale) Se  $A$  è una matrice hermitiana, esiste una matrice unitaria  $P$  tale che  $PAP^*$  è una matrice diagonale reale.
- (2) Se  $A$  è una matrice normale, esiste una matrice unitaria  $P$  tale che  $PAP^*$  è diagonale.

**CAMPO F ARBITRARIO:** Una matrice quadrata  $n \times n$  è antisimmetrica se  $a_{ii} = 0$  e  $a_{ij} = -a_{ji}$  per ogni  $i, j$ . Se  $A$  è una matrice antisimmetrica invertibile, allora  $n$  è pari, ed esiste una matrice invertibile  $P$  tale che  $PAP^t$  ha la forma:

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

(9.1) **Osservazione.** La regola:  $A' = (P^t)^{-1}A(P^{-1})$  per il cambiamento di base in una forma bilineare [cfr. (1.12)] è piuttosto complicata, per il modo in cui è definita la matrice  $P$  del cambiamento di coordinate. È possibile riordinare le equazioni (4.17) del capitolo 3, scrivendo:

$$(9.2) \quad v'_i = \sum_j q_{ij} v_j \quad \text{oppure} \quad \mathbf{B}'^t = Q\mathbf{B}^t.$$

Ne segue che  $Q = (P^{-1})^t$ , e in tal modo si ottiene la formula più semplice:

$$A' = QAQ^t.$$

Possiamo usare questa formula, se vogliamo.

La difficoltà con la formula (9.2) è che il cambiamento di base per un'applicazione lineare mette tutto in disordine; infatti, la formula  $A' = PAP^{-1}$  [cap. 4 (3.4)] è sostituita da  $A' = (Q^{-1})^t A Q^t$ . Cercare di mantenere le formule chiare e ordinate è come cercare di appianare un rigonfiamento in una moquette un po' sformata: lo schiacci da una parte, viene fuori dall'altra.

Ciò richiama l'attenzione su un punto importante. Gli operatori lineari su  $V$  e così pure le forme bilineari su  $V$  sono dati da una matrice  $n \times n$   $A$ , una volta fissata una base. Si può essere tentati di pensare che la teoria degli operatori lineari e la teoria delle forme bilineari siano in qualche modo equivalenti, ma ciò non è vero, a meno che non si fissi una base. Infatti, effettuando un *cambiamento di base*, la matrice di una forma bilineare si trasforma in  $(P^t)^{-1}AP^{-1}$  (1.12), mentre la matrice di un operatore lineare si trasforma in  $PAP^{-1}$  [cap. 4 (3.4)]. Pertanto le nuove matrici non sono più uguali tra loro. Più precisamente, ciò prova che le teorie divergono quando si cambia la base, a meno che la matrice  $P$  del cambiamento di base non sia ortogonale. Se  $P$  è ortogonale, allora  $P = (P^t)^{-1}$ , e tutto va bene, ossia le matrici restano uguali tra loro. Questo è uno dei vantaggi che si hanno lavorando con le basi ortonormali.



## Esercizi

### 1 Definizione di forma bilineare

1. Siano  $A$  e  $B$  matrici reali  $n \times n$ . Dimostrare che, se  $X^TAY = X^TBY$  per ogni coppia di vettori  $X, Y$  in  $\mathbb{R}^n$ , allora  $A = B$ .
2. Dimostrare direttamente che la forma bilineare rappresentata dalla matrice  $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$  è definita positiva se e solo se  $a > 0$  e  $ad - b^2 > 0$ .
3. Applicare il procedimento di Gram-Schmidt alla base  $((1, 1, 0)^t, (1, 0, 1)^t, (0, 1, 1)^t)$ , nel caso in cui la forma è il prodotto scalare.
4. Si consideri la matrice  $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ . Trovare una base ortonormale di  $\mathbb{R}^2$  rispetto alla forma  $X^TAY$ .
5. (a) Dimostrare che ogni matrice quadrata reale è la somma di una matrice simmetrica e di una matrice antisimmetrica ( $A^t = -A$ ), in modo unico.  
(b) Sia  $\langle , \rangle$  una forma bilineare su uno spazio vettoriale reale  $V$ . Dimostrare che esistono una forma simmetrica  $(,)$  e una forma antisimmetrica  $[,]$  tali che:  $\langle , \rangle = (, ) + [, ]$ .
6. Sia  $\langle , \rangle$  una forma bilineare simmetrica su uno spazio vettoriale  $V$  su un campo  $F$ . La funzione  $q : V \rightarrow F$  definita ponendo:  $q(v) = \langle v, v \rangle$  è chiamata la *forma quadratica* associata alla forma bilineare. Mostrare come sia possibile riottenere la forma bilineare a partire da  $q$ , se la caratteristica del campo  $F$  è diversa da 2, mediante lo sviluppo di  $q(v+w)$ .
- \*7. Siano  $X, Y$  vettori di  $\mathbb{C}^n$ , e supponiamo che  $X \neq 0$ . Dimostrare che esiste una matrice simmetrica  $B$  tale che  $BX = Y$ .

### 2 Forme simmetriche: ortogonalità

1. Dimostrare che una forma definita positiva è non degenere.
2. Una matrice  $A$  si dice *semidefinita positiva*, se  $X^TAX \geq 0$  per ogni  $X \in \mathbb{R}^n$ . Dimostrare che  $A^TA$  è semidefinita positiva per ogni matrice reale  $m \times n$ .
3. Trovare una base ortogonale per la forma su  $\mathbb{R}^n$  la cui matrice è:  
 (a)  $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$    (b)  $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ .
4. Estendere il vettore  $X_1 = (1, 1, 1)^t / \sqrt{3}$  ad una base ortonormale di  $\mathbb{R}^3$ .
- \*5. Dimostrare che, se le colonne di una matrice  $n \times n$   $A$  formano una base ortonormale, allora anche le righe formano una base ortonormale.

## Esercizi

6. Siano  $A, A'$  matrici simmetriche legate dalla relazione:  $A = P^T A' P$ , con  $P \in GL_n(F)$ . È vero che i ranghi di  $A$  e di  $A'$  sono uguali?
7. Sia  $A$  la matrice di una forma bilineare simmetrica  $\langle , \rangle$  rispetto a una base assegnata. È vero che gli autovalori di  $A$  sono indipendenti dalla base?
8. Dimostrare che l'unica matrice reale che sia ortogonale, simmetrica e definita positiva è l'identità.
9. Lo spazio vettoriale  $P$  di tutti i polinomi reali di grado  $\leq n$  ha una forma bilineare, definita da:

$$\langle f, g \rangle = \int_{-1}^1 f(x)g(x)dx.$$

Trovare una base ortonormale per  $P$ , in corrispondenza dei seguenti valori di  $n$ :

- (a) 1; (b) 2; (c) 3.

10. Si denoti con  $V$  lo spazio vettoriale delle matrici reali  $n \times n$ . Dimostrare che  $\langle A, B \rangle = \text{tr}(A^T B)$  è una forma bilineare definita positiva su  $V$ . Trovare una base ortonormale per tale forma.
11. Una matrice simmetrica  $A$  si dice *definita negativa*, se  $X^TAX < 0$  per ogni  $X \neq 0$ . Stabilire un criterio analogo a (1.26) affinché una matrice simmetrica  $A$  sia definita negativa.
12. Dimostrare che ogni matrice complessa non singolare simmetrica  $A$  ha la forma  $A = P^T P$ .
13. Con le notazioni di (2.12), dimostrare mediante un esempio che il sottospazio generato da  $(v_1, \dots, v_p)$  non è determinato dalla forma.
14. (a) Sia  $W$  un sottospazio di uno spazio vettoriale  $V$ , su cui è assegnata una forma bilineare simmetrica. Dimostrare che  $W^\perp$  è un sottospazio di  $V$ .  
(b) Provare che lo spazio annullatore  $N$  è un sottospazio di  $V$ .
15. Siano  $W_1, W_2$  sottospazi di uno spazio vettoriale  $V$  con una forma bilineare simmetrica. Dimostrare ciascuna delle seguenti relazioni:  
 (a)  $(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$   
 (b)  $W \subset W^{\perp\perp}$   
 (c) Se  $W_1 \subset W_2$ , allora  $W_1^\perp \supset W_2^\perp$ .
16. Dimostrare la proposizione (2.7), ossia che  $V = W \oplus W^\perp$ , se la forma è non degenere su  $W$ .
17. Sia  $V = \mathbb{R}^{2 \times 2}$  lo spazio vettoriale delle matrici reali  $2 \times 2$ .  
 (a) Determinare la matrice della forma bilineare  $\langle A, B \rangle = \text{tr}(AB)$  su  $V$ , rispetto alla base canonica  $\{e_{ij}\}$ .  
 (b) Determinare la segnatura di tale forma.  
 (c) Trovare una base ortogonale per tale forma.

- (d) Determinare la segnatura della forma sul sottospazio di  $V$  costituito dalle matrici con traccia zero.
- \*18. Determinare la segnatura della forma  $\langle A, B \rangle = \text{tr}(AB)$  sullo spazio  $\mathbb{R}^{n \times n}$  delle matrici reali  $n \times n$ .
19. Sia  $V = \mathbb{R}^{2 \times 2}$  lo spazio delle matrici  $2 \times 2$ .
- Dimostrare che la forma  $\langle A, B \rangle$  definita ponendo  $\langle A, B \rangle = \det(A + B) - \det A - \det B$  è simmetrica e bilineare.
  - Calcolare la matrice di tale forma rispetto alla base canonica  $\{e_{ij}\}$ , e determinare la segnatura della forma.
  - Determinare la segnatura della forma sul sottospazio di  $V$  costituito dalle matrici con traccia zero.
20. Risolvere l'esercizio 19 per lo spazio  $\mathbb{R}^{3 \times 3}$ , sostituendo la forma quadratica  $\det A$  con il coefficiente di  $t$  nel polinomio caratteristico di  $A$ .
21. Enunciare l'analogia della legge di Sylvester per le forme simmetriche sugli spazi vettoriali complessi, e dimostrarlo.
22. Utilizzando il metodo di dimostrazione del teorema (2.9), trovare condizioni necessarie e sufficienti su un campo  $F$  affinché ogni spazio vettoriale di dimensione finita  $V$  sopra  $F$  con una forma bilineare simmetrica  $\langle , \rangle$  abbia una base ortogonale.
23. Sia  $F = \mathbb{F}_2$ , e si consideri la matrice  $A = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$ .
- Dimostrare che la forma bilineare  $X^t A Y$  su  $F^2$  non può essere diagonalizzata.
  - Determinare le orbite rispetto all'azione:  $(P, A) \mapsto PAP^t$  di  $GL_2(F)$  sullo spazio delle matrici  $2 \times 2$  a elementi in  $F$ .

### 3 La geometria associata a una forma positiva

- Sia  $V$  uno spazio euclideo. Dimostrare la disegualanza di Schwarz e la disegualanza triangolare.
- Sia  $W$  un sottospazio di uno spazio euclideo  $V$ . Dimostrare che  $W = W^{\perp\perp}$ .
- Sia  $V$  uno spazio euclideo. Dimostrare che, se  $|v| = |w|$ , allora  $(v + w) \perp (v - w)$ . Interpretare geometricamente il risultato.
- Dimostrare la legge del parallelogramma:  $|v + w|^2 + |v - w|^2 = 2|v|^2 + 2|w|^2$  in uno spazio euclideo.
- Dimostrare che la proiezione ortogonale (3.7) è un'applicazione lineare.
- Si denoti con  $\pi: V \rightarrow W$  la proiezione ortogonale di  $V = \mathbb{R}^3$  su un sottospazio di dimensione due  $W$  tale che le immagini dei vettori della base canonica in  $V$  formino un triangolo equilatero. Determinare una base ortogonale  $(w_1, w_2)$  di  $W$  tale che  $\pi(e_1) = cw_1$ .
- \*7. Sia  $W$  un sottospazio di dimensione due di  $\mathbb{R}^3$ , e si consideri la proiezione ortogonale  $\pi$  di  $\mathbb{R}^3$  su  $W$ . Sia  $(a_i, b_i)$  il vettore delle coordinate di  $\pi(e_i)$  rispetto ad una base

- ortonormale fissata in  $W$ . Dimostrare che  $(a_1, a_2, a_3)$  e  $(b_1, b_2, b_3)$  sono vettori unitari ortogonali.
- \*8. Sia  $w \in \mathbb{R}^n$  un vettore di lunghezza 1.
- Dimostrare che la matrice  $P = I - 2ww^t$  è ortogonale.
  - Dimostrare che la moltiplicazione per  $P$  è una riflessione rispetto al sottospazio  $W$  ortogonale a  $w$ , ossia dimostrare che, se un vettore arbitrario  $v$  si scrive nella forma  $v = cw + w'$ , dove  $w' \in W^\perp$ , allora  $Pv = -cw + w'$ .
  - Siano  $X, Y$  vettori in  $\mathbb{R}^n$  aventi la stessa lunghezza. Determinare un vettore  $w$  tale che  $PX = Y$ .
- \*9. Utilizzare l'esercizio 8 per dimostrare che ogni matrice ortogonale  $n \times n$  è un prodotto di al più  $n$  riflessioni.
10. Sia  $A$  una matrice simmetrica reale, e sia  $T$  l'operatore lineare su  $\mathbb{R}^n$  rappresentato da  $A$ .
- Dimostrare che  $(\ker T) \perp (\text{im } T)$  e che  $V = (\ker T) \oplus (\text{im } T)$ .
  - Provare che  $T$  è una proiezione ortogonale su  $\text{im } T$  se e solo se, in aggiunta alla simmetria di  $A$ , si ha:  $A^2 = A$ .
11. Sia  $A$  una matrice reale simmetrica e definita positiva. Dimostrare che gli elementi massimali della matrice si trovano sulla diagonale.

### 4 Forme hermitiane

- Verificare le proprietà (4.4).
- Dimostrare che la forma data dal prodotto scalare:  $(X \cdot Y) = X^t Y$  non è definita positiva su  $\mathbb{C}^n$ .
- Dimostrare che una matrice  $A$  è hermitiana se e soltanto se la forma associata  $X^*AX$  è una forma hermitiana.
- Provare che se  $X^*AX$  è reale per ogni vettore complesso  $X$ ,  $A$  è hermitiana.
- Dimostrare che le matrici hermitiane  $n \times n$  formano uno spazio vettoriale reale, e trovare una base per tale spazio.
- Sia  $V$  uno spazio hermitiano [cfr. §5] di dimensione due. Sia  $(v_1, v_2)$  una base ortonormale di  $V$ . Descrivere tutte le basi ortonormali  $(v'_1, v'_2)$  con  $v_1 = v'_1$ .
- Siano  $X, Y \in \mathbb{C}^n$  vettori ortogonali. Dimostrare che  $|X + Y|^2 = |X|^2 + |Y|^2$ .
- È vero che  $\langle X, Y \rangle = x_1y_1 + ix_1y_2 - ix_2y_1 + ix_2y_2$  su  $\mathbb{C}^2$  è una forma hermitiana?
- Siano  $A, B$  matrici hermitiane definite positive. Quali tra le seguenti matrici:  $A^2, A^{-1}, AB, A + B$  sono hermitiane definite positive?
- Dimostrare che il determinante di una matrice hermitiana è un numero reale.
- Provare che una matrice  $A$  è hermitiana definita positiva se e soltanto se  $A = P^*P$  per qualche matrice invertibile  $P$ .
- Dimostrare il teorema (4.19) secondo cui una forma hermitiana su uno spazio vettoriale complesso  $V$  ammette una base ortonormale se e soltanto se è definita positiva.

13. Estendere alle matrici hermitiane il criterio (1.25) affinché una matrice sia definita positiva.
14. Enunciare e dimostrare un analogo della legge di Sylvester per le matrici hermitiane.
15. Sia  $\langle \cdot, \cdot \rangle$  una forma hermitiana su uno spazio vettoriale complesso  $V$ , e si denoti con  $\{v, w\}$  la parte reale del numero complesso  $\langle v, w \rangle$ . Dimostrare che, se  $V$  è considerato come uno spazio vettoriale reale, allora  $\{ \cdot, \cdot \}$  è una forma bilineare simmetrica su  $V$ , e se  $\langle \cdot, \cdot \rangle$  è definita positiva, tale risulta anche  $\{ \cdot, \cdot \}$ . Cosa si può dire sulla parte immaginaria?
16. Sia  $P$  lo spazio vettoriale dei polinomi di grado  $\leq n$ .

(a) Dimostrare che

$$\langle f, g \rangle = \int_0^{2\pi} \overline{f(e^{i\theta})} g(e^{i\theta}) d\theta$$

è una forma hermitiana definita positiva su  $P$ .

(b) Trovare una base ortonormale per tale forma.

17. Stabilire se le regole seguenti definiscono forme hermitiane sullo spazio delle matrici complesse  $\mathbb{C}^{n \times n}$ , e in caso affermativo, determinarne la segnatura:

(a)  $A, B \mapsto \text{tr}(A^*B)$  (b)  $A, B \mapsto \text{tr}(\bar{A}B)$ .

18. Sia  $A$  una matrice unitaria. Dimostrare che  $|\det A| = 1$ .

19. Sia  $P$  una matrice unitaria, e siano  $X_1, X_2$  autovettori di  $P$ , associati ad autovalori distinti  $\lambda_1, \lambda_2$ . Dimostrare che  $X_1$  e  $X_2$  sono ortogonali rispetto al prodotto hermitiano standard su  $\mathbb{C}^n$ .

- \*20. Sia  $A$  una matrice complessa. Provare che  $I + A^*A$  è non singolare.

21. Dimostrare la proposizione (4.20).

### 5 Il teorema spettrale

1. Dimostrare che se  $T$  è un operatore hermitiano la regola:  $\{v, w\} = \langle v, Tw \rangle = X^*MY$  definisce una nuova forma hermitiana su  $V$ .
2. Dimostrare che gli autovalori di una matrice simmetrica reale sono numeri reali.
3. Dimostrare che autovettori associati ad autovalori distinti di una matrice hermitiana  $A$  sono ortogonali.
4. Trovare una matrice unitaria  $P$  tale che  $PAP^*$  sia diagonale, essendo:

$$A = \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}.$$

5. Trovare una matrice reale ortogonale  $P$  tale che  $PAP^*$  sia diagonale, essendo:

$$(a) A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}; \quad (b) A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}; \quad (c) A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

6. Dimostrare l'equivalenza delle condizioni (a) e (b) del teorema spettrale.

7. Dimostrare che una matrice simmetrica reale  $A$  è definita positiva se e solo se i suoi autovalori sono positivi.

8. Dimostrare che l'unica matrice che sia hermitiana definita positiva e unitaria è l'identità  $I$ .

9. Sia  $A$  una matrice simmetrica reale. Dimostrare che  $e^A$  è simmetrica e definita positiva.

10. Dimostrare che per ogni matrice quadrata  $A$ , si ha  $\ker A = (\text{im } A^*)^\perp$  rispetto al prodotto hermitiano standard.

- \*11. Sia  $\zeta = e^{2\pi i/n}$ , e sia  $a_{jk} = \frac{\zeta^{jk}}{\sqrt{n}}$ . Dimostrare che la matrice  $A = (a_{jk})$  è unitaria.

12. Dimostrare che per ogni matrice complessa  $A$  esiste una matrice unitaria  $P$  tale che  $PAP^*$  è triangolare superiore.

13. Sia  $A$  una matrice hermitiana. Dimostrare che esiste una matrice unitaria  $P$  con determinante 1 tale che  $PAP^*$  è diagonale.

- \*14. Siano  $A, B$  matrici hermitiane che commutano tra loro. Dimostrare che esiste una matrice unitaria  $P$  tale che  $PAP^*$  e  $PBP^*$  sono entrambe diagonali.

15. Utilizzare il teorema spettrale per dare una nuova dimostrazione del fatto che una matrice  $n \times n$  reale simmetrica definita positiva  $P$  ha la forma  $P = AA^t$  per qualche matrice  $n \times n$   $A$ .

16. Siano  $\lambda, \mu$  autovalori distinti di una matrice simmetrica reale  $A$ , e siano  $X, Y$  autovettori associati a tali autovalori. Dimostrare che  $X$  è ortogonale a  $Y$  rispetto al prodotto scalare.

### 6 Coniche e quadriche

1. Determinare il tipo della quadrica di equazione:

$$x^2 + 4xy + 2xz + z^2 + 3x + z - 6 = 0.$$

2. Supponiamo che l'equazione (6.1) rappresenti un'ellisse. Invece di diagonalizzare la forma quadratica ed effettuare poi una traslazione per la riduzione a forma canonica, si potrebbe dapprima effettuare la traslazione. Mostrare come sia possibile determinare la traslazione richiesta mediante i calcoli.

3. Discutere tutte le coniche degeneri.

4. Dare una condizione necessaria e sufficiente, espressa mediante i coefficienti della sua equazione, affinché una conica risulti una circonferenza.

5. (a) Descrivere i tipi di coniche mediante la segnatura della forma quadratica.  
 (b) Fare la stessa cosa per le quadriche in  $\mathbb{R}^3$ .
6. Descrivere le quadriche degeneri, ossia quelle che non sono elencate in (6.14).

### 7 Il teorema spettrale per gli operatori normali

1. Dimostrare che, per ogni matrice normale  $A$ , si ha  $\ker A = (\text{im } A)^\perp$ .
2. È vero che, se  $A$  è una matrice normale e  $W$  è un sottospazio  $A$ -invariante di  $V = \mathbb{C}^n$ , allora anche  $W^\perp$  è  $A$ -invariante?
3. Una matrice  $A$  si dice *anti-hermitiana* se  $A^* = -A$ . Cosa si può dire sugli autovalori e sulla possibilità di diagonalizzare una matrice siffatta?
4. Dimostrare che l'operatore ciclico di spostamento:

$$\begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ 1 & & & 0 \end{bmatrix}$$

è normale, e determinare la sua forma diagonale.

5. Sia  $P$  una matrice reale normale e con autovalori reali. Dimostrare che  $P$  è simmetrica.
6. Sia  $P$  una matrice reale antisimmetrica. Dimostrare che  $P$  è normale.
- \*7. Dimostrare che la matrice *circolante*

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_n \\ c_n & c_0 & c_1 & \cdots & c_{n-1} \\ \vdots & & & & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$

è una matrice normale.

8. (a) Sia  $A$  una matrice complessa simmetrica. Dimostrare che autovettori di  $A$  associati ad autovalori distinti sono ortogonali tra loro rispetto alla forma bilineare  $X^t Y$ .  
 \*(b) Dare un esempio di una matrice complessa simmetrica  $A$  tale che non esiste alcuna matrice  $P \in O_n(\mathbb{C})$  con  $PAP^t$  diagonale.
9. Sia  $A$  una matrice normale. Dimostrare che  $A$  è hermitiana se e solo se tutti gli autovalori di  $A$  sono reali, e che  $A$  è unitaria se e solo se ogni autovalore ha modulo 1.
10. Sia  $V$  uno spazio vettoriale complesso di dimensione finita con una forma hermitiana definita positiva  $\langle \cdot, \cdot \rangle$ , e sia  $T : V \rightarrow V$  un operatore lineare su  $V$ . Sia  $A$  la matrice associata a  $T$  rispetto a una base ortonormale  $\mathbf{B}$ . L'operatore aggiunto  $T^* : V \rightarrow V$  è definito come l'operatore avente come matrice associata (rispetto alla stessa base  $\mathbf{B}$ ) la matrice  $A^*$ .

- (a) Dimostrare che  $T$  e  $T^*$  sono legati tra loro dalle equazioni:  $\langle Tv, w \rangle = \langle v, T^* w \rangle$  e  $\langle v, Tw \rangle = \langle T^* v, w \rangle$  per ogni  $v, w \in W$ . Provare che la prima di tali equazioni caratterizza  $T^*$ .

- (b) Dimostrare che  $T^*$  non dipende dalla scelta della base ortonormale.  
 (c) Sia  $v$  un autovettore di  $T$  associato a un autovalore  $\lambda$ , e sia  $W = v^\perp$  il sottospazio di  $V$  costituito dai vettori ortogonali a  $v$ . Dimostrare che  $W$  è  $T^*$ -invariante.

11. Dimostrare che, se  $T$  è un operatore lineare, l'operatore  $TT^*$  è hermitiano.
12. Sia  $V$  uno spazio vettoriale complesso di dimensione finita con una forma hermitiana definita positiva  $\langle \cdot, \cdot \rangle$ . Un operatore lineare  $T : V \rightarrow V$  si dice *normale* se  $TT^* = T^*T$ .
- (a) Dimostrare che  $T$  è normale se e soltanto se  $\langle Tv, Tw \rangle = \langle T^*v, T^*w \rangle$  per ogni  $v, w \in V$ , e verificare che gli operatori hermitiani e gli operatori unitari sono normali.
- (b) Sia  $T$  un operatore normale, e sia  $v$  un autovettore di  $T$  associato a un autovalore  $\lambda$ . Dimostrare che  $v$  è anche un autovettore di  $T^*$ , e determinare l'autovalore ad esso associato.
- (c) Dimostrare che se  $v$  è un autovettore, allora  $W = v^\perp$  è  $T$ -invariante, e utilizzare ciò per dimostrare il teorema spettrale per gli operatori normali.

### 8 Forme antisimmetriche

1. È vero che una matrice  $A$  è antisimmetrica se e soltanto se  $X^t AX = 0$  per ogni  $X$ ?
2. Dimostrare che una forma è antisimmetrica se e soltanto se la sua matrice ha le proprietà (8.3).
3. È vero che una matrice  $n \times n$  antisimmetrica è singolare, se  $n$  è dispari?
4. È vero che gli autovalori di una matrice reale antisimmetrica sono numeri immaginari puri?
- \*5. Sia  $S$  una matrice reale antisimmetrica. Dimostrare che  $I + S$  è invertibile, e che  $(I - S)(I + S)^{-1}$  è ortogonale.
- \*6. Sia  $A$  una matrice reale antisimmetrica.
- (a) Dimostrare che  $\det A \geq 0$ .
- (b) Dimostrare che se  $A$  è ad elementi interi  $\det A$  è il quadrato di un intero.
7. Sia  $\langle \cdot, \cdot \rangle$  una forma antisimmetrica su uno spazio vettoriale  $V$ . Definire l'ortogonalità, lo spazio annullatore e le forme non degeneri come nel § 2.
- (a) Dimostrare che la forma è non degenera se e solo se la matrice ad essa associata rispetto a una base qualsiasi è non singolare.
- (b) Dimostrare che se  $W$  è un sottospazio tale che la restrizione della forma a  $W$  è non degenera, allora  $V = W \oplus W^\perp$ .

- (c) Dimostrare che se la forma non è identicamente nulla esistono un sottospazio  $W$  e una base di  $W$  tali che la restrizione della forma a  $W$  è rappresentata, rispetto a tale base, dalla matrice  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ .
- (d) Dimostrare il teorema (8.6).

### 9 Sommario dei risultati, in notazione matriciale

1. Determinare la simmetria delle matrici  $AB + BA$  e  $AB - BA$  nei seguenti casi:

- (a)  $A, B$  simmetriche;
- (b)  $A, B$  hermitiane;
- (c)  $A, B$  antisimmetriche;
- (d)  $A$  simmetrica,  $B$  antisimmetrica.

2. Stabilire quali delle regole seguenti definiscono azioni di  $GL_n(\mathbb{C})$  sullo spazio  $\mathbb{C}^{n \times n}$  di tutte le matrici complesse:

$$P, A \mapsto PAP^t, (P^{-1})^t A (P^{-1}), (P^{-1})^t AP^t, P^{-1}AP^t, AP^t, P^t A.$$

3. (a) Per ciascuno dei seguenti tipi di matrici, descrivere i determinanti possibili:

- (i) reale ortogonale; (ii) complessa ortogonale; (iii) unitaria; (iv) hermitiana; (v) simplettica; (vi) reale simmetrica, definita positiva; (vii) reale simmetrica, definita negativa.

(b) Quali di questi tipi di matrici hanno soltanto autovalori reali?

4. (a) Sia  $E$  una matrice complessa. Dimostrare che la matrice  $\begin{bmatrix} I & E^* \\ -E & I \end{bmatrix}$  è invertibile.

(b) Trovare l'inversa, nella forma a blocchi, della matrice  $\begin{bmatrix} I & E^* \\ -E & I \end{bmatrix}$ .

\*5. (a) Dove sta l'errore nella seguente argomentazione? Sia  $P$  una matrice reale ortogonale. Sia  $X$  un autovettore di  $P$  (eventualmente complesso), associato all'autovalore  $\lambda$ . Allora  $X^t P^t X = (PX)^t X = \lambda X^t X$ . D'altra parte,  $X^t P^t X = X^t (P^{-1} X) = \lambda^{-1} X^t X$ . Pertanto  $\lambda = \lambda^{-1}$ , e quindi  $\lambda = \pm 1$ .

(b) Enunciare e dimostrare un teorema corretto basato su questa argomentazione.

\*6. Mostrare come sia possibile descrivere un elemento arbitrario di  $SO_4$  mediante rotazioni di due piani ortogonali in  $\mathbb{R}^4$ .

\*7. Sia  $A$  una matrice  $m \times n$  reale. Dimostrare che esistono matrici ortogonali  $P \in O_m$  e  $Q \in O_n$  tali che  $PAQ = D$  sia diagonale, con gli elementi diagonali non negativi.

## Capitolo 8

### Gruppi lineari

Di questi tempi l'angelo della topologia e il demone dell'algebra astratta lottano per l'anima di ogni singola disciplina della matematica.

Hermann Weyl

#### 1 I gruppi lineari classici

I sottogruppi del gruppo lineare generale  $GL_n$  sono chiamati *gruppi lineari*. In questo capitolo studieremo i gruppi lineari più importanti: il gruppo ortogonale, il gruppo unitario e il gruppo simplettico. Essi sono chiamati *gruppi classici*.

I gruppi classici si presentano come stabilizzatori rispetto ad alcune azioni naturali di  $GL_n$  sullo spazio delle matrici  $n \times n$ . La prima di tali azioni è quella che descrive il cambiamento di base in una forma bilineare. La regola

$$(1.1) \quad P, A \mapsto (P^t)^{-1} A P^{-1}$$

definisce un'azione di  $GL_n$  sull'insieme di tutte le matrici  $n \times n$ . Ciò è vero per un qualsiasi campo di scalari; tuttavia ci interesseremo, in particolare, del caso reale e del caso complesso. Come si è visto nel capitolo (1.15), l'orbita di una matrice  $A$  rispetto a tale azione è l'insieme delle matrici  $A'$  che rappresentano la forma  $X^t A Y$ , rispetto a basi diverse. Matrici appartenenti a una stessa orbita si dicono di solito *congruenti*. Ponendo  $Q = (P^t)^{-1}$ , si ottiene la definizione equivalente

$$(1.2) \quad A \text{ e } A' \text{ sono congruenti se } A' = Q A Q^t \text{ per qualche } Q \in GL_n(F).$$

La legge di Sylvester [cap. 7 (2.11)] descrive le varie orbite o classi di congruenza di matrici reali simmetriche. Ogni classe di congruenza di matrici reali simmetriche contiene una e una sola matrice della forma (2.10) (cap. 7). Il *gruppo ortogonale* (cfr. cap. 4) è lo stabilizzatore della matrice identica rispetto a tale azione. Come si è già visto, il gruppo ortogonale reale si indica con il simbolo  $O_n$ :

$$(1.3) \quad O_n = \{P \in GL_n(\mathbb{R}) \mid P^t P = I\}.$$

Il gruppo ortogonale complesso si definisce in modo analogo:

$$O_n(\mathbb{C}) = \{P \in GL_n(\mathbb{C}) \mid P^t P = I\}.$$

Lo stabilizzatore della *forma di Lorentz* [cap. 7 (2.1)], definita dalla matrice

$$I_{3,1} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix},$$

è chiamato il *gruppo di Lorentz*, e si denota con  $O_{3,1}(\mathbf{R})$  o semplicemente con  $O_{3,1}$ :

$$(1.4) \quad O_{3,1} = \{P \in GL_4(\mathbf{R}) \mid P^t I_{3,1} P = I_{3,1}\}.$$

Gli operatori lineari rappresentati da queste matrici vengono chiamati spesso *trasformazioni di Lorentz*. Gli indici (3, 1) posti in basso indicano la segnatura della matrice, ossia il numero di volte con cui compaiono +1 e -1. In modo analogo si può definire un gruppo  $O_{p,q}$  per una segnatura  $(p, q)$  qualsiasi.

L'azione (1.1) descrive anche il cambiamento di base in forme non simmetriche. Pertanto dal teorema (8.5) del capitolo 7 discende il risultato seguente:

(1.5) COROLLARIO *Se  $m$  è pari esiste un'unica classe di congruenza di matrici reali  $m \times m$  antisimmetriche non singolari.* ■

La forma antisimmetrica standard è definita dalla matrice  $2n \times 2n$   $J$  [cap. 7 (8.5)], e il suo stabilizzatore è detto *gruppo simplettico*:

$$(1.6) \quad SP_{2n}(\mathbf{R}) = \{P \in GL_{2n}(\mathbf{R}) \mid P^t J P = J\}.$$

Ancora una volta, il gruppo simplettico complesso  $SP_{2n}(\mathbf{C})$  si definisce in modo analogo.

Infine, il *gruppo unitario* si definisce per mezzo dell'azione

$$(1.7) \quad P, A \mapsto (P^*)^{-1} A P^{-1}.$$

Questa definizione ha senso solo nel caso in cui il campo degli scalari è il campo complesso. Così come accade con le forme bilineari, l'orbita di una matrice  $A$  è costituita dalle matrici che definiscono la forma  $\langle X, Y \rangle = X^* A Y$  rispetto a basi diverse [cfr. cap. 7 (4.12)]. Il gruppo unitario è lo stabilizzatore della matrice identica rispetto a tale azione:

$$(1.8) \quad U_n = \{P \mid P^* P = I\}.$$

Pertanto  $U_n$  è il gruppo delle matrici che rappresentano i cambiamenti di base che lasciano invariato il prodotto hermitiano standard [cap. 7 (4.2)]  $X^* Y$ .

L'aggettivo *speciale* viene aggiunto per indicare il sottogruppo delle matrici con determinante 1. Si hanno così altri gruppi:

*il gruppo lineare speciale*  $SL_n(\mathbf{R})$ : matrici  $n \times n$   $P$  con determinante 1;

*il gruppo ortogonale speciale*  $SO_n(\mathbf{R})$ : l'intersezione  $SL_n(\mathbf{R}) \cap O_n(\mathbf{R})$ ;

*il gruppo unitario speciale*  $SU_n$ : l'intersezione  $SL_n(\mathbf{C}) \cap U_n$ .

Le matrici simplettiche hanno determinante 1 (cosa peraltro non ovvia in base alla definizione), e pertanto il doppio significato dell'iniziale *S* non comporta problemi.

## 2 Il gruppo unitario speciale $SU_2$

Lo scopo principale di questo capitolo è quello di descrivere le proprietà geometriche dei gruppi lineari classici, considerandoli come sottoinsiemi degli spazi  $\mathbf{R}^{n \times n}$  o  $\mathbf{C}^{n \times n}$  di tutte le matrici  $n \times n$ . Conosciamo già la geometria di alcuni gruppi. Per esempio,  $GL_1(\mathbf{C}) = \mathbf{C}^*$  è il piano "bucato"  $\mathbf{C} - \{0\}$ . Inoltre, se  $p$  è una matrice  $1 \times 1$ , si ha  $p^* = \bar{p}$ . Pertanto

$$(2.1) \quad U_1 = \{p \in \mathbf{C}^* \mid \bar{p} p = 1\}.$$

Ricordiamo che  $U_1$  è l'insieme dei numeri complessi aventi valore assoluto 1, ossia la circonferenza unitaria nel piano complesso. Possiamo identificare  $U_1$  con la circonferenza unitaria in  $\mathbf{R}^2$ , di equazione

$$x_1^2 + x_2^2 = 1,$$

in virtù dell'applicazione che manda  $x_1 + x_2 i$  in  $(x_1, x_2)$ . Il gruppo  $SO_2$  delle rotazioni del piano è isomorfo a  $U_1$ . Anch'esso è una circonferenza, immersa in  $\mathbf{R}^{2 \times 2}$  mediante l'applicazione:

$$(2.2) \quad (x_1, x_2) \mapsto \begin{bmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{bmatrix}.$$

Descriveremo altre proprietà dei gruppi nei paragrafi successivi.

La *dimensione* di un gruppo lineare  $G$  è, grosso modo, il numero dei gradi di libertà di una matrice in  $G$ . Il gruppo  $SO_2$ , per esempio, ha dimensione 1; infatti una matrice in  $SO_2$  rappresenta una rotazione di un angolo  $\theta$ , e tale angolo è l'unico parametro necessario per determinare la rotazione. Studieremo la dimensione più accuratamente nel seguito (§ 7), ma prima vogliamo descrivere esplicitamente alcuni gruppi di dimensione piccola. La dimensione minima in cui compaiono gruppi davvero interessanti è 3, e tre di questi, precisamente  $SU_2$ ,  $SO_3$  e  $SL_2(\mathbf{R})$ , sono molto importanti. In questo paragrafo studieremo il gruppo unitario speciale  $SU_2$ .

Sia  $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  un elemento di  $SU_2$ , con  $a, b, c, d \in \mathbb{C}$ . Le equazioni che definiscono  $SU_2$  sono:  $P^*P = I$  e  $\det P = 1$ . In base alla regola di Cramer, si ha:

$$P^{-1} = (\det P)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Poiché  $P^{-1} = P^*$  per una matrice  $P \in SU_2$ , risulta  $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{d} \end{bmatrix}$ , ossia

$$(2.3) \quad \bar{a} = d, \quad \bar{b} = -c,$$

e quindi

$$(2.4) \quad P = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}.$$

Imponendo la condizione  $\det P = 1$  si ottiene:

$$(2.5) \quad \bar{a}a + \bar{b}b = 1.$$

Le condizioni (2.3) e (2.5) caratterizzano completamente gli elementi di una matrice in  $SU_2$ . La matrice  $P$  è descritta dal vettore unitario  $(a, b) \in \mathbb{C}^2$ , e viceversa ogni vettore unitario di  $\mathbb{C}^2$  individua una matrice  $P \in SU_2$  mediante la regola (2.4).

Se esprimiamo  $a, b$  mediante la parte reale e immaginaria, l'equazione (2.5) fornisce una corrispondenza biunivoca tra  $SU_2$  e i punti di  $\mathbb{R}^4$  appartenenti al luogo di equazione

$$(2.6) \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1.$$

Questa equazione è equivalente alla condizione (2.5), se poniamo  $a = x_1 + ix_2$  e  $b = x_3 + ix_4$ .

Il luogo (2.6) è chiamato la 3-sfera unitaria in  $\mathbb{R}^4$ , in analogia con la sfera unitaria in  $\mathbb{R}^3$ . Il numero 3 si riferisce alla sua dimensione, ossia al numero dei gradi di libertà di un punto sulla sfera. Così, ad esempio, la sfera unitaria in  $\mathbb{R}^3$

$$x_1^2 + x_2^2 + x_3^2 = 1,$$

essendo una superficie, è chiamata 2-sfera. La circonferenza unitaria in  $\mathbb{R}^2$ , essendo una curva, è chiamata 1-sfera. Denoteremo talvolta una sfera di dimensione  $d$  con  $S^d$ .

Un'applicazione biettiva  $f : S \rightarrow S'$  tra sottoinsiemi di spazi euclidei è un **omeomorfismo** se  $f$  e  $f^{-1}$  sono applicazioni continue (cfr. appendice, § 3). La corrispondenza tra  $SU_2$ , considerato come un sottoinsieme di  $\mathbb{C}^{2 \times 2}$ , e la sfera (2.6) è ovviamente continua, insieme con la sua inversa. Pertanto questi due spazi sono omeomorfi:

$$(2.7) \quad SU_2 \text{ è omeomorfo alla 3-sfera unitaria in } \mathbb{R}^4.$$

È conveniente identificare  $SU_2$  con la 3-sfera, cosa che si può fare rappresentando la matrice (2.4) mediante la sua prima riga, ossia il vettore  $(a, b) \in \mathbb{C}^2$ , oppure mediante il vettore  $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ . Si tratta di due modi diversi per indicare uno stesso elemento  $P$  del gruppo, e noi utilizzeremo indifferentemente l'uno o l'altro. Per la visualizzazione geometrica, le rappresentazioni  $P = (a, b)$  e  $P = (x_1, x_2, x_3, x_4)$  sono più convenienti.

Il fatto che la 3-sfera abbia una struttura di gruppo è notevole, perché per esempio è impossibile rendere la 2-sfera un gruppo con una legge di composizione continua. Infatti, un celebre teorema di topologia afferma che le uniche sfere con legge di gruppo continua sono la 1-sfera, che è realizzata come il gruppo delle rotazioni  $SO_2$ , e la 3-sfera  $SU_2$ .

Descriveremo ora le strutture algebriche dei sottoinsiemi di  $SU_2$  analoghi alle curve di latitudine costante e di longitudine costante sulla 2-sfera. Le matrici  $I, -I$  svolgeranno, rispettivamente, il ruolo del polo nord e del polo sud. Con la notazione vettoriale, esse sono i punti  $(\pm 1, 0, 0, 0)$  della sfera.

Se i poli della 2-sfera  $x_1^2 + x_2^2 + x_3^2 = 1$  sono situati nei punti  $(\pm 1, 0, 0)$ , allora le latitudini sono le circonferenze  $x_1 = c$ ,  $-1 < c < 1$ . Gli analoghi sulla 3-sfera  $SU_2$  di queste latitudini sono le superfici sulle quali la coordinata  $x_1$  è costante. Esse sono sfere di dimensione due, immerse in  $\mathbb{R}^4$  mediante le equazioni

$$(2.8) \quad x_1 = c, \quad x_2^2 + x_3^2 + x_4^2 = 1 - c^2, \quad \text{con } -1 < c < 1.$$

Questi insiemi possono essere descritti algebricamente come *classi di coniugio* in  $SU_2$ .

**(2.9) PROPOSIZIONE** *Ad eccezione di due classi speciali, le classi di coniugio in  $SU_2$  sono le latitudini, ossia gli insiemi definiti dalle equazioni (2.8). Fissato un numero reale  $c$  nell'intervallo  $(-1, 1)$ , l'insieme corrispondente è costituito da tutte le matrici  $P \in SU_2$  tali che  $\text{tr } P = 2c$ . Le classi di coniugio rimanenti sono  $\{I\}$  e  $\{-I\}$ , ciascuna formata da un solo elemento. Queste due classi costituiscono il centro  $Z = \{\pm I\}$  del gruppo  $SU_2$ .*

*Dimostrazione.* Il polinomio caratteristico della matrice  $P$  (2.4) è:

$$(2.10) \quad t^2 - (a + \bar{a})t + 1 = t^2 - 2x_1t + 1.$$

Tale polinomio ha una coppia  $\lambda, \bar{\lambda}$  di radici complesse coniugate sulla circonferenza unitaria: queste radici, ossia gli autovalori di  $P$ , dipendono soltanto dalla traccia di  $P$ ,  $\text{tr } P = 2x_1$ . Inoltre, matrici con tracce diverse hanno autovalori diversi. Per dimostrare la proposizione basta far vedere che la classe di coniugio di  $P$  contiene tutte le matrici di  $SU_2$  aventi gli stessi autovalori. I casi  $x_1 = 1, -1$  corrispondono alle due classi di coniugio speciali  $\{I\}, \{-I\}$ , sicché la dimostrazione è completata dal lemma seguente:

(2.11) LEMMA *Sia  $P$  un elemento di  $SU_2$ , con autovalori  $\lambda, \bar{\lambda}$ . Allora  $P$  è coniugata in  $SU_2$  alla matrice*

$$\begin{bmatrix} \lambda & \\ & \bar{\lambda} \end{bmatrix}.$$

*Dimostrazione.* In base al teorema spettrale per gli operatori normali [cap. 7 (7.3)], esiste una matrice unitaria  $Q$  tale che  $QPQ^*$  è diagonale. Occorre provare soltanto che  $Q$  può essere scelta in modo che abbia determinante 1. Sia  $\det Q = \delta$ . Poiché  $Q^*Q = I$ , si ha  $(\det Q^*)(\det Q) = \bar{\delta}\delta = 1$ ; pertanto  $\delta$  ha valore assoluto 1. Sia  $\epsilon$  una radice quadrata di  $\delta$ . Allora  $\bar{\epsilon}\epsilon = 1$ . La matrice  $Q_1 = \bar{\epsilon}Q$  appartiene a  $SU_2$ , e inoltre  $P_1 = Q_1PQ_1^*$  è diagonale. Gli elementi diagonali di  $P_1$  sono gli autovalori  $\lambda, \bar{\lambda}$ . Gli autovalori possono essere scambiati tra loro, se si vuole, per mezzo del coniugio mediante la matrice:

$$(2.12) \quad Q_2 = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix},$$

la quale è anch'essa un elemento di  $SU_2$ . ■

Introduciamo ora le longitudini di  $SU_2$ . Le longitudini sulla 2-sfera  $x_1^2 + x_2^2 + x_3^2 = 1$  possono essere descritte come le intersezioni della sfera con i piani contenenti i due poli  $(\pm 1, 0, 0)$ . Quando aggiungiamo una quarta variabile  $x_4$  per ottenere l'equazione della 3-sfera, un modo naturale di estendere questa definizione è quello di formare l'intersezione con un sottospazio di dimensione due di  $\mathbb{R}^4$  contenente i due poli  $\pm I$ . Essa è una circonferenza in  $SU_2$ , e noi considereremo tali circonferenze come le longitudini. Così, mentre le latitudini su  $SU_2$  sono 2-sfere, le *longitudini* sono 1-sfere, precisamente le "circonferenze massime" passanti per i poli.

Si noti che ogni punto  $P = (x_1, x_2, x_3, x_4)$  di  $SU_2$ , eccettuati i poli, è contenuto in una e una sola longitudine. Infatti, se  $P$  non è un polo,  $P$  e  $I$  sono linearmente indipendenti e pertanto generano un sottospazio  $V$  di  $\mathbb{R}^4$  di dimensione 2. L'intersezione  $SU_2 \cap V$  è l'unica longitudine che contiene  $P$ .

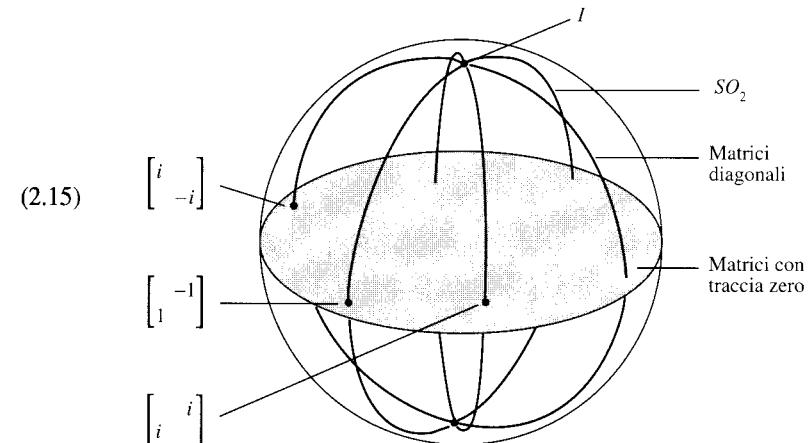
L'intersezione di  $SU_2$  con il piano  $W$  definito dalle equazioni  $x_3 = x_4 = 0$  è una longitudine particolarmente espressiva. Utilizzando la notazione matriciale, tale

circonferenza massima è costituita dalle matrici diagonali in  $SU_2$ , che formano un sottogruppo  $T$ :

$$(2.13) \quad T = \left\{ \begin{bmatrix} \lambda & \\ & \bar{\lambda} \end{bmatrix} \mid \lambda\bar{\lambda} = 1 \right\}.$$

Le altre longitudini sono descritte nella proposizione seguente.

(2.14) PROPOSIZIONE *Le longitudini di  $SU_2$  sono i sottogruppi coniugati  $QTQ^*$  del sottogruppo  $T$ .*



Alcune latitudini e longitudini in  $SU_2$ .

Nella figura (2.15) la 3-sfera  $SU_2$  è proiettata da  $\mathbb{R}^4$  sul disco unitario nel piano. La classe di coniugio illustrata è la latitudine "equatoriale" in  $\mathbb{R}^4$ , che è definita dall'equazione  $x_1 = 0$ . Così come la proiezione ortogonale di una circonferenza da  $\mathbb{R}^3$  su  $\mathbb{R}^2$  è un'ellisse, la proiezione di questa 2-sfera da  $\mathbb{R}^4$  su  $\mathbb{R}^3$  è un ellissoide, e l'ulteriore proiezione di tale ellissoide sul piano è il disco ellittico illustrato.

*Dimostrazione.* Il punto centrale della dimostrazione è provare che ogni sottogruppo coniugato  $QTQ^*$  è una longitudine. Il lemma (2.11) afferma che ogni elemento  $P \in SU_2$  appartiene a uno di questi sottogruppi coniugati (sebbene i ruoli di  $Q$  e  $Q^*$  siano stati scambiati). Poiché ogni matrice  $P \neq \pm I$  è contenuta in un'unica longitudine, ne segue che ogni longitudine è uno dei sottogruppi  $QTQ^*$ .

Proviamo dunque che un sottogruppo coniugato  $QTQ^*$  è una longitudine. Il motivo per cui ciò è vero è che il coniugio mediante un elemento fissato  $Q$  è un

operatore lineare che manda il sottospazio  $W$  in un altro sottospazio. Calcoleremo esplicitamente il coniugato per rendere chiaro questo punto. Sia ad esempio  $Q$  la matrice (2.4). Denotiamo con  $w = (w_1, w_2, 0, 0)$  un elemento variabile di  $W$ , e poniamo  $z = w_1 + w_2 i$ . Allora:

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \begin{bmatrix} z \\ \bar{z} \end{bmatrix} \begin{bmatrix} a & -b \\ \bar{b} & a \end{bmatrix} = \begin{bmatrix} a\bar{a}z + b\bar{b}\bar{z} & ab(\bar{z} - z) \\ * & * \end{bmatrix}.$$

Calcolando tali elementi, risulta che  $w$  viene mandato nel vettore  $u = (u_1, u_2, u_3, u_4)$ , dove

$$u_1 = w_1,$$

$$u_2 = (x_1^2 + x_2^2 - x_3^2 - x_4^2)w_2,$$

$$u_3 = 2(x_1x_4 + x_2x_3)w_2,$$

$$u_4 = 2(x_2x_4 - x_1x_3)w_2.$$

Le coordinate  $u_i$  sono combinazioni lineari reali di  $(w_1, w_2)$ . Ciò prova che l'applicazione  $w \mapsto u$  è un'applicazione lineare reale. Pertanto la sua immagine  $V$  è un sottospazio di  $\mathbb{R}^4$ . Il sottogruppo coniugato  $QTQ^*$  è  $SU_2 \cap V$ . Poiché  $QTQ^*$  contiene i poli  $\pm I$ , anche  $V$  possiede tale proprietà, e ciò dimostra che  $QTQ^*$  è una longitudine. ■

Descriviamo ora brevemente un'altra configurazione geometrica. Come abbiamo visto, il sottogruppo  $T$  delle matrici diagonali è una circonferenza massima sulla 3-sfera  $SU_2$ . Le classi laterali sinistre di  $T$ , ossia gli insiemi della forma  $QT$ , con  $Q \in SU_2$ , sono anch'esse circonferenze massime, e costituiscono una partizione del gruppo  $SU_2$ . Pertanto la 3-sfera possiede una partizione in circonferenze massime. Questa configurazione molto interessante è chiamata la *fibrazione di Hopf*.

### 3 La rappresentazione ortogonale di $SU_2$

Abbiamo visto nell'ultimo paragrafo che le classi di coniugio nel gruppo unitario speciale  $SU_2$  sono sfere di dimensione due. Poiché le classi di coniugio sono orbite rispetto all'azione di coniugio,  $SU_2$  agisce su tali sfere. In questo paragrafo dimostreremo che il coniugio mediante un elemento  $P \in SU_2$  agisce su ciascuna di queste sfere come una *rotazione*, e che l'applicazione che manda  $P$  nella matrice di tale rotazione definisce un omomorfismo suriettivo

$$(3.1) \quad \varphi : SU_2 \rightarrow SO_3,$$

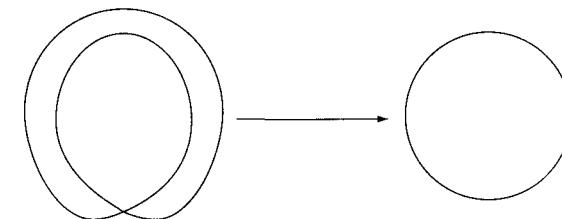
il cui nucleo è il centro  $Z = \{\pm I\}$  di  $SU_2$ . Questo omomorfismo è chiamato la *rappresentazione ortogonale* di  $SU_2$ . Essa rappresenta una matrice complessa  $2 \times 2$   $P$  in  $SU_2$  mediante una matrice di rotazione  $3 \times 3$  reale  $\varphi(P)$ .

Il modo più sicuro di dimostrare che  $P$  agisce ruotando una classe di coniugio può essere quello di scrivere esplicitamente la matrice che rappresenta la rotazione, cosa che faremo in (3.11). Tuttavia, la formula per  $\varphi(P)$  è complicata e non è particolarmente illuminante, quindi è meglio descrivere  $\varphi$  indirettamente, come faremo ora. Prima esamineremo l'applicazione dal punto di vista geometrico.

Poiché il nucleo di  $\varphi$  è  $\{\pm I\}$ , le sue classi laterali sono gli insiemi  $\{\pm P\}$ , che formano le fibre dell'omomorfismo. Pertanto ogni elemento di  $SO_3$  corrisponde ad una coppia di matrici unitarie che differiscono per il segno. A causa di ciò, il gruppo  $SU_2$  è chiamato *rivestimento doppio* del gruppo  $SO_3$ .

L'applicazione  $\mu : SO_3 \rightarrow SO_3$  della 1-sfera in sé, definita da  $\rho_\theta \mapsto \rho_{2\theta}$ , è un altro esempio di rivestimento doppio. Il suo nucleo è costituito anch'esso da due elementi: l'identità e la rotazione di  $\pi$ . Ogni fibra di  $\mu$  contiene due rotazioni:  $\rho_\theta$  e  $\rho_{\pi+\theta}$ .

(3.2)



Un rivestimento doppio della 1-sfera.

La rappresentazione ortogonale può essere usata per determinare la struttura topologica del gruppo delle rotazioni. Con la notazione vettoriale, se  $P = (x_1, \dots, x_4)$ , allora  $-P = (-x_1, \dots, -x_4)$ , e il punto  $-P$  è chiamato l'*antipodo* di  $P$ . Pertanto, poiché i punti del gruppo delle rotazioni corrispondono alle classi laterali  $\{\pm P\}$ , il gruppo  $SO_3$  può essere ottenuto identificando tra loro punti antipodali sulla 3-sfera  $SU_2$ . Lo spazio così ottenuto è chiamato lo *spazio proiettivo reale di dimensione 3*:

$$(3.3) \quad SO_3 \text{ è omeomorfo allo spazio proiettivo reale di dimensione 3.}$$

I punti dello spazio proiettivo reale di dimensione 3 sono inoltre in corrispondenza biunivoca con le rette passanti per l'origine (ossia i sottospazi di dimensione uno) di  $\mathbb{R}^4$ . Ogni retta per l'origine incontra la sfera unitaria in una coppia di punti antipodali.

Come abbiamo osservato nel capitolo 4 (§8), ogni elemento di  $SO_3$  diverso dall'identità può essere descritto mediante una coppia  $(v, \theta)$ , dove  $v$  è un vettore unitario sull'asse di rotazione e  $\theta$  è l'angolo di rotazione. Tuttavia, le due coppie  $(v, \theta)$  e  $(-v, -\theta)$  rappresentano la stessa rotazione. La scelta di una di tali coppie

corrisponde, in fisica, alla scelta di uno *spin*. Non è possibile fare una scelta di spin che vari in modo continuo sull'intero gruppo. Invece, le due scelte possibili definiscono un rivestimento doppio di  $SO_3 - \{I\}$ . L'insieme di tutte le coppie  $(v, \theta)$  può essere realizzato come lo spazio prodotto  $S \times \Theta$ , dove  $S$  è la 2-sfera dei vettori unitari in  $\mathbb{R}^3$ , e  $\Theta$  è l'insieme degli angoli non nulli  $0 < \theta < 2\pi$ . Esiste un'applicazione da questo spazio prodotto a  $SO_3$ :

$$(3.4) \quad \psi : S \times \Theta \rightarrow SO_3 - \{I\},$$

definita mandando  $(v, \theta)$  nella rotazione intorno a  $v$  di un angolo  $\theta$ . L'applicazione  $\psi$  è un rivestimento doppio di  $SO_3 - \{I\}$ , poiché ogni rotazione non banale è associata a due coppie:  $(v, \theta)$ ,  $(-v, -\theta)$ .

Abbiamo ora due rivestimenti doppi di  $SO_3 - \{I\}$ , precisamente  $S \times \Theta$  e  $SU_2 - \{\pm I\}$ , ed è plausibile che essi siano equivalenti. Infatti:

(3.5) PROPOSIZIONE *Esiste un omeomorfismo  $h : (SU_2 - \{\pm I\}) \rightarrow S \times \Theta$  che è compatibile con le applicazioni (3.1)  $\varphi : SU_2 \rightarrow SO_3$  e (3.4)  $\psi : S \times \Theta \rightarrow SO_3 - \{I\}$ , ossia tale che  $\psi \circ h = \varphi$ .*

Tale applicazione  $h$  non è un omomorfismo di gruppi perché né il suo dominio né il suo codominio sono gruppi.

La proposizione (3.5) non è molto difficile da dimostrare, ma resta comunque un po' ambigua, poiché esistono due omeomorfismi siffatti. Essi differiscono per uno scambio di spin. D'altra parte, l'esistenza di un tale omeomorfismo discende da un teorema generale di topologia, poiché lo spazio  $SU_2 - \{\pm I\}$  è semplicemente connesso. (Uno spazio semplicemente connesso è uno spazio connesso per archi e in cui ogni cappio può essere contratto in modo continuo ad un punto.) È meglio lasciare questa dimostrazione ai topologi. ■

Dunque ogni elemento di  $SU_2 - \{\pm I\}$  può essere descritto come una rotazione di  $\mathbb{R}^3$  insieme con una scelta di spin. Perciò  $SU_2$  è chiamato spesso il *gruppo degli spin*.

Passiamo ora a calcolare l'omomorfismo  $\varphi$ , e per cominciare dobbiamo scegliere una classe di coniugio. Conviene scegliere la classe costituita dalle matrici in  $SU_2$  con traccia zero, che è definita da  $x_1 = 0$  e che è illustrata nella figura (2.15). Il gruppo agisce allo stesso modo sulle altre classi. Denotiamo con  $C$  la classe di coniugio delle matrici con traccia zero. Un elemento  $A$  di  $C$  sarà una matrice della forma:

$$(3.6) \quad A = \begin{bmatrix} y_2 i & y_3 + y_4 i \\ -y_3 + y_4 i & -y_2 i \end{bmatrix},$$

dove

$$(3.7) \quad y_2^2 + y_3^2 + y_4^2 = 1.$$

Si noti che tale matrice è *anti-hermitiana*, ossia ha la proprietà:

$$(3.8) \quad A^* = -A.$$

(Non abbiamo incontrato finora le matrici anti-hermitiane, ma non sono molto diverse dalle matrici hermitiane. Infatti,  $A$  è anti-hermitiana se e soltanto se  $H = iA$  è hermitiana.) Le matrici anti-hermitiane  $2 \times 2$  con traccia zero formano uno spazio vettoriale reale  $V$  di dimensione 3, con base

$$(3.9) \quad \mathbf{B} = \left[ \begin{bmatrix} i & \\ & -i \end{bmatrix}, \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}, \begin{bmatrix} & i \\ i & \end{bmatrix} \right].$$

Con le notazioni usate in (3.6), si ha  $A = \mathbf{B}Y$ , dove  $Y = (y_2, y_3, y_4)^T$ . Pertanto la base  $\mathbf{B}$  corrisponde alla base canonica  $(e_2, e_3, e_4)$  nello spazio  $\mathbb{R}^3$ , e la relazione (3.7) dice che la classe di coniugio in questione è rappresentata come la sfera unitaria in tale spazio.

Si noti che  $SU_2$  agisce mediante il coniugio sull'intero spazio  $V$  delle matrici anti-hermitiane con traccia zero, e non soltanto sulla sua sfera unitaria. Infatti, se  $A \in V$ ,  $P \in SU_2$ , e se  $B = PAP^* = PAP^{-1}$ , allora  $\text{tr } B = 0$ , e  $B^* = (PAP^*)^* = PA^*P^* = P(-A)P^* = -B$ . Inoltre, il coniugio mediante una matrice fissata  $P$  individua un operatore lineare su  $V$ , poiché  $P(A + A')P^* = PAP^* + PA'P^*$ , e se  $r$  è un numero reale, allora  $P(rA)P^* = rPAP^*$ . La matrice di tale operatore lineare è, per definizione,  $\varphi(P)$ . Per determinare esplicitamente questa matrice, coniughiamo la base (3.9) mediante  $P$  e riscriviamo il risultato per mezzo della base. Per esempio,

$$(3.10) \quad \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \begin{bmatrix} i & \\ & -i \end{bmatrix} \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} = i \begin{bmatrix} a\bar{a} - b\bar{b} & -2ab \\ -2\bar{a}\bar{b} & b\bar{b} - a\bar{a} \end{bmatrix}.$$

Le coordinate di questa matrice sono  $y_2 = a\bar{a} - b\bar{b}$ ,  $y_3 = i(-ab + \bar{a}\bar{b})$ ,  $y_4 = -(ab + \bar{a}\bar{b})$ . Esse formano la prima colonna della matrice  $\varphi(P)$ . Effettuando calcoli simili per le altre colonne, si ottiene la matrice:

$$(3.11) \quad \begin{bmatrix} (a\bar{a} - b\bar{b}) & i(\bar{a}b - a\bar{b}) & (\bar{a}b + a\bar{b}) \\ i(\bar{a}b - ab) & \frac{1}{2}(a^2 + \bar{a}^2 + b^2 + \bar{b}^2) & \frac{i}{2}(a^2 - \bar{a}^2 - b^2 + \bar{b}^2) \\ -(\bar{a}b + ab) & \frac{i}{2}(\bar{a}^2 - a^2 + \bar{b}^2 - b^2) & \frac{1}{2}(a^2 + \bar{a}^2 - b^2 - \bar{b}^2) \end{bmatrix}.$$

Non faremo uso dei calcoli precedenti; anche senza di essi, sappiamo che  $\varphi(P)$  è una matrice reale  $3 \times 3$ , poiché essa è la matrice di un operatore lineare su uno spazio vettoriale reale  $V$  di dimensione 3.

(3.12) LEMMA *L'applicazione che manda  $P$  in  $\varphi(P)$  risulta un omomorfismo  $SU_2 \rightarrow GL_3(\mathbb{R})$ .*

*Dimostrazione.* Dalla proprietà associativa [cap. 5 (5.1)] dell'azione di coniugio segue che  $\varphi$  è compatibile con la moltiplicazione. Infatti, l'azione di un prodotto  $PQ$  su una matrice  $A$  è  $(PQ)A(PQ)^* = P(QAQ^*)P^*$ , che è la composizione delle azioni di coniugio mediante  $P$  e mediante  $Q$ . Poiché la matrice della composizione di operatori lineari è la matrice prodotto,  $\varphi(PQ) = \varphi(P)\varphi(Q)$ , ed essendo  $\varphi$  compatibile con la moltiplicazione, si ha  $\varphi(P^{-1})\varphi(P) = \varphi(I_2) = I_3$ . Pertanto  $\varphi(P)$  è invertibile per ogni  $P$ , e quindi  $\varphi$  è un omomorfismo da  $SU_2$  a  $GL_3(\mathbb{R})$ , come asserito. ■

(3.13) LEMMA *Per ogni  $P$ ,  $\varphi(P) \in SO_3$ . Pertanto l'applicazione che manda  $P$  in  $\varphi(P)$  risulta un omomorfismo  $SU_2 \rightarrow SO_3$ .*

*Dimostrazione.* Si potrebbe dimostrare questo lemma utilizzando la formula (3.11). Per dare invece una dimostrazione teorica, osserviamo che il prodotto scalare su  $\mathbb{R}^3$  si trasforma in una forma bilineare su  $V$  con un'espressione semplice ed elegante in termini di matrici. Utilizzando le notazioni di (3.6), definiamo  $\langle A, A' \rangle = y_2y'_2 + y_3y'_3 + y_4y'_4$ . Allora risulta:

$$(3.14) \quad \langle A, A' \rangle = -\frac{1}{2} \operatorname{tr}(AA').$$

Ciò si dimostra facendo il calcolo:

$$AA' = \begin{bmatrix} -(y_2y'_2 + y_3y'_3 + y_4y'_4) & * \\ * & -(y_2y'_2 + y_3y'_3 + y_4y'_4) \end{bmatrix},$$

e pertanto  $\operatorname{tr}(AA') = -2\langle A, A' \rangle$ .

Tale espressione per il prodotto scalare prova che esso è conservato dal coniugio mediante un elemento  $P \in SU_2$ :

$$\langle PAP^*, PA'P^* \rangle = -\frac{1}{2} \operatorname{tr}(PAP^*PA'P^*) = -\frac{1}{2} \operatorname{tr}(AA') = \langle A, A' \rangle.$$

Oppure, in termini dei vettori delle coordinate,  $(\varphi(P)Y \cdot \varphi(P)Y') = (Y \cdot Y')$ . Ne segue che  $\varphi(P)$  appartiene al gruppo ortogonale  $O_3 = O_3(\mathbb{R})$  [cap. 4 (5.13)].

Per completare la dimostrazione, verifichiamo che  $\varphi(P)$  ha determinante 1 per ogni  $P \in SU_2$ . Infatti, essendo una sfera,  $SU_2$  è connesso per archi. Pertanto uno solo dei due valori possibili  $\pm 1$  può essere assunto dalla funzione continua

$\det \varphi(P)$ . Poiché  $\varphi(I_2) = I_3$  e  $\det I_3 = 1$ , il valore è sempre +1, e  $\varphi(P) \in SO_3$ , come richiesto. ■

(3.15) LEMMA  $\ker \varphi = \{\pm I\}$ .

*Dimostrazione.* Il nucleo di  $\varphi$  è costituito dalle matrici  $P \in SU_2$  che agiscono in modo banale su  $V$ , ossia sono tali che  $PAP^* = A$  per ogni matrice anti-hermitiana con traccia zero. Supponiamo che  $P$  abbia la proprietà  $PAP^* = A$ , ossia  $PA = AP$ , per ogni  $A \in V$ . Applicando questa proprietà alle matrici della base (3.9) si ottiene  $b = 0$ ,  $a = \bar{a}$ , ciò che dà luogo alle due possibilità:  $P = \pm I$ , e tali matrici appartengono al nucleo. Pertanto  $\ker \varphi = \{\pm I\}$ , come asserito. ■

(3.16) LEMMA *L'immagine dell'applicazione  $\varphi$  è  $SO_3$ .*

*Dimostrazione.* Innanzitutto calcoliamo esplicitamente  $\varphi(P)$  sul sottogruppo  $T$  delle matrici diagonali in  $SU_2$ . Poniamo:  $z = y_3 + y_4i$ . Allora si ha

$$(3.17) \quad PAP^* = \begin{bmatrix} a & \\ \bar{a} & \end{bmatrix} \begin{bmatrix} y_2i & z \\ -\bar{z} & -y_2i \end{bmatrix} \begin{bmatrix} \bar{a} & \\ a & \end{bmatrix} = \begin{bmatrix} y_2i & a^2z \\ -\bar{a}^2\bar{z} & -y_2i \end{bmatrix}.$$

Pertanto  $\varphi(P)$  lascia fissa la prima coordinata  $y_2$  e moltiplica  $z$  per  $a^2$ . Poiché  $|a| = 1$ , possiamo scrivere  $a = e^{i\theta}$ . La moltiplicazione per  $a^2 = e^{2i\theta}$  definisce una rotazione di un angolo  $2\theta$  del piano complesso  $z$ . Pertanto risulta:

$$(3.18) \quad \varphi(P) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos 2\theta & -\sin 2\theta \\ 0 & \sin 2\theta & \cos 2\theta \end{bmatrix}.$$

Ciò prova che l'immagine di  $\varphi$  in  $SO_3$  contiene il sottogruppo  $H$  di tutte le rotazioni intorno al punto  $(1, 0, 0)^t$ . Tale punto corrisponde alla matrice  $E = \begin{bmatrix} i & \\ & -i \end{bmatrix}$ . Poiché la sfera unitaria  $C$  è una classe di coniugio, l'azione di  $SU_2$  è transitiva e quindi, se  $Y$  è un vettore unitario arbitrario in  $\mathbb{R}^3$ , esiste un elemento  $Q \in SU_2$  tale che  $\varphi(Q)(1, 0, 0)^t = Y$ , o, con la notazione matriciale, tale che  $QEQ^* = A$ . Il sottogruppo coniugato  $\varphi(Q)H\varphi(Q)^*$  delle rotazioni intorno a  $Y$  è contenuto anch'esso nell'immagine di  $\varphi$ . Poiché ogni elemento di  $SO_3$  è una rotazione,  $\varphi$  è suriettiva. ■

Le classi laterali che costituiscono la fibrazione di Hopf, menzionata alla fine dell'ultimo paragrafo, sono le fibre di un'applicazione suriettiva continua:

$$(3.19) \quad \pi : S^3 \rightarrow S^2$$

dalla 3-sfera alla 2-sfera. Per definire  $\pi$ , interpretiamo  $S^3$  come il gruppo unitario speciale  $SU_2$ , e  $S^2$  come la classe di coniugio  $C$  delle matrici con traccia zero, come sopra. Poniamo  $E = \begin{bmatrix} i & \\ & -i \end{bmatrix}$ , e definiamo  $\pi(P) = PEP^*$  per ogni  $P \in SU_2$ . La dimostrazione della proposizione seguente è lasciata come esercizio.

(3.20) PROPOSIZIONE *Le fibre dell'applicazione  $\pi$  sono le classi laterali sinistre  $QT$  del sottogruppo  $T$  delle matrici diagonali in  $SU_2$ .* ■

#### 4 Il gruppo lineare speciale $SL_2(\mathbb{R})$

Poiché il gruppo unitario speciale è una sfera, è un insieme compatto. Come esempio di gruppo non compatto, descriveremo il gruppo lineare speciale  $SL_2(\mathbb{R})$ . Per semplificare la notazione, denotiamo in questo paragrafo  $SL_2(\mathbb{R})$  con  $SL_2$ .

Le matrici  $2 \times 2$  invertibili agiscono mediante la moltiplicazione a sinistra sullo spazio  $\mathbb{R}^2$  dei vettori colonna, e possiamo considerare l'azione associata sui raggi in  $\mathbb{R}^2$ . Un raggio è una semiretta  $R = \{rX \mid r \geq 0\}$ . L'insieme dei raggi è in corrispondenza biunivoca con l'insieme dei punti della circonferenza unitaria  $S^1$ , e precisamente il raggio  $R$  corrisponde al punto  $R \cap S^1$ .

Il gruppo  $SL_2$  agisce mediante la moltiplicazione a sinistra sull'insieme dei raggi. Denotiamo con  $H$  lo stabilizzatore del raggio  $R_1 = \{re_1\}$  in  $SL_2(\mathbb{R})$ . Esso è costituito dalle matrici

$$(4.1) \quad B = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix},$$

dove  $a$  è positivo e  $b$  è arbitrario.

Il gruppo delle rotazioni  $SO_2$  è un altro sottogruppo di  $SL_2$ , e agisce transitivamente sull'insieme dei raggi.

(4.2) PROPOSIZIONE *L'applicazione  $f : SO_2 \times H \rightarrow SL_2$  definita da  $f(Q, B) = QB$  è un omeomorfismo (ma non è un omomorfismo di gruppi).*

*Dimostrazione.* Si noti che  $H \cap SO_2 = \{I\}$ . Pertanto  $f$  è iniettiva [cap. 2 (8.6)]. Per dimostrare la suriettività di  $f$ , sia  $P$  un elemento arbitrario di  $SL_2$ , e sia  $R_1$  il raggio  $\{re_1 \mid r \geq 0\}$ . Scegliamo una rotazione  $Q \in SO_2$  tale che  $PR_1 = QR_1$ . Allora  $Q^{-1}P$  appartiene allo stabilizzatore  $H$ , diciamo  $Q^{-1}P = B$ , oppure

$$(4.3) \quad P = QB.$$

Poiché  $f$  è definita mediante la moltiplicazione tra matrici, è un'applicazione continua. Inoltre, nella costruzione dell'applicazione inversa, la rotazione  $Q$  dipende

in modo continuo da  $P$ , poiché il raggio  $PR_1$  dipende in modo continuo da  $P$ . Allora  $B = Q^{-1}P$  è anch'essa una funzione continua di  $P$ , e ciò prova che  $f^{-1}$  è un'applicazione continua. ■

Si noti che  $H$  può essere identificato, mediante la legge  $B \leftrightarrow (a, b)$ , con lo spazio prodotto  $\{\text{reali positivi}\} \times \mathbb{R}$ . Ora, lo spazio dei reali positivi è omeomorfo, mediante la funzione logaritmo, allo spazio  $\mathbb{R}$  di tutti i numeri reali. Pertanto  $H$  è omeomorfo a  $\mathbb{R}^2$ . Poiché  $SO_2$  è una circonferenza, si ottiene che:

(4.4)  *$SL_2(\mathbb{R})$  è omeomorfo allo spazio prodotto  $S^1 \times \mathbb{R}^2$ .*

Il gruppo lineare speciale può essere messo in relazione con il gruppo di Lorentz  $O_{2,1}$  (dello spazio-tempo  $\mathbb{R}^3$ ) mediante un procedimento analogo a quello usato nel paragrafo 3 per la rappresentazione ortogonale di  $SU_2$ . Siano  $y_1, y_2, t$  le coordinate in  $\mathbb{R}^3$ , con la forma di Lorentz:

$$(4.5) \quad y_1y'_1 + y_2y'_2 - tt' = 1,$$

e sia  $W$  lo spazio delle matrici reali con traccia zero. Utilizzando la base

$$(4.6) \quad \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}, \quad \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \quad \begin{bmatrix} & 1 \\ -1 & \end{bmatrix},$$

associamo ad un vettore delle coordinate  $(y_1, y_2, t)^t$  la matrice

$$(4.7) \quad A = \begin{bmatrix} y_1 & y_2 + t \\ y_2 - t & -y_1 \end{bmatrix}.$$

Utilizziamo questa rappresentazione delle matrici con traccia zero poiché su tali matrici la forma di Lorentz (4.5) ammette una interpretazione matriciale semplice:

$$(4.8) \quad \langle A, A' \rangle = y_1y'_1 + y_2y'_2 - tt' = \frac{1}{2} \operatorname{tr}(AA').$$

Il gruppo  $SL_2$  agisce su  $W$  mediante il coniugio:

$$(4.9) \quad P, A \mapsto PAP^{-1},$$

e tale azione conserva la forma di Lorentz su  $W$ , poiché:

$$\operatorname{tr}(AA') = \operatorname{tr}((PAP^{-1})(PA'P^{-1})),$$

come nel paragrafo precedente. Poiché il coniugio è un operatore lineare su  $W$ , esso definisce un omomorfismo  $\varphi : SL_2 \rightarrow GL_3(\mathbb{R})$ . Inoltre, poiché il coniugio conserva la forma di Lorentz, l'immagine  $\varphi(P)$  di  $P$  è un elemento di  $O_{2,1}$ .

(4.10) TEOREMA Il nucleo dell'omomorfismo  $\varphi$  è il sottogruppo  $\{\pm I\}$ , e l'immagine è la componente连通的 per archi  $O_{2,1}^0$  di  $O_{2,1}$  contenente l'identità  $I$ . Pertanto  $O_{2,1}^0 \approx SL_2(\mathbb{R})/\{\pm I\}$ .

Si può dimostrare che il gruppo di Lorentz  $O_{2,1}$  ha quattro componenti connesse per archi.

Il fatto che il nucleo di  $\varphi$  è  $\{\pm I\}$  si verifica facilmente, e l'ultima asserzione del teorema segue dalle altre. Omettiamo la dimostrazione del fatto che l'immagine di  $\varphi$  è il sottogruppo  $O_{2,1}^0$ . ■

## 5 Sottogruppi a un parametro

Nel capitolo 4, abbiamo definito l'esponenziale di una matrice mediante la serie:

$$(5.1) \quad e^A = I + \frac{1}{1!} A + \frac{1}{2!} A^2 + \frac{1}{3!} A^3 + \dots$$

Utilizzeremo ora questa funzione per descrivere gli omomorfismi dal gruppo additivo dei numeri reali al gruppo lineare generale, che sono funzioni differenziabili della variabile  $t \in \mathbb{R}$ . Un omomorfismo con queste caratteristiche è chiamato un *sottogruppo a un parametro* di  $GL_n$ . (In realtà, questo uso dell'espressione "sottogruppo a un parametro" per descrivere l'omomorfismo non è appropriato. Tale espressione dovrebbe essere riferita all'immagine di  $\varphi$ .)

### (5.2) PROPOSIZIONE

- (a) Sia  $A$  una matrice reale o complessa arbitraria, e si denoti  $GL_n(\mathbb{R})$  o  $GL_n(\mathbb{C})$ , a seconda dei casi, con  $GL_n$ . L'applicazione  $\varphi : \mathbb{R} \rightarrow GL_n$  definita da  $\varphi(t) = e^{tA}$  è un omomorfismo di gruppi.
- (b) Viceversa, sia  $\varphi : \mathbb{R} \rightarrow GL_n$  un omomorfismo che sia una funzione differenziabile della variabile  $t \in \mathbb{R}$ , e si denoti con  $A$  la sua derivata  $\varphi'(0)$  nell'origine. Allora  $\varphi(t) = e^{tA}$  per ogni  $t$ .

*Dimostrazione.* Fissati arbitrariamente due numeri reali  $r, s$ , le due matrici  $rA$  e  $sA$  commutano tra loro. Pertanto la proposizione (8.9b) del capitolo 4 assicura che

$$(5.3) \quad e^{(r+s)A} = e^{rA} e^{sA}.$$

Ciò prova che  $\varphi(t) = e^{tA}$  è un omomorfismo. Viceversa, sia  $\varphi$  un omomorfismo differenziabile  $\mathbb{R} \rightarrow GL_n$ . L'ipotesi che  $\varphi$  sia un omomorfismo permette di calcolare la sua derivata in ogni punto. Precisamente, essa dice che  $\varphi(t + \Delta t) = \varphi(\Delta t)\varphi(t)$  e  $\varphi(t) = \varphi(0)\varphi(t)$ . Ne consegue che

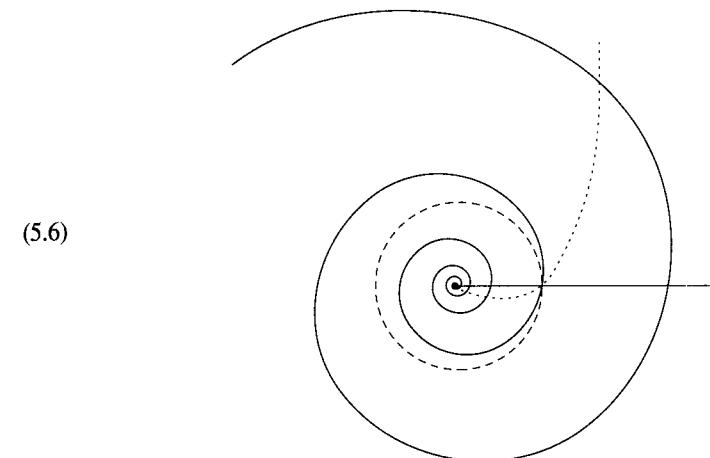
$$(5.4) \quad \frac{\varphi(t + \Delta t) - \varphi(t)}{\Delta t} = \frac{\varphi(\Delta t) - \varphi(0)}{\Delta t} \varphi(t).$$

Facendo tendere  $\Delta t \rightarrow 0$ , si ottiene  $\varphi'(t) = \varphi'(0)\varphi(t) = A\varphi(t)$ . Pertanto  $\varphi(t)$  è una funzione a valori matriciali che risolve l'equazione differenziale

$$(5.5) \quad \frac{d\varphi}{dt} = A\varphi.$$

La funzione  $e^{tA}$  è un'altra soluzione, ed entrambe le soluzioni assumono il valore  $I$  per  $t = 0$ . Quindi  $\varphi(t) = e^{tA}$  [cfr. cap. 4 (8.14)]. ■

In base alla proposizione appena dimostrata, i sottogruppi a un parametro hanno tutti la forma  $\varphi(t) = e^{tA}$ . Essi sono in corrispondenza biunivoca con le matrici  $n \times n$ .



Alcuni sottogruppi a un parametro di  $\mathbb{C}^* = GL_1(\mathbb{C})$ .

Supponiamo ora che sia dato un sottogruppo  $G$  di  $GL_n$ . Possiamo chiederci quali sono i sottogruppi a un parametro di  $G$ , ossia gli omomorfismi  $\varphi : \mathbb{R} \rightarrow G$ , o, equivalentemente, gli omomorfismi da  $\mathbb{R}$  a  $GL_n$  la cui immagine è contenuta in  $G$ . Poiché un sottogruppo a un parametro di  $GL_n$  è determinato da una matrice, ciò equivale a chiedere quali sono le matrici  $A$  tali che  $e^{tA} \in G$  per ogni  $t$ . Si dimostra che i gruppi lineari di dimensione positiva possiedono sempre sottogruppi a un parametro e inoltre che questi non sono difficili da determinare per un gruppo particolare assegnato.

### (5.7) Esempi

- (a) La parametrizzazione usuale della circonferenza unitaria nel piano complesso è un sottogruppo a un parametro di  $U_1$ :

$$t \mapsto e^{ti} = \cos t + i \sin t.$$

(b) Un esempio collegato al precedente si ottiene per  $SO_2$ , ponendo

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \text{ Allora } e^{tA} = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}.$$

Questa è la parametrizzazione standard delle matrici di rotazione.

Negli esempi (a) e (b), l'immagine dell'omomorfismo è l'intero sottogruppo.

(c) Sia  $A$  l'unità matriciale  $2 \times 2$   $e_{12}$ . Allora, poiché  $A^2 = 0$ , tutti i termini, tranne due, dello sviluppo in serie relativo all'esponenziale si annullano, e risulta:

$$e^{tA} = I + e_{12}t = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

In questo caso, la funzione esponenziale definisce un isomorfismo da  $\mathbb{R}$  alla sua immagine, che è il gruppo delle matrici triangolari con gli elementi diagonali uguali a 1.

(d) I sottogruppi a un parametro di  $SU_2$  sono i coniugati del sottogruppo delle matrici unitarie speciali diagonali, ossia le longitudini descritte in (2.13). ■

Invece di tentare di stabilire un teorema generale che descriva i sottogruppi a un parametro di un gruppo, determineremo quelli relativi al gruppo ortogonale e al gruppo lineare speciale come esempi dei metodi usati. Avremo bisogno di sapere che la funzione esponenziale definita sulle matrici possiede una funzione inversa.

**(5.8) PROPOSIZIONE** *La funzione esponenziale di una matrice manda, mediante un omeomorfismo, un piccolo intorno  $S$  di 0 in  $\mathbb{R}^{n \times n}$  in un intorno  $T$  di  $I$ .*

*Dimostrazione.* Tale proposizione segue dal teorema della funzione inversa, il quale afferma che una funzione differenziabile  $f : \mathbb{R}^k \rightarrow \mathbb{R}^k$  possiede una funzione inversa in un punto  $p$  se la matrice jacobiana  $(\partial f_i / \partial x_j)(p)$  è invertibile. Dobbiamo verificare ciò per l'esponenziale di una matrice, nella matrice nulla in  $\mathbb{R}^{n \times n}$ . Si tratta di un calcolo poco piacevole per le notazioni, ma facile. Denotiamo una matrice variabile con  $X$ . La matrice jacobiana è la matrice  $n^2 \times n^2$  i cui elementi sono

$$\frac{\partial(e^X)_{\alpha\beta}}{\partial X_{ij}} \Big|_{X=0}.$$

Utilizziamo il fatto che  $\frac{d}{dt}(e^{tA}) \Big|_{t=0} = A$ . Dalla definizione della derivata parziale segue direttamente che

$$\frac{\partial e^X}{\partial X_{ij}} \Big|_{X=0} = \frac{de^{te_{ij}}}{dt} \Big|_{t=0} = e_{ij}.$$

Pertanto

$$\frac{\partial(e^X)_{\alpha\beta}}{\partial X_{ij}} \Big|_{X=0} = 0,$$

se  $(\alpha, \beta) \neq (i, j)$  e

$$\frac{\partial(e^X)_{ij}}{\partial X_{ij}} \Big|_{X=0} = 1.$$

La matrice jacobiana è la matrice identica  $n^2 \times n^2$ . ■

Passiamo ora a descrivere i sottogruppi a un parametro del gruppo ortogonale  $O_n$ . In questo caso, cerchiamo le matrici  $A$  tali che  $e^{tA}$  sia ortogonale per ogni  $t$ .

**(5.9) LEMMA** *Se  $A$  è antisimmetrica, allora  $e^A$  è ortogonale. Viceversa, esiste un intorno  $S'$  di 0 in  $\mathbb{R}^{n \times n}$  tale che, se  $e^A$  è ortogonale e  $A \in S'$ , allora  $A$  è antisimmetrica.*

*Dimostrazione.* Per evitare di confondere la variabile  $t$  con il simbolo che indica la matrice trasposta, denotiamo qui con  $A^*$  la trasposta della matrice  $A$ . Se  $A$  è antisimmetrica, allora  $e^{(A^*)} = e^{-A}$ . La relazione  $e^{(A^*)} = (e^A)^*$  segue dalla definizione dell'esponenziale; inoltre  $e^{-A} = (e^A)^{-1}$ , in base al corollario (8.10) del capitolo 4. Pertanto  $(e^A)^* = e^{(A^*)} = e^{-A} = (e^A)^{-1}$ . Ciò prova che  $e^A$  è ortogonale. Per dimostrare il viceversa, scegliamo  $S'$  abbastanza piccolo in modo tale che se  $A \in S'$ , allora  $-A$  e  $A^*$  appartengono all'intorno  $S$  citato nella proposizione (5.8). Supponiamo che  $A \in S'$  e che  $e^A$  sia ortogonale. Allora  $e^{(A^*)} = e^{-A}$ , e in virtù della proposizione (5.8), ciò significa che  $A$  è antisimmetrica. ■

**(5.10) COROLLARIO** *I sottogruppi a un parametro del gruppo ortogonale  $O_n$  sono gli omomorfismi  $t \mapsto e^{tA}$ , dove  $A$  è una matrice reale antisimmetrica.*

*Dimostrazione.* Se  $A$  è antisimmetrica,  $tA$  è antisimmetrica per ogni  $t$ . Pertanto  $e^{tA}$  è ortogonale per ogni  $t$ , ossia  $e^{tA}$  è un sottogruppo a un parametro di  $O_n$ . Viceversa, supponiamo che  $e^{tA}$  sia ortogonale per ogni  $t$ . Allora, per  $\epsilon$  abbastanza piccolo,  $\epsilon A$  appartiene all'intorno  $S'$  del lemma (5.9), e inoltre  $e^{\epsilon A}$  è ortogonale. Pertanto  $\epsilon A$  è antisimmetrica, e ciò implica che anche  $A$  è antisimmetrica. ■

Il corollario (5.10) è illustrato dall'esempio (5.7b).

Consideriamo infine il gruppo lineare speciale  $SL_n(\mathbb{R})$ .

(5.11) PROPOSIZIONE Sia  $A$  una matrice avente traccia zero. Allora  $e^A$  ha determinante 1. Viceversa, esiste un intorno  $S'$  di 0 in  $\mathbb{R}^{n \times n}$  tale che, se  $A \in S'$  e  $\det e^A = 1$ , allora  $\text{tr } A = 0$ .

*Dimostrazione.* La prima asserzione segue dalla formula semplice ed elegante:

$$(5.12) \quad e^{\text{tr } A} = \det e^A,$$

dove  $\text{tr } A$  denota come al solito la traccia di  $A$ . Tale formula discende a sua volta dal fatto che, se gli autovalori di una matrice complessa  $A$  sono  $\lambda_1, \dots, \lambda_n$ , allora gli autovalori di  $e^A$  sono  $e^{\lambda_1}, \dots, e^{\lambda_n}$ . La dimostrazione di questo fatto è lasciata come esercizio. In base a ciò, si ottiene

$$e^{\text{tr } A} = e^{\lambda_1 + \dots + \lambda_n} = e^{\lambda_1} \cdot \dots \cdot e^{\lambda_n} = \det e^A.$$

Per dimostrare il viceversa, osserviamo che se  $|x| < 1$ , allora  $e^x = 1$  implica  $x = 0$ . Sceglio  $S'$  abbastanza piccolo in modo tale che  $\text{tr } A < 1$ , se  $A \in S'$ . Allora, se  $\det e^A = e^{\text{tr } A} = 1$  e se  $A \in S'$ , risulta  $\text{tr } A = 0$ . ■

(5.13) COROLLARIO I sottogruppi a un parametro del gruppo lineare speciale  $SL_n(\mathbb{R})$  sono gli omomorfismi  $t \mapsto e^{tA}$ , dove  $A$  è una matrice reale  $n \times n$  avente traccia zero. ■

Il più semplice sottogruppo a un parametro di  $SL_2(\mathbb{R})$  è descritto nell'esempio (5.7c).

## 6 L'algebra di Lie

Consideriamo, come sempre, un gruppo lineare  $G$  come un sottoinsieme di  $\mathbb{R}^{n \times n}$  o di  $\mathbb{C}^{n \times n}$ . Lo spazio dei vettori tangentici a  $G$  nella matrice identica  $I$ , che descriveremo in questo paragrafo, è l'*algebra di Lie* del gruppo.

Cominciamo col richiamare la definizione di vettore tangente. Se  $\varphi(t) = (\varphi_1(t), \dots, \varphi_k(t))$  è un cammino differenziabile in  $\mathbb{R}^k$ , il suo vettore velocità  $v = \varphi'(t)$  è tangente al cammino nel punto  $x = \varphi(t)$ . Questa è l'osservazione fondamentale che sta alla base della definizione di vettore tangente.

Supponiamo che sia dato un sottoinsieme  $S$  di  $\mathbb{R}^k$ . Un vettore  $v$  si dice *tangente* a  $S$  in un punto  $x$  se esiste un cammino differenziabile  $\varphi(t)$  contenuto interamente in  $S$ , tale che  $\varphi(0) = x$  e  $\varphi'(0) = v$ .

Se il sottoinsieme  $S$  è il luogo degli zeri di una o più funzioni polinomiali  $f(x_1, \dots, x_k)$ , è chiamato *insieme algebrico reale*:

$$(6.1) \quad S = \{x \mid f(x) = 0\}.$$

Per esempio, la circonferenza unitaria in  $\mathbb{R}^2$  è un insieme algebrico reale, poiché è il luogo degli zeri del polinomio  $f(x_1, x_2) = x_1^2 + x_2^2 - 1$ .

La regola per la derivazione della funzione composta fornisce una condizione necessaria affinché un vettore sia tangente ad un insieme algebrico reale  $S$ . Sia  $\varphi(t)$  un cammino in  $S$ , e poniamo  $x = \varphi(t)$  e  $v = \varphi'(t)$ . Poiché il cammino è contenuto in  $S$ , le funzioni  $f(\varphi(t))$  si annullano identicamente; anche le loro derivate, quindi, saranno identicamente nulle:

$$(6.2) \quad 0 = \frac{d}{dt} f(\varphi(t)) = \frac{\partial f}{\partial x_1} v_1 + \dots + \frac{\partial f}{\partial x_k} v_k = (\nabla f(x) \cdot v),$$

dove  $\nabla f = \left( \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_k} \right)$  è il vettore gradiente.

(6.3) COROLLARIO Sia  $S$  un insieme algebrico reale in  $\mathbb{R}^k$  definito come il luogo degli zeri di una o più funzioni polinomiali  $f(x)$ . Allora i vettori tangentici a  $S$  in  $x$  sono ortogonali ai gradienti  $\nabla f(x)$ . ■

Per esempio, se  $S$  è la circonferenza unitaria e  $x$  è il punto  $(1, 0)$ , allora il vettore gradiente  $\nabla f(x)$  è  $(2, 0)$ . Il corollario (6.3) afferma che i vettori tangentici in  $(1, 0)$  hanno la forma  $(0, c)$ , ossia, che essi sono verticali, come dovrebbe essere.

Il calcolo dei vettori tangentici per mezzo di cammini parametrizzati non è consigliabile, poiché vi sono molti cammini con la stessa tangente. Se siamo interessati soltanto al vettore tangente, possiamo scartare tutte le informazioni contenute in un cammino, ad eccezione del termine del primo ordine del suo sviluppo di Taylor. Per fare ciò in modo sistematico, introduciamo formalmente un *elemento infinitesimo*  $\epsilon$ ; lavoriamo cioè algebricamente con la regola:

$$(6.4) \quad \epsilon^2 = 0.$$

Così come facciamo con i numeri complessi, dove la regola è  $i^2 = -1$ , possiamo usare la (6.4) per definire una moltiplicazione sullo spazio vettoriale

$$E = \{a + b\epsilon \mid a, b \in \mathbb{R}\}$$

delle combinazioni lineari formali di  $1, \epsilon$  a coefficienti reali. La regola per la moltiplicazione è la seguente:

$$(6.5) \quad (a + b\epsilon)(c + d\epsilon) = ac + (bc + ad)\epsilon.$$

In altre parole, calcoliamo formalmente il prodotto utilizzando le relazioni  $ec = ce$  per ogni  $c \in \mathbb{R}$ ,  $\epsilon^2 = 0$ . Come per i numeri complessi, l'addizione è l'addizione tra vettori:

$$(a + b\epsilon) + (c + d\epsilon) = (a + c) + (b + d)\epsilon.$$

La differenza principale tra  $C$  ed  $E$  è che  $E$  non è un campo, poiché  $\epsilon$  non ha l'inverso rispetto alla moltiplicazione. (Tuttavia,  $E$  è un anello; cfr. cap. 10).

Dati un punto  $x$  di  $\mathbb{R}^k$  e un vettore  $v \in \mathbb{R}^k$ , la somma  $x + v\epsilon$  è un vettore ad elementi in  $E$  che interpretiamo intuitivamente come uno *spostamento infinitesimo in  $x$ , nella direzione di  $v$* . Si noti che possiamo calcolare un polinomio  $f(x) = f(x_1, \dots, x_k)$  in  $x + v\epsilon$  utilizzando lo sviluppo di Taylor. Poiché  $\epsilon^2 = 0$ , i termini di grado  $\geq 2$  in  $\epsilon$  scompaiono, e ci resta un elemento di  $E$ :

$$(6.6) \quad f(x + v\epsilon) = f(x) + \left( \frac{\partial f}{\partial x_1} v_1 + \dots + \frac{\partial f}{\partial x_k} v_k \right) \epsilon = f(x) + (\nabla f(x) \cdot v)\epsilon.$$

Lavorare con la regola (6.4) equivale a trascurare i termini di ordine superiore in  $\epsilon$ . Pertanto il prodotto scalare  $(\nabla f(x) \cdot v)$  rappresenta la variazione infinitesima di  $f$  che si ottiene effettuando uno spostamento infinitesimo in  $x$  nella direzione di  $v$ .

Ritornando a un insieme algebrico reale  $S$  definito dalle equazioni polinomiali  $f(x) = 0$ , sia  $x$  un punto di  $S$ . Allora  $f(x) = 0$ , e pertanto dalla (6.6) si ottiene:

$$(6.7) \quad f(x + v\epsilon) = 0 \text{ se e soltanto se } (\nabla f(x) \cdot v) = 0,$$

ossia la stessa condizione stabilita nel corollario (6.3).

Ciò suggerisce la definizione seguente. Sia  $S$  un insieme algebrico reale definito dalle equazioni polinomiali  $f(x) = 0$ . Un vettore  $v$  è un *vettore tangente infinitesimo a  $S$  in  $x$*  se

$$(6.8) \quad f(x + v\epsilon) = 0.$$

(6.9) COROLLARIO Sia  $x$  un punto di un insieme algebrico reale  $S$ . Ogni vettore tangente a  $S$  in  $x$  è un vettore tangente infinitesimo. ■

Si noti che, se si fissa un punto  $x \in S$ , le equazioni  $(\nabla f(x) \cdot v) = 0$  sono lineari e omogenee in  $v$ . Pertanto i vettori tangenti infinitesimi a  $S$  in  $x$  formano un sottospazio dello spazio di tutti i vettori.

In realtà, la terminologia introdotta è leggermente ambigua. La definizione di vettore tangente infinitesimo dipende dalle equazioni  $f$ , e non soltanto dall'insieme  $S$ . Dobbiamo avere in mente equazioni particolari quando parliamo di vettori tangenti infinitesimi.

Nel caso in cui  $S$  è un insieme sufficientemente liscio, è vero anche il viceversa di (6.9), ossia, ogni vettore tangente infinitesimo è un vettore tangente. Quando ciò accade, possiamo calcolare lo spazio dei vettori tangenti in un punto  $x \in S$  risolvendo le equazioni lineari  $(\nabla f(x) \cdot v) = 0$  in  $v$ , che è relativamente facile. Tuttavia, il viceversa non vale nei "punti singolari" dell'insieme  $S$ , oppure se le equazioni che definiscono  $S$  non sono scelte bene. Per esempio, si denoti con  $S$  l'unione dei due assi coordinati in  $\mathbb{R}^2$ .  $S$  è un insieme algebrico reale definito dalla sola equazione  $x_1 x_2 = 0$ . È chiaro che un vettore tangente nell'origine deve essere

parallelo ad uno dei due assi. D'altra parte,  $\nabla f = (x_2, x_1)$ , che è zero se  $x_1 = x_2 = 0$ . Pertanto ogni vettore è un vettore tangente infinitesimo a  $S$  nell'origine.

Questo completa lo studio delle proprietà generali dei vettori tangentici. Applicheremo ora tali proprietà al caso in cui l'insieme  $S$  è uno dei nostri gruppi lineari  $G$  in  $\mathbb{R}^{n \times n}$  o in  $\mathbb{C}^{n \times n}$ . I vettori tangentici a  $G$  saranno vettori di uno spazio di dimensione  $n^2$ , e saranno rappresentati anch'essi mediante matrici. Come si è detto all'inizio, i vettori tangentici a  $G$  nell'identità  $I$  formano l'*algebra di Lie* del gruppo.

La prima cosa da osservare è che ogni sottogruppo a un parametro  $e^{tA}$  di uno dei nostri gruppi lineari  $G$  è un cammino parametrizzato. Già sappiamo che il suo vettore velocità  $(de^{tA}/dt)_{t=0}$  nell'identità  $I$  è  $A$ . Pertanto  $A$  rappresenta un vettore tangente a  $G$  nell'identità, e dunque appartiene all'algebra di Lie. Per esempio, il gruppo unitario  $U_1$  è la circonferenza unitaria nel piano complesso, e  $e^{ti}$  è un sottogruppo a un parametro di  $U_1$ . Il vettore velocità di  $e^{ti}$  in  $t=0$  è il vettore  $i$ , che è effettivamente tangente alla circonferenza unitaria nel punto 1.

Un gruppo di matrici  $G$  che è un insieme algebrico reale in  $\mathbb{R}^{n \times n}$  è chiamato *gruppo algebrico reale*. I gruppi lineari classici quali  $SL_n(\mathbb{R})$  e  $O_n$  sono algebrici reali, poiché le equazioni che li definiscono sono equazioni polinomiali negli elementi delle matrici. Per esempio, il gruppo  $SL_2(\mathbb{R})$  è definito dalla sola equazione polinomiale  $\det P = 1$ :

$$x_{11}x_{22} - x_{12}x_{21} - 1 = 0.$$

Il gruppo ortogonale  $O_3$  è definito da nove polinomi  $f_{ij}$  che esprimono la condizione  $P^t P = I$ :

$$f_{ij} = x_{1i}x_{1j} + x_{2i}x_{2j} + x_{3i}x_{3j} - \delta_{ij} = 0, \quad \delta_{ij} = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}.$$

I gruppi complessi, quali i gruppi unitari, possono anche essere trasformati in gruppi algebrici reali in  $\mathbb{R}^{2n \times 2n}$ , separando gli elementi delle matrici nella loro parte reale e immaginaria.

Si può dimostrare che per ogni vettore tangente infinitesimo  $A$  ad un gruppo algebrico reale  $G$  nell'identità,  $e^{tA}$  è un sottogruppo a un parametro di  $G$ . In altre parole, esiste un sottogruppo a un parametro che conduce fuori dall'identità in una direzione tangente arbitraria. Si tratta di un risultato notevole per un gruppo non abeliano; tuttavia esso vale sostanzialmente senza restrizioni. Purtroppo, sebbene tale proprietà sia piuttosto facile da verificare per un gruppo particolare, è abbastanza difficile dare una dimostrazione generale. Pertanto ci accontenteremo di verificare alcuni casi particolari.

Se abbiamo a disposizione un elemento infinitesimo, possiamo lavorare con matrici i cui elementi stanno in  $E$ . Una matrice siffatta avrà la forma:  $A + B\epsilon$ , dove  $A, B$  sono matrici reali. Intuitivamente,  $A + B\epsilon$  rappresenta uno spostamento

infinitesimo di  $A$  nella direzione della matrice  $B$ . La regola per moltiplicare due matrici siffatte è la stessa regola data da (6.5):

$$(6.10) \quad (A + B\epsilon)(C + D\epsilon) = AC + (AD + BC)\epsilon.$$

Il prodotto  $B\epsilon D\epsilon$  è zero poiché  $(b_{ij}\epsilon)(d_{kl}\epsilon) = 0$  per tutti i valori degli indici.

Sia  $G$  un gruppo algebrico reale. Per determinare i suoi vettori tangentini infinitesimi nell'identità, dobbiamo determinare le matrici  $A$  tali che

$$(6.11) \quad I + A\epsilon,$$

che rappresenta uno spostamento infinitesimo di  $I$  nella direzione della matrice  $A$ , soddisfi le equazioni che definiscono  $G$ . Questa è la definizione (6.8) di un vettore tangente infinitesimo.

Facciamo questo calcolo per il gruppo lineare speciale  $SL_n(\mathbb{R})$ . L'equazione che definisce tale gruppo è  $\det P = 1$ . Pertanto  $A$  è un vettore tangente infinitesimo, se  $\det(I + A\epsilon) = 1$ . Per descrivere questa condizione, dobbiamo calcolare la variazione del determinante in conseguenza di uno spostamento infinitesimo in  $I$ . La formula è semplice ed elegante:

$$(6.12) \quad \det(I + A\epsilon) = 1 + (\text{tr } A)\epsilon.$$

La dimostrazione di questa formula è lasciata come esercizio. Utilizzando la (6.12), si ottiene che  $A$  è un vettore tangente infinitesimo se e soltanto se  $\text{tr } A = 0$ .

(6.13) PROPOSIZIONE *Le seguenti condizioni su una matrice reale  $n \times n$   $A$  sono equivalenti:*

- (i)  $\text{tr } A = 0$ ;
- (ii)  $e^{tA}$  è un sottogruppo a un parametro di  $SL_n(\mathbb{R})$ ;
- (iii)  $A$  appartiene all'algebra di Lie di  $SL_n(\mathbb{R})$ ;
- (iv)  $A$  è un vettore tangente infinitesimo a  $SL_n(\mathbb{R})$  in  $I$ .

*Dimostrazione.* La proposizione (5.11) dice che (i)  $\Rightarrow$  (ii). Poiché  $A$  è tangente al cammino  $e^{tA}$  in  $t = 0$ , (ii)  $\Rightarrow$  (iii). Dal corollario (6.9) segue che (iii)  $\Rightarrow$  (iv), e l'implicazione (iv)  $\Rightarrow$  (i) è conseguenza della formula (6.12). ■

Vi è un principio generale che agisce qui. Abbiamo tre insiemi di matrici  $A$ : quelle tali che  $e^{tA}$  è un sottogruppo a un parametro di  $G$ , quelle che appartengono all'algebra di Lie, e quelle che sono vettori tangentini infinitesimi. Denotiamo questi tre insiemi con  $\text{Exp}(G)$ ,  $\text{Lie}(G)$ ,  $\text{Inf}(G)$ , rispettivamente. Essi sono collegati tra loro mediante le seguenti inclusioni:

$$(6.14) \quad \text{Exp}(G) \subset \text{Lie}(G) \subset \text{Inf}(G).$$

La prima inclusione è vera perché  $A$  è il vettore tangente ad  $e^{tA}$  in  $t = 0$ , e la seconda vale perché ogni vettore tangente è un vettore tangente infinitesimo. Se  $\text{Exp}(G) = \text{Inf}(G)$ , allora questi due insiemi risultano anche uguali a  $\text{Lie}(G)$ . Poiché è facile calcolare  $\text{Exp}(G)$  e  $\text{Inf}(G)$ , ciò fornisce un modo pratico per determinare l'algebra di Lie. Esiste un teorema generale, da cui segue che  $\text{Exp}(G) = \text{Inf}(G)$  per ogni gruppo algebrico reale  $G$ , purché le equazioni che definiscono  $G$  siano scelte opportunamente. Tuttavia, non vale la pena di dimostrare qui il teorema generale.

Faremo ora il calcolo per il gruppo ortogonale  $O_n$ . L'equazione che definisce  $O_n$  è l'equazione matriciale  $P^t P = I$ . Affinché  $A$  sia un vettore tangente infinitesimo nell'identità, deve soddisfare la relazione:

$$(6.15) \quad (I + A\epsilon)^t (I + A\epsilon) = I.$$

Il primo membro di tale relazione si sviluppa in  $I + (A^t + A)\epsilon$ ; pertanto la condizione affinché  $I + A\epsilon$  sia ortogonale è  $A^t + A = 0$ , ossia  $A$  è antisimmetrica. Ciò è in accordo con la condizione (5.10) affinché  $e^{tA}$  sia un sottogruppo a un parametro di  $O_n$ .

(6.16) PROPOSIZIONE *Le seguenti condizioni su una matrice reale  $n \times n$   $A$  sono equivalenti:*

- (i)  $A$  è antisimmetrica;
- (ii)  $e^{tA}$  è un sottogruppo a un parametro di  $O_n$ ;
- (iii)  $A$  appartiene all'algebra di Lie di  $O_n$ ;
- (iv)  $A$  è un vettore tangente infinitesimo a  $O_n$  in  $I$ . ■

L'algebra di Lie di un gruppo lineare possiede un'ulteriore struttura: precisamente, un'operazione chiamata la *parentesi di Lie*. La parentesi di Lie è la legge di composizione definita da:

$$(6.17) \quad [A, B] = AB - BA.$$

Tale legge di composizione non è associativa. Tuttavia, essa soddisfa un'identità, chiamata l'*identità di Jacobi*:

$$(6.18) \quad [A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0,$$

che è un surrogato della proprietà associativa.

Per dimostrare che la parentesi di Lie è una legge di composizione sull'algebra di Lie, dobbiamo verificare che se  $A, B$  appartengono a  $\text{Lie}(G)$  anche  $[A, B]$  appartiene a  $\text{Lie}(G)$ . Ciò si può fare facilmente per qualunque gruppo fissato.

Per il gruppo lineare speciale, si tratta di verificare che se  $A, B$  hanno traccia zero anche  $AB - BA$  ha traccia zero. Ciò è vero, poiché  $\text{tr } AB = \text{tr } BA$ . Sia ora  $G = O_n$ , sicché l'algebra di Lie è lo spazio delle matrici antisimmetriche. Dobbiamo verificare che, se  $A, B$  sono antisimmetriche, allora anche  $[A, B]$  è antisimmetrica. Si ha:

$$[A, B]^t = (AB - BA)^t = B^t A^t - A^t B^t = BA - AB = -[A, B].$$

come richiesto.

La parentesi di Lie è un'operazione importante, poiché essa è la versione infinitesimale del commutatore  $PQP^{-1}Q^{-1}$ . Per renderci conto di ciò, dobbiamo lavorare con due infinitesimi  $\epsilon, \delta$ , utilizzando le regole:  $\epsilon^2 = \delta^2 = 0$ ,  $\epsilon\delta = \delta\epsilon$ . Si noti che l'inversa della matrice  $I + A\epsilon$  è  $I - A\epsilon$ . Pertanto, se  $P = I + A\epsilon$  e  $Q = I + B\delta$ , il commutatore si sviluppa in:

$$(6.19) \quad (I + A\epsilon)(I + B\delta)(I - A\epsilon)(I - B\delta) = I + (AB - BA)\epsilon\delta.$$

Intuitivamente, la parentesi appartiene all'algebra di Lie, poiché il prodotto di due elementi di  $G$ , anche infinitesimi, appartiene a  $G$ , e pertanto il commutatore di due elementi appartiene anch'esso a  $G$ .

Utilizzando l'operazione data dalla parentesi di Lie, possiamo definire inoltre la nozione di algebra di Lie, in senso astratto:

(6.20) DEFINIZIONE *Un'algebra di Lie  $V$  su un campo  $F$  è uno spazio vettoriale insieme con una legge di composizione*

$$\begin{aligned} V \times V &\longrightarrow V \\ (v, w) &\mapsto [v, w], \end{aligned}$$

chiamata operazione di parentesi o semplicemente parentesi, avente le seguenti proprietà:

$$\text{Bilinearità: } [v_1 + v_2, w] = [v_1, w] + [v_2, w], \quad [cv, w] = c[v, w].$$

$$[v, w_1 + w_2] = [v, w_1] + [v, w_2], \quad [v, cw] = c[v, w];$$

$$\text{Antisimmetria: } [v, v] = 0;$$

$$\text{Identità di Jacobi: } [u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0;$$

per ogni  $u, v, w \in V$  e per ogni  $c \in F$ .

L'importanza delle algebre di Lie viene dal fatto che, essendo spazi vettoriali, sono molto più facili da trattare dei gruppi lineari stessi, e nello stesso tempo i gruppi classici sono pressoché determinati dalle loro algebre di Lie. In altre parole,

la struttura infinitesimale del gruppo nell'elemento neutro è quasi sufficiente per determinare il gruppo.

## 7 Traslazione in un gruppo

In questo paragrafo faremo uso di un'ulteriore nozione presa dalla topologia: la definizione di varietà in  $\mathbb{R}^k$ . Tale definizione è richiamata nell'appendice [definizione (3.12)]. Il lettore non deve scoraggiarsi se la nozione di varietà non gli è familiare. Egli può imparare ciò che è necessario, senza molte difficoltà, cammin facendo.

Sia  $P$  un elemento fissato di un gruppo di matrici  $G$ . Sappiamo che la moltiplicazione a sinistra per  $P$  è un'applicazione biettiva di  $G$  in sé:

$$(7.1) \quad \begin{aligned} G &\xrightarrow{m_P} G \\ X &\longmapsto PX, \end{aligned}$$

poiché essa ha la funzione inversa  $m_{P^{-1}}$ . Le applicazioni  $m_P$  e  $m_{P^{-1}}$  sono continue, poiché la moltiplicazione tra matrici è continua. Pertanto  $m_P$  è un omeomorfismo di  $G$  in sé (non un omomorfismo). Esso è chiamato anche la *traslazione a sinistra* mediante  $P$ , in analogia con la traslazione nel piano, la quale è una traslazione a sinistra nel gruppo additivo  $\mathbb{R}^2$ .

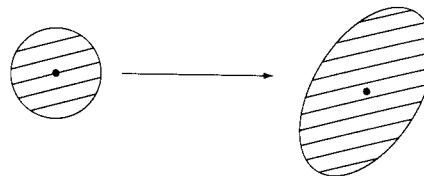
La proprietà importante di un gruppo che è conseguenza dell'esistenza di tali applicazioni è l'*omogeneità*. La moltiplicazione per  $P$  è un omeomorfismo che porta l'identità  $I$  in  $P$ . Pertanto la struttura topologica del gruppo  $G$  nell'intorno di  $I$  è la stessa struttura che  $G$  possiede nell'intorno di  $P$  e, data l'arbitrarietà di  $P$ , essa è la stessa nell'intorno di ogni punto del gruppo. Ciò è analogo al fatto che il piano si presenta allo stesso modo in due qualsiasi dei suoi punti.

La moltiplicazione a sinistra in  $SU_2$  risulta definita da un cambiamento *ortogonale* delle coordinate  $(x_1, x_2, x_3, x_4)$  e pertanto essa è un movimento rigido della 3-sfera. Tuttavia la moltiplicazione mediante una matrice non è necessariamente un movimento rigido, sicché il fatto che ogni gruppo è omogeneo non va inteso in tal senso. Per esempio, sia  $G$  il gruppo delle matrici diagonali reali invertibili  $2 \times 2$ , e identifichiamo gli elementi di  $G$  con i punti  $(a, d)$  del piano che non appartengono agli assi coordinati. La moltiplicazione per la matrice:

$$(7.2) \quad P = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$$

induce una distorsione nel gruppo  $G$ , ma in modo continuo.

(7.3)



Moltiplicazione a sinistra in un gruppo.

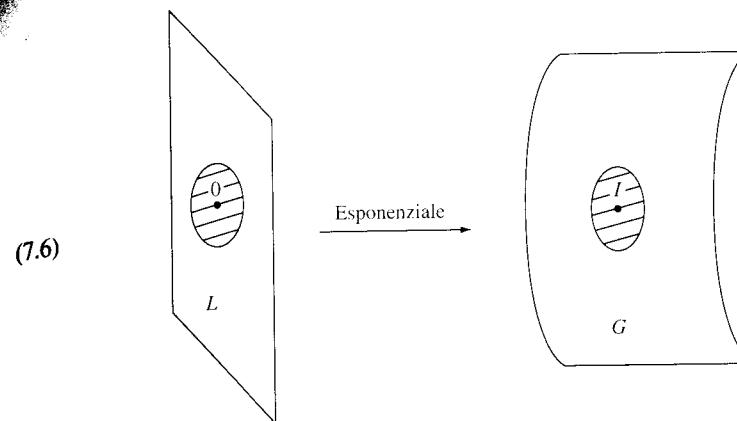
Ora, gli unici sottoinsiemi “ragionevoli”, dal punto di vista geometrico, di  $\mathbb{R}^k$  che hanno questa proprietà di omogeneità sono le varietà. Una varietà  $M$  di dimensione  $d$  è un sottoinsieme che è localmente omeomorfo a  $\mathbb{R}^d$  in ogni suo punto, ossia tale che ogni punto  $p \in M$  ha un intorno omeomorfo ad un insieme aperto di  $\mathbb{R}^d$  [cfr. app. (3.12)]. Non è sorprendente il fatto che i gruppi classici, essendo omogenei, sono delle varietà, sebbene esistano sottogruppi di  $GL_n(\mathbb{R})$  che non lo sono. Ad esempio, il gruppo  $GL_n(\mathbb{Q})$  delle matrici invertibili a elementi razionali è un insieme piuttosto brutto, dal punto di vista geometrico, sebbene sia un gruppo interessante. Il teorema seguente fornisce una risposta soddisfacente al problema di stabilire quali sono i gruppi lineari che risultano delle varietà:

(7.4) TEOREMA *Sia dato un sottogruppo  $G$  di  $GL_n(\mathbb{R})$  tale che  $G$  sia un sottoinsieme chiuso in  $\mathbb{R}^{n \times n}$ . Allora  $G$  è una varietà.*

Dare qui la dimostrazione di questo teorema ci porterebbe troppo lontano. Invece, illustreremo il teorema provando che i gruppi ortogonali  $O_n$  sono delle varietà. Le dimostrazioni relative agli altri gruppi classici sono simili.

(7.5) PROPOSIZIONE *Il gruppo ortogonale  $O_n$  è una varietà di dimensione  $\frac{1}{2}n(n - 1)$ .*

*Dimostrazione.* Denotiamo il gruppo  $O_n$  con  $G$  e la sua algebra di Lie, ossia lo spazio delle matrici antisimmetriche, con  $L$ . La proposizione (5.9) dice che se  $A$  è una matrice vicina a  $0$ , allora  $A \in L$  se e soltanto se  $e^A \in G$ . Inoltre, l'esponenziale è un omeomorfismo da un intorno di  $0$  in  $\mathbb{R}^{n \times n}$  ad un intorno di  $I$ . Mettendo insieme questi due fatti, otteniamo che l'esponenziale definisce un omeomorfismo da un intorno di  $0$  in  $L$  ad un intorno di  $I$  in  $G$ . Poiché  $L$  è uno spazio vettoriale di dimensione  $\frac{1}{2}n(n - 1)$ ,  $L$  è una varietà. Ciò prova che la condizione di essere una varietà è soddisfatta dal gruppo ortogonale nell'identità. D'altra parte, abbiamo visto sopra che due punti arbitrari di  $G$  hanno intorni omeomorfi. Pertanto  $G$  è una varietà, come affermato. ■



Ecco un'altra applicazione del principio di omogeneità:

(7.7) PROPOSIZIONE *Sia  $G$  un gruppo di matrici connesso per cammini, e sia  $H \subset G$  un sottogruppo contenente un sottoinsieme aperto non vuoto di  $G$ . Allora  $H = G$ .*

*Dimostrazione.* Per ipotesi,  $H$  contiene un sottoinsieme aperto non vuoto  $U$  di  $G$ . Poiché la moltiplicazione a sinistra per  $g \in G$  è un omeomorfismo, anche  $gU$  è aperto in  $G$ . Ciascun sottoinsieme  $gU$  è contenuto in un'unica classe laterale di  $H$ , precisamente in  $gH$ . Poiché i sottoinsiemi della forma  $gU(g \in G)$  ricoprono  $G$ , essi ricoprono ciascuna classe laterale. In tal modo, ogni classe laterale è un'unione di sottoinsiemi aperti di  $G$ , e quindi essa stessa è un aperto. Pertanto  $G$  possiede una partizione mediante sottoinsiemi aperti, precisamente le classi laterali di  $H$ . Ora un insieme connesso per archi non è un'unione disgiunta di sottoinsiemi aperti propri [cfr. app. (3.11)]. Ne segue che vi può essere soltanto una classe laterale, e quindi  $H = G$ . ■

Utilizzeremo ora tale proposizione per determinare i sottogruppi normali di  $SU_2$ .

(7.8) TEOREMA *L'unico sottogruppo normale proprio di  $SU_2$  è il suo centro  $\{\pm I\}$ .*

Poiché esiste un omomorfismo suriettivo  $\varphi : SU_2 \rightarrow SO_3$ , il cui nucleo è  $\{\pm I\}$  [cfr. §3), il gruppo delle rotazioni è isomorfo ad un gruppo quoziente di  $SU_2$  [cap. 2 (10.9)]:

$$(7.9) \quad SO_3 \approx SU_2 / \{\pm I\}.$$

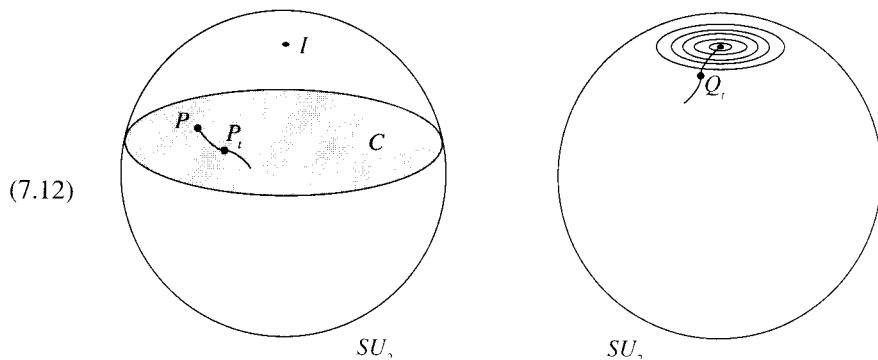
(7.10) COROLLARIO  $SO_3$  è un gruppo semplice, ossia, non possiede sottogruppi normali propri.

*Dimostrazione.* L'immagine inversa di un sottogruppo normale di  $SO_3$  è un sottogruppo normale di  $SU_2$  che contiene  $\{\pm I\}$  [cap. 2 (7.4)]. Il teorema (7.8) assicura che non esistono sottogruppi normali propri. ■

*Dimostrazione del teorema (7.8).* Basta provare che, se  $N$  è un sottogruppo normale di  $SU_2$  che non è contenuto nel centro  $\{\pm I\}$ , allora  $N$  è l'intero gruppo. Ora, poiché  $N$  è normale,  $N$  è un'unione di classi di coniugio [cap. 6 (2.5)]. Inoltre, abbiamo visto che le classi di coniugio sono le latitudini, ossia le 2-sfere (2.8). Per ipotesi,  $N$  contiene una matrice  $P \neq \pm I$ ; pertanto  $N$  contiene l'intera classe di coniugio  $C = C_P$ , che è una 2-sfera. Intuitivamente, tale insieme sembra abbastanza grande per generare  $SU_2$ . Infatti esso ha dimensione 2 e non è un sottogruppo, quindi l'insieme  $S$  di tutti i prodotti  $P^{-1}Q$  con  $P, Q \in C$  è più grande di  $C$ . Ne segue che  $S$  dovrebbe avere dimensione 3, che è proprio la dimensione di  $SU_2$ , sicché  $S$  dovrebbe contenere un sottoinsieme aperto del gruppo.

Per rendere preciso questo ragionamento intuitivo, sceglieremo un'applicazione continua non costante dall'intervallo unitario  $[0, 1]$  a  $C$  tale che  $P_0 = P$  e  $P_1 \neq P$ . Consideriamo il cammino:

$$(7.11) \quad Q_t = P^{-1}P_t.$$



Allora  $Q_0 = I$ , e  $Q_1 \neq I$ , sicché questo cammino esce da  $I$ . Poiché  $P$  e  $P_t$  appartengono a  $N$ ,  $Q_t$  appartiene a  $N$  per ogni  $t \in [0, 1]$ .

Sia  $f(t)$  la funzione  $\text{tr } Q_t$ . Essa è una funzione continua sull'intervallo  $[0, 1]$ . Si noti che  $f(0) = 2$ , mentre  $f(1) = \tau < 2$  poiché  $Q_1 \neq I$ . Per continuità, tutti i valori compresi tra  $\tau$  e 2 sono assunti da  $f$  nell'intervallo.

Poiché  $N$  è normale, esso contiene la classe di coniugio di  $Q_t$  per ogni  $t$ . Pertanto, poiché la traccia di  $Q_t$  assume tutti i valori prossimi a 2, la proposizione (2.9) ci dice che  $N$  contiene tutte le matrici di  $SU_2$  la cui traccia è abbastanza vicina a 2, e quindi in particolare tutte le matrici abbastanza vicine a  $I$ . Dun-

que  $N$  contiene un intorno aperto di  $I$  in  $SU_2$ . Ora  $SU_2$ , essendo una sfera, è connesso per archi, e quindi la proposizione (7.7) completa la dimostrazione. ■

Possiamo applicare la traslazione in un gruppo  $G$  anche ai vettori tangentici. Se  $A$  è un vettore tangente nell'identità e se  $P$  è un elemento arbitrario di  $G$ , allora  $PA$  è un vettore tangente a  $G$  nel punto  $P$ . Intuitivamente, ciò è vero poiché  $P(I + A\epsilon) = P + PA\epsilon$  è il prodotto di elementi di  $G$  e quindi appartiene a  $G$ . Come sempre, questa osservazione di tipo euristico è facile da verificare per un gruppo particolare. Fissiamo  $A$ , e associamo il vettore tangente  $PA$  all'elemento  $P$  di  $G$ . In tal modo otteniamo ciò che è chiamato un *campo di vettori tangentici* sul gruppo  $G$ . Poiché  $A$  è non nulla e  $P$  è invertibile, tale campo di vettori non si annulla in nessun punto. Ebbene proprio l'esistenza di un campo di vettori tangentici che non si annulla mai impone forti restrizioni sullo spazio  $G$ . Per esempio, esiste un teorema di topologia che assicura che ogni campo di vettori sulla 2-sfera deve annullarsi in qualche punto. Ecco il motivo per cui la 2-sfera non ha una struttura di gruppo. Invece la 3-sfera, essendo un gruppo, ha campi di vettori tangentici che non si annullano mai.

## 8 Gruppi semplici

Ricordiamo che un gruppo  $G$  si dice *semplice* se non è il gruppo banale e se non contiene sottogruppi normali propri (cap. 6, § 2). Finora abbiamo visto due gruppi semplici non abeliani: il gruppo icosaedrale  $I \approx A_5$  [cap. 6 (2.3)] e il gruppo delle rotazioni  $SO_3$  (7.10). Questo paragrafo tratta la classificazione dei gruppi semplici. La maggior parte delle dimostrazioni verranno omesse.

I gruppi semplici sono importanti per due motivi. Innanzitutto, se un gruppo  $G$  ha un sottogruppo normale proprio  $N$ , allora la struttura di  $G$  è in parte descritta, quando si conosce la struttura di  $N$  e del gruppo quoziante  $G/N$ . Se  $N$  o  $G/N$  hanno un sottogruppo normale, possiamo scomporre ulteriormente la struttura di tali gruppi. In questo modo, possiamo sperare di descrivere un gruppo finito particolare  $G$ , costruendolo induttivamente a partire da gruppi semplici.

In secondo luogo, sebbene la condizione di essere un gruppo semplice sia una restrizione molto forte, i gruppi semplici compaiono spesso. I gruppi lineari classici sono pressoché semplici. Per esempio, abbiamo visto nell'ultimo paragrafo che  $SU_2$  ha centro  $\{\pm I\}$  e che  $SU_2/\{\pm I\} \approx SO_3$  è un gruppo semplice. Gli altri gruppi classici hanno proprietà simili.

Allo scopo di concentrare l'attenzione, ci limiteremo qui a trattare i gruppi complessi. Useremo il simbolo  $Z$  per denotare il centro di un gruppo. Il teorema seguente richiederebbe troppo tempo per essere dimostrato qui, tuttavia lo illustreremo nel caso speciale di  $SL_2(\mathbb{C})$ .

## (8.1) TEOREMA

- (a) Il centro  $Z$  del gruppo lineare speciale  $SL_n(\mathbb{C})$  è un gruppo ciclico, generato dalla matrice  $\zeta I$ , dove  $\zeta = e^{2\pi i/n}$ . Il gruppo quoziante  $SL_n(\mathbb{C})/Z$  è semplice se  $n \geq 2$ .
- (b) Il centro  $Z$  del gruppo ortogonale speciale complesso  $SO_n(\mathbb{C})$  è  $\{\pm I\}$  se  $n$  è pari, ed è il gruppo banale  $\{I\}$  se  $n$  è dispari. Il gruppo  $SO_n/Z$  è semplice se  $n=3$  oppure se  $n \geq 5$ .
- (c) Il centro  $Z$  del gruppo simplettico  $SP_{2n}(\mathbb{C})$  è  $\{\pm I\}$ , e  $SP_{2n}(\mathbb{C})/Z$  è semplice se  $n \geq 1$ . ■

Il gruppo  $SL_n(\mathbb{C})/Z$  è chiamato il *gruppo proiettivo* e si denota con  $PSL_n(\mathbb{C})$ :

$$(8.2) \quad PSL_n(\mathbb{C}) = SL_n(\mathbb{C})/Z, \quad \text{dove } Z = \{\zeta I \mid \zeta^n = 1\}.$$

Per illustrare il teorema (8.1), proveremo che  $PSL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{\pm I\}$  è semplice. Infatti, dimostreremo che  $PSL_2(F)$  è un gruppo semplice per quasi tutti i campi  $F$ .

(8.3) TEOREMA Sia  $F$  un campo che non sia di caratteristica 2 e che contenga almeno sette elementi. Allora l'unico sottogruppo normale proprio di  $SL_2(F)$  è il sottogruppo  $\{\pm I\}$ . Pertanto  $PSL_2(F) = SL_2(F)/\{\pm I\}$  è un gruppo semplice.

Poiché il centro di  $SL_2(F)$  è un sottogruppo normale, segue dal teorema che esso è il gruppo  $\{\pm I\}$ .

## (8.4) COROLLARIO Esistono infiniti gruppi semplici finiti non abeliani. ■

*Dimostrazione del teorema (8.3).* La dimostrazione è algebrica, ma è strettamente collegata alla dimostrazione geometrica data per l'analogo risultato relativo a  $SU_2$  nel paragrafo precedente. Procederemo coniugando e moltiplicando finché il gruppo non sarà generato. Per semplificare le notazioni denoteremo  $SL_2(F)$  con  $SL_2$ . Sia  $N$  un sottogruppo normale di  $SL_2$  che contenga una matrice  $A \neq \pm I$ . Dobbiamo dimostrare che  $N = SL_2$ . Poiché è possibile che  $N$  sia il sottogruppo normale generato da  $A$  e dalle sue coniugate, dobbiamo dimostrare che le matrici coniugate di  $A$  sono sufficienti per generare l'intero gruppo.

Il primo passo nella dimostrazione sarà provare che  $N$  contiene una matrice triangolare diversa da  $\pm I$ . Ora, se la matrice data  $A$  ha gli autovalori nel campo  $F$ , essa sarà coniugata a una matrice triangolare. Ma poiché vogliamo trattare il caso di un campo arbitrario, non possiamo fare questo passo tanto facilmente. Sebbene ciò sia facile per i numeri complessi, questo passo è la parte più difficile della dimostrazione per un campo qualsiasi.

(8.5) LEMMA  $N$  contiene una matrice triangolare  $A \neq \pm I$ .

## 8 | Gruppi semplici

*Dimostrazione.* Sia  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  una matrice in  $N$  che sia diversa da  $\pm I$ . Se  $c=0$ , allora  $A$  è la matrice richiesta.

Supponiamo che  $c \neq 0$ . In tal caso, costruiremo una matrice triangolare a partire da  $A$  e dalle sue coniugate. Calcoliamo innanzitutto la coniugata:

$$\begin{bmatrix} 1+x \\ 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1-x \\ 1 \end{bmatrix} = \begin{bmatrix} a+xc & * \\ c & d-xc \end{bmatrix} = A'.$$

Poiché  $c \neq 0$ , possiamo scegliere  $x$  in modo che  $a+xc=0$ . La matrice  $A'$  sta in  $N$ , e quindi  $N$  contiene una matrice il cui elemento in alto a sinistra è zero. Sostituiamo  $A$  con questa matrice, sicché essa ha la forma  $A = \begin{bmatrix} b \\ c & d \end{bmatrix}$ . Purtroppo lo zero sta nel posto sbagliato.

Si noti che, poiché  $\det A = 1$ ,  $bc = -1$  nella nuova matrice  $A$ . Calcoliamo ora il commutatore  $P^{-1}A^{-1}PA$  con una matrice diagonale:

$$P^{-1}A^{-1}PA = \begin{bmatrix} u & \\ & u^{-1} \end{bmatrix} \begin{bmatrix} d & -b \\ -c & \end{bmatrix} \begin{bmatrix} u^{-1} & \\ & u \end{bmatrix} \begin{bmatrix} b \\ c & d \end{bmatrix} = \begin{bmatrix} u^2 & (1-u^2)bd \\ & u^{-2} \end{bmatrix}.$$

Tale matrice, che appartiene al sottogruppo normale  $N$ , è del tipo richiesto a meno che non sia uguale a  $\pm I$ . In tal caso,  $u^2 = \pm 1$  e  $u^4 = 1$ . Ma la matrice  $P$  è formata con un elemento arbitrario  $u$  di  $F^*$ . D'altra parte, dimostreremo [cap. 11 (1.8)] che il polinomio  $x^4 - 1$  ha al più quattro radici in un campo arbitrario. Pertanto esistono al più quattro elementi  $u \in F$  con  $u^4 = 1$ . Per ipotesi, il campo  $F$  contiene almeno sette elementi, sicché possiamo scegliere  $u \in F^*$  con  $u^4 \neq 1$ . Allora  $P^{-1}A^{-1}PA$  è la matrice richiesta. ■

(8.6) LEMMA  $N$  contiene una matrice della forma  $\begin{bmatrix} 1 & u \\ & 1 \end{bmatrix}$ , con  $u \neq 0$ .

*Dimostrazione.* In base al lemma precedente,  $N$  contiene una matrice triangolare  $A = \begin{bmatrix} a & b \\ & d \end{bmatrix} \neq \pm I$ . Se  $d \neq a$ , sia  $A' = \begin{bmatrix} a & b' \\ & d \end{bmatrix}$  la sua coniugata mediante la matrice  $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ . Allora  $b' = b + d - a$ . Poiché  $\det A = ad = 1$ , il prodotto:

$$A'^{-1}A = \begin{bmatrix} d & -b' \\ & a \end{bmatrix} \begin{bmatrix} a & b \\ & d \end{bmatrix} = \begin{bmatrix} 1 & ad - d^2 \\ & 1 \end{bmatrix}$$

è la matrice richiesta. Se  $a = d$ , allora  $a = \pm 1$  poiché  $\det A = 1$ , e quindi  $b \neq 0$ . In tal caso, una delle due matrici  $A$ ,  $A^2$  è del tipo richiesto. ■

(8.7) LEMMA Sia  $F$  un campo. La classe di coniugio in  $SL_2$  della matrice  $\begin{bmatrix} 1 & u \\ 1 & 1 \end{bmatrix}$  contiene le matrici  $\begin{bmatrix} 1 & a^2u \\ -u & 1 \end{bmatrix}$  e  $\begin{bmatrix} 1 & a^2u \\ 1 & 1 \end{bmatrix}$ , per ogni  $a \neq 0$ .

*Dimostrazione.*

$$\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & u \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & u \\ -u & 1 \end{bmatrix} \quad \text{e}$$

$$\begin{bmatrix} a & a^{-1} \\ a^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & u \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & a \\ 1 & a \end{bmatrix} = \begin{bmatrix} 1 & a^2u \\ 1 & 1 \end{bmatrix}. \blacksquare$$

(8.8) LEMMA Sia  $F$  un campo di caratteristica  $\neq 2$ . Il gruppo additivo  $F(+)$  del campo è generato dai quadrati degli elementi di  $F$ .

*Dimostrazione.* Proviamo che ogni elemento  $x \in F$  può essere scritto nella forma:  $a^2 - b^2 = (a+b)(a-b)$ , con  $a, b \in F$ . Per ottenere ciò, basta risolvere il sistema di equazioni lineari:  $a+b=1$ ,  $a-b=x$ . Questo è il punto in cui viene usata l'ipotesi che la caratteristica di  $F$  sia diversa da 2. In caratteristica 2, tali equazioni non hanno necessariamente soluzioni. ■

(8.9) LEMMA Sia  $F$  un campo di caratteristica  $\neq 2$ . Se un sottogruppo normale  $N$  di  $SL_2(F)$  contiene una matrice  $\begin{bmatrix} 1 & u \\ 1 & 1 \end{bmatrix}$  con  $u \neq 0$ , allora esso contiene tutte le matrici di questa forma.

*Dimostrazione.* L'insieme degli elementi  $x$  tali che  $\begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix} \in N$  è un sottogruppo di  $F$ , diciamo  $S$ . Vogliamo provare che  $S = F$ . Dal lemma (8.7) segue che, se  $u \in S$ , allora  $a^2u \in S$  per ogni  $a \in F$ . Poiché i quadrati generano il gruppo additivo  $F$ , l'insieme di elementi  $\{a^2u \mid a \in F\}$  genera il sottogruppo additivo  $F_u$  di  $F$ , e tale sottogruppo è uguale a  $F$ , poiché  $u$  è invertibile. Pertanto  $S = F$ , come richiesto. ■

(8.10) LEMMA Per ogni campo  $F$ , il gruppo  $SL_2(F)$  è generato dalle matrici elementari  $\begin{bmatrix} 1 & u \\ 1 & 1 \end{bmatrix}$  e  $\begin{bmatrix} 1 & u \\ u & 1 \end{bmatrix}$ .

*Dimostrazione.* Sia  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(F)$ . La riduciamo per righe utilizzando soltanto matrici della forma data. Cominciamo a lavorare sulla prima colonna.

Riducendola a  $e_1$ . Eliminiamo il caso  $c=0$  aggiungendo, se necessario, la prima riga alla seconda. Aggiungiamo poi un multiplo della seconda riga alla prima per trasformare  $a$  in 1. Infine, eliminiamo l'elemento  $c$ . A questo punto, la matrice ha la forma  $A' = \begin{bmatrix} 1 & b' \\ 0 & d' \end{bmatrix}$ . Allora  $d' = \det A' = \det A = 1$ , e possiamo eliminare l'elemento  $b'$ , ottenendo alla fine la matrice identica. Poiché abbiamo utilizzato quattro operazioni o anche meno per ridurre la matrice  $A$  all'identità,  $A$  è un prodotto di al più quattro di tali matrici elementari. ■

La dimostrazione del teorema (8.3) è completata combinando i lemmi (8.5), (8.6), (8.7), (8.9) e (8.10). ■

Un celebre teorema di Cartan afferma che la lista (8.1) di gruppi semplici è pressoché completa. Naturalmente esistono altri gruppi semplici (per esempio, abbiamo appena dimostrato che  $PSL_2(F)$  è semplice per la maggior parte dei campi  $F$ ), ma se ci limitiamo ai gruppi algebrici complessi, la lista dei gruppi semplici diventa molto corta.

Un sottogruppo  $G$  di  $GL_n(\mathbb{C})$  è chiamato *gruppo algebrico complesso* se è l'insieme delle soluzioni di un sistema finito di equazioni polinomiali negli elementi delle matrici. Si tratta di un concetto analogo a quello di gruppo algebrico reale introdotto nel § 6. Non sarà evidente il motivo per cui la proprietà di essere definito da equazioni polinomiali è "ragionevole", ma c'è una cosa facile da vedere: fatta eccezione per i gruppi unitari  $U_n$  e  $SU_n$ , tutti i gruppi classici complessi sono gruppi algebrici complessi.

### (8.11) TEOREMA

- (a) I gruppi  $PSL_n(\mathbb{C}) = SL_n(\mathbb{C})/Z$ ,  $SO_n(\mathbb{C})/Z$  e  $SP_{2n}(\mathbb{C})/Z$  sono gruppi algebrici complessi connessi per archi.
- (b) In aggiunta alle classi di isomorfismo di tali gruppi, vi sono esattamente cinque classi di isomorfismo di gruppi algebrici complessi connessi per archi, semplici, chiamati gruppi eccezionali.

Il teorema (8.11) è troppo difficile per poter essere dimostrato qui. Esso è basato su una classificazione delle algebre di Lie corrispondenti. Ciò che dovremmo imparare è che non vi sono molti gruppi algebrici semplici. Ciò dovrebbe essere rassicurante dopo l'ultimo capitolo, in cui sono state introdotte varie strutture su uno spazio vettoriale, una dopo l'altra, ciascuna con il proprio gruppo di simmetria. Sembrava non dovesse esserci mai fine. Ora vediamo che in realtà abbiamo incontrato la maggior parte dei tipi possibili di simmetrie, almeno quelli associati ai gruppi algebrici semplici. Non è un caso che tali strutture siano importanti. ■

Un vasto progetto, consistente nella classificazione dei gruppi semplici *finiti*, è stato completato nel 1980. I gruppi semplici finiti che abbiamo visto sono i gruppi di ordine primo, il gruppo icosaedrale  $I \approx A_5$  [cap. 6 (2.3)], e i gruppi  $PSL_2(F)$ , dove  $F$  è un campo finito (8.3), ma ve ne sono molti di più. I gruppi alterni  $A_n$  sono semplici per ogni  $n \geq 5$ .

I gruppi lineari svolgono un ruolo di primo piano nella classificazione dei gruppi semplici finiti come pure dei gruppi algebrici complessi. Ciascuno degli enunciati (8.11) dà origine a un'intera serie di gruppi semplici finiti, sostituendo il campo complesso con campi finiti. Inoltre, alcuni gruppi semplici finiti sono analoghi ai gruppi unitari. Tutti questi gruppi lineari finiti prendono il nome di gruppi del *tipo di Lie*.

In base al teorema (8.3),  $PSL_2(\mathbb{F}_7)$  è un gruppo semplice finito, il suo ordine è 168. Esso è il secondo gruppo semplice più piccolo,  $A_5$  è il più piccolo. Gli ordini dei più piccoli gruppi semplici non abeliani sono:

$$(8.12) \quad 60, 168, 360, 504, 660, 1092, 2448.$$

Per ciascuno di questi sette interi  $N$  esiste un'unica classe di isomorfismo di gruppi semplici di ordine  $N$ , rappresentata da  $PSL_2(F)$ , essendo  $F$  un campo finito opportuno. [Il gruppo alterno  $A_5$  risulta isomorfo a  $PSL_2(\mathbb{F}_5)$ .]

In aggiunta ai gruppi di ordine primo, ai gruppi alterni, e ai gruppi del tipo di Lie, esistono esattamente 26 gruppi semplici finiti chiamati i *gruppi sporadici*. Il gruppo sporadico più piccolo è il *gruppo di Mathieu*  $M_{11}$ , il cui ordine è 7920. Il più grande è chiamato il *Mostro*; il suo ordine è approssimativamente  $10^{53}$ . Pertanto i gruppi semplici finiti formano una lista che, sebbene sia più lunga, è abbastanza analoga alla lista (8.11) di gruppi algebrici semplici.

Non mi par bello, menare vanto dei successi di una teoria e occultarne i fallimenti sotto il tappeto.  
Richard Brauer

### Esercizi

#### 1 I gruppi lineari classici

- (a) Trovare un sottogruppo di  $GL_2(\mathbb{R})$  che sia isomorfo a  $\mathbb{C}^*$ .  
 (b) Dimostrare che, per ogni  $n$ ,  $GL_n(\mathbb{C})$  è isomorfo ad un sottogruppo di  $GL_{2n}(\mathbb{R})$ .
- Dimostrare che  $SO_2(\mathbb{C})$  non è un insieme limitato in  $\mathbb{C}^4$ .
- Dimostrare che  $SP_2(\mathbb{R}) = SL_2(\mathbb{R})$ , ma che  $SP_4(\mathbb{R}) \neq SL_4(\mathbb{R})$ .
- In base alla legge di Sylvester ogni matrice simmetrica reale  $2 \times 2$  è congruente a un'unica matrice appartenente ad un insieme di sei forme standard. Elencare tali forme. Se consideriamo l'azione di  $GL_2(\mathbb{R})$  sulle matrici  $2 \times 2$  data da  $P, A \mapsto PAP^t$ , allora la legge di Sylvester afferma che le matrici simmetriche formano sei orbite. Possiamo considerare le matrici simmetriche come punti di  $\mathbb{R}^3$ , facendo corrispondere

### Esercizi

alla matrice  $\begin{bmatrix} x & y \\ y & z \end{bmatrix}$  il punto  $(x, y, z)$ . Trovare esplicitamente la partizione di  $\mathbb{R}^3$  in orbite, e fare un disegno che illustri chiaramente la configurazione geometrica che ne risulta.

- Una matrice  $P$  è ortogonale se e solo se le sue colonne formano una base ortonormale. Descrivere le proprietà che le colonne di una matrice devono avere affinché essa appartenga al gruppo di Lorentz  $O_{3,1}$ .
- Dimostrare che non esiste nessun isomorfismo continuo dal gruppo ortogonale  $O_4$  al gruppo di Lorentz  $O_{3,1}$ .
- Descrivere mediante equazioni il gruppo  $O_{1,1}$ , e dimostrare che esso ha quattro componenti connesse.
- Descrivere le orbite per l'azione di  $SL_2(\mathbb{R})$  sullo spazio delle matrici simmetriche reali data da  $P, A \mapsto PAP^t$ .
- Sia  $F$  un campo con caratteristica diversa da 2. Descrivere le orbite per l'azione:  $P, A \mapsto PAP^t$  di  $GL_2(F)$  sullo spazio delle matrici simmetriche  $2 \times 2$  a elementi in  $F$ .
- Classificare le orbite di  $GL_n(\mathbb{F}_2)$  per l'azione sullo spazio delle matrici simmetriche  $n \times n$ , trovando rappresentanti per ciascuna classe di congruenza.
- Dimostrare che le seguenti matrici sono simplettiche, essendo i blocchi matrici  $n \times n$ :

$$\begin{bmatrix} -I \\ I \end{bmatrix}, \begin{bmatrix} A^t & \\ & A^{-1} \end{bmatrix}, \begin{bmatrix} I & B \\ & I \end{bmatrix}, \text{ dove } B = B^t \text{ e } A \text{ è invertibile.}$$

- Dimostrare che il gruppo simplettico  $SP_{2n}(\mathbb{R})$  agisce transitivamente su  $\mathbb{R}^{2n}$ .
- Dimostrare che  $SP_{2n}(\mathbb{R})$  è connesso per archi, e concludere che ogni matrice simplettica ha determinante 1.

#### 2 Il gruppo unitario speciale $SU_2$

- Siano  $P, Q$  elementi di  $SU_2$  rappresentati dai vettori reali  $(x_1, x_2, x_3, x_4)$ ,  $(y_1, y_2, y_3, y_4)$ . Calcolare il vettore reale che corrisponde al prodotto  $PQ$ .
- Dimostrare che il sottogruppo  $SO_2$  di  $SU_2$  è coniugato al sottogruppo  $T$  delle matrici.
- Dimostrare che  $SU_2$  è connesso per archi, e così pure  $SO_3$ .
- Dimostrare che  $U_2$  è omeomorfo al prodotto  $S^3 \times S^1$ .
- Sia  $G$  il gruppo delle matrici della forma  $\begin{bmatrix} x & y \\ & 1 \end{bmatrix}$ , dove  $x, y \in \mathbb{R}$  e  $x > 0$ . Determinare le classi di coniugio in  $G$ , e disegnarle nel piano  $(x, y)$ .
- (a) Dimostrare che ogni elemento  $P$  (2.4) di  $SU_2$  può essere scritto come un prodotto:  $P = DRD'$ , dove  $D, D' \in T$  (2.13), e  $R \in SO_2$  è una rotazione di un angolo  $\theta$ , con  $0 \leq \theta \leq \pi/2$ .

(b) Supponiamo che gli elementi  $a, b$  della matrice  $P$  siano diversi da zero. Dimostrare che tale rappresentazione è unica, a meno di sostituire la coppia  $D, D'$  con  $-D, -D'$ .

(c) Descrivere le classi laterali doppie  $TPT$ , con  $P \in SU_2$ . Dimostrare che, se gli elementi  $a, b$  di  $P$  sono diversi da zero, allora la classe laterale doppia è omeomorfa ad un toro, e descrivere le rimanenti classi laterali doppie.

### 3 La rappresentazione ortogonale di $SU_2$

1. Calcolare lo stabilizzatore  $H$  della matrice  $\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$  per l'azione di coniugio mediante  $SU_2$ , e descrivere  $\varphi(P)$  per  $P \in H$ .
2. Dimostrare che ogni circonferenza massima in  $SU_2$  è una classe laterale di una delle longitudini (2.14).
3. Trovare un sottoinsieme di  $\mathbb{R}^3$  che sia omeomorfo allo spazio  $S \times \Theta$  che compare in (3.4).
4. Ricavare una formula per  $\langle A, A \rangle$  espressa mediante il determinante di  $A$ .
5. Si consideri l'applicazione dal gruppo delle rotazioni  $SO_3$  nella 2-sfera ottenuta mandando una matrice di rotazione nella sua prima colonna. Descrivere le fibre di tale applicazione.
6. Estendere l'omomorfismo  $\varphi$  definito in (3.1) ad un omomorfismo  $\Phi : U_2 \rightarrow SO_3$ , e descrivere il nucleo di  $\Phi$ .
7. Dimostrare con un calcolo diretto che la matrice (3.11) appartiene a  $SO_3$ .
- \*8. Descrivere accuratamente le classi di coniugio in  $SO_3$ , mettendole in relazione con le classi di coniugio in  $SU_2$ .
9. Dimostrare che l'azione di  $SU_2$  su una classe di coniugio diversa da  $\{I\}, \{-I\}$  è data da rotazioni della sfera.
10. Stabilire una corrispondenza biunivoca tra gli elementi di  $SO_3$  e le coppie  $(p, v)$  costituite da un punto  $p$  sulla 2-sfera unitaria  $S$  e un vettore tangente unitario  $v$  a  $S$  in  $p$ .
11. Dimostrare la proposizione (3.20).
- \*12. (a) Calcolare esplicitamente la moltiplicazione a sinistra per una matrice  $P$  fissata in  $SU_2$ , per mezzo delle coordinate  $x_1, x_2, x_3, x_4$ . Dimostrare che essa è la moltiplicazione per una matrice ortogonale  $4 \times 4 Q$ , e quindi che è un movimento rigido della 3-sfera unitaria  $S^3$ .
- (b) Dimostrare che  $Q$  è ortogonale con un metodo simile a quello usato nella descrizione della rappresentazione ortogonale, ossia esprimendo il prodotto scalare dei vettori  $(x_1, x_2, x_3, x_4)$ ,  $(x'_1, x'_2, x'_3, x'_4)$  corrispondenti alle due matrici  $P, P' \in SU_2$  mediante operazioni sulle matrici.
- (c) Determinare la matrice che descrive l'azione di coniugio mediante una matrice  $P$  fissata in  $SU_2$ .
- \*13. (a) Sia  $H_i$  il sottogruppo di  $SO_3$  delle rotazioni intorno all'asse  $x_i$ ,  $i = 1, 2, 3$ . Dimostrare che ogni elemento di  $SO_3$  può essere scritto come un prodotto

$ABA'$ , dove  $A, A' \in H_1$  e  $B \in H_2$ . Dimostrare che tale rappresentazione è unica, a meno che  $B = I$ .

(b) Descrivere geometricamente le classi laterali doppie  $H_1 Q H_1$ .

\*14. Sia  $H_i$  il sottogruppo di  $SO_3$  delle rotazioni intorno all'asse  $x_i$ . Dimostrare che ogni elemento  $Q \in SO_3$  può essere scritto nella forma  $A_1 A_2 A_3$ , con  $A_i \in H_i$ .

### 4 Il gruppo lineare speciale $SL_2(\mathbb{C})$

1. Sia  $G = SL_2(\mathbb{C})$ . Utilizzare l'azione di  $G$  sui raggi  $\{rX \mid r \in \mathbb{R}, r \geq 0\}$  in  $\mathbb{C}^2$  per dimostrare che  $G$  è omeomorfo al prodotto  $SU_2 \times H$ , dove  $H$  è lo stabilizzatore del raggio  $\{re_1\}$ , e descrivere esplicitamente  $H$ .

2. (a) Dimostrare che la legge  $P, A \mapsto PAP^*$  definisce un'azione di  $SL_2(\mathbb{C})$  sullo spazio  $W$  di tutte le matrici hermitiane.

(b) Dimostrare che la funzione  $\langle A, A' \rangle = \det(A + A') - \det A - \det A'$  è una forma bilineare su  $W$ , la cui segnatura è  $(3, 1)$ .

(c) Utilizzare (a) e (b) per definire un omomorfismo  $\varphi : SL_2(\mathbb{C}) \rightarrow O_{3,1}$ , il cui nucleo è  $\{\pm I\}$ .

\*(d) Dimostrare che l'immagine di  $\varphi$  è la componente connessa dell'identità in  $O_{3,1}$ .

3. Sia  $P$  una matrice in  $SO_3(\mathbb{C})$ .

(a) Dimostrare che 1 è un autovalore di  $P$ .

(b) Siano  $X_1, X_2$  autovettori di  $P$ , con autovalori  $\lambda_1, \lambda_2$ . Dimostrare che  $X_1^t X_2 = 0$ , a meno che  $\lambda_1 = \lambda_2^{-1}$ .

(c) Dimostrare che, se  $X$  è un autovettore con autovalore 1 e se  $P \neq I$  allora  $X^t X \neq 0$ .

4. Sia  $G = SO_3(\mathbb{C})$ .

(a) Dimostrare che la moltiplicazione a sinistra mediante  $G$  è un'azione transitiva sull'insieme dei vettori  $X$  tali che  $X^t X = 1$ .

(b) Determinare lo stabilizzatore di  $e_1$  per la moltiplicazione a sinistra mediante  $G$ .

(c) Dimostrare che  $G$  è connesso per archi.

### 5 Sottogruppi a un parametro

1. Determinare gli omomorfismi differenziabili da  $\mathbb{C}$  a  $SL_n(\mathbb{C})$ .

2. Descrivere tutti i sottogruppi a un parametro di  $\mathbb{C}^*$ .

3. Descrivere mediante equazioni le immagini di tutti i sottogruppi a un parametro del gruppo delle matrici diagonali reali  $2 \times 2$ , e illustrarle in modo chiaro con un disegno.

4. Sia  $\varphi : \mathbb{R} \rightarrow GL_n(\mathbb{R})$  un sottogruppo a un parametro. Dimostrare che  $\ker \varphi$  o è banale, o è l'intero gruppo, oppure è un gruppo ciclico infinito.

5. Trovare le condizioni su una matrice  $A$  affinché  $e^{tA}$  sia un sottogruppo a un parametro del gruppo unitario speciale  $SU_n$ , e calcolare la dimensione di quel gruppo.

6. Sia  $G$  il gruppo delle matrici reali della forma:  $\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$ , con  $x > 0$ .

- (a) Determinare le matrici  $A$  tali che  $e^{tA}$  sia un sottogruppo a un parametro di  $G$ .  
 (b) Calcolare esplicitamente  $e^A$  per le matrici determinate in (a).

- (c) Disegnare una figura che mostri i sottogruppi a un parametro nel piano  $(x, y)$ .

7. Dimostrare che le immagini dei sottogruppi a un parametro di  $SU_2$  sono i coniugati di  $T$  (cfr. §3). Utilizzare ciò per dare una dimostrazione alternativa del fatto che questi coniugati sono le longitudini.

8. Determinare i sottogruppi a un parametro di  $U_2$ .

9. Sia  $\varphi(t) = e^{tA}$  un sottogruppo a un parametro di  $G$ . Dimostrare che le classi laterali di  $\text{im } \varphi$  sono soluzioni matriciali dell'equazione differenziale  $dX/dt = AX$ .

10. Può accadere che il cammino tracciato da un sottogruppo a un parametro di  $GL_n(\mathbb{R})$  intersechi se stesso?

- \*11. Determinare gli omomorfismi differenziabili da  $SO_2$  a  $GL_n(\mathbb{R})$ .

## 6 L'algebra di Lie

1. Calcolare  $(A + B\epsilon)^{-1}$ , supponendo che  $A$  sia invertibile.

2. Calcolare i vettori tangentici infinitesi alla curva piana di equazione  $y^2 = x^3$  nel punto  $(1, 1)$  e nel punto  $(0, 0)$ .

3. (a) Disegnare la curva  $C$ :  $x_2^2 = x_1^3 - x_1^2$ .

- (b) Dimostrare che tale luogo è una varietà di dimensione 1, se è privato dell'origine.

- (c) Determinare i vettori tangentici infinitesimi a  $C$  nell'origine.

4. Sia  $S$  un insieme algebrico reale definito da una sola equazione  $f = 0$ .

- (a) Dimostrare che l'equazione  $f^2 = 0$  definisce lo stesso luogo  $S$ .

- (b) Dimostrare che  $\nabla(f^2)$  si annulla in ogni punto  $x$  di  $S$ , e quindi che ogni vettore è un vettore tangente infinitesimo in  $x$ , quando  $S$  si considera definito dall'equazione  $f^2 = 0$ .

5. Dimostrare che l'insieme definito dall'equazione  $xy = 1$  è un sottogruppo del gruppo delle matrici diagonali  $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$ , e calcolare la sua algebra di Lie.

6. Determinare l'algebra di Lie del gruppo unitario.

7. (a) Dimostrare la formula:  $\det(I + A\epsilon) = 1 + \text{tr}(A\epsilon)$ .

- (b) Sia  $A$  una matrice invertibile. Calcolare  $\det(A + B\epsilon)$ .

8. (a) Dimostrare che  $O_2$  agisce mediante il coniugio sulla sua algebra di Lie.

- (b)** Dimostrare che l'azione considerata in (a) è compatibile con la forma bilineare:  $\langle A, B \rangle = \frac{1}{2} \text{tr}(AB)$ .  
**(c)** Utilizzare l'azione considerata in (a) per definire un omomorfismo  $O_2 \rightarrow O_2$ , e descrivere esplicitamente tale omomorfismo.

9. Calcolare l'algebra di Lie dei seguenti gruppi:

- (a)  $U_n$ ; (b)  $SU_n$ ; (c)  $O_{3,1}$ ; (d)  $SO_n(\mathbb{C})$ .

In ciascuno dei casi in esame, dimostrare che  $e^{tA}$  è un sottogruppo a un parametro se e soltanto se  $I + Ae$  appartiene al gruppo.

- \*10. Determinare l'algebra di Lie di  $G = SP_{2n}(\mathbb{R})$ , utilizzando la forma a blocchi  $M =$

$$= \left[ \begin{array}{c|c} A & B \\ \hline C & D \end{array} \right].$$

11. (a) Dimostrare che  $\mathbb{R}^3$  diventa un'algebra di Lie se la parentesi è definita come il prodotto vettoriale:

$$[X, Y] = X \times Y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

- (b) Dimostrare che tale algebra di Lie è isomorfa all'algebra di Lie di  $SO_3$ .

12. Classificare tutte le algebre di Lie complesse di dimensione  $\leq 3$ .

- \*13. La rappresentazione aggiunta di un gruppo lineare  $G$  è la rappresentazione mediante il coniugio sulla sua algebra di Lie:  $G \times L \rightarrow L$  definito da  $P, A \mapsto PAP^{-1}$ . La forma  $\langle A, A' \rangle = \text{tr}(AA')$  su  $L$  è chiamata la forma di Killing. Per ciascuno dei gruppi seguenti, verificare che, se  $P \in G$  e  $A \in L$ , allora  $PAP^{-1} \in L$ , e dimostrare che la forma di Killing è simmetrica e bilineare e che l'azione è compatibile con la forma, ossia, che  $\langle A, A' \rangle = \langle PAP^{-1}, PA'P^{-1} \rangle$ :

- (a)  $SO_n$ ; (b)  $SU_n$ ; (c)  $O_{3,1}$ ; (d)  $SO_n(\mathbb{C})$ ; (e)  $SP_{2n}(\mathbb{R})$ .

14. Dimostrare che la forma di Killing è definita negativa sull'algebra di Lie di

- (a)  $SO_n$ ; (b)  $SU_n$ .

15. Determinare la segnatura della forma di Killing sull'algebra di Lie di  $SL_n(\mathbb{R})$ .

16. (a) Utilizzare la rappresentazione aggiunta del gruppo  $SU_n$  per definire un omomorfismo  $\varphi : SU_n \rightarrow SO_m$ , dove  $m = n^2 - 1$ .

- (b) Dimostrare che, per  $n = 2$ , questa rappresentazione è equivalente alla rappresentazione ortogonale definita nel §3.

17. Definire un isomorfismo  $SL_2(\mathbb{C})/\{\pm 1\} \approx SO_3(\mathbb{C})$  utilizzando la rappresentazione aggiunta di  $SL_2(\mathbb{C})$ .

## 7 Traslazione in un gruppo

1. Calcolare le dimensioni dei seguenti gruppi:

- (a)  $SU_n$ ; (b)  $SO_n(\mathbb{C})$ ; (c)  $SP_{2n}(\mathbb{R})$ ; (d)  $O_{3,1}$ .

2. Utilizzando l'esponenziale, trovare tutte le soluzioni vicine a  $I$  dell'equazione  $P^2 = I$ .

3. Trovare un sottogruppo non abeliano, connesso per archi, di  $GL_2(\mathbb{R})$  di dimensione 2.
4. (a) Dimostrare che ogni matrice hermitiana definita positiva  $A$  è il quadrato di un'altra matrice hermitiana definita positiva  $B$ .  
 (b) Dimostrare che  $B$  è univocamente determinata da  $A$ .
- \*5. Sia  $A$  una matrice non singolare, e sia  $B$  una matrice hermitiana definita positiva tale che  $B^2 = AA^*$ .  
 (a) Dimostrare che  $A^*B^{-1}$  è unitaria.  
 (b) Dimostrare l'esistenza della *decomposizione polare*, ossia che ogni matrice non singolare  $A$  è un prodotto  $A = PU$ , dove  $P$  è una matrice hermitiana definita positiva e  $U$  è una matrice unitaria.  
 (c) Dimostrare che la decomposizione polare è unica.  
 (d) Cosa dice ciò riguardo all'azione di moltiplicazione a sinistra mediante il gruppo unitario  $U_n$  sul gruppo  $GL_n$ ?
- \*6. Enunciare e dimostrare un risultato analogo alla decomposizione polare per le matrici reali.
- \*7. (a) Dimostrare che l'applicazione esponenziale definisce una biiezione tra l'insieme di tutte le matrici hermitiane e l'insieme delle matrici hermitiane definite positive.  
 (b) Descrivere la struttura topologica di  $GL_2(\mathbb{C})$  utilizzando la decomposizione polare e (a).
8. Sia  $B$  una matrice invertibile. Descrivere le matrici  $A$  tali che  $P = e^A$  appartiene al centralizzante di  $B$ .
- \*9. Si denoti con  $S$  l'insieme delle matrici  $P \in SL_2(\mathbb{R})$  con traccia  $r$ . Tali matrici possono essere scritte nella forma  $\begin{bmatrix} x & y \\ z & r-x \end{bmatrix}$ , dove  $(x, y, z)$  appartiene alla quadrica di equazione:  $x(r-x) - yz = 1$ .  
 (a) Dimostrare che la quadrica è un iperboloido a una o a due falde, oppure è un cono, e determinare i valori di  $r$  che corrispondono a ciascun tipo.  
 (b) In ciascuno dei casi descritti, determinare la decomposizione della quadrica in classi di coniugio.  
 (c) Estendere il metodo di dimostrazione del teorema (7.11) per provare che l'unico sottogruppo normale proprio di  $SL_2(\mathbb{R})$  è  $\{\pm I\}$ .
10. Disegnare il campo di vettori tangentì  $PA$  al gruppo  $\mathbb{C}^*$ , quando  $A = (1+i)I$ .

## 8 Gruppi semplici

1. Quali dei seguenti sottogruppi di  $GL_n(\mathbb{C})$  sono gruppi algebrici complessi:  
 (a)  $GL_n(\mathbb{Z})$ ; (b)  $SU_n$ ; (c) matrici triangolari superiori?
2. (a) Scrivere le equazioni polinomiali che definiscono  $SO_n(\mathbb{C})$ .  
 (b) Scrivere le equazioni polinomiali che definiscono il gruppo simplettico.

- (c) Dimostrare che il gruppo unitario  $U_n$  può essere definito da equazioni polinomiali reali nelle parti reali e nelle parti immaginarie degli elementi delle matrici.
3. Determinare i centri dei gruppi  $SL_n(\mathbb{R})$  e  $SL_n(\mathbb{C})$ .
  4. Descrivere gli isomorfismi:  
 (a)  $PSL_2(\mathbb{F}_2) \approx S_3$ ; (b)  $PSL_2(\mathbb{F}_3) \approx A_4$ .
  5. Determinare le classi di coniugio di  $GL_2(\mathbb{F}_3)$ .
  6. Dimostrare che  $SL_2(F) = PSL_2(F)$  per ogni campo  $F$  di caratteristica 2.
  7. (a) Determinare tutti i sottogruppi normali di  $GL_2(\mathbb{C})$  che contengono il suo centro  $Z = \{cI\}$ .  
 (b) Fare la stessa cosa per  $GL_2(\mathbb{R})$ .
  8. Per ciascuno dei sette ordini (8.12), determinare l'ordine del campo  $F$  tale che  $PSL_2(F)$  abbia ordine  $n$ .
  - \*9. Dimostrare che esiste un gruppo semplice di ordine 3420.
  10. (a) Sia  $Z$  il centro di  $GL_n(\mathbb{C})$ . È vero che  $PSL_n(\mathbb{C})$  è isomorfo a  $GL_n(\mathbb{C})/Z$ ?  
 (b) Risolvere lo stesso problema posto in (a), sostituendo  $\mathbb{C}$  con  $\mathbb{R}$ .
  11. Dimostrare che  $PSL_2(\mathbb{F}_5)$  è isomorfo ad  $A_5$ .
  - \*12. Analizzare la dimostrazione del teorema (8.3) per provare che  $PSL_2(F)$  è un gruppo semplice quando  $F$  è un campo di caratteristica 2, eccetto il solo caso in cui  $F = \mathbb{F}_2$ .
  13. (a) Sia  $P$  una matrice appartenente al centro di  $SO_n$ , e sia  $A$  una matrice antisimmetrica. Dimostrare che  $PA = AP$  derivando la funzione di matrice  $e^{At}$ .  
 (b) Dimostrare che il centro di  $SO_n$  è banale se  $n$  è dispari ed è  $\{\pm I\}$  se  $n$  è pari e  $\geq 4$ .
  14. Calcolare gli ordini dei seguenti gruppi:  
 (a)  $SO_2(\mathbb{F}_3)$  e  $SO_3(\mathbb{F}_3)$ .  
 (b)  $SO_2(\mathbb{F}_5)$  e  $SO_3(\mathbb{F}_5)$ .
  - \*15. (a) Si consideri l'azione di  $SL_2(\mathbb{C})$  mediante il coniugio sullo spazio  $V$  delle matrici complesse  $2 \times 2$ . Dimostrare che, fissata la base  $(e_{11}, e_{12}, e_{21}, e_{22})$  di  $V$ , la matrice del coniugio mediante  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  ha la forma a blocchi  $\begin{bmatrix} aB & bB \\ cB & dB \end{bmatrix}$ , dove  

$$B = (A^t)^{-1} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$
  
 (b) Dimostrare che tale azione definisce un omomorfismo  $\varphi : SL_2(\mathbb{C}) \rightarrow GL_4(\mathbb{C})$ , e che l'immagine di  $\varphi$  è isomorfa a  $PSL_2(\mathbb{C})$ .  
 (c) Dimostrare che  $PSL_2(\mathbb{C})$  è un gruppo algebrico, trovando equazioni polinomiali negli elementi  $y_{ij}$  di una matrice  $4 \times 4$  le cui soluzioni sono esattamente le matrici appartenenti a  $\text{im } \varphi$ .
  - \*16. Dimostrare che  $PSL_n(\mathbb{C})$  è un gruppo semplice.

- \*17. Non esiste nessun gruppo semplice di ordine  $2^5 \cdot 7 \cdot 11$ . Ammettendo questo risultato, determinare il più piccolo ordine, maggiore di 2448, per un gruppo semplice non abeliano.

### Esercizi vari

1. I *quaternioni* sono espressioni della forma  $\alpha = a + bi + cj + dk$ , dove  $a, b, c, d \in \mathbb{R}$ . Essi possono essere sommati, e moltiplicati usando le regole della moltiplicazione per il gruppo  $H$  [cap. 2 (2.13)].

- (a) Posto  $\bar{\alpha} = a - bi - cj - dk$ , calcolare  $\alpha\bar{\alpha}$ .
- (b) Dimostrare che ogni quaternione  $\alpha \neq 0$  ha un inverso moltiplicativo.
- (c) Dimostrare che l'insieme dei quaternioni  $\alpha$  tali che  $a^2 + b^2 + c^2 + d^2 = 1$  forma un gruppo rispetto alla moltiplicazione che è isomorfo a  $SU_2$ .

2. Il *gruppo affine*  $A_n = A_n(\mathbb{R})$  è il gruppo dei cambiamenti di coordinate in  $(x_1, \dots, x_n)$  che è generato da  $GL_n(\mathbb{R})$  e dal gruppo  $T_n$  delle traslazioni:  $t_a(x) = x + a$ . Dimostrare che  $T_n$  è un sottogruppo normale di  $A_n$  e che  $A_n/T_n$  è isomorfo a  $GL_n(\mathbb{R})$ .

3. *Trasformata di Cayley*. Denotiamo con  $U$  l'insieme delle matrici  $A$  tali che  $I + A$  è invertibile, e definiamo  $A' = (I - A)(I + A)^{-1}$ .

- (a) Dimostrare che se  $A \in U$  allora  $A' \in U$ , e dimostrare che  $A'' = A$ .
- (b) Si denoti con  $V$  lo spazio vettoriale delle matrici reali antisimmetriche  $n \times n$ . Dimostrare che la legge:  $A \mapsto (I - A)(I + A)^{-1}$  definisce un omeomorfismo da un intorno di  $O$  in  $V$  ad un intorno di  $I$  in  $SO_n$ .
- (c) Trovare un risultato analogo per il gruppo unitario.
- (d) Posto:  $J = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$ , dimostrare che una matrice  $A \in U$  è simplettica se e soltanto se  $A^T J = -JA$ .

- \*4. Sia  $p(t) = t^2 - ut + 1$  un polinomio di secondo grado a coefficienti nel campo  $F = \mathbb{F}_p$ .

- (a) Dimostrare che se  $p$  ha due radici distinte in  $F$  le matrici con polinomio caratteristico  $p$  formano due classi di coniugio in  $SL_2(F)$ , e determinare i loro ordini.
- (b) Dimostrare che se  $p$  ha due radici coincidenti le matrici con polinomio caratteristico  $p$  formano tre classi di coniugio in  $SL_n(F)$ , e determinare i loro ordini.
- (c) Supponiamo che  $p$  non abbia radici in  $F$ . Determinare il centralizzante della matrice  $A = \begin{bmatrix} -1 & \\ 1 & u \end{bmatrix}$  in  $SL_2(F)$ , e calcolare l'ordine della classe di coniugio di  $A$ .

- (d) Trovare le equazioni delle classi di  $SL_2(\mathbb{F}_3)$  e  $SL_2(\mathbb{F}_5)$ .
- (e) Trovare le equazioni delle classi di  $PSL_2(\mathbb{F}_3)$  e  $PSL_2(\mathbb{F}_5)$ , e confrontare i risultati ottenuti con le equazioni delle classi di  $A_4$  e  $A_5$ .
- (f) Calcolare le equazioni delle classi di  $SL_2(\mathbb{F}_7)$  e  $PSL_2(\mathbb{F}_7)$ . Utilizzare l'equazione delle classi di  $PSL_2(\mathbb{F}_7)$  per dimostrare che tale gruppo è semplice.

## Capitolo 9

### Rappresentazioni di gruppi

Per più di un secolo i matematici hanno compiuto sforzi giganteschi per eliminare il caos in teoria dei gruppi. Ciò nonostante, non siamo in grado di dare risposta ad alcuni dei problemi più semplici.

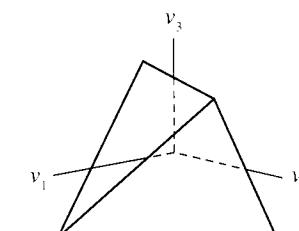
Richard Brauer

#### 1 Definizione di rappresentazione di un gruppo

Le azioni di un gruppo su un insieme sono state studiate nel capitolo 5. In questo capitolo consideriamo il caso in cui gli elementi di un gruppo  $G$  agiscono come operatori lineari su uno spazio vettoriale. Una tale azione definisce un omomorfismo da  $G$  al gruppo lineare generale, e un omomorfismo da un gruppo al gruppo lineare generale è chiamato una *rappresentazione matriciale*.

I gruppi finiti di rotazioni sono dei buoni esempi da tenere a mente. Il gruppo  $T$  delle rotazioni di un tetraedro, per esempio, agisce su uno spazio  $V$  di dimensione tre mediante rotazioni. Non abbiamo mai scritto esplicitamente le matrici che rappresentano questa azione nel capitolo 5, quindi lo facciamo adesso. Una scelta naturale della base consiste nel prendere gli assi coordinati passanti per i punti medi di tre degli spigoli, come illustrato qui sotto:

(1.1)



Indichiamo con  $y_i \in T$  la rotazione di  $\pi$  intorno a uno spigolo e con  $x \in T$  la rotazione di  $2\pi/3$  intorno al vertice anteriore. Le matrici che rappresentano queste

azioni sono:

$$(1.2) \quad R_{y_1} = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}, \quad R_{y_2} = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}, \quad R_{y_3} = \begin{bmatrix} -1 & & \\ & -1 & \\ & & 1 \end{bmatrix},$$

$$R_x = \begin{bmatrix} & 1 \\ 1 & \\ & 1 \end{bmatrix}.$$

Le rotazioni  $\{y_i, x\}$  generano il gruppo  $T$ , e le matrici  $\{R_{y_i}, R_x\}$  generano un gruppo isomorfo di matrici.

È anche facile scrivere esplicitamente matrici che rappresentino le azioni di  $C_n$ ,  $D_n$  e  $O$ , ma l'azione del gruppo icosaedrale  $I$  è abbastanza complicata.

Una *rappresentazione matriciale* di dimensione  $n$  di un gruppo  $G$  è un omomorfismo:

$$(1.3) \quad R : G \rightarrow GL_n(F),$$

dove  $F$  è un campo. Useremo la notazione  $R_g$  per l'immagine di  $g$ . Pertanto ogni matrice  $R_g$  è invertibile, e la moltiplicazione in  $G$  si trasporta alla moltiplicazione tra matrici, ossia  $R_{gh} = R_g R_h$ . Le matrici (1.2) descrivono una rappresentazione matriciale di dimensione tre di  $T$ . Essa risulta *fedele*, cioè  $R$  è un'applicazione iniettiva e pertanto induce un isomorfismo da  $T$  alla sua immagine, che è un sottogruppo di  $GL_3(\mathbb{R})$ . Le rappresentazioni matriciali non sono necessariamente fedeli.

Studiando le rappresentazioni è essenziale lavorare il più possibile senza fissare una base; per facilitare la cosa, introduciamo il concetto di rappresentazione di un gruppo su uno spazio vettoriale di dimensione finita  $V$ . Denotiamo con

$$(1.4) \quad GL(V)$$

il gruppo degli operatori lineari invertibili su  $V$ , con legge di composizione data, come sempre, dalla composizione di funzioni. La scelta di una base di  $V$  definisce un isomorfismo di questo gruppo con il gruppo delle matrici invertibili:

$$(1.5) \quad \begin{aligned} GL(V) &\longrightarrow GL_n(F) \\ T &\longmapsto \text{matrice di } T. \end{aligned}$$

Si definisce *rappresentazione di  $G$  su  $V$*  un omomorfismo

$$(1.6) \quad \rho : G \rightarrow GL(V).$$

La dimensione dello spazio vettoriale  $V$  prende il nome di *dimensione della rappresentazione*  $\rho$ . Studieremo soltanto le rappresentazioni sugli spazi vettoriali di *dimensione finita*.

Le rappresentazioni matriciali possono essere considerate come rappresentazioni di  $G$  sullo spazio  $F^n$  dei vettori colonne.

Sia  $\rho$  una rappresentazione. Denoteremo l'immagine di un elemento  $g$  in  $GL(V)$  con  $\rho_g$ . Pertanto  $\rho_g$  è un operatore lineare su  $V$ , e  $\rho_{gh} = \rho_g \rho_h$ . Se è data una base  $\mathbf{B} = (v_1, \dots, v_n)$ , la rappresentazione  $\rho$  definisce una rappresentazione matriciale  $R$  mediante la regola:

$$(1.7) \quad R_g = \text{matrice di } \rho_g.$$

Simbolicamente, possiamo denotare questa matrice con:

$$(1.8) \quad \rho_g(\mathbf{B}) = \mathbf{B} R_g,$$

come nel capitolo 4 (3.2).

Se  $X$  è il vettore delle coordinate di un vettore  $v \in V$ , ossia se  $v = \mathbf{B} X$ , allora

$$(1.9) \quad R_g X \text{ è il vettore delle coordinate di } \rho_g(v).$$

I gruppi di rotazioni sono esempi di rappresentazioni su uno spazio vettoriale reale  $V$  ottenute senza ricorrere alla scelta di una base. Le rotazioni sono operatori lineari in  $GL(V)$ . In (1.1) abbiamo scelto una base per  $V$ , rappresentando così gli elementi di  $T$  con le matrici (1.2) e ottenendo una rappresentazione matriciale.

Pertanto tutte le rappresentazioni di  $G$  su uno spazio vettoriale di dimensione finita possono essere ridotte a rappresentazioni matriciali, se siamo disposti a scegliere una base. Possiamo aver bisogno di sceglierne una per fare calcoli esplicativi, ma allora dobbiamo studiare cosa accade quando cambiamo una base, quali proprietà sono indipendenti dalla scelta di una base, e quali sono le scelte buone.

Un cambiamento di base in  $V$  dato da una matrice  $P$  trasforma una rappresentazione matriciale  $R$  in una *rappresentazione coniugata*  $R' = P R P^{-1}$ , ossia:

$$(1.10) \quad R'_g = P R_g P^{-1} \quad \text{per ogni } g.$$

Ciò segue dalla regola (3.4) del cap. 4 relativa a un cambiamento di base.

Esiste un concetto equivalente, precisamente quello di *azione* di un gruppo  $G$  su uno spazio vettoriale  $V$ . Quando parliamo di azione su uno spazio vettoriale intendiamo sempre un'azione compatibile con la struttura di spazio vettoriale, altrimenti non dovremmo considerare  $V$  come uno spazio vettoriale. Un'azione siffatta è dunque un'azione di un gruppo nel senso usuale [cap. 5 (5.1)]:

$$(1.11) \quad 1v = v \quad \text{e} \quad (gh)v = g(hv),$$

per ogni  $g, h \in G$  e per ogni  $v \in V$ . Inoltre, si richiede che ogni elemento del gruppo agisca su  $V$  come un *operatore lineare*. Esplicitando ciò, otteniamo le regole:

$$(1.12) \quad g(v + v') = gv + gv' \quad \text{e} \quad g(cv) = cgv,$$

le quali, aggiunte a (1.11), danno un insieme completo di assiomi per un'azione di  $G$  sullo spazio vettoriale  $V$ . Poiché  $G$  agisce sull'insieme sostegno di  $V$ , possiamo parlare di orbite e stabilizzatori come in precedenza.

I due concetti di *azione di  $G$  su  $V$*  e *rappresentazione di  $G$  su  $V$*  sono equivalenti per lo stesso motivo per cui un'azione di un gruppo  $G$  su un insieme  $S$  è equivalente ad una rappresentazione mediante permutazioni (cap. 5, §8). Precisamente, data una rappresentazione  $\rho$  di  $G$  su  $V$ , definiamo un'azione mediante la legge:

$$(1.13) \quad gv = \rho_g(v),$$

e viceversa, data un'azione, la (1.13) può essere usata per definire l'operatore  $\rho_g$  per ogni  $g \in G$ . Si tratta di un operatore lineare in virtù di (1.12), e la proprietà associativa (1.11) prova che  $\rho_g \rho_h = \rho_{gh}$ .

Abbiamo così due notazioni (1.13) per l'azione di  $g$  su  $v$ , e le useremo entrambe, indifferentemente. La notazione  $gv$  è più compatta, e pertanto useremo questa quando sarà possibile.

Nel resto del presente capitolo, per focalizzare l'attenzione, ci concentreremo sulle rappresentazioni *complesse*, che sono anche le più facili da trattare. Gli spazi vettoriali che incontreremo verranno dunque interpretati come spazi vettoriali complessi, e  $GL_n$  denoterà il gruppo lineare generale complesso  $GL_n(\mathbb{C})$ . Ogni rappresentazione matriciale reale, ad esempio la rappresentazione di dimensione tre (1.2) del gruppo delle rotazioni  $T$ , può essere usata per definire una rappresentazione complessa, semplicemente interpretando le matrici reali come matrici complesse. Faremo ciò sistematicamente, senza ulteriori commenti.

## 2 Forme $G$ -invarianti e rappresentazioni unitarie

Una rappresentazione matriciale  $R : G \rightarrow GL_n$  si dice *unitaria* se tutte le matrici  $R_g$  sono unitarie, ossia se l'immagine dell'omomorfismo  $R$  è contenuta nel gruppo unitario. In altre parole, una rappresentazione unitaria è un omomorfismo

$$(2.1) \quad R : G \rightarrow U_n$$

da  $G$  al gruppo unitario.

In questo paragrafo dimostreremo il seguente notevole risultato sulle rappresentazioni dei gruppi finiti:

### (2.2) TEOREMA

- (a) *Ogni sottogruppo finito di  $GL_n$  è coniugato a un sottogruppo di  $U_n$ .*
- (b) *Ogni rappresentazione matriciale  $R : G \rightarrow GL_n$  di un gruppo finito  $G$  è coniugata a una rappresentazione unitaria. In altre parole, data  $R$ , esiste una matrice  $P \in GL_n$  tale che  $PR_g P^{-1} \in U_n$  per ogni  $g \in G$ .*

### (2.3) COROLLARIO

- (a) *Sia  $A$  una matrice invertibile di ordine finito in  $GL_n$ , ossia tale che  $A^r = I$  per qualche  $r$ . Allora  $A$  è diagonalizzabile, cioè esiste una matrice  $P \in GL_n$  tale che  $PAP^{-1}$  è diagonale.*
- (b) *Sia  $R : G \rightarrow GL_n$  una rappresentazione di un gruppo finito  $G$ . Allora, per ogni  $g \in G$ ,  $R_g$  è una matrice diagonalizzabile.*

*Dimostrazione del corollario.* (a) La matrice  $A$  genera un sottogruppo finito di  $GL_n$ . In base al teorema (2.2), questo sottogruppo è coniugato a un sottogruppo del gruppo unitario. Ne segue che  $A$  è coniugata a una matrice unitaria. Il teorema spettrale per gli operatori normali [cap. 7 (7.3)] dice che ogni matrice unitaria è diagonalizzabile. Pertanto  $A$  è diagonalizzabile.

(b) La seconda parte del corollario segue dalla prima, poiché ogni elemento  $g$  di un gruppo finito ha ordine finito. Poiché  $R$  è un omomorfismo, anche  $R_g$  ha ordine finito. ■

Le due parti del teorema (2.2) sono enunciati equivalenti. Possiamo ricavare (a) da (b) considerando l'inclusione di un sottogruppo finito in  $GL_n$  come una rappresentazione matriciale del gruppo. Viceversa, (b) si ottiene applicando (a) all'immagine di  $R$ .

Per dimostrare la parte (b), la rienunciamo con una terminologia che non fa uso delle basi. Consideriamo uno spazio vettoriale hermitiano  $V$  (ossia, uno spazio vettoriale complesso insieme con una forma hermitiana definita positiva  $\langle , \rangle$ ). Un operatore lineare  $T$  su  $V$  è unitario se  $\langle v, w \rangle = \langle T(v), T(w) \rangle$  per ogni  $v, w \in V$  [cap. 7 (5.3b)]. Pertanto è naturale chiamare *unitaria* una rappresentazione  $\rho : G \rightarrow GL(V)$  se  $\rho_g$  è un operatore unitario per ogni  $g \in G$ , ossia se

$$(2.4) \quad \langle v, w \rangle = \langle \rho_g(v), \rho_g(w) \rangle,$$

per ogni  $v, w \in V$  e per ogni  $g \in G$ . Purché la base sia ortonormale, la rappresentazione matriciale  $R$  (1.7) associata ad una rappresentazione unitaria  $\rho$  sarà unitaria nel senso di (2.1). Ciò segue dal capitolo 7 (5.3b).

Per semplificare le notazioni scriviamo la condizione (2.4) nella forma:

$$(2.5) \quad \langle v, w \rangle = \langle gv, gw \rangle.$$

Reinterpretiamo ora tale formula, considerandola come una condizione sulla forma invece che sull'azione. Data una rappresentazione  $\rho$  di  $G$  su uno spazio vettoriale  $V$ , una forma  $\langle \cdot, \cdot \rangle$  su  $V$  si dice  $G$ -invariante se vale la (2.4), o equivalentemente, la (2.5).

(2.6) TEOREMA *Sia  $\rho$  una rappresentazione di un gruppo finito  $G$  su uno spazio vettoriale complesso  $V$ . Allora su  $V$  esiste una forma hermitiana definita positiva,  $G$ -invariante.*

*Dimostrazione.* Prendiamo una qualsiasi forma hermitiana definita positiva su  $V$ , e indichiamola con  $\{ \cdot, \cdot \}$ . Con essa definiamo una forma  $G$ -invariante *facendo una media sul gruppo*. Fare la media su  $G$  è un procedimento generale che sarà usato ancora. Esso è stato già usato nel capitolo 5 (3.2) per trovare un punto fisso rispetto all'azione di un gruppo finito sul piano. La forma  $\langle \cdot, \cdot \rangle$  che vogliamo è definita dalla legge:

$$(2.7) \quad \langle v, w \rangle = \frac{1}{N} \sum_{g \in G} \{gv, gw\},$$

dove  $N = |G|$  è l'ordine di  $G$ . Il fattore di normalizzazione  $1/N$  viene usato comunemente, ma non è importante. Il teorema (2.6) segue dal lemma:

(2.8) LEMMA *La forma (2.7) è hermitiana, definita positiva e  $G$ -invariante.*

*Dimostrazione.* La verifica delle prime due proprietà è completamente automatica. Per esempio:

$$\{gv, g(w + w')\} = \{gv, gw + gw'\} = \{gv, gw\} + \{gv, gw'\},$$

pertanto

$$\begin{aligned} \langle v, w + w' \rangle &= \frac{1}{N} \sum_{g \in G} \{gv, g(w + w')\} = \frac{1}{N} \sum_{g \in G} \{gv, gw\} + \frac{1}{N} \sum_{g \in G} \{gv, gw'\} = \\ &= \langle v, w \rangle + \langle v, w' \rangle. \end{aligned}$$

Per dimostrare che la forma  $\langle \cdot, \cdot \rangle$  è  $G$ -invariante, consideriamo un elemento  $g_0$  di  $G$ . Dobbiamo provare che  $\langle g_0v, g_0w \rangle = \langle v, w \rangle$  per ogni  $v, w \in V$ . Per definizione, si ha:

$$\langle g_0v, g_0w \rangle = \frac{1}{N} \sum_{g \in G} \{gg_0v, gg_0w\}.$$

Esiste un artificio importante per analizzare una tale somma, basato sul fatto che la moltiplicazione a destra per  $g_0$  è un'applicazione biiettiva  $G \rightarrow G$ . Al variare di  $g$  nel gruppo, anche i prodotti  $gg_0$  prendono tutti i valori possibili nel gruppo, in un

**ordine** diverso. Cambiamo le notazioni, scrivendo  $g'$  al posto di  $gg_0$ . Allora, nella **somma**,  $g'$  prende tutti i valori possibili nel gruppo. Pertanto possiamo riscrivere la somma facendo variare  $g'$  anziché  $g$  in  $G$ . Ciò cambia soltanto l'ordine in cui viene effettuata la somma. Allora risulta:

$$\langle g_0v, g_0w \rangle = \frac{1}{N} \sum_{g \in G} \{gg_0v, gg_0w\} = \frac{1}{N} \sum_{g' \in G} \{g'v, g'w\} = \langle v, w \rangle,$$

come richiesto. ■

Il teorema (2.2) è una facile conseguenza del teorema (2.6). Ogni omomorfismo  $R : G \rightarrow GL_n$  è la rappresentazione matriciale associata ad una rappresentazione (con  $V = \mathbb{C}^n$  e  $B = E$ ). In base al teorema (2.6), esiste una forma  $G$ -invariante ( $\langle \cdot, \cdot \rangle$ ) su  $V$ , e scegliamo una base ortonormale per  $V$  rispetto a tale forma. La rappresentazione matriciale  $R'$  ottenuta mediante questa base è coniugata a  $R$  (1.10) e unitaria [cap. 7 (5.3b)]. ■

### (2.9) Esempio

La matrice  $A = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$  ha ordine 3, e pertanto definisce una rappresentazione matriciale  $\{I, A, A^2\}$  del gruppo ciclico  $G$  di ordine 3. Il procedimento di calcolo della media (2.7) produce una forma  $G$ -invariante a partire dal prodotto hermitiano standard  $X^*Y$  su  $\mathbb{C}^2$ :

$$(2.10) \quad \langle X, Y \rangle = \frac{1}{3} [X^*Y + (AX)^*(AY) + (A^2X)^*(A^2Y)] = X^*BX,$$

dove

$$(2.11) \quad B = \frac{1}{3} [I + A^*A + (A^2)^*(A^2)] = \frac{2}{3} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

## 3 Gruppi compatti

Un gruppo lineare di dice *compatto* se è un sottoinsieme chiuso e limitato dello spazio delle matrici [app. (3.8)]. I gruppi compatti più importanti sono il gruppo ortogonale e il gruppo unitario:

(3.1) PROPOSIZIONE *Il gruppo ortogonale e il gruppo unitario sono gruppi compatti.*

*Dimostrazione.* Le colonne di una matrice ortogonale  $P$  formano una base ortonormale, e hanno dunque lunghezza 1. Ne segue che tutti gli elementi della

matrice hanno valore assoluto  $\leq 1$ . Ciò prova che  $O_n$  è contenuto nell'insieme di matrici definito dalle disuguaglianze  $|p_{ij}| \leq 1$ , e quindi è un insieme limitato. Poiché è definito come il luogo degli zeri di un insieme di funzioni continue,  $O_n$  è anche chiuso, e quindi compatto. La dimostrazione relativa al gruppo unitario è la stessa. ■

I teoremi principali (2.2, 2.6) del paragrafo 2 si estendono, senza variazioni di rilievo, al caso dei gruppi lineari compatti. Consideriamo ad esempio il caso del gruppo della circonferenza  $G = SO_2$ . Nel capitolo 5 la rotazione del piano di un angolo  $\theta$  era stata denotata con  $\rho_\theta$ . Qui considereremo una rappresentazione arbitraria di  $G$ . Per evitare confusione, denotiamo l'elemento

$$(3.2) \quad \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \in SO_2$$

con il suo angolo  $\theta$ , anziché con  $\rho_\theta$ . La formula (3.2) definisce una particolare rappresentazione matriciale del gruppo in esame, ma ve ne sono altre.

Supponiamo che sia data una rappresentazione continua  $\sigma$  di  $G$  su uno spazio vettoriale di dimensione finita  $V$ , non necessariamente la rappresentazione (3.2). Poiché la legge di gruppo è l'addizione di angoli, la regola per lavorare con  $\sigma$  è  $\sigma_{\theta+\eta} = \sigma_\theta \sigma_\eta$ .

Dire che la rappresentazione è continua significa che, se scegliamo una base per  $V$ , rappresentando così l'azione di  $\theta$  su  $V$  mediante una matrice  $S_\theta$ , allora gli elementi di  $S_\theta$  sono funzioni continue di  $\theta$ .

Proviamo a copiare la dimostrazione di (2.6). Per calcolare la media sul gruppo infinito  $G$ , sostituiamo la somma con un integrale. Sceglieremo una forma hermitiana definita positiva arbitraria  $\{\cdot, \cdot\}$  su  $V$  e definiamo una nuova forma mediante la legge:

$$(3.3) \quad \langle v, w \rangle = \frac{1}{2\pi} \int_0^{2\pi} \{\sigma_\theta v, \sigma_\theta w\} d\theta.$$

Tale forma ha le proprietà richieste. Per verificare la  $G$ -invarianza, fissiamo un elemento  $\theta_0 \in G$ , e poniamo  $\eta = \theta + \theta_0$ . Allora  $d\eta = d\theta$ . Pertanto risulta:

$$(3.4) \quad \begin{aligned} \langle \sigma_{\theta_0} v, \sigma_{\theta_0} w \rangle &= \frac{1}{2\pi} \int_0^{2\pi} \{\sigma_\theta \sigma_{\theta_0} v, \sigma_\theta \sigma_{\theta_0} w\} d\theta = \\ &= \frac{1}{2\pi} \int_0^{2\pi} \{\sigma_\eta v, \sigma_\eta w\} d\eta = \langle v, w \rangle, \end{aligned}$$

come richiesto.

Non faremo la dimostrazione nel caso generale, poiché occorre fare molto lavoro per trovare un elemento di volume opportuno, analogo a  $d\theta$ , in un gruppo compatto  $G$  qualsiasi. Nel calcolo (3.4), è cruciale il fatto che  $d\theta = d(\theta + \theta_0)$ , e siamo stati fortunati poiché l'integrale che si presentava in modo naturale era proprio quello da usare.

Per ogni gruppo compatto  $G$  esiste un elemento di volume  $dg$  chiamato *misura di Haar*, che ha la proprietà di essere invariante per traslazione. Precisamente, se  $g_0 \in G$  è fissato e  $g' = gg_0$ , allora

$$(3.5) \quad dg = dg'.$$

Utilizzando questa misura, la dimostrazione si generalizza. Non dimostreremo l'esistenza di una misura di Haar, ma ammettendo che una tale misura esista, la stessa argomentazione usata in (2.8) prova i risultati seguenti, analoghi a (2.6) e (2.2):

(3.6) COROLLARIO *Sia  $G$  un sottogruppo compatto di  $GL_n$ . Allora:*

- (a) *Sia  $\sigma$  una rappresentazione di  $G$  su uno spazio vettoriale di dimensione finita  $V$ . Allora su  $V$  esiste una forma hermitiana definita positiva e  $G$ -invariante.*
- (b) *Ogni rappresentazione matriciale continua  $R$  di  $G$  è coniugata ad una rappresentazione unitaria.*
- (c)  *$G$  è coniugato ad un sottogruppo di  $U_n$ .*

#### 4 Sottospazi $G$ -invarianti e rappresentazioni irriducibili

Data una rappresentazione di un gruppo finito  $G$  su uno spazio vettoriale  $V$ , il corollario (2.3) dice che, per ciascun elemento  $g$  del gruppo, esiste una base di  $V$  tale che la matrice dell'operatore  $\rho_g$  è diagonale. Ovviamente, sarebbe molto comodo avere una sola base che diagonalizzasse  $\rho_g$  per tutti gli elementi  $g$  del gruppo nello stesso tempo. Ma ciò non si verifica molto spesso, poiché le matrici diagonali commutano, e quindi, affinché le matrici di tutti gli operatori  $\rho_g$  possano essere diagonalizzate simultaneamente, questi operatori devono commutare tra loro. Ne segue che ogni gruppo  $G$  che ha una rappresentazione fedele mediante matrici diagonali è abeliano. Vedremo più avanti (§ 8) che anche il viceversa è vero, cioè: se  $G$  è un gruppo abeliano finito ogni rappresentazione matriciale  $R$  di  $G$  è diagonalizzabile, ossia esiste una sola matrice  $P$  tale che  $PR_gP^{-1}$  è diagonale per ogni  $g \in G$ . In questo paragrafo esamineremo ciò che si può fare per i gruppi finiti, in generale.

Sia  $\rho$  una rappresentazione di un gruppo  $G$  su uno spazio vettoriale  $V$ . Un sottospazio  $W$  di  $V$  si dice  *$G$ -invariante*, se

$$(4.1) \quad gw \in W \quad \text{per ogni } w \in W \quad \text{e per ogni } g \in G.$$

Pertanto l'azione mediante ogni elemento  $g$  del gruppo deve portare  $W$  in sé, ossia  $gW \subset W$ . Questa è un'estensione del concetto di sottospazio  $T$ -invariante introdotto nel capitolo 4 (§3). In una rappresentazione gli elementi di  $G$  rappresentano operatori lineari su  $V$ , e noi richiediamo che  $W$  sia un sottospazio invariante per ciascuno di tali operatori. Se  $W$  è  $G$ -invariante, l'azione di  $G$  su  $V$  si restringerà a un'azione su  $W$ .

Come esempio, consideriamo la rappresentazione di dimensione tre del gruppo diedrale definito dalle simmetrie di un poligono regolare di  $n$  lati  $\Delta$  [cap. 5 (9.1)]. In tal caso  $G = D_n$ . Vi sono due sottospazi  $G$ -invarianti propri: il piano contenente  $\Delta$  e la retta perpendicolare a  $\Delta$ . D'altra parte, non esiste nessun sottospazio  $T$ -invariante proprio per la rappresentazione (1.2) del gruppo tetraedrale  $T$ , perché non esistono rette o piani mandati in se stessi da ogni elemento di  $T$ .

Se una rappresentazione  $\rho$  di un gruppo  $G$  su uno spazio vettoriale non nullo  $V$  non ha sottospazi propri  $G$ -invarianti è detta *irriducibile*. Se esiste un sottospazio proprio  $G$ -invariante  $\rho$  si dice *riducibile*. La rappresentazione standard di dimensione tre di  $T$  è irriducibile.

Se  $V$  è la somma diretta di sottospazi  $G$ -invarianti:  $V = W_1 \oplus W_2$ , si dice che la rappresentazione  $\rho$  su  $V$  è *somma diretta* delle sue restrizioni  $\rho_i$  a  $W_i$ , e si scrive:

$$(4.2) \quad \rho = \rho_1 \oplus \rho_2.$$

In questo caso, scegliamo basi  $\mathbf{B}_1, \mathbf{B}_2$  di  $W_1, W_2$ , e sia  $\mathbf{B} = (\mathbf{B}_1, \mathbf{B}_2)$  la base di  $V$  ottenuta scrivendo i vettori delle due basi uno dopo l'altro [cap. 3 (6.6)]. Allora la matrice  $R_g$  di  $\rho_g$  avrà la forma a blocchi:

$$(4.3) \quad R_g = \left[ \begin{array}{c|c} A_g & 0 \\ \hline 0 & B_g \end{array} \right],$$

dove  $A_g$  è la matrice di  $\rho_{1g}$  rispetto a  $\mathbf{B}_1$  e  $B_g$  è la matrice di  $\rho_{2g}$  rispetto a  $\mathbf{B}_2$ . Viceversa, se le matrici  $R_g$  si possono scrivere nella forma a blocchi (4.3), allora la rappresentazione è una somma diretta.

Per esempio, consideriamo il gruppo delle rotazioni  $G = D_n$  che agisce su  $\mathbb{R}^3$  mediante le simmetrie di un poligono regolare di  $n$  lati  $\Delta$ . Se scegliamo una base ortonormale  $\mathbf{B}$  tale che  $v_1$  sia perpendicolare al piano di  $\Delta$  e  $v_2$  passi per un vertice, allora le rotazioni corrispondenti ai generatori standard  $x, y$  [cap. 5 (3.6)] sono rappresentate dalle matrici:

$$(4.4) \quad R_x = \begin{bmatrix} 1 & & \\ c_n & -s_n & \\ s_n & c_n \end{bmatrix}, \quad R_y = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix},$$

dove  $c_n = \cos(2\pi/n)$  e  $s_n = \sin(2\pi/n)$ . Quindi  $R$  è una somma diretta di una rappresentazione  $A$  di dimensione uno:

$$(4.5) \quad A_x = [1], \quad A_y = [-1],$$

e di una rappresentazione  $B$  di dimensione due:

$$(4.6) \quad B_x = \begin{bmatrix} c_n & -s_n \\ s_n & c_n \end{bmatrix}, \quad B_y = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}.$$

La rappresentazione  $B$  è la rappresentazione fondamentale di dimensione due di  $D_n$  mediante le simmetrie di  $\Delta$  nel piano.

D'altra parte, anche se una rappresentazione  $\rho$  è riducibile, le matrici  $R_g$  avranno una forma a blocchi solo se la base assegnata per  $V$  sarà compatibile con la decomposizione in somma diretta. Fino a che non avremo fatto un'analisi più approfondita, sarà difficile stabilire che una rappresentazione è riducibile, quando è presentata utilizzando una base sbagliata.

**(4.7) PROPOSIZIONE** *Sia  $\rho$  una rappresentazione unitaria di  $G$  su uno spazio vettoriale hermitiano  $V$ , e sia  $W$  un sottospazio  $G$ -invariante. Allora anche il complemento ortogonale  $W^\perp$  è  $G$ -invariante, e  $\rho$  è la somma diretta delle sue restrizioni a  $W$  e a  $W^\perp$ .*

*Dimostrazione.* Consideriamo un vettore  $v \in W^\perp$ , cioè  $v \perp W$ . Poiché gli operatori  $\rho_g$  sono unitari, conservano l'ortogonalità [cap. 7 (5.2)]; pertanto si ha  $gv \perp gW$ . Poiché  $W$  è  $G$ -invariante,  $W = gW$ , e quindi  $gv \perp W$ . Pertanto  $gv \in W^\perp$ . Ciò prova che  $W^\perp$  è  $G$ -invariante; d'altra parte, sappiamo dal capitolo 7 (2.7) che  $V = W \oplus W^\perp$ . ■

Questa proposizione permette di decomporre una rappresentazione in una somma diretta, purché esista un sottospazio invariante proprio. Procedendo per induzione, essa fornisce il corollario seguente:

**(4.8) COROLLARIO** *Ogni rappresentazione unitaria  $\rho : G \rightarrow GL(V)$  su uno spazio vettoriale hermitiano  $V$  è una somma diretta di rappresentazioni irriducibili.*

Combinando questo corollario con il teorema (2.2), otteniamo il risultato seguente:

**(4.9) COROLLARIO** (Teorema di Maschke) *Ogni rappresentazione di un gruppo finito  $G$  è una somma diretta di rappresentazioni irriducibili.* ■

## 5 Caratteri

Due rappresentazioni  $\rho : G \rightarrow GL(V)$  e  $\rho' : G \rightarrow GL(V')$  di un gruppo  $G$  si dicono *isomorfe*, o *equivalenti*, se esiste un isomorfismo di spazi vettoriali  $T : V \rightarrow V'$  che sia compatibile con l'azione di  $G$ :

$$(5.1) \quad gT(v) = T(gv) \quad \text{ossia} \quad \rho'_g T(v) = T(\rho_g(v)),$$

per ogni  $v \in V$ , e per ogni  $g \in G$ . Se  $\mathbf{B}$  è una base di  $V$  e se  $\mathbf{B}' = T(\mathbf{B})$  è la base corrispondente di  $V'$ , allora le rappresentazioni matriciali associate  $R_g$  e  $R'_g$  saranno *uguali*.

Per i prossimi quattro paragrafi, ci limiteremo a considerare le rappresentazioni di gruppi finiti. Vedremo che le classi di isomorfismo di rappresentazioni irriducibili di un gruppo finito sono relativamente poche. Tuttavia, ogni rappresentazione ha una descrizione complicata in termini di matrici. Il segreto per comprendere le rappresentazioni è quello di non scrivere esplicitamente le matrici, a meno che non sia assolutamente necessario. Per facilitare la classificazione, trascureremo dunque la maggior parte delle informazioni contenute in una rappresentazione  $\rho$ , conservando soltanto una parte essenziale. Ciò con cui lavoreremo è la traccia, chiamata il *carattere* di  $\rho$ . I caratteri si denotano di solito con  $\chi$ .

Il *carattere*  $\chi$  di una rappresentazione  $\rho$  è l'applicazione  $\chi : G \rightarrow \mathbb{C}$  definita da

$$(5.2) \quad \chi(g) = \text{tr}(\rho_g).$$

Se  $R$  è la rappresentazione matriciale ottenuta da  $\rho$  mediante la scelta di una base per  $V$ , allora risulta:

$$(5.3) \quad \chi(g) = \text{tr}(R_g) = \lambda_1 + \cdots + \lambda_n,$$

dove i  $\lambda_i$  sono gli autovalori di  $R_g$ , o di  $\rho_g$ .

Si definisce *dimensione* di un carattere  $\chi$  la dimensione della rappresentazione  $\rho$ . Il carattere di una rappresentazione irriducibile è un *carattere irriducibile*.

Vediamo ora le proprietà fondamentali del carattere:

(5.4) PROPOSIZIONE *Sia  $\chi$  il carattere di una rappresentazione  $\rho$  di un gruppo finito  $G$  su uno spazio vettoriale  $V$ . Allora:*

- (a)  $\chi(1)$  è la dimensione del carattere [la dimensione di  $V$ ].
- (b)  $\chi(g) = \chi(hgh^{-1})$  per ogni  $g, h \in G$ . In altre parole, il carattere è costante su ciascuna classe di coniugio.
- (c)  $\chi(g^{-1}) = \overline{\chi(g)}$  [il complesso coniugato di  $\chi(g)$ ].
- (d) Se  $\chi'$  è il carattere di un'altra rappresentazione  $\rho'$ , allora il carattere della somma diretta  $\rho \oplus \rho'$  è  $\chi + \chi'$ .

## 5 | Caratteri

**Dimostrazione.** Il simbolo 1 nell'enunciato (a) denota l'identità di  $G$ , e quindi questa proprietà è banale:  $\chi(1) = \text{tr} I = \dim V$ . La proprietà (b) è vera perché la rappresentazione matriciale  $R$  associata a  $\rho$  è un omomorfismo (il che implica  $R_{hgh^{-1}} = R_h R_g R_h^{-1}$ ) e perché  $\text{tr}(R_h R_g R_h^{-1}) = \text{tr} R_g$  [cap. 4 (4.18)]. Anche la proprietà (d) è chiara, poiché la traccia della matrice a blocchi (4.3) è la somma delle tracce di  $A_g$  e  $B_g$ .

La proprietà (c) è meno ovvia. Se gli autovalori di  $R_g$  sono  $\lambda_1, \dots, \lambda_n$ , allora gli autovalori di  $R_g^{-1} = (R_g)^{-1}$  sono  $\lambda_1^{-1}, \dots, \lambda_n^{-1}$ . Occorre dimostrare che

$$\chi(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \bar{\lambda}_1 + \cdots + \bar{\lambda}_n = \overline{\chi(g)}.$$

A questo scopo utilizziamo il fatto che  $G$  è un gruppo finito. Ogni elemento  $g$  di  $G$  ha ordine finito. Se  $g$  ha ordine  $r$ , e  $g^r = 1$ ,  $R_g$  è una matrice di ordine  $r$ , e pertanto i suoi autovalori  $\lambda_1, \dots, \lambda_n$  sono radici dell'unità. Ciò implica che  $|\lambda_i| = 1$ , da cui  $\lambda_i^{-1} = \bar{\lambda}_i$  per ogni  $i$ . ■

In questo capitolo, per non confondere i gruppi ciclici con le classi di coniugio, denoteremo le classi di coniugio con il carattere tondo C, anziché col corsivo  $C$ . Pertanto la classe di coniugio di un elemento  $g \in G$  sarà denotata con  $C_g$ .

Il calcolo di un carattere può essere semplificato ove si tenga conto di due cose. Innanzitutto, poiché il valore di  $\chi$  dipende soltanto dalla classe di coniugio di un elemento  $g \in G$  (5.4b), dobbiamo determinare soltanto i valori di  $\chi$  su un rappresentante in ciascuna classe. In secondo luogo, poiché il valore del carattere  $\chi(g)$  è la traccia dell'operatore  $\rho_g$  e poiché la traccia non dipende dalla scelta di una base, siamo liberi di sceglierne una opportuna. Per di più, possiamo scegliere una base opportuna per ciascun elemento del gruppo. Non è necessario usare la stessa base per tutti gli elementi.

Come esempio, determiniamo il carattere  $\chi$  della rappresentazione matriciale del gruppo tetraedrale  $T$  definita da (1.2). Vi sono quattro classi di coniugio in  $T$ , e sono rappresentate dagli elementi  $1, x, x^2, y$ , dove, come prima,  $x$  è una rotazione di  $2\pi/3$  intorno a un vertice e  $y$  è una rotazione di  $\pi$  intorno al centro di uno spigolo. I valori del carattere su questi rappresentanti possono essere ottenuti direttamente dalle matrici (1.2):

$$(5.5) \quad \chi(1) = 3, \quad \chi(x) = 0, \quad \chi(x^2) = 0, \quad \chi(y) = -1.$$

Talvolta è utile considerare un carattere  $\chi$  come un vettore. Per fare ciò, elenchiamo gli elementi di  $G$  in un certo ordine:  $G = \{g_1, \dots, g_N\}$ ; allora il vettore che rappresenta  $\chi$  sarà

$$(5.6) \quad \chi = (\chi(g_1), \dots, \chi(g_N))^t.$$

Poiché  $\chi$  è costante sulle classi di coniugio, è naturale descrivere gli elementi di  $G$  elencando le classi di coniugio e scrivendo poi gli elementi di ciascuna classe in

un certo ordine. Nel caso, ad esempio, del carattere (5.5), scrivendo, nell'ordine  $C_1, C_x, C_{x^2}, C_y$ , otteniamo il vettore:

$$(5.7) \quad \chi = (3; 0, 0, 0, 0; 0, 0, 0, 0; -1, -1, -1)^t.$$

Il teorema principale sui caratteri li mette in relazione con il prodotto hermitiano standard su  $\mathbb{C}^N$ . È uno dei più bei teoremi di algebra, perché il suo enunciato è di per sé molto elegante e perché semplifica notevolmente il problema della classificazione delle rappresentazioni. Definiamo:

$$(5.8) \quad \langle \chi, \chi' \rangle = \frac{1}{N} \sum_g \overline{\chi(g)} \chi'(g),$$

dove  $N = |G|$ . Se  $\chi, \chi'$  sono rappresentati da vettori come in (5.7), questo è il prodotto hermitiano standard, rinormalizzato mediante il fattore  $1/N$ .

(5.9) TEOREMA *Sia  $G$  un gruppo di ordine  $N$ , siano  $\rho_1, \rho_2, \dots$  rappresentanti delle classi distinte di isomorfismo di rappresentazioni irriducibili di  $G$ , e sia  $\chi_i$  il carattere di  $\rho_i$ . Allora valgono le seguenti proprietà*

- (a) (Relazioni di ortogonalità) *I caratteri  $\chi_i$  sono ortonormali. In altre parole,  $\langle \chi_i, \chi_j \rangle = 0$ , se  $i \neq j$ , e  $\langle \chi_i, \chi_i \rangle = 1$  per ogni  $i$ .*
- (b) *Esiste un numero finito di classi di isomorfismo di rappresentazioni irriducibili ed è lo stesso numero delle classi di coniugio nel gruppo.*
- (c) *Sia  $d_i$  la dimensione della rappresentazione irriducibile  $\rho_i$ , e sia  $r$  il numero delle classi di isomorfismo di rappresentazioni irriducibili. Allora  $d_i$  divide  $N$ , e inoltre risulta*

$$(5.10) \quad N = d_1^2 + \dots + d_r^2.$$

Questo teorema sarà dimostrato nel paragrafo 9, ad eccezione dell'asserzione che  $d_i$  divide  $N$ , che non verrà dimostrata.

Una funzione a valori complessi  $\varphi : G \rightarrow \mathbb{C}$  che sia costante su ciascuna classe di coniugio è chiamata *funzione di classe*. Poiché una funzione di classe è costante su ciascuna classe, può essere descritta anche come una funzione sull'insieme delle classi di coniugio. Le funzioni di classe formano uno spazio vettoriale complesso, che denotiamo con  $\mathcal{C}$ . Usiamo la forma definita da (5.8) per rendere  $\mathcal{C}$  uno spazio hermitiano.

(5.11) COROLLARIO *I caratteri irriducibili formano una base ortonormale di  $\mathcal{C}$ .*

Ciò segue da (5.9a,b). I caratteri sono linearmente indipendenti perché sono ortogonali, e generano  $\mathcal{C}$  perché la dimensione di  $\mathcal{C}$  è il numero delle classi di coniugio, che è uguale a  $r$ . ■

Il corollario permette di esprimere un carattere assegnato come una combinazione lineare dei caratteri irriducibili, utilizzando la formula per la proiezione ortogonale [cap. 7 (3.8)]. Infatti, sia  $\chi$  il carattere di una rappresentazione  $\rho$ . In base al corollario (4.9),  $\rho$  è isomorfa a una somma diretta di rappresentazioni irriducibili appartenenti a  $\{\rho_1, \dots, \rho_r\}$ , e pertanto può essere scritta nella forma:  $\rho = n_1 \rho_1 \oplus \dots \oplus n_r \rho_r$ , dove gli  $n_i$  sono interi non negativi e  $n_i \rho_i$  sta a indicare la somma diretta di  $n_i$  copie della rappresentazione  $\rho_i$ . Allora  $\chi = n_1 \chi_1 + \dots + n_r \chi_r$ . Poiché  $(\chi_1, \dots, \chi_r)$  è una base ortonormale, si hanno i risultati seguenti:

(5.12) COROLLARIO *Siano  $\chi_1, \dots, \chi_r$  i caratteri irriducibili di un gruppo finito  $G$ , e sia  $\chi$  un carattere arbitrario. Allora  $\chi = n_1 \chi_1 + \dots + n_r \chi_r$ , dove  $n_i = \langle \chi, \chi_i \rangle$ .*

(5.13) COROLLARIO *Se due rappresentazioni hanno lo stesso carattere sono isomorfe.*

Infatti, siano  $\chi, \chi'$  i caratteri di due rappresentazioni  $\rho, \rho'$ , dove  $\rho = n_1 \rho_1 \oplus \dots \oplus n_r \rho_r$  e  $\rho' = n'_1 \rho_1 \oplus \dots \oplus n'_r \rho_r$ . Risulta  $\chi = n_1 \chi_1 + \dots + n_r \chi_r$  e  $\chi' = n'_1 \chi_1 + \dots + n'_r \chi_r$ . Poiché  $\chi_1, \dots, \chi_r$  sono linearmente indipendenti,  $\chi = \chi'$  implica che  $n_i = n'_i$  per ogni  $i$ . ■

(5.14) COROLLARIO *Un carattere  $\chi$  ha la proprietà  $\langle \chi, \chi \rangle = 1$  se e solo se è irriducibile.*

Infatti, se  $\chi = n_1 \chi_1 + \dots + n_r \chi_r$ , allora  $\langle \chi, \chi \rangle = n_1^2 + \dots + n_r^2$ , che vale 1 se e soltanto se un solo coefficiente  $n_i$  è uguale a 1 e tutti gli altri sono uguali a 0. ■

Il calcolo di  $\langle \chi, \chi \rangle$  è un modo molto pratico per verificare l'irriducibilità di una rappresentazione. Per esempio, sia  $\chi$  il carattere (5.7) della rappresentazione (1.2). Allora  $\langle \chi, \chi \rangle = (3^2 + 1 + 1 + 1)/12 = 1$ , quindi  $\chi$  è irriducibile.

La parte (c) del teorema (5.9) dovrebbe essere esaminata in antitesi con l'equazione delle classi [cap. 6 (1.7)]. Siano  $C_1, \dots, C_r$  le classi di coniugio in  $G$  e sia  $c_i = |C_i|$  l'ordine della classe di coniugio. Allora  $c_i$  divide  $N$ , e  $N = c_1 + \dots + c_r$ . Sebbene il numero delle classi di coniugio sia uguale al numero delle rappresentazioni irriducibili, la relazione precisa tra di esse è molto sottile.

Come primo esempio, determineremo le rappresentazioni irriducibili del gruppo diedrale  $D_3$  [cap. 5 (3.6)]. Vi sono tre classi di coniugio:  $C_1 = \{1\}$ ,  $C_2 = \{y, xy, x^2y\}$ ,  $C_3 = \{x, x^2\}$  [cap. 6 (1.8)], e quindi tre rappresentazioni irriducibili. L'unica soluzione dell'equazione (5.10) è  $6 = 1^2 + 1^2 + 2^2$ , perciò  $D_3$  ha due rappresentazioni di dimensione uno  $\rho_1, \rho_2$  e una rappresentazione irriducibile di dimensione due  $\rho_3$ . Ogni gruppo  $G$  ha la rappresentazione di dimensione uno *banale* ( $R_g = 1$  per ogni  $g$ ), chiamiamola  $\rho_1$ . L'altra rappresentazione di dimensione uno è la *rappresentazione mediante il segno* del gruppo simmetrico  $S_3$ , il quale è isomorfo a  $D_3$ :  $R_g = \text{sign}(g) = \pm 1$ . Questa è la rappresentazione (4.5), chiamiamola  $\rho_2$ . La rappresentazione di dimensione due è definita da (4.6), chiamiamola  $\rho_3$ .

Piuttosto che elencare i caratteri  $\chi_i$  pensati come vettori, di solito li raggrupperemo in una *tabella dei caratteri*. Nella tabella seguente, le tre classi di coniugio sono rappresentate dagli elementi  $1, y, x$ . Sopra ogni elemento è riportato l'ordine della classe. Così, ad esempio,  $|C_y| = 3$ .

	Classe di coniugio			Ordine della classe Elemento rappresentativo
	(1)	(3)	(2)	
Carattere irriducibile	1	$y$	$x$	Valore del carattere
	$\chi_1$	1	1	
	$\chi_2$	1	-1	
	$\chi_3$	2	0	-1

Tabella dei caratteri di  $D_3$ 

La prima riga della tabella, corrispondente al carattere banale, è costituita da elementi tutti uguali a 1. La prima colonna contiene le dimensioni delle rappresentazioni, poiché  $\chi_i(1) = \dim \rho_i$ .

Per calcolare la forma bilineare (5.8) sui caratteri, ricordiamo che vi sono tre elementi nella classe di  $y$  e due elementi nella classe di  $x$ . Pertanto si ha:

$$\begin{aligned} \langle \chi_3, \chi_3 \rangle &= \frac{1}{N} \sum_g \overline{\chi_3(g)} \chi_3(g) = \\ &= (1 \cdot (\overline{\chi_3(1)} \chi_3(1)) + 3 \cdot (\overline{\chi_3(y)} \chi_3(y)) + 2 \cdot (\overline{\chi_3(x)} \chi_3(x))) / 6 = \\ &= (1 \cdot \bar{2} \cdot 2 + 3 \cdot \bar{0} \cdot 0 + 2 \cdot (-\bar{1}) \cdot (-1)) / 6 = 1. \end{aligned}$$

Ciò conferma il fatto che  $\rho_3$  è irriducibile. ■

Come secondo esempio, consideriamo il gruppo ciclico di ordine 3  $C_3 = \{1, x, x^2\}$ . Poiché  $C_3$  è abeliano, vi sono tre classi di coniugio, ciascuna costituita da un solo elemento. Il teorema (5.9) prova che vi sono tre rappresentazioni irriducibili, e che ciascuna di esse ha dimensione 1. Sia  $\zeta = \frac{1}{2}(-1 + \sqrt{3}i)$  una radice cubica di 1. Le tre rappresentazioni sono:

$$(5.16) \quad \rho_{1x} = 1, \quad \rho_{2x} = \zeta, \quad \rho_{3x} = \zeta^2.$$

	1	$x$	$x^2$
$\chi_1$	1	1	1
$\chi_2$	1	$\zeta$	$\zeta^2$
$\chi_3$	1	$\zeta^2$	$\zeta$

Tabella dei caratteri di  $C_3$ 

Si noti che  $\bar{\zeta} = \zeta^2$ ; pertanto risulta

$$\langle \chi_2, \chi_3 \rangle = (\bar{1} \cdot 1 + \bar{\zeta} \zeta^2 + \bar{\zeta}^2 \zeta) / 3 = (1 + \zeta + \zeta^2) / 3 = 0,$$

il che è in accordo con le relazioni di ortogonalità. ■

Come terzo esempio, determiniamo la tabella dei caratteri del gruppo tetraedrale  $T$ . Le classi di coniugio  $C_1, C_x, C_{x^2}, C_y$  sono state determinate in precedenza, e l'equazione delle classi è  $12 = 1 + 4 + 4 + 3$ . L'unica soluzione di (5.10) è  $12 = 1^2 + 1^2 + 3^2$ , quindi esistono 4 rappresentazioni irriducibili, di dimensioni 1, 1, 1, 3. Ora, abbiamo che  $T$  possiede un sottogruppo normale  $H$  di ordine 4 isomorfo al gruppo quadrinomio di Klein, e tale che il quoziente  $\bar{T} = T/H$  è ciclico di ordine 3. Ogni rappresentazione  $\bar{\rho}$  di  $\bar{T}$  darà luogo a una rappresentazione di  $T$ , con la composizione:

$$T \xrightarrow{\pi} \bar{T} \xrightarrow{\bar{\rho}} GL(V).$$

In tal modo, le tre rappresentazioni di dimensione uno del gruppo ciclico determinano delle rappresentazioni di  $T$ . I loro caratteri  $\chi_1, \chi_2, \chi_3$  possono essere determinati dalla tabella (5.17). Il carattere (5.5) è denotato con  $\chi_4$  nella tabella riportata qui sotto:

	(1)	(4)	(4)	(3)
	1	$x$	$x^2$	$y$
$\chi_1$	1	1	1	1
$\chi_2$	1	$\zeta$	$\zeta^2$	1
$\chi_3$	1	$\zeta^2$	$\zeta$	1
$\chi_4$	3	0	0	-1

Tabella dei caratteri di  $T$ 

Dalla tabella dei caratteri si possono ricavare facilmente varie informazioni sul gruppo. Dimentichiamo per un momento che essa si riferisce ai caratteri di  $T$ , e supponiamo che sia stata assegnata come la tabella dei caratteri di un gruppo incognito  $G$ . Dopotutto, è concepibile che un'altra classe di isomorfismo di gruppi abbia gli stessi caratteri.

L'ordine di  $G$  è 12, pari alla somma degli ordini delle classi di coniugio. Inoltre, poiché la dimensione di  $\rho_2$  è 1,  $\chi_2(y)$  è la traccia della matrice  $1 \times 1 \rho_2$ . Pertanto il fatto che  $\chi_2(y) = 1$  mostra che anche  $\rho_{2y} = 1$ , ossia che  $y$  appartiene al nucleo di  $\rho_2$ . Infatti, il nucleo di  $\rho_2$  è costituito dall'unione delle due classi di coniugio  $C_1 \cup C_y$ , ed è un sottogruppo  $H$  di ordine 4 di  $G$ . Inoltre,  $H$  è il gruppo quadrinomio di Klein: infatti, se  $H$  fosse il gruppo  $C_4$ , il suo unico elemento di ordine 2 dovrebbe appartenere da solo ad una classe di coniugio. Dal valore di

$\chi_2(x)$  segue inoltre che l'ordine di  $x$  è divisibile per 3. Ritornando alla lista dei gruppi di ordine 12 determinata in precedenza [cap. 6 (5.1)], vediamo che  $G \approx A_4$ . ■

## 6 Le rappresentazioni mediante permutazioni e la rappresentazione regolare

Sia  $S$  un insieme finito. Possiamo costruire una rappresentazione di un gruppo  $G$  a partire da un'azione di  $G$  su  $S$ , passando allo spazio vettoriale  $V = V(S)$  delle combinazioni lineari formali [cfr. cap. 3 (3.21)]:

$$v = \sum_i a_i s_i, \quad a_i \in \mathbb{C}, \quad s_i \in S.$$

Un elemento  $g \in G$  agisce sui vettori permutando gli elementi di  $S$  e lasciando inalterati i coefficienti:

$$(6.1) \quad gv = \sum_i a_i g s_i.$$

Dato un ordinamento  $s_1, \dots, s_n$  di  $S$  e scelta la base  $(s_1, \dots, s_n)$  per  $V$ ,  $R_g$  è la matrice di permutazione che descrive l'azione di  $g$  su  $S$ .

Per esempio, prendiamo  $G = T$  e sia  $S$  l'insieme delle facce del tetraedro:  $S = (f_1, \dots, f_4)$ . L'azione di  $G$  su  $S$  definisce una rappresentazione di  $G$  di dimensione quattro. Sia  $x$  la rotazione di  $2\pi/3$  intorno a una faccia  $f_1$  e  $y$  la rotazione di  $\pi$  intorno a uno spigolo, come prima. Allora, se le facce sono numerate opportunamente, avremo

$$(6.2) \quad R_x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{e} \quad R_y = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Chiameremo  $\rho$  (o  $R$ ) la rappresentazione associata all'azione di  $G$  su  $S$  e parleremo spesso di  $\rho$  come di una rappresentazione mediante permutazioni, sebbene tale espressione abbia un significato anche in un altro contesto (cap. 5, § 8).

Se decomponiamo in orbite un insieme su cui agisce  $G$ , otterremo una decomposizione in una somma diretta della rappresentazione associata, in modo ovvio. Ma vi è una novità importante: il fatto che in  $V(S)$  sono disponibili combinazioni lineari permette di decomporre ulteriormente la rappresentazione. Anche se  $S$  può essere costituito da una sola orbita, la rappresentazione associata  $\rho$  non sarà mai irriducibile, a meno che  $S$  non abbia un solo elemento. Ciò accade poiché il vettore  $w = s_1 + \dots + s_n$  è lasciato fisso da ogni permutazione della base, e di conseguenza il sottospazio di dimensione uno  $W = \{cw\}$  è  $G$ -invariante. La rappresentazione banale è un addendo di ogni rappresentazione mediante permutazioni.

È facile calcolare il carattere di una rappresentazione mediante permutazioni:

$$(6.3) \quad \chi(g) = \text{numero degli elementi di } S \text{ lasciati fissi da } g,$$

poiché per ogni indice lasciato fisso da una permutazione vi è un 1 sulla diagonale della matrice di permutazione associata, e gli altri elementi della diagonale sono uguali a 0. Per esempio, il carattere  $\chi$  della rappresentazione di  $T$  sulle facce di un tetraedro è

$$(6.4) \quad \begin{array}{c|cccc} & 1 & x & x^2 & y \\ \hline x & 4 & 1 & 1 & 0 \end{array},$$

e la tabella dei caratteri (5.18) prova che  $\chi = \chi_1 + \chi_4$ . Pertanto  $\rho \approx \rho_1 \oplus \rho_4$ , in base al corollario (5.13). Come altro esempio, il carattere dell'azione di  $T$  sui sei spigoli del tetraedro è

$$(6.5) \quad \begin{array}{c|cccc} & 1 & x & x^2 & y \\ \hline x & 6 & 0 & 0 & 2 \end{array},$$

e utilizzando ancora (5.18), si ottiene che  $\chi = \chi_1 + \chi_2 + \chi_3 + \chi_4$ .

La rappresentazione regolare  $\rho^{\text{reg}}$  di  $G$  è la rappresentazione associata all'azione di  $G$  su se stesso mediante la moltiplicazione a sinistra. In altre parole, poniamo  $S = G$ , con l'azione della moltiplicazione a sinistra. Tale azione non è particolarmente interessante, mentre lo è la sua rappresentazione associata. Il suo carattere  $\chi^{\text{reg}}$  è particolarmente semplice:

$$(6.6) \quad \chi^{\text{reg}}(1) = N, \quad \text{e} \quad \chi^{\text{reg}}(g) = 0 \quad \text{se } g \neq 1,$$

con  $N = |G|$ . La prima formula è chiara:  $\chi(1) = \dim \rho$ , per qualsiasi rappresentazione  $\rho$ , e  $\rho^{\text{reg}}$  ha dimensione  $N$ . La seconda è conseguenza di (6.3), poiché la moltiplicazione per  $g$  non lascia fisso alcun elemento di  $G$ , tranne il caso in cui  $g = 1$ .

Utilizzando questa formula, è facile calcolare  $\langle \chi^{\text{reg}}, \chi \rangle$ , essendo  $\chi$  il carattere di una rappresentazione  $\rho$  arbitraria, mediante la formula della proiezione ortogonale (5.12):

$$(6.7) \quad \langle \chi^{\text{reg}}, \chi \rangle = \dim \rho,$$

poiché  $\chi(1) = \dim \rho$ . Ciò permette di scrivere  $\chi^{\text{reg}}$  come una combinazione lineare dei caratteri irriducibili:

$$(6.8) \quad \text{COROLLARIO. } \chi^{\text{reg}} = d_1 \chi_1 + \dots + d_r \chi_r, \quad \text{e} \quad \rho^{\text{reg}} \approx d_1 \rho_1 \oplus \dots \oplus d_r \rho_r, \quad \text{dove } d_i \text{ è la dimensione di } \rho_i \text{ e } d_i \rho_i \text{ sta a indicare la somma diretta di } d_i \text{ copie di } \rho_i. ■$$

Non è vero che questa è una formula elegante? Possiamo dedurre la formula (5.10) da (6.8) contando le dimensioni. Ciò prova che la formula (5.10) del teorema (5.9) è conseguenza delle relazioni di ortogonalità.

Per esempio, per il gruppo  $D_3$ , il carattere della rappresentazione regolare è:

$$\begin{array}{c|ccc} & 1 & x & y \\ \hline \chi^{\text{reg}} & 6 & 0 & 0 \end{array},$$

e la tabella (5.15) dimostra che  $\chi^{\text{reg}} = \chi_1 + \chi_2 + 2\chi_3$ , come ci si aspettava.

Come altro esempio, consideriamo la rappresentazione regolare  $R$  del gruppo ciclico  $\{1, x, x^2\}$  di ordine 3. La matrice di permutazione che rappresenta  $x$  è:

$$R_x = \begin{bmatrix} & 1 \\ 1 & & \\ & 1 \end{bmatrix}.$$

I suoi autovalori sono  $1, \zeta, \zeta^2$ , dove  $\zeta = \frac{1}{2}(-1 + \sqrt{3}i)$ . Pertanto  $R_x$  è coniugata a

$$R'_x = \begin{bmatrix} 1 & & \\ & \zeta & \\ & & \zeta^2 \end{bmatrix}.$$

Tale matrice mostra la decomposizione  $\rho^{\text{reg}} \approx \rho_1 \oplus \rho_2 \oplus \rho_3$  della rappresentazione regolare in rappresentazioni irriducibili di dimensione uno.

## 7 Le rappresentazioni del gruppo icosaedrale

In questo paragrafo determineremo i caratteri irriducibili del gruppo icosaedrale. Fino ad ora, abbiamo visto soltanto la sua rappresentazione banale  $\rho_1$  e la rappresentazione di dimensione 3 come gruppo di rotazioni, che denotiamo con  $\rho_2$ . Vi sono cinque classi di coniugio in  $I$  [cap. 6 (2.2)], precisamente:

$$(7.1) \quad C_1 = \{1\},$$

$$C_2 = \{15 \text{ rotazioni "x" di un angolo } \pi\},$$

$$C_3 = \{20 \text{ rotazioni "y" di } 2\pi/3, 4\pi/3\},$$

$$C_4 = \{12 \text{ rotazioni "z" di } 2\pi/5, 8\pi/5\},$$

$$C_5 = \{12 \text{ rotazioni "z"}^2 \text{ di } 4\pi/5, 6\pi/5\}.$$

e quindi ci sono altre tre rappresentazioni irriducibili. Per quanto già sappiamo, l'unica soluzione della (5.10) è  $d_i = 1, 3, 3, 4, 5$ :

$$60 = 1^2 + 3^2 + 3^2 + 4^2 + 5^2.$$

Indichiamo le rappresentazioni rimanenti con  $\rho_3, \rho_4, \rho_5$ , dove  $\dim \rho_3 = 3$ , e così via. Un buon metodo per trovare le rappresentazioni irriducibili mancanti è quello di decomporre alcune rappresentazioni mediante permutazioni, già note. Sappiamo che  $I$  agisce su un insieme di cinque elementi [cap. 6 (2.6)]: ciò fornisce una rappresentazione di dimensione cinque  $\rho'$ . Come abbiamo visto (§ 6), la rappresentazione banale è un addendo di  $\rho'$ . Il suo complemento ortogonale risulta essere la rappresentazione irriducibile di dimensione quattro richiesta:  $\rho' = \rho_1 \oplus \rho_4$ . Inoltre,  $I$  permuta l'insieme dei sei assi passanti per i centri delle facce opposte del dodecaedro. Sia  $\rho''$  la rappresentazione di dimensione sei corrispondente. Allora  $\rho'' = \rho_1 \oplus \rho_5$ . Possiamo verificarlo calcolando i caratteri di  $\rho_4$  e  $\rho_5$ , e applicando il teorema (5.9). I caratteri  $\chi_4, \chi_5$  si calcolano a partire da  $\chi', \chi''$  sottraendo  $\chi_1 = 1$  da ciascun valore (5.4d). Per esempio,  $\rho'$  realizza  $x$  come una permutazione pari di  $\{1, \dots, 5\}$  di ordine 2, e quindi è un prodotto di due trasposizioni disgiunte, che lascia fisso un solo indice. Pertanto  $\chi'(x) = 1$ , e  $\chi_4(x) = 0$ .

La seconda rappresentazione di dimensione tre  $\rho_3$  è abbastanza sottile, perché è molto simile a  $\rho_2$ . Può essere ottenuta nel modo che ora illustreremo. Poiché  $I$  è isomorfo ad  $A_5$ , possiamo considerare  $I$  come un sottogruppo normale del gruppo simmetrico  $S_5$ . Il coniugio mediante un elemento  $p$  di  $S_5$  che non appartiene ad  $A_5$  definisce un automorfismo  $\sigma$  di  $A_5$  che scambia tra loro le due classi di coniugio  $C_4, C_5$ . Le altre classi di coniugio non vengono invece scambiate, poiché i loro elementi hanno ordini diversi. Per esempio, con la notazione in cicli, sia  $z = (12345)$  e  $p = (2354)$ . Allora  $p^{-1}zp = (4532)(12345)(2354) = (13524) = z^2$ . La rappresentazione  $\rho_3$  è  $\rho_2 \circ \sigma$ .

Il carattere di  $\rho_3$  si calcola a partire da quello di  $\rho_2$  scambiando tra loro i valori di  $z$  e  $z^2$ . Una volta calcolati tali caratteri, la verifica delle relazioni  $\langle \chi_i, \chi_j \rangle = 0$ ,  $\langle \chi_i, \chi_i \rangle = 1$  prova che le rappresentazioni sono irriducibili e che la nostra lista è corretta.

	(1)	(15)	(20)	(12)	(12)
	1	x	y	z	$z^2$
$\chi_1$	1	1	1	1	1
$\chi_2$	3	-1	0	$\alpha$	$\beta$
$\chi_3$	3	-1	0	$\beta$	$\alpha$
$\chi_4$	4	0	1	-1	-1
$\chi_5$	5	1	-1	0	0

Tabella dei caratteri di  $I = A_5$

In questa tabella,  $\alpha$  è la traccia di una rotazione dello spazio di un angolo  $2\pi/5$ , sicché:

$$\alpha = 1 + 2 \cos \frac{2\pi}{5} = \frac{1}{2}(-1 + \sqrt{5}),$$

$$\text{e } \beta \text{ si calcola in modo simile: } \beta = 1 + 2 \cos \frac{4\pi}{5} = \frac{1}{2}(-1 - \sqrt{5}).$$

## 8 Rappresentazioni di dimensione uno

Sia  $\rho$  una rappresentazione di dimensione uno di un gruppo  $G$ . Dunque  $R_g$  è una matrice  $1 \times 1$ , e  $\chi(g) = R_g$ , purché identifichiamo una matrice  $1 \times 1$  con il suo unico elemento. Pertanto in questo caso il carattere  $\chi$  è un omomorfismo  $\chi : G \rightarrow \mathbb{C}^*$ , ossia soddisfa la proprietà:

$$(8.1) \quad \chi(gh) = \chi(g)\chi(h) \quad \text{se } \dim \rho = 1.$$

Un carattere con questa proprietà si dice *abeliano*. Conviene notare che la formula (8.1) non è vera per caratteri di dimensione  $> 1$ .

Se  $G$  è un gruppo finito, i valori assunti da un carattere abeliano  $\chi$  sono sempre radici di 1:

$$(8.2) \quad \chi(g)^r = 1$$

per qualche  $r$ , poiché l'elemento  $g$  ha ordine finito.

I caratteri di dimensione uno formano un gruppo rispetto alla moltiplicazione di funzioni:

$$(8.3) \quad \chi\chi'(g) = \chi(g)\chi'(g).$$

Tale gruppo è chiamato il *gruppo dei caratteri* di  $G$  e si indica spesso con  $\hat{G}$ . Il gruppo dei caratteri è particolarmente importante quando  $G$  è abeliano, a causa del risultato seguente:

(8.4) TEOREMA *Se  $G$  è un gruppo abeliano finito, ogni rappresentazione irriducibile di  $G$  ha dimensione uno.*

*Dimostrazione.* Poiché  $G$  è abeliano, ogni classe di coniugio è costituita da un solo elemento e quindi il numero delle classi di coniugio è  $N$ . In base al teorema (5.9), vi sono  $N$  rappresentazioni irriducibili, e  $d_1 = d_2 = \dots = d_r = 1$ . ■

## 9 Lemma di Schur, e dimostrazione delle relazioni di ortogonalità

Siano  $\rho, \rho'$  rappresentazioni di un gruppo  $G$  su due spazi vettoriali  $V, V'$ . Diremo che un'applicazione lineare  $T : V \rightarrow V'$  è  *$G$ -invariante* se è compatibile con le due azioni di  $G$  su  $V$  e  $V'$ , ossia se risulta

$$(9.1) \quad gT(v) = T(gv), \quad \text{oppure } \rho'_g(T(v)) = T(\rho_g(v)),$$

per ogni  $g \in G$  e per ogni  $v \in V$ . In tal modo, un isomorfismo di rappresentazioni (§5) è un'applicazione  $G$ -invariante biiettiva. Potremmo anche scrivere la (9.1) nella forma:

$$(9.2) \quad \rho'_g \circ T = T \circ \rho_g, \quad \text{per ogni } g \in G.$$

Siano date due basi  $\mathbf{B}, \mathbf{B}'$ , rispettivamente di  $V, V'$ , e denotiamo con  $R_g, R'_g$  e  $A$  le matrici di  $\rho_g, \rho'_g$  e  $T$  rispetto ad esse. Allora (9.2) può essere riscritta nella forma:

$$(9.3) \quad R'_g A = A R_g, \quad \text{per ogni } g \in G.$$

Il caso  $\rho = \rho'$  è molto importante. Un operatore lineare  $G$ -invariante  $T$  su  $V$  è un operatore che commuta con  $\rho_g$  per ogni  $g \in G$ :

$$(9.4) \quad \rho_g \circ T = T \circ \rho_g \quad \text{oppure } R_g A = A R_g.$$

Se  $\rho = \rho'$  le (9.4) sono semplici ripetizioni di (9.2) e (9.3).

(9.5) PROPOSIZIONE *Il nucleo e l'immagine di un'applicazione lineare  $G$ -invariante  $T : V \rightarrow V'$  sono sottospazi  $G$ -invarianti, rispettivamente di  $V$  e  $V'$ .*

*Dimostrazione.* Il nucleo e l'immagine di una qualsiasi applicazione lineare sono sottospazi. Dimostriamo che  $\ker T$  è  $G$ -invariante: vogliamo provare che  $gv \in \ker T$  se  $v \in \ker T$ , ossia che  $T(gv) = 0$  se  $T(v) = 0$ . Ebbene si ha:

$$T(gv) = gT(v) = g0 = 0.$$

Analogamente, se  $v' \in \text{im } T$ , allora  $v' = T(v)$  per qualche  $v \in V$ . Allora risulta:

$$gv' = gT(v) = T(gv),$$

sicché anche  $gv' \in \text{im } T$ . ■

(9.6) TEOREMA (Lemma di Schur) *Siano  $\rho, \rho'$  due rappresentazioni irriducibili di  $G$  su due spazi vettoriali  $V, V'$  rispettivamente, e sia  $T : V \rightarrow V'$  un'applicazione lineare  $G$ -invariante.*

- (a) Esistono due sole possibilità per  $T$ :  $T$  è un isomorfismo, oppure  $T = 0$ .  
 (b) Se  $V = V'$  e  $\rho = \rho'$ , allora  $T$  è la moltiplicazione per uno scalare.

*Dimostrazione.* (a) Poiché  $\rho$  è irriducibile e poiché  $\ker T$  è un sottospazio  $G$ -invariante, si ha  $\ker T = V$  oppure  $\ker T = 0$ . Nel primo caso  $T = 0$ . Nel secondo caso  $T$  è iniettiva e porta, mediante un isomorfismo,  $V$  nella sua immagine. Allora  $\text{im } T \neq 0$ . Poiché  $\rho'$  è irriducibile e  $\text{im } T$  è  $G$ -invariante, si ha  $\text{im } T = V'$ . Pertanto  $T$  è un isomorfismo.

(b) Supponiamo che  $V = V'$ , sicché  $T$  è un operatore lineare su  $V$ . Scegliamo un autovalore  $\lambda$  di  $T$ . Allora  $(T - \lambda I) = T_1$  è anch'esso  $G$ -invariante. Il suo nucleo è diverso da zero perché contiene un autovettore. Poiché  $\rho$  è irriducibile,  $\ker T_1 = V$ , il che implica che  $T_1 = 0$ . Allora  $T = \lambda I$ . ■

Il procedimento di calcolo della media può essere usato per costruire un'applicazione  $G$ -invariante a partire da un'applicazione lineare arbitraria  $T : V \rightarrow V'$ . Per fare ciò, riscriviamo la condizione (9.1) nella forma:

$$T(v) = \rho_g^{-1}(T(\rho_g(v))),$$

oppure

$$(9.7) \quad T(v) = g^{-1}(T(gv)).$$

La media è l'operatore lineare  $\tilde{T}$  definito da

$$(9.8) \quad \tilde{T}(v) = \frac{1}{N} \sum_g g^{-1}(T(gv)),$$

dove  $N = |G|$ , come prima. Se sono date delle basi per  $V, V'$  e se le matrici per  $\rho_g, \rho'_g, T, \tilde{T}$  sono, rispettivamente,  $R_g, R'_g, A, \tilde{A}$ , allora:

$$(9.9) \quad \tilde{A} = \frac{1}{N} \sum_g R_g^{-1} A R_g.$$

Poiché le composizioni e le somme di applicazioni lineari sono ancora lineari,  $\tilde{T}$  è un'applicazione lineare. Per dimostrare che è  $G$ -invariante, fissiamo un elemento  $h \in G$  e poniamo  $g' = gh$ . Cambiando gli indici come nella dimostrazione del lemma (2.8), si ha:

$$h^{-1}\tilde{T}(hv) = \frac{1}{N} \sum_g h^{-1}g^{-1}(T(ghv)) = \frac{1}{N} \sum_{g'} g'^{-1}(T(g'v)) = \tilde{T}(v).$$

Pertanto  $\tilde{T}(hv) = h\tilde{T}(v)$ . Poiché  $h$  è arbitrario, ciò prova che  $\tilde{T}$  è  $G$ -invariante. ■

Può accadere che alla fine si ottenga l'applicazione lineare banale, ossia  $\tilde{T} = 0$ , sebbene  $T$  sia diverso da zero. Infatti, il lemma di Schur afferma che *dobbiamo*

ottenere  $\tilde{T} = 0$  se  $\rho$  e  $\rho'$  sono irriducibili ma non isomorfe. Faremo un buon uso di questo fatto apparentemente negativo nella dimostrazione delle relazioni di ortogonalità.

Quando  $\rho = \rho'$ , si ottiene spesso che la media è diversa da zero, utilizzando la proposizione seguente:

(9.10) PROPOSIZIONE *Sia  $\rho$  una rappresentazione di un gruppo finito  $G$  su uno spazio vettoriale  $V$ , e sia  $T : V \rightarrow V$  un operatore lineare. Definiamo  $\tilde{T}$  mediante la formula (9.8). Allora  $\text{tr } \tilde{T} = \text{tr } T$ . Quindi, se la traccia di  $T$  è diversa da zero, anche  $\tilde{T}$  è diverso da zero.*

*Dimostrazione.* Scriviamo la (9.9), con  $R' = R$ . Poiché  $\text{tr } A = \text{tr}(R_g^{-1} A R_g)$ , l'enunciato è dimostrato. ■

Vediamo ora un esempio di calcolo. Sia  $G = C_3 = \{1, x, x^2\}$ , e sia  $\rho = \rho'$  la rappresentazione regolare (§ 6) di  $G$ , sicché  $V = \mathbb{C}^3$  e

$$R_x = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Sia  $T$  l'operatore lineare la cui matrice è

$$B = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Allora la matrice di  $\tilde{T}$  è

$$\tilde{B} = \frac{1}{3} (IBI + R_x^{-1}BR_x + R_x^{-2}BR_x^2) =$$

$$= \frac{1}{3} (B + R_x^2 BR_x + R_x BR_x^2) = \frac{1}{3} \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}.$$

Oppure, sia  $T$  l'operatore lineare la cui matrice è la matrice di permutazione corrispondente alla trasposizione  $y = (1 \ 2)$ . La media sul gruppo è una somma delle tre trasposizioni:  $(y + x^{-1}yx + x^{-2}yx)/3 = (y + xy + x^2y)/3$ . In questo caso si ha

$$P = \frac{1}{3} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \tilde{P} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Si noti che  $\tilde{B}$  e  $\tilde{P}$  commutano con  $R_x$  come asserito [cfr. (9.4)], anche se ciò non accade per le matrici originarie  $B$  e  $P$ .

Dimostreremo ora le relazioni di ortogonalità, ossia il teorema (5.9a); abbiamo visto (§ 6) che la formula (5.10) è una conseguenza di tali relazioni.

Siano  $\chi, \chi'$  due caratteri irriducibili non isomorfi, corrispondenti a rappresentazioni  $\rho, \rho'$  di  $G$  su  $V, V'$ . Utilizzando la proprietà

$$\chi'(g^{-1}) = \overline{\chi'(g)},$$

possiamo riscrivere la relazione di ortogonalità  $\langle \chi', \chi \rangle = 0$  che ci proponiamo di dimostrare, nella forma:

$$(9.11) \quad \frac{1}{N} \sum_g \chi'(g^{-1}) \chi(g) = 0.$$

Ora il lemma di Schur afferma che ogni applicazione lineare  $G$ -invariante  $V \rightarrow V'$  è nulla. In particolare, è nulla l'applicazione lineare  $\tilde{T}$  che otteniamo con un procedimento di media a partire da un'applicazione lineare arbitraria  $T$ . Tenuto conto della formula (9.9), se ne deduce quanto segue:

(9.12) LEMMA *Se  $R, R'$  sono rappresentazioni irriducibili non isomorfe di  $G$  si ha:*

$$\sum_g R'_{g^{-1}} A R_g = 0,$$

per ogni matrice  $A$  della dimensione opportuna. ■

Cominciamo a entrare nel vivo del problema verificando l'ortogonalità quando  $\rho$  e  $\rho'$  hanno dimensione 1. In questo caso,  $R_g$  e  $R'_g$  sono matrici  $1 \times 1$ , ossia scalari, e  $\chi(g) = R_g$ . Se poniamo  $A = 1$ , allora, fatta eccezione per il fattore  $1/N$ , la proprietà enunciata in (9.12) si riduce alla relazione (9.11), e la tesi è dimostrata.

Inoltre, dal lemma (9.12) si deduce, dopo qualche calcolo, l'ortogonalità in dimensioni superiori. Denotiamo gli elementi di una matrice  $M$  con  $(M)_{ij}$ , come nel cap. 4 (§ 7). Allora  $\chi(g) = \text{tr } R_g = \sum_i (R_g)_{ii}$ . Pertanto  $\langle \chi', \chi \rangle$  si sviluppa nella forma seguente:

$$(9.13) \quad \langle \chi', \chi \rangle = \frac{1}{N} \sum_g \sum_{i,j} (R'_{g^{-1}})_{ii} (R_g)_{jj}.$$

Possiamo invertire l'ordine delle sommatorie, e quindi, per dimostrare che  $\langle \chi', \chi \rangle = 0$ , basta far vedere che per ogni  $i, j$ , si ha:

$$(9.14) \quad \sum_g (R'_{g^{-1}})_{ii} (R_g)_{jj} = 0.$$

La dimostrazione del lemma seguente è elementare:

(9.15) LEMMA *Siano  $M, N$  matrici e poniamo  $P = M e_{\alpha\beta} N$ , dove  $e_{\alpha\beta}$  è una unità matriciale di dimensione opportuna. Allora gli elementi di  $P$  sono  $(P)_{ij} = (M)_{i\alpha} (N)_{\beta j}$ . ■*

Sostituendo  $A$  con  $e_{ij}$  nel lemma (9.12) e applicando il lemma (9.15), otteniamo:

$$0 = (0)_{ij} = \sum_g (R'_{g^{-1}} e_{ij} R_g)_{ij} = \sum_g (R'_{g^{-1}})_{ii} (R_g)_{jj},$$

come richiesto. Ciò prova che se  $\chi$  e  $\chi'$  sono caratteri di rappresentazioni irriducibili non isomorfe,  $\langle \chi', \chi \rangle = 0$ .

Supponiamo ora che  $\chi = \chi'$ . Dobbiamo far vedere che  $\langle \chi, \chi \rangle = 1$ . Calcolando la media di  $A$  come nella (9.9) non si ottiene ora necessariamente la matrice nulla, ma, in base al lemma di Schur, si ottiene una matrice scalare:

$$(9.16) \quad \frac{1}{N} \sum_g R_{g^{-1}} A R_g = \tilde{A} = aI.$$

Per la (9.10), si ha  $\text{tr } A = \text{tr } \tilde{A}$ , e  $\text{tr } \tilde{A} = da$ , dove  $d = \dim \rho$ . Pertanto risulta:

$$(9.17) \quad a = \text{tr } A/d.$$

Poniamo  $A = e_{ij}$  in (9.16) e applichiamo di nuovo il lemma (9.15), ottenendo

$$(9.18) \quad (aI)_{ij} = \frac{1}{N} \sum_g (R_{g^{-1}} A R_g)_{ij} = \frac{1}{N} \sum_g (R_{g^{-1}})_{ii} (R_g)_{jj},$$

dove  $a = (\text{tr } e_{ij})/d$ . Il primo membro della (9.18) è uguale a zero se  $i \neq j$ , ed è uguale a  $1/d$  se  $i = j$ . Ne segue che i termini con  $i \neq j$  nella (9.13) si annullano, e che

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{N} \sum_g \sum_i (R_{g^{-1}})_{ii} (R_g)_{ii} = \sum_i \left[ \frac{1}{N} \sum_g (R_{g^{-1}})_{ii} (R_g)_{ii} \right] = \\ &= \sum_i 1/d = 1. \end{aligned}$$

Ciò completa la dimostrazione del fatto che i caratteri irriducibili  $\chi_1, \chi_2, \dots$  sono ortonormali.

Dobbiamo ancora dimostrare che il numero dei caratteri irriducibili è uguale al numero delle classi di coniugio o, equivalentemente, che i caratteri irriducibili generano lo spazio  $\mathcal{C}$  delle funzioni di classe. Sia  $\mathcal{H}$  il sottospazio da essi generato. Allora [cap. 7 (2.15)] risulta  $\mathcal{C} = \mathcal{H} \oplus \mathcal{H}^\perp$ . Pertanto dobbiamo far vedere che  $\mathcal{H}^\perp = 0$ , ossia, che una funzione di classe  $\phi$  ortogonale ad ogni carattere è la funzione nulla.

Sia  $\phi$  una funzione di classe, cioè una funzione a valori complessi su  $G$  che è costante sulle classi di coniugio. Sia  $\chi$  il carattere di una rappresentazione  $\rho$ , e consideriamo l'operatore lineare  $T : V \rightarrow V$  definito da

$$(9.19) \quad T = \frac{1}{N} \sum_g \overline{\phi(g)} \rho_g.$$

La sua traccia è

$$(9.20) \quad \text{tr } T = \frac{1}{N} \sum_g \overline{\phi(g)} \chi(g) = \langle \phi, \chi \rangle = 0,$$

poiché  $\phi$  è ortogonale a  $\chi$ .

(9.21) LEMMA *L'operatore  $T$  definito da (9.19) è  $G$ -invariante.*

*Dimostrazione.* Dobbiamo provare, in virtù della (9.2), che  $\rho_h \circ T = T \circ \rho_h$ , ossia  $T = \rho_h^{-1} \circ T \circ \rho_h$ , per ogni  $h \in G$ . Poniamo  $g'' = h^{-1}gh$ . Allora, quando  $g$  varia nel gruppo  $G$ , altrettanto fa  $g''$ , e naturalmente  $\rho_h^{-1} \rho_{g''} \rho_h = \rho_{g''}$ . Inoltre  $\phi(g) = \phi(g'')$  poiché  $\phi$  è una funzione di classe. Pertanto

$$\rho_h^{-1} T \rho_h = \frac{1}{N} \sum_g \overline{\phi(g)} \rho_h^{-1} \rho_{g''} \rho_h = \frac{1}{N} \sum_{g''} \overline{\phi(g'')} \rho_{g''} = T,$$

come richiesto. ■

Ora, se  $\rho$  è irriducibile, applicando il lemma di Schur (9.6b), si ottiene che  $T = cI$ . Poiché  $\text{tr } T = 0$  [cfr. (9.20)], ne segue che  $T = 0$ . Ogni rappresentazione  $\rho$  è una somma diretta di rappresentazioni irriducibili, e l'operatore (9.19) è compatibile con le somme dirette. Pertanto in ogni caso risulta  $T = 0$ .

Applichiamo ciò al caso in cui  $\rho = \rho^{\text{reg}}$  è la rappresentazione regolare. Lo spazio vettoriale è  $V(G)$ . Calcoliamo  $T(1)$ , dove  $1$  è l'identità di  $G$ . In base alla definizione di rappresentazione regolare,  $\rho_g(1) = g$  e quindi

$$(9.22) \quad 0 = T(1) = \frac{1}{N} \sum_g \overline{\phi(g)} \rho_g(1) = \frac{1}{N} \sum_g \overline{\phi(g)} g.$$

Poiché gli elementi di  $G$  sono una base per  $V = V(G)$ , ciò mostra che  $\overline{\phi(g)} = 0$  per ogni  $g$ , e quindi che  $\phi = 0$ . ■

## 10 Rappresentazioni del gruppo $SU_2$

Buona parte dei risultati dei paragrafi 6-9 si generalizza senza cambiamenti al caso delle rappresentazioni *continue* di gruppi compatti  $G$ , una volta trovata una misura (di Haar) invariante per traslazioni  $dg$ . Si tratta soltanto di sostituire

la somma con un integrale sul gruppo. Tuttavia, se  $G$  non è finito, vi saranno infinite rappresentazioni irriducibili.

Quando parliamo di una rappresentazione  $\rho$  di un gruppo compatto, intendiamo sempre un omomorfismo continuo da  $G$  a  $GL(V)$ , dove  $V$  è uno spazio vettoriale complesso di dimensione finita. Allora il carattere  $\chi$  di  $\rho$  è una funzione a valori complessi, continua su  $G$ , che è costante su ciascuna classe di coniugio; è cioè una funzione di classe.

Per esempio, l'applicazione identica è una rappresentazione di  $SU_2$  di dimensione due. Il suo carattere è la traccia ordinaria delle matrici  $2 \times 2$ . Chiameremo questa rappresentazione la *rappresentazione standard* di  $SU_2$ . Le classi di coniugio in  $SU_2$  sono gli insiemi di matrici con traccia assegnata  $2c$ ; esse corrispondono alle latitudini  $\{x_1 = c\}$  sulla 3-sfera  $SU_2$  [cap. 8 (2.8)]. Quindi una funzione di classe su  $SU_2$  dipende soltanto da  $x_1$ , e pertanto può essere considerata come una funzione continua sull'intervallo  $[-1, 1]$ . Con le notazioni del capitolo 8 (2.5), il carattere della rappresentazione standard di  $SU_2$  è

$$\chi(P) = \text{tr } P = a + \bar{a} = 2x_1.$$

Denotiamo con  $|G|$  il volume del gruppo compatto  $G$  in esame rispetto alla misura  $dg$ :

$$(10.1) \quad |G| = \int_G 1 dg.$$

Allora la forma hermitiana che sostituisce (5.8) è

$$(10.2) \quad \langle \chi, \chi' \rangle = \frac{1}{|G|} \int_G \overline{\chi(g)} \chi'(g) dg.$$

Con questa definizione si estendono le relazioni di ortogonalità. Valgono inoltre le seguenti estensioni ai gruppi compatti di risultati già visti, e con le stesse dimostrazioni sviluppate per i gruppi finiti:

### (10.3) TEOREMA

- (a) *Ogni rappresentazione di dimensione finita di un gruppo compatto  $G$  è una somma diretta di rappresentazioni irriducibili.*
- (b) *(Lemma di Schur) Siano  $\rho, \rho'$  rappresentazioni irriducibili, e sia  $T : V \rightarrow V'$  un'applicazione lineare  $G$ -invariante. Allora, o  $T$  è un isomorfismo, oppure  $T = 0$ . Se  $\rho = \rho'$ , allora  $T$  è la moltiplicazione per uno scalare.*
- (c) *I caratteri delle rappresentazioni irriducibili sono ortogonali rispetto alla forma (10.2).*
- (d) *Se i caratteri di due rappresentazioni sono uguali le rappresentazioni sono isomorfe.*

- (e) Un carattere  $\chi$  ha la proprietà  $\langle \chi, \chi \rangle = 1$  se e soltanto se  $\rho$  è irriducibile.  
(f) Se  $G$  è abeliano ogni rappresentazione irriducibile ha dimensione uno. ■

Tuttavia, le altre parti del teorema (5.9) non si estendono immediatamente. Il cambiamento più significativo nella teoria riguarda il paragrafo 6. Se  $G$  è connesso non può agire in modo continuo e non banale su un insieme finito, e pertanto le rappresentazioni di dimensione finita non possono essere ottenute da azioni su insiemi. In particolare, la rappresentazione regolare non è di dimensione finita. Per estendere quella parte della teoria sono necessari metodi analitici.

Poiché è facile trovare una misura di Haar per i gruppi  $U_1$  e  $SU_2$ , possiamo ritenere dimostrate per essi tutte le proprietà elencate in (10.3).

Le rappresentazioni del gruppo della circonferenza  $U_1$ , fondamentali per comprendere i gruppi compatti arbitrari, sono facili da descrivere. Sarà conveniente usare di volta in volta la notazione additiva o la notazione moltiplicativa:

$$(10.4) \quad \begin{aligned} SO_2(\mathbb{R}) &\xrightarrow{\sim} U_1 \\ (\text{rotazione di } \theta) &\mapsto e^{i\theta} = \alpha. \end{aligned}$$

(10.5) TEOREMA Le rappresentazioni irriducibili di  $U_1$  sono le applicazioni date dalle potenze  $n$ -esime:

$$U_1 \xrightarrow{n} U_1,$$

le quali mandano  $\alpha$  in  $\alpha^n$ , ovvero  $\theta$  in  $n\theta$ . Esiste un'unica rappresentazione di questo tipo per ogni intero  $n$ .

*Dimostrazione.* In base alla (10.3f), le rappresentazioni irriducibili sono tutte di dimensione uno e inoltre, in virtù di (2.2), sono coniugate a rappresentazioni unitarie. Poiché  $GL_1 = \mathbb{C}^*$  è abeliano, il coniugio è banale, e pertanto una rappresentazione matriciale di dimensione uno è automaticamente unitaria. Ne segue che una rappresentazione irriducibile di  $U_1$  è un omomorfismo continuo di  $U_1$  in sé. Dobbiamo dimostrare che gli unici omomorfismi di questo tipo sono le applicazioni date dalle potenze  $n$ -esime.

(10.6) LEMMA Gli omomorfismi continui dal gruppo additivo  $\mathbb{R}$  in se stesso sono le moltiplicazioni per uno scalare:  $\psi(x) = cx$ , per qualche  $c \in \mathbb{R}$ .

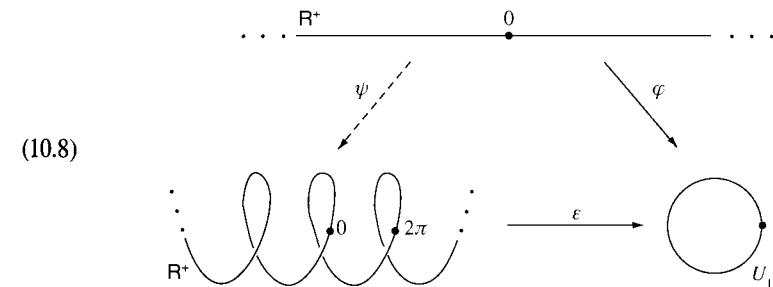
*Dimostrazione.* Sia  $\psi : \mathbb{R} \rightarrow \mathbb{R}$  un omomorfismo continuo. Faremo vedere che  $\psi(x) = x\psi(1)$  per ogni  $x$  e ciò dimostrerà che  $\psi$  è la moltiplicazione per  $c = \psi(1)$ .

Poiché  $\psi$  è un omomorfismo,  $\psi(nr) = \psi(r + \dots + r) = n\psi(r)$  per ogni numero reale  $r$  e per ogni intero non negativo  $n$ . In particolare,  $\psi(n) = n\psi(1)$ . Inoltre,  $\psi(-n) = -\psi(n) = -n\psi(1)$ , e quindi  $\psi(n) = n\psi(1)$  per ogni intero  $n$ . Prendiamo poi un numero razionale  $r = m/n$ . Allora  $n\psi(r) = \psi(nr) = \psi(m) = m\psi(1)$ . Dividendo

per  $n$ , si ottiene:  $\psi(r) = r\psi(1)$  per ogni numero razionale  $r$ . Poiché i razionali sono densi in  $\mathbb{R}$  e  $\psi$  è un'applicazione continua, si ha  $\psi(x) = cx$ , per ogni  $x$ . ■

(10.7) LEMMA Gli omomorfismi continui dal gruppo additivo  $\mathbb{R}$  in  $U_1$  sono del tipo  $\varphi(x) = e^{icx}$  per qualche  $c \in \mathbb{R}$ .

*Dimostrazione.* Se  $\varphi$  è differenziabile, l'asserto può essere dimostrato mediante l'applicazione esponenziale studiata nel capitolo 8 (§5). Dimostriamo ora per un omomorfismo continuo arbitrario. Consideriamo l'omomorfismo  $\epsilon : \mathbb{R} \rightarrow U_1$  definito da  $\epsilon(x) = e^{ix}$ . Tale omomorfismo avvolge la retta intorno alla circonferenza unitaria con periodo  $2\pi$  [cfr. fig. (10.8)]. Data una funzione continua arbitraria  $\varphi : \mathbb{R} \rightarrow U_1$  tale che  $\varphi(0) = 1$ , esiste un unico sollevamento continuo  $\psi$  di tale funzione alla retta reale tale che  $\psi(0) = 0$ . In altre parole, possiamo trovare un'unica funzione continua  $\psi : \mathbb{R} \rightarrow \mathbb{R}$  tale che  $\psi(0) = 0$  e  $\varphi(x) = \epsilon(\psi(x))$  per ogni  $x$ . Il sollevamento si costruisce partendo dalla condizione  $\psi(0) = 0$  ed estendendo poi  $\psi$  un intervallino alla volta.



Dimostreremo ora che se  $\varphi$  è un omomorfismo il suo sollevamento  $\psi$  è anch'esso un omomorfismo. Dopodiché concluderemo che  $\psi(x) = cx$  per qualche  $c$ , in base al lemma (10.6), e quindi che  $\varphi(x) = e^{icx}$ , come richiesto.

La relazione  $\varphi(x+y) = \varphi(x)\varphi(y)$  implica che  $\epsilon(\psi(x+y) - \psi(x) - \psi(y)) = 1$ . Ne segue che  $\psi(x+y) - \psi(x)\psi(y) = 2\pi m$  per qualche intero  $m$  che dipende in modo continuo da  $x$  e  $y$ . Poiché varia con continuità,  $m$  deve essere costante, e ponendo  $x = y = 0$ , si ottiene  $m = 0$ . Pertanto  $\psi$  è un omomorfismo, come affermato. ■

Ora, per completare la dimostrazione del teorema (10.5), sia  $\rho : U_1 \rightarrow U_1$  un omomorfismo continuo. Allora  $\varphi = \rho \circ \epsilon : \mathbb{R} \rightarrow U_1$  è anch'esso un omomorfismo continuo, e pertanto  $\varphi(x) = e^{icx}$ , in base al lemma (10.7). Inoltre,  $\varphi(2\pi) = \rho(1)$ , il che accade se e solo se  $c$  è un intero, diciamo  $n$ . Ne segue che  $\rho(e^{ix}) = e^{inx} = (e^{ix})^n$ . ■

Esaminiamo ora le rappresentazioni del gruppo  $SU_2$ . Anche in questo caso, esiste una famiglia infinita di rappresentazioni irriducibili che vengono fuori in

modo naturale, e che formano di fatto una lista completa. Sia  $V_n$  l'insieme dei polinomi omogenei di grado  $n$  nelle variabili  $u, v$ , cioè le funzioni della forma:

$$(10.9) \quad f(u, v) = x_0 u^n + x_1 u^{n-1} v + \cdots + x_{n-1} u v^{n-1} + x_n v^n,$$

dove i coefficienti  $x_i$  sono numeri complessi. Ovviamente,  $V_n$  è uno spazio vettoriale di dimensione  $n+1$ , con base  $(u^n, u^{n-1} v, \dots, u v^{n-1}, v^n)$ . Il gruppo  $G = GL_2$  agisce su  $V_n$  nel modo che ora illustreremo. Sia  $P \in GL_2$ , diciamo:

$$P = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

e lasciamo agire  $P$  sulla base  $(u, v)$  di  $V_1$  nel modo solito:

$$(u', v') = (u, v)P = (au + cv, bu + dv).$$

Definiamo poi  $\rho_{nP}$  mediante la legge:

$$(10.10) \quad \begin{aligned} u^i v^j &\mapsto u'^i v'^j, \\ f(u, v) &\mapsto x_0 u'^n + x_1 u'^{n-1} v' + \cdots + x_n v'^n; \end{aligned}$$

essa è una rappresentazione:

$$(10.11) \quad \rho_n : G \rightarrow GL(V_n) \approx GL_{n+1}.$$

La rappresentazione banale è  $\rho_0$ , e la rappresentazione standard è  $\rho_1$ .

Per esempio, la matrice di  $\rho_{2P}$  è:

$$(10.12) \quad R_{2P} = \begin{bmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{bmatrix}.$$

La sua prima colonna è il vettore delle coordinate di  $\rho_{2P}(u^2) = (au + cv)^2 = a^2 u^2 + 2acuv + c^2 v^2$ , e così via.

(10.13) TEOREMA *Le rappresentazioni  $\rho_n$  ( $n = 0, 1, 2, \dots$ ) ottenute restringendo la (10.11) al sottogruppo  $SU_2$  sono le rappresentazioni irriducibili di  $SU_2$ .*

*Dimostrazione.* Consideriamo il sottogruppo  $T$  di  $SU_2$  costituito dalle matrici diagonali

$$(10.14) \quad \begin{bmatrix} \alpha & \\ & \bar{\alpha} \end{bmatrix},$$

dove  $\alpha = e^{i\theta}$ . Questo gruppo è isomorfo a  $U_1$ . La classe di coniugio di una matrice unitaria arbitraria  $P$  contiene due matrici diagonali, precisamente:

$$\begin{bmatrix} \lambda & \\ & \bar{\lambda} \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} \bar{\lambda} & \\ & \lambda \end{bmatrix}.$$

dove  $\lambda, \bar{\lambda}$  sono gli autovalori di  $P$  [cap. 7 (7.4)]. Esse coincidono soltanto quando  $\lambda = \pm 1$ . Pertanto ogni classe di coniugio, ad eccezione di  $\{I\}$  e  $\{-I\}$ , interseca  $T$  in una coppia di matrici.

### (10.15) PROPOSIZIONE

- (a) Una funzione di classe su  $SU_2$  è determinata dalla sua restrizione al sottogruppo  $T$ .  
(b) La restrizione a  $T$  di una funzione di classe  $\varphi$  è una funzione pari, cioè:

$$\varphi(\alpha) = \varphi(\bar{\alpha}) \quad \text{ovvero} \quad \varphi(\theta) = \varphi(-\theta). \blacksquare$$

Inoltre, ogni rappresentazione  $\rho$  di  $SU_2$  si restringe a una rappresentazione sul sottogruppo  $T$ , e  $T$  è isomorfo a  $U_1$ . La restrizione a  $T$  di una rappresentazione irriducibile di  $SU_2$  sarà di solito riducibile, ma essa può essere decomposta in una somma diretta di rappresentazioni irriducibili di  $T$ . Pertanto la restrizione del carattere  $\chi$  a  $T$  fornisce una somma di caratteri irriducibili su  $U_1$ . Il teorema (10.5) afferma che i caratteri irriducibili di  $T$  sono le potenze  $n$ -esime  $e^{in\theta}$ , con  $n \in \mathbb{Z}$ . Si ottiene pertanto il risultato seguente:

(10.16) PROPOSIZIONE *La restrizione a  $T$  di un carattere  $\chi$  su  $SU_2$  è una somma finita di funzioni esponenziali  $e^{in\theta}$ .  $\blacksquare$*

Calcoliamo la restrizione a  $T$  del carattere  $\chi_n$  di  $\rho_n$  (10.11). La matrice (10.14) agisce sui monomi nel modo seguente:

$$u^i v^j \mapsto (\alpha^i u^i)(\bar{\alpha}^j v^j) = \alpha^{i-j} u^i v^j.$$

Pertanto la sua matrice, rispetto alla base  $(u^n, u^{n-1} v, \dots, v^n)$ , è la matrice diagonale:

$$\begin{bmatrix} \alpha^n & & & & \\ & \alpha^{n-2} & & & \\ & & \ddots & \ddots & \\ & & & \ddots & \\ & & & & \alpha^{-n} \end{bmatrix},$$

e il valore del carattere è:

$$(10.17) \quad \chi_n(\alpha) = \alpha^n + \alpha^{n-2} + \cdots + \alpha^{-n} = e^{in\theta} + e^{i(n-2)\theta} + \cdots + e^{-in\theta}.$$

ovvero

$$(10.18) \quad \chi_0 = 1$$

$$\chi_1 = 2 \cos \theta = e^{i\theta} + e^{-i\theta}$$

$$\chi_2 = 1 + 2 \cos 2\theta = e^{2i\theta} + 1 + e^{-2i\theta}$$

$$\chi_3 = 2 \cos 3\theta + 2 \cos \theta$$

⋮

Ora, sia  $\chi'$  un carattere irriducibile arbitrario su  $SU_2$ . La sua restrizione a  $T$  è pari (10.15b) ed è una somma di esponenziali  $e^{in\theta}$  (10.16). Affinché sia pari,  $e^{in\theta}$  ed  $e^{-in\theta}$  devono comparire con lo stesso coefficiente, sicché il carattere è una combinazione lineare delle funzioni  $\cos n\theta = \frac{1}{2}(e^{in\theta} + e^{-in\theta})$ . Le funzioni (10.18) formano una base per lo spazio vettoriale generato da  $\{\cos n\theta\}$ . Pertanto risulta:

$$(10.19) \quad \chi' = \sum_i r_i \chi_i,$$

dove gli  $r_i$  sono numeri razionali. A priori, ciò è vero su  $T$ , ma in base a (10.15a), è vero anche su tutto  $SU_2$ . Eliminando i denominatori e portando i termini negativi a sinistra in (10.19), si ottiene una relazione della forma:

$$(10.20) \quad m\chi' + \sum_j n_j \chi_j = \sum_k n_k \chi_k,$$

dove  $n_j, n_k$  sono interi positivi e gli insiemi di indici  $\{j\}, \{k\}$  sono disgiunti. Tale relazione implica:

$$m\rho' \oplus \sum_j n_j \rho_j = \sum_k n_k \rho_k.$$

Pertanto  $\rho'$  è una delle rappresentazioni  $\rho_k$ . Ciò completa la dimostrazione del teorema (10.13). ■

Le generalizzazioni ovvie le lasciamo al lettore.

Israel Herstein

### Esercizi

#### 1 Definizione di rappresentazione di un gruppo

- Sia  $\rho$  una rappresentazione di un gruppo  $G$ . Dimostrare che  $\det \rho$  è una rappresentazione di dimensione uno.

### Esercizi

- Supponiamo che  $G$  sia un gruppo con una rappresentazione fedele mediante matrici diagonali. Dimostrare che  $G$  è abeliano.

- Dimostrare che la legge  $S_n \rightarrow \mathbb{R}^*$  definita da  $p \mapsto \text{sign } p$  è una rappresentazione di dimensione uno del gruppo simmetrico.

- Dimostrare che le uniche rappresentazioni di dimensione uno del gruppo simmetrico  $S_5$  sono la rappresentazione banale definita da  $\rho(g) = 1$  per ogni  $g$  e la rappresentazione mediante il segno.

- (a) Scrivere esplicitamente la rappresentazione standard del gruppo ottaedrale  $O$  mediante rotazioni, scegliendo una base opportuna per  $\mathbb{R}^3$ .

- (b) Fare la stessa cosa per il gruppo diedrale  $D_n$ .

- (c) Fare la stessa cosa per il gruppo icosaedrale  $I$ .

- Dimostrare che la legge

$$\sigma(\theta) = \begin{bmatrix} \alpha & \alpha^2 - \alpha \\ 0 & \alpha^2 \end{bmatrix}, \quad \text{con } \alpha = e^{i\theta},$$

è una rappresentazione di  $SO_2$ , quando una rotazione in  $SO_2$  è rappresentata dal suo angolo.

- Sia  $H$  un sottogruppo di indice 2 di un gruppo  $G$ , e sia  $\rho : G \rightarrow GL(V)$  una rappresentazione. Definiamo  $\rho' : G \rightarrow GL(V)$  ponendo:  $\rho'(g) = \rho(g)$  se  $g \in H$ , e  $\rho'(g) = -\rho(g)$  se  $g \notin H$ . Dimostrare che  $\rho'$  è una rappresentazione di  $G$ .

- Dimostrare che ogni gruppo finito  $G$  ha una rappresentazione fedele su uno spazio vettoriale complesso di dimensione finita.

- Sia  $N$  un sottogruppo normale di un gruppo  $G$ . Mettere in relazione le rappresentazioni di  $G/N$  con le rappresentazioni di  $G$ .

- Scegliere tre assi in  $\mathbb{R}^3$  passanti per i vertici di un tetraedro regolare avente il centro nell'origine. (Non è un sistema di coordinate ortogonali.) Trovare le coordinate del quarto vertice, e scrivere esplicitamente la rappresentazione matriciale del gruppo tetraedrale  $T$  in questo sistema di coordinate.

#### 2 Forme $G$ -invarianti e rappresentazioni unitarie

- (a) Verificare che la forma  $X^*BY$  (2.10) è  $G$ -invariante.  
 (b) Trovare una base ortonormale per questa forma, e determinare la matrice  $P$  del cambiamento di base. Verificare che  $PAP^{-1}$  è unitaria.
- Dimostrare l'analogo reale di (2.2). Precisamente, sia  $R : G \rightarrow GL_n(\mathbb{R})$  una rappresentazione di un gruppo finito  $G$ . Allora esiste una matrice  $P \in GL_n(\mathbb{R})$  tale che  $PR_gP^{-1}$  è ortogonale per ogni  $g \in G$ .
- Sia  $\rho : G \rightarrow SL_2(\mathbb{R})$  una rappresentazione fedele di un gruppo finito mediante matrici  $2 \times 2$  reali di determinante 1. Dimostrare che  $G$  è un gruppo ciclico.
- Determinare tutti i gruppi finiti che hanno una rappresentazione reale fedele di dimensione due.

5. Descrivere i gruppi finiti  $G$  che ammettono rappresentazioni reali fedeli di dimensione tre con determinante 1.
6. Sia  $V$  uno spazio vettoriale hermitiano. Dimostrare che gli operatori unitari su  $V$  formano un sottogruppo  $U(V)$  di  $GL(V)$ , e che una rappresentazione  $\rho$  su  $V$  l'immagine in  $U(V)$  se e solo se la forma  $\langle \cdot, \cdot \rangle$  è  $G$ -invariante.
7. Sia  $\langle \cdot, \cdot \rangle$  una forma antisimmetrica non degenere su uno spazio vettoriale  $V$ , e sia  $\rho$  una rappresentazione di un gruppo finito  $G$  su  $V$ .
  - (a) Dimostrare che il procedimento di calcolo della media (2.7) dà luogo a una forma antisimmetrica  $G$ -invariante su  $V$ .
  - (b) È vero che ciò dimostra che ogni sottogruppo finito di  $GL_{2n}$  è coniugato a un sottogruppo di  $SP_{2n}$ ?
8. (a) Sia  $R$  la rappresentazione standard di dimensione due di  $D_3$ , con il triangolo posizionato in modo che l'asse  $x$  sia una retta di riflessione. Riscrivere questa rappresentazione per mezzo della base:  $x' = x$  e  $y' = x + y$ .
- (b) Utilizzare il procedimento di calcolo della media per ottenere una forma  $G$ -invariante a partire dal prodotto scalare nelle coordinate  $(x', y')$ .

### 3 Gruppi compatti

1. Dimostrare che  $dx/x$  è una misura di Haar sul gruppo moltiplicativo  $\mathbb{R}^*$ .
2. (a) Sia  $P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$  una matrice  $2 \times 2$  variabile, e si denoti con  $dV = dp_{11} dp_{12} dp_{21} dp_{22}$  la forma di volume ordinaria su  $\mathbb{R}^{2 \times 2}$ . Dimostrare che  $(\det P)^{-2} dV$  è una misura di Haar su  $GL_2(\mathbb{R})$ .
- (b) Generalizzare i risultati di (a).
- \*3. Dimostrare che la forma  $\frac{dx_2 dx_3 dx_4}{x_1}$  sulla 3-sfera definisce una misura di Haar su  $SU_2$ . Con che cosa si può sostituire quest'espressione nei punti in cui  $x_1 = 0$ ?
4. Considerare la rappresentazione complessa di  $SO_2$  in  $\mathbb{R}^2$  data da:

$$\sigma(\theta) = \begin{bmatrix} \alpha & \alpha^2 - \alpha \\ 0 & \alpha^2 \end{bmatrix}, \quad \text{con } \alpha = e^{i\theta},$$

e ridurla ad una rappresentazione unitaria calcolando la media del prodotto hermitiano su  $\mathbb{R}^2$ .

### 4 Sottospazi $G$ -invarianti e rappresentazioni irriducibili

1. Dimostrare che la rappresentazione standard di dimensione tre del gruppo tetraedrale  $T$  è irriducibile, come rappresentazione complessa.
2. Determinare tutte le rappresentazioni irriducibili di un gruppo ciclico  $C_n$ .
3. Determinare le rappresentazioni del gruppo icosaedrale  $I$  che non sono fedeli.

### Esercizi

4. Sia  $\rho$  una rappresentazione di un gruppo finito  $G$  su uno spazio vettoriale  $V$  e sia  $v$  un vettore di  $V$ .
  - (a) Dimostrare che, calcolando la media di  $gv$  su  $G$ , si ottiene un vettore  $\bar{v} \in V$  che è lasciato fisso da  $G$ .
  - (b) Cosa si può dire su tale vettore, se  $\rho$  è una rappresentazione irriducibile?
5. Sia  $H$  un sottogruppo di  $G$ , sia  $\rho$  una rappresentazione di  $G$  su  $V$ , e sia  $v$  un vettore di  $V$ . Poniamo  $w = \sum_{h \in H} hv$ . Che cosa si può dire sull'ordine della  $G$ -orbita di  $w$ ?
6. Si consideri la rappresentazione standard di dimensione due del gruppo diedrale  $D_n$  mediante le simmetrie del poligono regolare di  $n$  lati. Per quali valori di  $n$  essa è irriducibile, come rappresentazione complessa?
- \*7. Sia  $G$  il gruppo diedrale  $D_3$ , presentato come nel capitolo 5 (3.6).
  - (a) Sia  $\rho$  una rappresentazione unitaria irriducibile di dimensione 2. Dimostrare che esiste una base ortonormale di  $V$  tale che  $R_y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ .
  - (b) Supponiamo che  $R_y$  sia come sopra. Utilizzare le relazioni di definizione:  $yx = x^2y$ ,  $x^3 = 1$ , per determinare le possibilità per  $R_x$ .
  - (c) Dimostrare che tutte le rappresentazioni irriducibili di dimensione due di  $G$  sono isomorfe.
  - (d) Sia  $\rho$  una rappresentazione di  $G$ , e sia  $v \in V$  un autovettore per l'operatore  $\rho_x$ . Dimostrare che  $v$  è contenuto in un sottospazio  $G$ -invariante  $W$  di dimensione  $\leq 2$ .
  - (e) Determinare tutte le rappresentazioni irriducibili di  $G$ .
5. Caratteri
1. Il corollario (5.11) descrive una base per lo spazio delle funzioni di classe. Trovare un'altra base.
2. Trovare la decomposizione in rappresentazioni irriducibili della rappresentazione di dimensione due standard del gruppo ciclico  $C_n$  mediante rotazioni.
3. È vero che se  $\chi$  è un carattere di un gruppo finito  $G$  e se si definisce  $\bar{\chi}(g) = \overline{\chi(g)}$ , allora anche  $\bar{\chi}$  è un carattere di  $G$ ?
4. Trovare le dimensioni delle rappresentazioni irriducibili del gruppo  $O$  delle rotazioni di un cubo, del gruppo dei quaternioni, e dei gruppi diedrali  $D_4$ ,  $D_5$  e  $D_6$ .
5. Descrivere come sia possibile ottenere una matrice unitaria, adattando opportunamente gli elementi di una tabella dei caratteri.
6. Confrontare le tabelle dei caratteri per il gruppo quaternionale e per il gruppo diedrale  $D_4$ .
7. Determinare la tabella dei caratteri per  $D_6$ .
8. (a) Determinare la tabella dei caratteri per i gruppi  $C_5$  e  $D_5$ .

- (b)** Decomporre la restrizione di ciascun carattere irriducibile di  $D_5$  in caratteri irriducibili di  $C_5$ .
- 9.** **(a)** Sia  $\rho$  una rappresentazione di dimensione  $d$ , con carattere  $\chi$ . Dimostrare che il nucleo di  $\rho$  è l'insieme degli elementi del gruppo tali che  $|\chi(g)| = d$ .
- (b)** Dimostrare che, se  $G$  ha un sottogruppo normale proprio, allora esiste una rappresentazione  $\rho$  tale che  $\ker \rho$  è un sottogruppo proprio.
- \*10.** Sia  $\chi$  il carattere di una rappresentazione  $\rho$  di dimensione  $d$ . Dimostrare che  $|\chi(g)| \leq d$  per ogni  $g \in G$ , e che, se  $|\chi(g)| = d$ , allora  $\rho(g) = \zeta I$ , per qualche radice dell'unità  $\zeta$ .
- 11.** Sia  $G' = G/N$  un gruppo quoziante di un gruppo finito  $G$ , e sia  $\rho'$  una rappresentazione irriducibile di  $G'$ . Dimostrare che la rappresentazione di  $G$  definita da  $\rho'$  è irriducibile, in due modi: direttamente, e utilizzando il teorema (5.9).
- 12.** Trovare le righe mancanti nella seguente tabella di caratteri:
- |          | (1) | (3) | (6) | (6) | (8) |
|----------|-----|-----|-----|-----|-----|
|          | 1   | $a$ | $b$ | $c$ | $d$ |
| $\chi_1$ | 1   | 1   | 1   | 1   | 1   |
| $\chi_2$ | 1   | 1   | -1  | -1  | 1   |
| $\chi_3$ | 3   | -1  | 1   | -1  | 0   |
| $\chi_4$ | 3   | -1  | -1  | 1   | 0   |
- 13.** Si consideri la tabella riportata qui sotto che è una tabella parziale di caratteri di un gruppo finito, in cui  $\zeta = \frac{1}{2}(-1 + \sqrt{3}i)$  e  $\gamma = \frac{1}{2}(-1 + \sqrt{7}i)$ . Le classi di coniugio sono tutte presenti.
- |          | (1) | (3)            | (3)            | (7)     | (7)           |
|----------|-----|----------------|----------------|---------|---------------|
|          | 1   | 1              | 1              | $\zeta$ | $\bar{\zeta}$ |
| $\chi_1$ | 1   | 1              | 1              | $\zeta$ | $\bar{\zeta}$ |
| $\chi_2$ | 3   | $\gamma$       | $\bar{\gamma}$ | 0       | 0             |
| $\chi_3$ | 3   | $\bar{\gamma}$ | $\gamma$       | 0       | 0             |
- (a)** Determinare l'ordine del gruppo e il numero e le dimensioni delle rappresentazioni irriducibili.
- (b)** Determinare i caratteri rimanenti.
- (c)** Descrivere il gruppo mediante generatori e relazioni.
- \*14.** Descrivere il sottogruppo commutatore di un gruppo  $G$  per mezzo della tabella dei caratteri.
- \*15.** Si consideri la seguente tabella parziale di caratteri, in cui manca una classe di coniugio:

	(1)	(1)	(2)	(2)	(3)
	1	$u$	$v$	$w$	$x$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	1	1	-1
$\chi_3$	1	-1	1	-1	$i$
$\chi_4$	1	-1	1	-1	$-i$
$\chi_5$	2	-2	-1	-1	0

**(a)** Completare la tabella.

**(b)** Dimostrare che  $u$  ha ordine 2,  $x$  ha ordine 4,  $w$  ha ordine 6, e  $v$  ha ordine 3. Determinare gli ordini degli elementi nella classe di coniugio mancante.

**(c)** Dimostrare che  $v$  genera un sottogruppo normale.

**(d)** Descrivere il gruppo.

**\*16.** **(a)** Trovare le righe mancanti nella tabella di caratteri riportata qui sotto.

**(b)** Dimostrare che il gruppo  $G$  con questa tabella di caratteri ha un sottogruppo  $H$  di ordine 10, e descrivere tale sottogruppo come unione di classi di coniugio.

**(c)** Stabilire se  $H$  è  $C_{10}$  o  $D_5$ .

**(d)** Determinare il sottogruppo commutatore di  $G$ .

**(e)** Determinare tutti i sottogruppi normali di  $G$ .

**(f)** Determinare gli ordini degli elementi  $a, b, c, d$ .

**(g)** Determinare il numero dei 2-sottogruppi di Sylow e il numero dei 5-sottogruppi di Sylow di questo gruppo.

	(1)	(4)	(5)	(5)	(5)
	1	$a$	$b$	$c$	$d$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	-1	-1	1
$\chi_3$	1	1	$-i$	$i$	-1
$\chi_4$	1	1	$i$	$-i$	-1

**\*17.** Si consideri la seguente tabella di caratteri, con  $\zeta = \frac{1}{2}(-1 + \sqrt{3}i)$ :

	(1)	(6)	(7)	(7)	(7)	(7)	(7)
	1	$a$	$b$	$c$	$d$	$e$	$f$
$\chi_1$	1	1	1	1	1	1	1
$\chi_2$	1	1	1	$\zeta$	$\bar{\zeta}$	$\zeta$	$\bar{\zeta}$
$\chi_3$	1	1	1	$\bar{\zeta}$	$\zeta$	$\bar{\zeta}$	$\zeta$
$\chi_4$	1	1	-1	$-\zeta$	$-\bar{\zeta}$	$\zeta$	$\bar{\zeta}$
$\chi_5$	1	1	-1	$-\bar{\zeta}$	$-\zeta$	$\bar{\zeta}$	$\zeta$
$\chi_6$	1	1	-1	-1	-1	1	1
$\chi_7$	6	-1	0	0	0	0	0

- Dimostrare che  $G$  ha un sottogruppo normale  $N$  isomorfo a  $D_7$ , e determinare la struttura di  $G/N$ .
- Decomporre la restrizione di ciascun carattere a  $N$  in  $N$ -caratteri irriducibili.
- Determinare il numero dei  $p$ -sottogruppi di Sylow, per  $p = 2, 3, 7$ .
- Determinare gli ordini degli elementi rappresentativi  $c, d, e, f$ .

### 6 Le rappresentazioni mediante permutazioni e la rappresentazione regolare

- Verificare i valori dei caratteri (6.4) e (6.5).
- Utilizzare le relazioni di ortogonalità per decomporre il carattere della rappresentazione regolare per il gruppo tetraedrale.
- Dimostrare che la dimensione di una rappresentazione irriducibile arbitraria di un gruppo  $G$  di ordine  $N > 1$  è al più  $N - 1$ .
- Determinare le tabelle dei caratteri per i gruppi non abeliani di ordine 12.
- Decomporre la rappresentazione regolare di  $C_3$  in rappresentazioni *reali* irriducibili.
- Dimostrare il corollario (6.8).
- Sia  $\rho$  la rappresentazione associata all'azione di  $D_3$  su se stesso mediante il coniugio. Decomporre il carattere di  $\rho$  in caratteri irriducibili.
- Sia  $S$  un  $G$ -insieme e sia  $\rho$  la rappresentazione mediante permutazioni di  $G$  sullo spazio  $V(S)$ . Dimostrare che la decomposizione di  $S$  in orbite induce una decomposizione di  $\rho$  in somma diretta.
- Dimostrare che la rappresentazione standard del gruppo simmetrico  $S_n$  mediante matrici di permutazione è la somma di una rappresentazione banale e di una rappresentazione irriducibile.
- \*10.** Sia  $H$  un sottogruppo di un gruppo finito  $G$ . Data una rappresentazione irriducibile  $\rho$  di  $G$ , possiamo decomporre la sua restrizione a  $H$  in  $H$ -rappresentazioni irriducibili. Dimostrare che ogni rappresentazione irriducibile di  $H$  può essere ottenuta in questo modo.

### 7 Le rappresentazioni del gruppo icosaedrale

- Calcolare i caratteri  $\chi_2, \chi_4, \chi_5$  di  $I$  e utilizzare le relazioni di ortogonalità per determinare il carattere rimanente  $\chi_3$ .
- Decomporre le rappresentazioni del gruppo icosaedrale sugli insiemi delle facce, degli spigoli, e dei vertici in rappresentazioni irriducibili.
- Il gruppo  $S_5$  agisce mediante il coniugio sul suo sottogruppo  $A_5$ . Come opera tale azione sull'insieme delle rappresentazioni irriducibili di  $A_5$ ?
- \*4.** Trovare un algoritmo per verificare che un gruppo è semplice, osservando la sua tabella dei caratteri.
- Utilizzare la tabella dei caratteri del gruppo icosaedrale per dimostrare che esso è un gruppo semplice.

- Sia  $H$  un sottogruppo di indice 2 di un gruppo  $G$ , e sia  $\sigma : H \rightarrow GL(V)$  una rappresentazione. Sia  $a$  un elemento di  $G$  non appartenente a  $H$ . Definire una rappresentazione *coniugata*  $\sigma' : H \rightarrow GL(V)$  mediante la legge:  $\sigma'(h) = \sigma(a^{-1}ha)$ .

- Dimostrare che  $\sigma'$  è una rappresentazione di  $H$ .
- Dimostrare che, se  $\sigma$  è la restrizione a  $H$  di una rappresentazione di  $G$ , allora  $\sigma'$  è isomorfa a  $\sigma$ .
- Dimostrare che, se  $b$  è un altro elemento di  $G$  non appartenente a  $H$ , allora la rappresentazione  $\sigma''(h) = \sigma(b^{-1}hb)$  è isomorfa a  $\sigma'$ .
- 7.**
  - Scegliere le coordinate e scrivere esplicitamente la rappresentazione matriciale standard di dimensione tre del gruppo ottaedrale  $O$ .
  - Determinare le cinque classi di coniugio in  $O$ , e trovare gli ordini delle sue rappresentazioni irriducibili.
  - Il gruppo  $O$  agisce sui seguenti insiemi:
    - sei facce del cubo,
    - tre coppie di facce opposte,
    - otto vertici,
    - quattro coppie di vertici opposti,
    - sei coppie di spigoli opposti,
    - due tetraedri inscritti.

Identificare le rappresentazioni irriducibili di  $O$  come addendi di queste rappresentazioni, e calcolare la tabella dei caratteri per  $O$ . Verificare le relazioni di ortogonalità.

- Decomporre ciascuna delle rappresentazioni (c) in rappresentazioni irriducibili.
- Utilizzare la tabella dei caratteri per trovare tutti i sottogruppi normali di  $O$ .
- 8.**
  - Il gruppo icosaedrale  $I$  contiene un sottogruppo  $T$ : lo stabilizzatore di uno dei cubi [cap. 6 (2.7)]. Decomporre le restrizioni a  $T$  dei caratteri irriducibili di  $I$ .
  - Fare la stessa cosa, come in (a), con un sottogruppo  $D_5$  di  $I$ .
- Ecco la tabella dei caratteri per il gruppo  $G = PSL_2(\mathbb{F}_7)$ , con  $\gamma = \frac{1}{2}(-1 + \sqrt{7}i)$ ,  $\gamma' = \frac{1}{2}(-1 - \sqrt{7}i)$ :

	(1)	(21)	(24)	(24)	(42)	(56)
	1	$a$	$b$	$c$	$d$	$e$
$\chi_1$	1	1	1	1	1	1
$\chi_2$	3	-1	$\gamma$	$\gamma'$	1	0
$\chi_3$	3	-1	$\gamma'$	$\gamma$	1	0
$\chi_4$	6	2	-1	-1	0	0
$\chi_5$	7	-1	0	0	-1	1
$\chi_6$	8	0	1	1	0	-1

- (a) Utilizzare la tabella per dare due dimostrazioni diverse del fatto che questo gruppo è semplice.
- (b) Provare a identificare le classi di coniugio degli elementi:

$$\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 2 & \\ & 4 \end{bmatrix},$$

e trovare delle matrici che rappresentano le rimanenti classi di coniugio.

- (c)  $G$  agisce sull'insieme dei sottospazi di dimensione uno di  $F^2(F = \mathbb{F}_7)$ . Decomporre il carattere associato in caratteri irriducibili.

### 8 Rappresentazioni di dimensione uno

1. Dimostrare che i caratteri abeliani di un gruppo  $G$  formano un gruppo.
2. Determinare il gruppo dei caratteri per il gruppo quadrinomio di Klein e per il gruppo dei quaternioni.
3. Siano  $A, B$  matrici tali che qualche potenza di ciascuna di esse sia l'identità e tali che  $A$  e  $B$  commutino tra loro. Dimostrare che esiste una matrice invertibile  $P$  tale che  $PAP^{-1}$  e  $PBP^{-1}$  sono entrambe diagonali.
4. Sia  $G$  un gruppo abeliano finito. Dimostrare che l'ordine del gruppo dei caratteri è uguale all'ordine di  $G$ .
- \*5. Dimostrare che la rappresentazione data dal segno:  $p \mapsto \text{sign } p$  e la rappresentazione banale sono le uniche rappresentazioni di dimensione uno del gruppo simmetrico  $S_n$ .
6. Sia  $G$  un gruppo ciclico di ordine  $n$ , generato da un elemento  $x$ , e poniamo  $\zeta = e^{2\pi i/n}$ .
  - (a) Dimostrare che, se  $\rho_k : G \rightarrow \mathbb{C}^*$  è data da  $\rho_k(x) = \zeta^k$ , le rappresentazioni irriducibili sono  $\rho_0, \dots, \rho_{n-1}$ .
  - (b) Determinare il gruppo dei caratteri di  $G$ .
  - (c) Verificare esplicitamente le relazioni di ortogonalità per  $G$ .
7. (a) Sia  $\varphi : G \rightarrow G'$  un omomorfismo di gruppi abeliani. Definire un omomorfismo indotto  $\hat{\varphi} : \hat{G}' \rightarrow \hat{G}$  tra i loro gruppi dei caratteri.
- (b) Dimostrare che  $\hat{\varphi}$  è suriettivo se  $\varphi$  è iniettivo, e viceversa.

### 9 Lemma di Schur, e dimostrazione delle relazioni di ortogonalità

1. Sia  $\rho$  una rappresentazione di  $G$ . È vero che, se gli unici operatori  $G$ -invarianti su  $V$  sono le moltiplicazioni per uno scalare, allora  $\rho$  è irriducibile?
2. Sia  $\rho$  la rappresentazione standard di dimensione tre di  $T$ , e sia  $\rho'$  la rappresentazione mediante permutazioni ottenuta dall'azione di  $T$  sui quattro vertici. Dimostrare, mediante il calcolo della media, che  $\rho$  è un addendo di  $\rho'$ .
3. Sia  $\rho = \rho'$  la rappresentazione di dimensione due (4.6) del gruppo diedrale  $D_3$ , e si consideri la matrice  $A = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ . Utilizzare il procedimento di calcolo della media

per ottenere un'applicazione  $G$ -invariante a partire dalla moltiplicazione a sinistra per  $A$ .

4. (a) Dimostrare che  $R_x = \begin{bmatrix} 1 & 1 & -1 \\ & 1 \\ 1 & -1 \end{bmatrix}$ ,  $R_y = \begin{bmatrix} & -1 & -1 \\ -1 & & 1 \\ & & -1 \end{bmatrix}$  definiscono una rappresentazione di  $D_3$ .

- (b) Possiamo considerare la rappresentazione  $\rho_2$  di (5.15) come una rappresentazione matriciale  $1 \times 1$ . Sia  $T$  l'applicazione lineare  $\mathbb{C}^1 \rightarrow \mathbb{C}^3$  la cui matrice è  $(1, 0, 0)^t$ . Utilizzare il procedimento di calcolo della media per ottenere un'applicazione lineare  $G$ -invariante a partire da  $T$ , usando  $\rho_2$  e la rappresentazione  $R$  definita in (a).
- (c) Risolvere la parte (b) dell'esercizio, sostituendo  $\rho_2$  con  $\rho_1$  e  $\rho_3$ .
- (d) Decomporre esplicitamente  $R$  in rappresentazioni irriducibili.

### 10 Rappresentazioni del gruppo $SU_2$

1. Determinare le rappresentazioni irriducibili del gruppo delle rotazioni  $SO_3$ .
2. Determinare le rappresentazioni irriducibili del gruppo ortogonale  $O_2$ .
3. Dimostrare che la rappresentazione ortogonale  $SU_2 \rightarrow SO_3$  è irriducibile, e individuare il suo carattere nella lista (10.18).
4. Dimostrare che le funzioni (10.18) formano una base per lo spazio vettoriale generato da  $\{\cos n\theta\}$ .
5. La moltiplicazione a sinistra definisce una rappresentazione di  $SU_2$  sullo spazio  $\mathbb{R}^4$  con coordinate  $x_1, \dots, x_4$ , come nel cap. 8 (§2). Decomporre la rappresentazione complessa associata in rappresentazioni irriducibili.
6. (a) Calcolare il volume della palla di dimensione 4 di raggio  $r : B^4 = \{x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq r^2\}$ , intersecandola con sottospazi di dimensione tre.
- (b) Calcolare il volume della 3-sfera  $S^3$ , di nuovo intersecando la sfera. (È consigliabile rivedere innanzitutto il calcolo analogo della superficie di una 2-sfera. Si dovrebbe ottenere:  $\frac{d}{dr} (\text{volume di } B^4) = (\text{volume di } S^3)$ , altrimenti occorre tentare di nuovo.)
- \*7. Dimostrare le relazioni di ortogonalità per i caratteri irriducibili (10.17) di  $SU_2$ , mediante integrazione su  $S^3$ .

### Esercizi vari

1. Dimostrare che un gruppo semplice finito che non sia di ordine primo non possiede rappresentazioni non banali di dimensione 2.
- \*2. Sia  $H$  un sottogruppo di indice 2 di un gruppo finito  $G$ , e sia  $a$  un elemento di  $G$  non appartenente a  $H$ , sicché  $aH$  è la seconda classe laterale di  $H$  in  $G$ . Sia

$S : H \rightarrow GL_n$  una rappresentazione matriciale di  $H$ . Definire una rappresentazione  $\text{ind } S : G \rightarrow GL_{2n}$  di  $G$ , chiamata la rappresentazione *indotta*, nel modo seguente:

$$(\text{ind } S)_h = \begin{bmatrix} S_h & \\ & S_{a^{-1}ha} \end{bmatrix}, \quad (\text{ind } S)_{ah} = \begin{bmatrix} & S_{aha} \\ S_h & \end{bmatrix}.$$

- (a) Dimostrare che  $\text{ind } S$  è una rappresentazione di  $G$ .
- (b) Descrivere il carattere  $\chi_{\text{ind } S}$  di  $\text{ind } S$  per mezzo del carattere  $\chi_S$  di  $S$ .
- (c) Se  $R : G \rightarrow GL_n$  è una rappresentazione di  $G$ , possiamo restringere  $R$  a  $H$ . Denotiamo la restrizione con  $\text{res } R : H \rightarrow GL_n$ . Dimostrare che  $\text{res}(\text{ind } S) \approx S \oplus S'$ , dove  $S'$  è la rappresentazione coniugata definita da:  $S'_h = S_{a^{-1}ha}$ .
- (d) Dimostrare la *legge di reciprocità di Frobenius*:

$$\langle \chi_{\text{ind } S}, \chi_R \rangle = \langle \chi_S, \chi_{\text{res } R} \rangle.$$

- (e) Utilizzare la legge di reciprocità di Frobenius per dimostrare che, se  $S$  e  $S'$  sono rappresentazioni non isomorfe, allora la rappresentazione indotta  $\text{ind } S$  di  $G$  è irriducibile. D'altra parte, se  $S \approx S'$ , allora  $\text{ind } S$  è una somma di due rappresentazioni irriducibili  $R, R'$ .

\*3. Sia  $H$  un sottogruppo di indice 2 di un gruppo  $G$ , e sia  $R$  una rappresentazione matriciale di  $G$ . Denotiamo con  $R'$  la rappresentazione *coniugata*, definita da  $R'_g = R_g$  se  $g \in H$ , e  $R'_g = -R_g$  altrimenti.

- (a) Dimostrare che  $R'$  è isomorfa a  $R$  se e soltanto se il carattere di  $R$  è identicamente nullo sulla classe laterale  $gH$ , dove  $g \notin H$ .
- (b) Utilizzare la reciprocità di Frobenius per dimostrare che  $\text{ind}(\text{res } R) \approx R \oplus R'$ .
- (c) Dimostrare che, se  $R$  non è isomorfa a  $R'$ , allora  $\text{res } R$  è irriducibile, e se queste due rappresentazioni sono isomorfe, allora  $\text{res } R$  è una somma di due rappresentazioni irriducibili di  $H$ .

\*4. Utilizzando la reciprocità di Frobenius, ricavare la tabella dei caratteri di  $S_n$  da quella di  $A_n$ , quando

- (a)  $n = 3$ ; (b)  $n = 4$ ; (c)  $n = 5$ .

\*5. Determinare i caratteri del gruppo diedrale  $D_n$ , utilizzando le rappresentazioni indotte da  $C_n$ .

6. (a) Dimostrare che l'unico elemento di  $SU_2$  di ordine 2 è  $-I$ .
- (b) Si consideri l'omomorfismo  $\varphi : SU_2 \rightarrow SO_3$ . Sia  $A$  un elemento di  $SU_2$  tale che  $\varphi(A) = \bar{A}$  abbia ordine finito  $\bar{n}$  in  $SO_3$ . Dimostrare che l'ordine  $n$  di  $A$  è uguale a  $\bar{n}$  oppure a  $2\bar{n}$ . Dimostrare inoltre che, se  $\bar{n}$  è pari, allora  $n = 2\bar{n}$ .

\*7. Sia  $G$  un sottogruppo finito di  $SU_2$ , e sia  $\bar{G} = \varphi(G)$ , dove  $\varphi : SU_2 \rightarrow SO_3$  è la rappresentazione ortogonale (cap. 8, §3). Dimostrare le seguenti proprietà:

- (a) Se  $|\bar{G}|$  è pari, allora  $|G| = 2|\bar{G}|$  e  $G = \varphi^{-1}(\bar{G})$ .
- (b)  $G = \varphi^{-1}(\bar{G})$ , oppure  $G$  è un gruppo ciclico di ordine dispari.

- (c) Sia  $G$  un sottogruppo ciclico di  $SU_2$  di ordine  $n$ . Dimostrare che  $G$  è coniugato al sottogruppo generato da  $\begin{bmatrix} \zeta & \\ & \zeta^{-1} \end{bmatrix}$ , dove  $\zeta = e^{2\pi i/n}$ .

- (d) Dimostrare che, se  $\bar{G}$  è il gruppo  $D_2$ , allora  $G$  è il gruppo dei quaternioni. Determinare la rappresentazione matriciale del gruppo dei quaternioni  $H$  come un sottogruppo di  $SU_2$ , rispetto a una base ortonormale opportuna in  $\mathbb{C}^2$ .

- (e) Se  $\bar{G} = T$ , dimostrare che  $G$  è un gruppo di ordine 24 non isomorfo al gruppo simmetrico  $S_4$ .

- \*8. Sia  $\rho$  una rappresentazione irriducibile di un gruppo finito  $G$ . Cosa si può dire sull'unicità della forma hermitiana  $G$ -invariante definita positiva?

- \*9. Sia  $G$  un sottogruppo finito di  $GL_n(\mathbb{C})$ . Dimostrare che, se  $\Sigma_g \text{tr } g = 0$ , allora  $\Sigma_g g = 0$ .

- \*10. Sia  $\rho : G \rightarrow GL(V)$  una rappresentazione di dimensione due di un gruppo finito  $G$ , e supponiamo che 1 sia un autovalore di  $\rho_g$  per ogni  $g \in G$ . Dimostrare che  $\rho$  è una somma di due rappresentazioni di dimensione uno.

- \*11. Sia  $\rho : G \rightarrow GL_n(\mathbb{C})$  una rappresentazione irriducibile di un gruppo finito  $G$ . Data una rappresentazione arbitraria  $\sigma : GL_n \rightarrow GL(V)$  di  $GL_n$ , possiamo considerare la composizione  $\sigma \circ \rho$  come una rappresentazione di  $G$ .

- (a) Determinare il carattere della rappresentazione ottenuta in questo modo, quando  $\sigma$  è la moltiplicazione a sinistra di  $GL_n$  sullo spazio  $\mathbb{C}^{n \times n}$  delle matrici  $n \times n$ . Decomporre in questo caso  $\sigma \circ \rho$  in rappresentazioni irriducibili.

- (b) Trovare il carattere di  $\sigma \circ \rho$ , nel caso in cui  $\sigma$  è l'azione di coniugio sullo spazio  $\mathbb{C}^{n \times n}$ .

# Capitolo 10

## Anelli

Dimentica, per favore, tutto quel che hai studiato a scuola; tanto non lo hai imparato.

Emil Landau

### 1 Definizione di anello

I numeri interi costituiscono il modello fondamentale per il concetto di anello: sono un insieme chiuso rispetto all'addizione, alla sottrazione e alla moltiplicazione, ma non rispetto alla divisione.

Prima di dare la definizione astratta di anello, possiamo vedere alcuni esempi considerando sottoanelli di  $\mathbb{C}$ . Un *sottoanello* di  $\mathbb{C}$  è un sottoinsieme che è chiuso rispetto all'addizione, alla sottrazione e alla moltiplicazione e che contiene 1 (quindi ogni sottocampo [cap. 3 (2.1)] è un sottoanello). Un altro esempio è l'anello degli *interi di Gauss*, cioè i numeri complessi della forma  $a + bi$ , con  $a$  e  $b$  interi. Tale anello si denota con

$$(1.1) \quad \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Gli interi di Gauss sono i punti di un reticolo quadrato nel piano complesso.

Possiamo formare un sottoanello  $\mathbb{Z}[\alpha]$ , analogo all'anello degli interi di Gauss, partendo da un qualunque numero complesso  $\alpha$ . Definiamo  $\mathbb{Z}[\alpha]$  come il più piccolo sottoanello di  $\mathbb{C}$  contenente  $\alpha$ , e lo chiamiamo il sottoanello *generato da  $\alpha$* . Non è difficile descriverlo. Se un anello contiene  $\alpha$ , allora esso contiene tutte le potenze positive di  $\alpha$ , poiché è chiuso rispetto alla moltiplicazione. Inoltre, esso contiene somme e differenze di tali potenze, e contiene 1. Pertanto esso contiene ogni numero complesso  $\beta$  che sia esprimibile come un polinomio in  $\alpha$  a coefficienti interi:

$$(1.2) \quad \beta = a_n \alpha^n + \cdots + a_1 \alpha + a_0, \quad \text{con } a_i \in \mathbb{Z}.$$

D'altra parte, l'insieme di tutti i numeri di questa forma è chiuso rispetto alle operazioni di addizione, sottrazione e moltiplicazione, e contiene 1, e quindi esso è il

*sottoanello* generato da  $\alpha$ . Nella maggior parte dei casi, tuttavia,  $\mathbb{Z}[\alpha]$  non si rappresenta come un reticolo nel piano complesso. Per esempio, l'anello  $\mathbb{Z} \left[ \frac{1}{2} \right]$  è costituito dai numeri razionali che possono essere espressi come polinomi in  $\frac{1}{2}$  a coefficienti interi. Tali numeri possono essere descritti semplicemente come quei numeri razionali il cui denominatore è una potenza di 2. Essi formano un sottoinsieme denso della retta reale.

Un numero complesso  $\alpha$  si dice *algebrico* se è radice di un polinomio non nullo a coefficienti interi, ossia se qualche espressione della forma (1.2) è uguale a zero. Per esempio,  $i + 3$ ,  $1/7$ ,  $7 + \sqrt[3]{2}$ ,  $\sqrt{3} + \sqrt{-5}$  sono numeri algebrici.

Se non esiste *nessun* polinomio non nullo a coefficienti interi che ammetta  $\alpha$  come radice,  $\alpha$  è chiamato un numero *trascendente*. I numeri  $e$ ,  $\pi$  sono trascendenti, sebbene ciò non sia facile da dimostrare. Se  $\alpha$  è trascendente, allora due espressioni polinomiali distinte (1.2) devono rappresentare numeri complessi distinti. In tal caso, gli elementi dell'anello  $\mathbb{Z}[\alpha]$  corrispondono biunivocamente ai polinomi  $p(x)$  a coefficienti interi, mediante la legge  $p(x) \longleftrightarrow p(\alpha)$ .

Se  $\alpha$  è un numero algebrico, vi saranno molte espressioni polinomiali (1.2) che rappresentano  $\alpha$ . Per esempio, se  $\alpha = i$ , le potenze  $\alpha^n$  assumono i quattro valori  $\pm 1$ ,  $\pm i$ . Utilizzando la relazione  $i^2 = -1$ , ogni espressione (1.2) può essere ridotta a una di grado  $\leq 1$  in  $i$ . Ciò è in accordo con la descrizione dell'anello degli interi di Gauss data all'inizio.

I due tipi di numeri, algebrici e trascendenti, sono un po' analoghi ai due tipi di gruppi ciclici, finiti e infiniti [cap. 2 (2.7)].

La definizione di anello astratto è simile a quella di campo [cap. 3 (2.3)], ad eccezione del fatto che non si richiede l'esistenza degli elementi inversi rispetto alla moltiplicazione:

(1.3) DEFINIZIONE *Un anello  $R$  è un insieme con due leggi di composizione  $+$  e  $\times$ , chiamate addizione e moltiplicazione, che soddisfano i seguenti assiomi:*

- (a)  *$R$  è un gruppo abeliano rispetto all'addizione, con identità 0. Tale gruppo abeliano si denota con  $R(+)$ .*
- (b) *La moltiplicazione è associativa e ha un elemento neutro denotato con 1.*
- (c) *(Proprietà distributiva) Per ogni  $a, b, c \in R$ , si ha*

$$(a + b)c = ac + bc \quad \text{e} \quad c(a + b) = ca + cb.$$

Un *sottoanello* di un anello è un sottoinsieme che è chiuso rispetto alle operazioni di addizione, sottrazione e moltiplicazione e che contiene l'elemento 1.

La definizione (1.3) non è del tutto standard. Alcuni autori non richiedono, in un anello, l'esistenza di un'identità rispetto alla moltiplicazione. In questo testo, studieremo prevalentemente *anelli commutativi*, ossia anelli che soddisfano

la proprietà commutativa  $ab = ba$  per la moltiplicazione. Con il termine *anello* intenderemo dunque un *anello commutativo con identità*, a meno di non menzionare esplicitamente la non commutatività. Per gli anelli commutativi le due proprietà distributive (c) sono equivalenti.

L'anello  $\mathbb{R}^{n \times n}$  di tutte le matrici  $n \times n$  a elementi reali, con  $n > 1$ , è un esempio importante di anello non commutativo.

Oltre ai sottoanelli di  $\mathbb{C}$ , gli anelli più importanti sono gli anelli di polinomi. Dato un anello  $R$ , un polinomio in  $x$  a coefficienti in  $R$  è un'espressione della forma

$$(1.4) \quad a_n x^n + \cdots + a_1 x + a_0,$$

con  $a_i \in R$ . L'insieme di questi polinomi forma un anello che si denota di solito con  $R[x]$ . Studieremo gli anelli di polinomi nel prossimo paragrafo.

### (1.5) Esempi

- (a) Ogni campo è un anello.
- (b) L'insieme  $\mathcal{R}$  delle funzioni continue di una variabile reale  $x$  a valori reali forma un anello rispetto alle operazioni di addizione e moltiplicazione di funzioni:

$$[f+g](x) = f(x) + g(x) \quad \text{e} \quad [fg](x) = f(x)g(x).$$

- (c) L'anello nullo  $R = \{0\}$  è costituito dal solo elemento 0.

Nella definizione di campo [cap. 3 (2.3)] si richiede che l'identità moltiplicativa 1 appartenga a  $F^* = F - \{0\}$ . Pertanto un campo ha almeno due elementi distinti, precisamente 1 e 0. La relazione  $1 = 0$  non è stata scartata in un anello, ma compare una sola volta:

### (1.6) PROPOSIZIONE Se $R$ è un anello in cui $1 = 0$ , $R$ è l'anello nullo.

*Dimostrazione.* Osserviamo innanzitutto che  $0a = 0$  per ogni elemento  $a$  di un anello  $R$ . Ciò si ottiene ripetendo la stessa dimostrazione già vista per gli spazi vettoriali [cap. 3 (1.7a)]. Supponiamo che  $1 = 0$  in  $R$ , e sia  $a$  un elemento arbitrario di  $R$ . Allora  $a = 1a = 0a = 0$ . Pertanto ogni elemento di  $R$  è 0, sicché  $R$  è l'anello nullo. ■

Anche se in un anello non si richiede l'esistenza di inversi rispetto alla moltiplicazione, un elemento particolare può avere un inverso, e l'inverso se esiste è unico. Gli elementi che possiedono un inverso rispetto alla moltiplicazione sono chiamati *unità*. Per esempio, le unità nell'anello degli interi sono 1 e  $-1$ , e le unità nell'anello  $\mathbb{R}[x]$  dei polinomi reali sono i polinomi costanti non nulli. I campi sono anelli diversi dall'anello nullo, in cui ogni elemento non nullo è un'unità.

L'identità 1 di un anello è sempre un'unità, e viene chiamato anche "l'"elemento *unità* di  $R$ . Tale terminologia è ambigua, ma è troppo tardi per cambiarla.

### 2 Costruzione formale degli interi e dei polinomi

Abbiamo imparato nella scuola elementare che per i numeri interi valgono gli assiomi di un anello. Tuttavia, consideriamo di nuovo gli interi per vedere cosa occorre per scrivere esplicitamente le dimostrazioni di proprietà quali la associativa e la distributiva. Le dimostrazioni complete sono molto lunghe, e pertanto ci limiteremo qui a verifiche parziali. Di solito si comincia col definire l'addizione e la moltiplicazione per gli interi positivi; i numeri negativi vengono introdotti in un secondo momento. Ciò implica la necessità di analizzare parecchi casi nel corso della trattazione (cosa abbastanza noiosa), a meno di trovare una notazione ingegnosa che consenta di evitare tutto ciò. Ci accontenteremo dunque di descrivere le operazioni sugli interi positivi, chiamati anche *numeri naturali*.

L'insieme  $\mathbb{N}$  dei numeri naturali è caratterizzato dalle seguenti proprietà (*assiomi di Peano*):

- (2.1) (a) L'insieme  $\mathbb{N}$  contiene un elemento privilegiato 1.
- (b) Esiste un'applicazione  $\sigma : \mathbb{N} \rightarrow \mathbb{N}$  che manda ogni intero  $n \in \mathbb{N}$  in un altro intero, chiamato l'intero seguente o il successore di  $n$ . Tale applicazione è iniettiva e, per ogni  $n \in \mathbb{N}$ ,  $\sigma(n) \neq 1$ .
- (c) (Assioma di induzione) Supponiamo che un sottoinsieme  $S$  di  $\mathbb{N}$  abbia le seguenti proprietà:
  - (i)  $1 \in S$ ;
  - (ii) se  $n \in S$ , allora  $\sigma(n) \in S$ .
 Allora  $S$  contiene ogni numero naturale, ossia  $S = \mathbb{N}$ .

L'intero  $\sigma(n)$  si scriverà  $n + 1$  quando sarà stata definita l'addizione. Ora, invece, la notazione  $n + 1$  potrebbe creare confusione, ed è quindi preferibile usare una notazione neutra; spesso denoteremo il successore di  $n$  con  $n'$  [ $= \sigma(n)$ ]. Si noti che si suppone che  $\sigma$  sia iniettiva, sicché se  $m, n$  sono numeri naturali distinti, ossia se  $m \neq n$ , allora anche  $m', n'$  sono distinti.

L'applicazione  $\sigma$  permette di usare i numeri naturali per contare, che è la base dell'aritmetica.

La proprietà (c) è la proprietà di induzione degli interi. Intuitivamente, dice che i numeri naturali si ottengono a partire da 1 prendendo ripetutamente il successore:  $\mathbb{N} = \{1, 1', 1'', \dots\}$  ( $= \{1, 2, 3, \dots\}$ ); ossia, contando si ottengono tutti i numeri naturali. Tale proprietà è la base, dal punto di vista formale, delle dimostrazioni per induzione.

Supponiamo che vi sia da dimostrare un enunciato  $P_n$  per ogni intero positivo  $n$ , e sia  $S$  l'insieme degli interi  $n$  tale che  $P_n$  è vero. Dire che  $P_n$  è vero per ogni  $n$  equivale a dire che  $S = \mathbb{N}$ . Per questo insieme  $S$ , l'assioma di induzione si traduce nei passi usuali dell'induzione:

- (2.2) (i)  $P_1$  è vero.  
(ii) Se  $P_n$  è vero, allora  $P_{n'}$  è vero.

Possiamo utilizzare inoltre gli assiomi di Peano per dare delle definizioni ricorsive. L'espressione *definizione ricorsiva*, o *induttiva*, si riferisce alla definizione di una successione di oggetti  $C_n$ , aventi come indici i numeri naturali, ciascuno dei quali è definito per mezzo del precedente. Un esempio è dato dalla funzione  $C_n = x^n$ . Una definizione ricorsiva di questa funzione è:

$$x^1 = x \quad \text{e} \quad x^{n'} = x^n x.$$

I punti importanti sono i seguenti:

- (2.3) (i)  $C_1$  è definita.  
(ii) È data una regola per determinare  $C_{n'}$  ( $= C_{n+1}$ ) a partire da  $C_n$ .

È chiaro intuitivamente che (2.3) determina univocamente la successione  $C_n$ , ma dimostrarlo a partire dagli assiomi di Peano è complicato. Un modo naturale per tentare una dimostrazione è il seguente. Sia  $S$  l'insieme degli interi  $n$  tali che (2.3) determini  $C_k$  per ogni  $k \leq n$ . Dalla (2.3i) si deduce che  $1 \in S$ . Inoltre, (2.3ii) mostra che, se  $n \in S$  allora  $n' \in S$ . In virtù dell'assioma di induzione, si ha  $S = \mathbb{N}$ , da cui segue che  $C_n$  è definita univocamente per ogni  $n$ . Purtroppo, la relazione  $\leq$  non è inclusa tra gli assiomi di Peano; per poterla utilizzare dovremmo innanzitutto definirla e ricavare le sue proprietà. Una dimostrazione basata su questo approccio risulterebbe piuttosto lunga, sicché la ometteremo.

Dato l'insieme degli interi positivi, possiamo definire in modo ricorsivo l'addizione e la moltiplicazione di interi positivi, come segue:

- (2.4) DEFINIZIONE (Addizione)  $m + 1 = m'$  e  $m + n' = (m + n)'$ .  
(Moltiplicazione)  $m \cdot 1 = m$  e  $m \cdot n' = m \cdot n + m$ .

In queste definizioni prendiamo un intero arbitrario  $m$  e definiamo in modo ricorsivo l'addizione e la moltiplicazione per quell'intero  $m$  e per ogni  $n$ . In tal modo,  $m + n$  e  $m \cdot n$  risultano definiti per ogni  $m$  e per ogni  $n$ .

Le dimostrazioni della proprietà associativa, della proprietà commutativa e delle proprietà distributive per gli interi sono esercizi sull'induzione e potrebbero essere chiamati "giochi di Peano". Effettueremo due di tali verifiche a mo' di esempio.

**Dimostrazione della proprietà associativa dell'addizione.** Dobbiamo far vedere che  $(a + b) + n = a + (b + n)$  per ogni  $a, b, n \in \mathbb{N}$ . Innanzitutto verifichiamo il caso  $n = 1$  per ogni  $a, b$ . Applicando tre volte la definizione (2.4), otteniamo

$$(a + b) + 1 = (a + b)' = a + b' = a + (b + 1).$$

Supponiamo poi che la proprietà associativa sia vera per un valore particolare di  $n$  e per ogni  $a, b$ . Dopodiché verifichiamo la proprietà per  $n'$  nel modo seguente:

$$\begin{array}{ll} (\text{definizione}) & (a + b) + n' = (a + b) + (n + 1) = \\ (\text{caso } n = 1) & = ((a + b) + n) + 1 = \\ (\text{ipotesi induttiva}) & = (a + (b + n)) + 1 = \\ (\text{caso } n = 1) & = a + ((b + n) + 1) = \\ (\text{caso } n = 1) & = a + (b + (n + 1)) = \\ (\text{definizione}) & = a + (b + n'). \blacksquare \end{array}$$

**Dimostrazione della proprietà commutativa per la moltiplicazione, supponendo che sia stata dimostrata per l'addizione.** Innanzitutto dimostriamo che

$$(2.5) \quad m' \cdot n = m \cdot n + n.$$

Il caso  $n = 1$  è chiaro:  $m' \cdot 1 = m' = m + 1 = m \cdot 1 + 1$ . Pertanto supponiamo che la relazione (2.5) sia vera per un valore particolare di  $n$  e per ogni valore di  $m$ , e verifichiamola per  $n'$ :

$$\begin{array}{ll} (\text{definizione}) & m' \cdot n' = m' \cdot n + m' = m' \cdot n + (m + 1) = \\ (\text{induzione}) & = (m \cdot n + n) + (m + 1) = \\ (\text{varie proprietà dell'addizione}) & = (m \cdot n + m) + (n + 1) = \\ (\text{definizione}) & = m \cdot n' + n'. \end{array}$$

Successivamente, verifichiamo che  $1 \cdot n = n$ , per induzione su  $n$ . Infine, dimostriamo che  $m \cdot n = n \cdot m$ , per induzione su  $n$ , sapendo che  $m \cdot 1 = m = 1 \cdot m$ . Allora, supposto vero il risultato per  $n$ , otteniamo  $m \cdot n' = m \cdot n + m = n \cdot m + m = n' \cdot m$ , come richiesto. ■

Le dimostrazioni delle altre proprietà dell'addizione e della moltiplicazione si sviluppano in modo simile.

Passiamo ora alla definizione degli anelli di polinomi. Possiamo definire un *polinomio* a coefficienti in un anello  $R$  arbitrario come una combinazione lineare di potenze della variabile:

$$(2.6) \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

con  $a_i \in R$ . Tali espressioni vengono chiamate spesso *polinomi formali*, per distinguerli dalle funzioni polinomiali. Ogni polinomio formale a coefficienti reali individua una funzione polinomiale sui numeri reali.

La variabile  $x$  che compare in (2.6) è un simbolo arbitrario, e i monomi  $x^i$  sono considerati indipendenti. Ciò significa che se

$$(2.9) \quad g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

è un altro polinomio a coefficienti in  $R$ , allora  $f(x)$  e  $g(x)$  sono uguali se e soltanto se  $a_i = b_i$  per ogni  $i = 0, 1, 2, \dots$ .

Il *grado* di un polinomio non nullo è il più grande intero  $k$  tale che il coefficiente  $a_k$  di  $x^k$  sia diverso da zero. (Il grado del polinomio nullo è considerato indeterminato). Il coefficiente di grado massimo di un polinomio non nullo è chiamato il suo *coefficiente direttore*, e un polinomio *monico* è un polinomio con coefficiente direttore 1.

La possibilità che alcuni coefficienti di un polinomio siano nulli dà luogo a qualche seccatura. Occorre trascurare i termini con coefficienti nulli: per esempio,  $x^2 + 3 = 0x^3 + x^2 + 3$ . Pertanto il polinomio  $f(x)$  possiede più di una rappresentazione (2.6). Un modo per ottenere una notazione standard è quello di scrivere soltanto i coefficienti non nulli, ossia, di omettere tutti i termini  $0x^i$  nell'espressione (2.6). Ma coefficienti nulli possono comparire nel corso dei calcoli, e dovranno essere scartati. Un'altra possibilità è quella di richiedere che il coefficiente del monomio di grado massimo  $a_n$  di (2.6) sia diverso da zero e di scrivere tutti i termini di grado più basso, ma anche qui si presenta lo stesso problema. Pertanto tali convenzioni richiedono una discussione di casi particolari nella descrizione della struttura di anello. Ciò è un po' irritante, poiché l'ambiguità causata dai coefficienti nulli non è un punto interessante.

Un modo per aggirare il problema delle notazioni è quello di scrivere i coefficienti di *tutti* i monomi, siano essi nulli oppure no. Ciò non va bene per i calcoli, ma permette di verificare in modo efficiente gli assiomi di un anello. Per definire le operazioni di un anello scriveremo un polinomio nella forma canonica:

$$(2.7) \quad f(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

dove i coefficienti  $a_i$  appartengono tutti all'anello  $R$  e *soltanto un numero finito di essi sono diversi da zero*. Formalmente, il polinomio (2.7) è individuato dal suo vettore (o successione) dei coefficienti  $a_i$ :

$$(2.8) \quad a = (a_0, a_1, \dots),$$

dove gli  $a_i$  appartengono a  $R$  e ad eccezione di un numero finito, sono tutti nulli. Ogni vettore siffatto corrisponde a un polinomio. Nel caso in cui  $R$  è un campo questi vettori infiniti formano lo spazio vettoriale  $Z$  con la base infinita  $e_i$ .

definito nel capitolo 3 (5.2d). Il vettore  $e_i$  corrisponde al monomio  $x^i$ , e i monomi formano una base dello spazio di tutti i polinomi.

L'addizione e la moltiplicazione di polinomi imitano fedelmente le operazioni ben note sulle funzioni polinomiali reali. Sia  $f(x)$  come sopra, e sia

$$(2.9) \quad g(x) = b_0 + b_1 x + b_2 x^2 + \cdots,$$

un altro polinomio a coefficienti nello stesso anello  $R$ , individuato dal vettore  $b = (b_0, b_1, \dots)$ . La *somma* di  $f$  e  $g$  è:

$$(2.10) \quad f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots = \\ = \sum_k (a_k + b_k)x^k,$$

che corrisponde alla somma di vettori:  $a + b = (a_0 + b_0, a_1 + b_1, \dots)$ .

Il *prodotto* di due polinomi  $f, g$  si calcola con la moltiplicazione termine a termine e raccogliendo i coefficienti dei monomi che hanno lo stesso grado in  $x$ . Se sviluppiamo il prodotto utilizzando la proprietà distributiva, ma senza raccogliere i termini, otteniamo

$$(2.11) \quad f(x)g(x) = \sum_{i,j} a_i b_j x^{i+j}.$$

Si noti che vi è soltanto un numero finito di coefficienti non nulli  $a_i b_j$ . Questa è una formula corretta, ma il secondo membro non è espresso nella forma canonica (2.7), poiché lo stesso monomio  $x^n$  compare più volte, precisamente una per ciascuna coppia  $i, j$  di indici tali che  $i + j = n$ . Occorre dunque raccogliere i termini in modo da riscrivere il secondo membro in forma canonica. Siamo così condotti alla definizione:

$$f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \cdots,$$

dove

$$(2.12) \quad p_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j.$$

Nel corso dei calcoli, può essere preferibile rinviare per un po' la raccolta dei termini di ugual grado.

(2.13) PROPOSIZIONE Esiste un'unica struttura di anello commutativo sull'insieme dei polinomi  $R[x]$  con le seguenti proprietà:

- (a) L'addizione di polinomi è l'addizione di vettori (2.10).
- (b) La moltiplicazione di polinomi è data dalla regola (2.12).

(c) L'anello  $R$  è un sottoanello di  $R[x]$ , quando gli elementi di  $R$  sono identificati con i polinomi costanti.

La dimostrazione è faticosa per via delle notazioni, e d'altra parte non offre motivi d'interesse, sicché verrà omessa. ■

I polinomi sono di importanza fondamentale per la teoria degli anelli, e dobbiamo considerare anche polinomi in più variabili, come ad esempio  $x^2y^2 + 4x^3 - 3x^2y - 4y^2 + 2$ . Non vi sono cambiamenti di rilievo nelle definizioni.

Siano  $x_1, \dots, x_n$  delle variabili. Dicesi *monomio* ogni prodotto del tipo

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

dove gli esponenti  $i_\nu$  sono interi non negativi. La  $n$ -upla  $(i_1, \dots, i_n)$ , detta *multiindice*, individua il monomio. Particolarmente conveniente è la notazione vettoriale  $i = (i_1, \dots, i_n)$ , con la quale possiamo scrivere il monomio simbolicamente nella forma:

$$(2.14) \quad x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Il monomio  $x^0$ , dove  $0 = (0, \dots, 0)$ , si indica con 1.

Un *polinomio* a coefficienti in un anello  $R$  è una combinazione lineare finita di monomi a coefficienti in  $R$ . Utilizzando la notazione abbreviata (2.14), ogni polinomio  $f(x) = f(x_1, \dots, x_n)$  può essere scritto in uno e un sol modo nella forma

$$(2.15) \quad f(x) = \sum_i a_i x^i,$$

dove  $i$  varia nell'insieme di tutti i multi-indici  $(i_1, \dots, i_n)$ , i coefficienti  $a_i$  appartengono a  $R$ , e soltanto un numero finito di essi sono diversi da zero.

Un polinomio che sia il prodotto di un monomio per un elemento non nullo di  $R$  è chiamato anch'esso *monomio*. Così

$$(2.16) \quad m = rx^i$$

è un monomio, se  $r \in R$  è diverso da zero e  $x^i$  è come nella (2.14). Un monomio può essere considerato come un polinomio che ha esattamente un solo coefficiente non nullo.

Utilizzando la notazione con i multi-indici, le formule (2.10) e (2.12) definiscono l'addizione e la moltiplicazione di polinomi in più variabili, e inoltre vale l'analogo della proposizione (2.13).

L'anello dei polinomi a coefficienti in  $R$  si denota con uno dei simboli:

$$(2.17) \quad R[x_1, \dots, x_n] \quad \text{oppure} \quad R[x],$$

Se il simbolo  $x$  si intende riferito all'insieme delle variabili  $(x_1, \dots, x_n)$ . Se non è stato introdotto nessun insieme di variabili, la notazione  $R[x]$  si riferisce all'anello dei polinomi in una variabile  $x$ .

### 3 Omomorfismi e ideali

Un *omomorfismo*  $\varphi : R \rightarrow R'$  da un anello  $R$  a un anello  $R'$  è un'applicazione compatibile con le leggi di composizione che porta 1 in 1, ossia un'applicazione tale che

$$(3.1) \quad \varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1_R) = 1_{R'},$$

per ogni  $a, b \in R$ . Un *isomorfismo* di anelli è un omomorfismo biiettivo. Se esiste un isomorfismo  $R \rightarrow R'$ , i due anelli si dicono *isomorfi*.

Un breve commento sulla terza parte di (3.1) è opportuno. L'ipotesi che un omomorfismo  $\varphi$  sia compatibile con l'addizione implica che esso è un omomorfismo di gruppi  $R(+)$  →  $R'(+)$ . Sappiamo che un omomorfismo di gruppi porta l'identità nell'identità, sicché  $\varphi(0) = 0$ . Ma  $R$  non è un gruppo rispetto alla moltiplicazione, e non possiamo concludere che  $\varphi(1) = 1$  dalla compatibilità rispetto alla moltiplicazione. Pertanto la condizione  $\varphi(1) = 1$  deve essere enunciata separatamente. Per esempio, l'*applicazione nulla*  $R \rightarrow R'$  che manda tutti gli elementi di  $R$  nello zero è compatibile con l'addizione e la moltiplicazione, ma non manda 1 in 1, a meno che  $1 = 0$  in  $R'$ . L'applicazione nulla non è un omomorfismo di anelli a meno che  $R'$  non sia l'anello nullo [cfr. (1.6)].

Gli omomorfismi di anelli più importanti sono quelli ottenuti calcolando i valori dei polinomi in costanti prefissate. Così calcolando un polinomio reale in un numero reale  $a$  si definisce un omomorfismo:

$$(3.2) \quad R[x] \rightarrow R, \quad \text{che manda } p(x) \text{ in } p(a).$$

Anche il calcolo dei polinomi reali in un numero complesso, ad esempio  $i$ , dà luogo a un omomorfismo:

$$(3.3) \quad R[x] \rightarrow \mathbb{C}, \quad \text{che manda } p(x) \text{ in } p(i).$$

In generale, si ha:

(3.4) PROPOSIZIONE (Principio di sostituzione) *Sia  $\varphi : R \rightarrow R'$  un omomorfismo di anelli.*

(a) *Dato un elemento  $\alpha \in R'$ , esiste uno e un solo omomorfismo  $\Phi : R[x] \rightarrow R'$  che coincide con l'applicazione  $\varphi$  sui polinomi costanti e che manda  $x$  in  $\alpha$ .*

(b) *Più in generale, dati  $n$  elementi  $\alpha_1, \dots, \alpha_n \in R'$ , esiste uno e un solo omo-*

*morfismo*  $\Phi : R[x_1, \dots, x_n] \rightarrow R'$  dall'anello dei polinomi in  $n$  variabili a  $R'$ , che coincide con  $\varphi$  sui polinomi costanti e che manda  $x_\nu$  in  $\alpha_\nu$ , per  $\nu = 1, \dots, n$ .

*Dimostrazione.* Utilizzando la notazione vettoriale per gli indici, la dimostrazione di (b) è la stessa di (a). Chiamiamo  $r'$  l'immagine di un elemento  $r \in R$  in  $R'$ . Utilizzando il fatto che  $\Phi$  è un omomorfismo che si restringe a  $\varphi$  su  $R$  e manda  $x_\nu$  in  $\alpha_\nu$ , troviamo che esso agisce su un polinomio  $f(x) = \sum r_i x^i$  nel modo seguente:

$$(3.5) \quad \sum r_i x^i \mapsto \sum \varphi(r_i) \alpha^i = \sum r'_i \alpha^i.$$

In altre parole,  $\Phi$  agisce sui coefficienti di un polinomio come  $\varphi$ , e sostituisce  $x$  con  $\alpha$ . Poiché tale formula descrive  $\Phi$ , abbiamo dimostrato l'unicità dell'omomorfismo di sostituzione. Per dimostrarne l'esistenza, prendiamo questa formula come definizione di  $\Phi$ , e facciamo vedere che tale applicazione è un omomorfismo  $R[x] \rightarrow R'$ . È facile dimostrare che  $\Phi$  manda 1 in 1 e che è compatibile con l'addizione di polinomi. La compatibilità con la moltiplicazione può essere verificata utilizzando la formula (2.11):

$$\begin{aligned} \Phi(fg) &= \Phi\left(\sum a_i b_j x^{i+j}\right) = \sum \Phi(a_i b_j x^{i+j}) = \sum_{i,j} a'_i b'_j \alpha^{i+j} = \\ &= \left(\sum_i a'_i \alpha^i\right) \left(\sum_j b'_j \alpha^j\right) = \Phi(f)\Phi(g). \blacksquare \end{aligned}$$

Vediamo ora un'applicazione del principio di sostituzione, in cui cambia l'anello dei coefficienti  $R$ . Sia  $\psi : R \rightarrow R_1$  un omomorfismo di anelli. Componendo  $\psi$  con l'inclusione di  $R_1$  come sottoanello di  $R_1[x]$ , otteniamo un omomorfismo  $\varphi : R \rightarrow R_1[x]$ . Il principio di sostituzione afferma che esiste una e una sola estensione di  $\varphi$  a un omomorfismo  $\Phi : R[x] \rightarrow R_1[x]$  che manda  $x$  in  $x$ . Questa è l'applicazione che agisce sui coefficienti di un polinomio, lasciando fissa la variabile  $x$ . Se denotiamo  $\psi(a)$  con  $a'$ , allora  $\Phi$  manda un polinomio  $a_n x^n + \dots + a_1 x + a_0$  in  $a'_n x^n + \dots + a'_1 x + a'_0$ .

Un esempio importante è dato dall'omomorfismo  $\mathbb{Z} \rightarrow \mathbb{F}_p$ , dove  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  è il campo con  $p$  elementi. Tale applicazione si estende a un omomorfismo:

$$(3.6) \quad \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x], \quad \text{che manda}$$

$$f(x) = a_n x^n + \dots + a_0 \quad \text{in} \quad \bar{a}_n x^n + \dots + \bar{a}_0 = \bar{f}(x),$$

dove  $\bar{a}_i$  denota la classe resto di  $a_i$  modulo  $p$ . È naturale chiamare il polinomio  $\bar{f}(x)$  il *resto di  $f(x)$  modulo  $p$* .

Il principio di sostituzione è anche un modo efficiente per dimostrare che varie costruzioni di anelli di polinomi sono equivalenti; l'isomorfismo

$$R[x, y] \approx R[x][y]$$

è un esempio tipico. In tale relazione, il secondo membro indica l'anello dei polinomi in  $y$  i cui coefficienti sono polinomi in  $x$ . L'affermazione che questi due anelli sono isomorfi è una formalizzazione del procedimento che consiste nel raccogliere i termini dello stesso grado in  $y$  in un polinomio  $f(x, y)$ , per scriverlo come un polinomio in  $y$ . Per esempio:

$$x^2 y^2 + 4x^3 - 3x^2 y - 4y^2 + 2 = (x^2 - 4)y^2 - (3x^2)y + (4x^3 + 2).$$

(3.7) COROLLARIO Si denotino con  $x = (x_1, \dots, x_m)$  e  $y = (y_1, \dots, y_n)$  due insiemi di variabili. Allora esiste uno e un solo isomorfismo  $R[x, y] \rightarrow R[x][y]$  che è l'identità su  $R$  e che manda le variabili in se stesse.

*Dimostrazione.* Si noti che  $R$  è un sottoanello di  $R[x]$ , e che  $R[x]$  è un sottoanello di  $R[x][y]$ . Pertanto  $R$  è anche un sottoanello di  $R[x][y]$ . Consideriamo l'applicazione data dall'inclusione  $\varphi : R \rightarrow R[x][y]$ . Il principio di sostituzione (3.4) assicura che esiste uno ed un solo omomorfismo  $\Phi : R[x, y] \rightarrow R[x][y]$  che estende tale applicazione e manda le variabili  $x_\mu, y_\nu$  in elementi assegnati di  $R[x][y]$ ; quindi possiamo mandare le variabili in se stesse. L'applicazione  $\Phi$  così costruita è l'omomorfismo richiesto. Possiamo dimostrare che  $\Phi$  ha un'inversa, utilizzando ancora una volta il principio di sostituzione. Osserviamo innanzitutto che  $R[x]$  è un sottoanello di  $R[x, y]$ , sicché possiamo estendere l'applicazione data dall'inclusione  $\psi : R[x] \rightarrow R[x, y]$  a un'applicazione  $\Psi : R[x][y] \rightarrow R[x, y]$  che manda le  $y_j$  in se stesse. Allora l'omomorfismo composto  $\Psi \Phi : R[x, y] \rightarrow R[x, y]$  è l'identità su  $R$  e su  $\{x_\mu, y_\nu\}$ . In virtù dell'unicità dell'omomorfismo di sostituzione,  $\Psi \Phi$  è l'applicazione identica. Analogamente,  $\Phi \Psi$  è l'identità, e quindi  $\Phi$  è un isomorfismo. ■

Poiché un polinomio reale  $f(x)$  può essere calcolato in un numero reale, esso definisce una funzione polinomiale sulla retta reale. Il termine *polinomio* viene usato spesso con riferimento a una funzione ottenuta in questo modo, e ciò non è molto pericoloso, poiché possiamo ricostruire il polinomio a partire dalla sua funzione:

(3.8) PROPOSIZIONE Sia  $\mathcal{R}$  l'anello delle funzioni a valori reali continue su  $\mathbb{R}^n$ . Allora l'applicazione  $\varphi : \mathbb{R}[x_1, \dots, x_n] \rightarrow \mathcal{R}$  che manda un polinomio nella funzione polinomiale ad esso associata è un omomorfismo iniettivo.

*Dimostrazione.* L'esistenza di tale omomorfismo segue dal principio di sostituzione. Dimostriamo l'iniettività. Basta far vedere che, se la funzione associata a

un polinomio  $f(x)$  è la funzione nulla, allora  $f(x)$  è il polinomio nullo. Sia  $\tilde{f}(x)$  la funzione associata a  $f(x)$ . Se  $\tilde{f}(x)$  è identicamente nulla, allora anche tutte le sue derivate sono nulle. D'altra parte, possiamo derivare formalmente un polinomio usando la regola di derivazione per le funzioni polinomiali. Se qualche coefficiente del polinomio  $f$  in esame è diverso da zero, allora il termine costante di una derivata opportuna di  $f(x)$  sarà anch'esso diverso da zero, e quindi quella derivata non si annullerà nell'origine. Dunque  $\tilde{f}(x)$  non può essere la funzione nulla.

Un altro esempio importante di omomorfismo di anelli è l'applicazione dall'anello degli interi a un anello arbitrario:

(3.9) PROPOSIZIONE *Sia  $R$  un anello arbitrario. Esiste uno e un solo omomorfismo*

$$\varphi : \mathbb{Z} \rightarrow R$$

dall'anello degli interi a  $R$ , dato dall'applicazione definita ponendo:  $\varphi(n) = "n \text{ volte } 1_R" = 1_R + \dots + 1_R$  ( $n$  volte) se  $n > 0$ , e  $\varphi(-n) = -\varphi(n)$ .

*Dimostrazione.* Sia  $\varphi : \mathbb{Z} \rightarrow R$  un omomorfismo. In base alla definizione di omomorfismo,  $\varphi(1) = 1_R$ , e  $\varphi(n+1) = \varphi(n) + \varphi(1)$ . Pertanto  $\varphi$  è determinato sui numeri naturali dalla definizione ricorsiva:

$$\varphi(1) = 1 \quad \text{e} \quad \varphi(n') = \varphi(n) + 1,$$

dove l'apice ' denota la funzione che definisce l'intero successivo (2.1b). Questa formula, insieme con  $\varphi(-n) = -\varphi(n)$  se  $n > 0$  e  $\varphi(0) = 0$ , determina univocamente  $\varphi$ . Pertanto l'applicazione sopra definita è l'unica possibile. Per dimostrare formalmente che essa è un omomorfismo, dobbiamo tornare agli assiomi di Peano. Verifichiamo che  $\varphi$  è compatibile con l'addizione di interi positivi. Per dimostrare che  $\varphi(m+n) = \varphi(m) + \varphi(n)$ , osserviamo che ciò è vero per  $n = 1$ , in base alla definizione di  $\varphi$ . Supponendo che la proprietà valga per ogni  $m$  e per qualche  $n$  particolare, dimostriamo che essa vale per ogni  $m$  e per  $n'$ :

$$\begin{aligned} (\text{proprietà dell'addizione di interi}) \quad \varphi(m+n') &= \varphi((m+n)+1) = \\ (\text{definizione di } \varphi) \quad &= \varphi(m+n)+1 = \\ (\text{ipotesi induttiva}) \quad &= \varphi(m)+\varphi(n)+1 = \\ (\text{definizione di } \varphi) \quad &= \varphi(m)+\varphi(n'). \end{aligned}$$

Per induzione,  $\varphi(m+n) = \varphi(m) + \varphi(n)$  per ogni  $m, n$ . La dimostrazione della compatibilità con la moltiplicazione di interi positivi è lasciata come esercizio. ■

Questa proposizione permette di identificare le immagini degli interi in un anello arbitrario  $R$ . Possiamo dunque interpretare il simbolo 3 come l'elemento  $1+1+1$  in  $R$ , e un polinomio a coefficienti interi, quale ad esempio  $3x^2+2x$ , come un elemento dell'anello di polinomi  $R[x]$ .

Consideriamo nuovamente un omomorfismo di anelli  $\varphi : R \rightarrow R'$ . Il *nucleo* di  $\varphi$  è definito esattamente come il nucleo di un omomorfismo di gruppi:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}.$$

Come abbiamo visto a suo tempo, il nucleo di un omomorfismo di gruppi è un sottogruppo, più precisamente un sottogruppo normale [cap. 2 (4.9)]. Analogamente, il nucleo di un omomorfismo di anelli è chiuso rispetto alle operazioni di addizione e moltiplicazione, e inoltre possiede una proprietà più forte della chiusura rispetto alla moltiplicazione:

(3.10) *Se  $a \in \ker \varphi$  e  $r \in R$ , allora  $ra \in \ker \varphi$ .*

Infatti, se  $\varphi(a) = 0$ , allora  $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$ . D'altra parte,  $\ker \varphi$  non contiene l'elemento unità 1 di  $R$ , e pertanto il *nucleo non è un sottoanello*, a meno che non sia l'intero anello  $R$ . (Se  $1 \in \ker \varphi$ , allora  $r = r1 \in \ker \varphi$  per ogni  $r \in R$ ). Inoltre, se  $\ker \varphi = R$ , allora  $\varphi$  è l'applicazione nulla, e per quanto detto sopra,  $R'$  è l'anello nullo.

Per esempio, sia  $\varphi$  l'omomorfismo  $\mathbb{R}[x] \rightarrow \mathbb{R}$  definito calcolando ogni polinomio  $f(x) \in \mathbb{R}[x]$  nel numero reale 2. Allora  $\ker \varphi$  è l'insieme dei polinomi che hanno 2 come radice. Esso può essere descritto anche come l'insieme dei polinomi divisibili per  $x - 2$ .

La proprietà del nucleo di un omomorfismo di anelli, di essere chiuso rispetto alla moltiplicazione per un elemento arbitrario dell'anello, viene formalizzata nel concetto di *ideale*. Un ideale  $I$  di un anello  $R$  è, per definizione, un sottoinsieme di  $R$  con le seguenti proprietà:

- (3.11) (i)  $I$  è un sottogruppo di  $R(+)$ .  
(ii) Se  $a \in I$  e  $r \in R$ , allora  $ra \in I$ .

Questo termine particolare, "ideale", è un'abbreviazione di "elemento ideale", usato in passato nella teoria dei numeri; vedremo nel capitolo 11 qual'è la sua origine. La proprietà (ii) implica che un ideale è chiuso rispetto alla moltiplicazione, ma anche qualcosa di più. Per considerare le proprietà (i) e (ii) insieme, conviene utilizzare la formulazione equivalente:

- (3.12) *I è non vuoto, e una combinazione lineare  $r_1a_1 + \dots + r_ka_k$  di elementi  $a_i \in I$  con coefficienti  $r_i \in R$  appartiene ad  $I$ .*

In un anello  $R$ , l'insieme dei multipli di un elemento particolare  $a$ , o equivalentemente, l'insieme degli elementi divisibili per  $a$ , forma un ideale chiamato *l'ideale principale* generato da  $a$ . Questo ideale viene indicato in vari modi:

$$(3.13) \quad (a) = aR = Ra = \{ra \mid r \in R\}.$$

Pertanto il nucleo dell'omomorfismo  $\mathbb{R}[x] \rightarrow \mathbb{R}$  definito calcolando ogni polinomio in  $x$  può essere denotato con  $(x-2)$  oppure con  $(x-2)\mathbb{R}[x]$ . In realtà la notazione  $(a)$  per un ideale principale, anche se comoda, è ambigua poiché l'anello non è menzionato. Per esempio,  $(x-2)$  può indicare un ideale in  $\mathbb{R}[x]$  oppure in  $\mathbb{Z}[x]$ , a seconda delle circostanze. Quando compaiono parecchi anelli, può essere preferibile usare una notazione diversa.

Possiamo considerare anche l'ideale  $I$  generato da un insieme di elementi  $a_1, \dots, a_n$  di  $R$ , definito come il più piccolo ideale contenente gli elementi. Può essere descritto come l'insieme di tutte le combinazioni lineari

$$(3.14) \quad r_1a_1 + \dots + r_na_n,$$

con coefficienti  $r_i$  in  $R$ . Infatti, se un ideale contiene  $a_1, \dots, a_n$ , allora (3.12) assicura che esso contiene ogni combinazione lineare di questi elementi. D'altra parte, l'insieme delle combinazioni lineari è chiuso rispetto all'addizione, alla sottrazione, e alla moltiplicazione per elementi di  $R$ , quindi è proprio l'ideale  $I$ . Questo ideale si denota spesso con

$$(3.15) \quad (a_1, \dots, a_n) = \{r_1a_1 + \dots + r_na_n \mid r_i \in R\}.$$

Per esempio, se  $R$  è l'anello  $\mathbb{Z}[x]$  dei polinomi a coefficienti interi, la notazione  $(2, x)$  sta a indicare l'ideale formato dalle combinazioni lineari di  $2$  e di  $x$  aventi come coefficienti polinomi a coefficienti interi. Tale ideale può essere descritto anche come l'insieme di tutti i polinomi  $f(x)$  a coefficienti interi il cui termine noto è divisibile per  $2$ . Esso è il nucleo dell'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{Z}/2\mathbb{Z}$  definito da  $f(x) \mapsto (\text{resto di } f(0) \text{ modulo } 2)$ .

Per il resto del paragrafo, descriveremo gli ideali in alcuni casi semplici. In un anello  $R$  l'insieme costituito soltanto dallo zero è un ideale, chiamato *l'ideale nullo*. Esso è ovviamente un ideale principale, al pari dell'intero anello. Essendo generato come ideale dall'elemento  $1$ ,  $R$  è chiamato *l'ideale unità*, e viene indicato spesso con  $(1)$ ; l'ideale unità è l'unico ideale che contiene un'unità. Un ideale  $I$  si dice *proprio* se è diverso da  $(0)$  e da  $(1)$ .

I campi possono essere caratterizzati dal fatto che non hanno ideali propri:

### (3.16) PROPOSIZIONE

- (a) Sia  $F$  un campo. Gli unici ideali di  $F$  sono l'ideale nullo e l'ideale unità.
- (b) Viceversa, se un anello  $R$  ha esattamente due ideali, allora  $R$  è un campo.

**Dimostriamo (b).** Supponiamo che  $R$  abbia esattamente due ideali. Tra gli anelli, i campi si caratterizzano mediante le proprietà che  $1 \neq 0$ , e ogni elemento non nullo ha un inverso rispetto alla moltiplicazione. Come abbiamo visto sopra, si ha  $1 = 0$  soltanto nell'anello nullo, il quale ha un solo elemento; tale anello ha un unico ideale. Poiché per ipotesi  $R$  ha due ideali, in  $R$   $1 \neq 0$ . I due ideali  $(1)$  e  $(0)$  sono distinti, e sono gli unici ideali di  $R$ .

Proviamo ora che ogni elemento non nullo di  $R$  ha un inverso. Sia  $a \in R$  un elemento non nullo, e consideriamo l'ideale principale  $(a)$ . Allora  $(a) \neq (0)$  poiché  $a \in (a)$ . Pertanto  $(a) = (1)$ . Ciò implica che  $1$  è un multiplo, diciamo  $ra$ , di  $a$ . L'equazione  $ra = 1$  prova che  $a$  ha un inverso. ■

**(3.17) COROLLARIO** Sia  $F$  un campo e sia  $R'$  un anello non nullo. Ogni omomorfismo  $\varphi : F \rightarrow R'$  è iniettivo.

**Dimostrazione.** Applichiamo (3.16). Se  $\ker \varphi = (1)$ , allora  $\varphi$  è l'applicazione nulla. Ma l'applicazione nulla non è un omomorfismo, poiché  $R$  non è l'anello nullo. Pertanto  $\ker \varphi = (0)$ . ■

Inoltre è facile determinare gli ideali nell'anello degli interi.

**(3.18) PROPOSIZIONE** Ogni ideale nell'anello  $\mathbb{Z}$  degli interi è un ideale principale.

Infatti, ogni sottogruppo del gruppo additivo  $\mathbb{Z}(+)$  degli interi è della forma  $n\mathbb{Z}$  [cap. 2 (2.3)], e questi sottogruppi sono precisamente gli ideali principali. ■

La *caratteristica* di un anello  $R$  è l'intero non negativo  $n$  che genera il nucleo dell'omomorfismo  $\varphi : \mathbb{Z} \rightarrow R$  [cfr. (3.9)]. Di conseguenza, se  $\ker \varphi \neq (0)$ ,  $n$  è il più piccolo intero positivo tale che " $n$  volte  $1_R$ " = 0, mentre se  $\ker \varphi = (0)$ , la caratteristica è zero (cfr. cap. 3, § 2). Quindi  $\mathbb{R}$ ,  $\mathbb{C}$ , e  $\mathbb{Z}$  hanno caratteristica zero, mentre il campo  $\mathbb{F}_p$  con  $p$  elementi ha caratteristica  $p$ .

La dimostrazione del fatto che ogni ideale dell'anello degli interi è principale può essere adattata per provare che ogni ideale nell'anello dei polinomi  $R[x]$  è principale. Per dimostrarlo ciò, abbiamo bisogno della divisione con resto tra polinomi.

**(3.19) PROPOSIZIONE** Sia  $R$  un anello e siano  $f, g$  polinomi in  $R[x]$ . Supponiamo che il coefficiente direttore di  $f$  sia un'unità in  $R$ . (Ciò è vero, per esempio, se  $f$  è un polinomio monico). Allora esistono polinomi  $q, r \in R[x]$  tali che

$$g(x) = f(x)q(x) + r(x),$$

ove il resto  $r$  ha grado minore di  $f$  oppure è nullo.

Questo risultato può essere dimostrato per induzione sul grado di  $g$ . ■

Si noti che quando l'anello dei coefficienti è un campo, l'ipotesi che il coefficiente direttore di  $f$  sia un'unità è soddisfatta, purché esista un coefficiente direttore, ossia  $f \neq 0$ .

(3.20) COROLLARIO Sia  $g(x)$  un polinomio monico in  $R[x]$ , e sia  $\alpha$  un elemento di  $R$  tale che  $g(\alpha) = 0$ . Allora  $x - \alpha$  divide  $g$  in  $R[x]$ . ■

(3.21) PROPOSIZIONE Sia  $F$  un campo. Allora ogni ideale nell'anello  $F[x]$  dei polinomi in una sola variabile  $x$  è un ideale principale.

*Dimostrazione.* Sia  $I$  un ideale di  $F[x]$ . Poiché l'ideale nullo è principale, possiamo supporre che  $I \neq (0)$ . Nel caso di  $\mathbb{Z}$ , il primo passo per trovare un generatore di un sottogruppo non nullo consiste nella scelta del suo più piccolo elemento positivo. Nel nostro caso, scegliamo un polinomio non nullo  $f$  in  $I$  di grado minimo e dimostriamo che  $I$  è l'ideale principale generato da  $f$ . Dalla definizione di ideale segue che l'ideale principale  $(f)$  è contenuto in  $I$ . Per provare che  $I \subset (f)$ , utilizziamo la divisione con resto per scrivere  $g = fq + r$ , dove  $r$  ha grado minore del grado di  $f$ , oppure  $r = 0$ . Ora, se  $g$  appartiene all'ideale  $I$ , essendo  $f \in I$ , dalla definizione di ideale segue che anche  $r = g - fq$  appartiene a  $I$ . Poiché  $f$  ha grado minimo fra tutti i polinomi non nulli di  $I$ , l'unica possibilità è che  $r = 0$ . Pertanto  $f$  divide  $g$ , come affermato. ■

La dimostrazione del corollario seguente è simile a quella della proposizione (2.6) del capitolo 2.

(3.22) COROLLARIO Sia  $F$  un campo, e siano  $f, g$  polinomi in  $F[x]$  non entrambi nulli. Allora esiste uno ed un solo polinomio monico  $d(x)$ , chiamato il massimo comune divisore di  $f, g$ , avente le seguenti proprietà:

- (a)  $d$  genera l'ideale  $(f, g)$  di  $F[x]$  generato dai due polinomi  $f, g$ ;
- (b)  $d$  divide  $f, g$ ;
- (c) se  $h$  è un divisore di  $f$  e  $g$ , allora  $h$  divide  $d$ ;
- (d) esistono polinomi  $p, q \in F[x]$  tali che  $d = pf + qg$ . ■

#### 4 Anelli quoziante e relazioni in un anello

Sia  $I$  un ideale di un anello  $R$ . Le classi laterali del sottogruppo additivo  $I(+)$  di  $R(+)$  sono i sottoinsiemi

$$a + I, \quad \text{con } a \in R.$$

Da ciò che è stato dimostrato per i gruppi segue che l'insieme delle classi laterali  $R/I = \bar{R}$  è un gruppo rispetto all'addizione. Esso è anche un anello:

(4.1) TEOREMA Sia  $I$  un ideale di un anello  $R$ .

- (a) Esiste un'unica struttura di anello sull'insieme delle classi laterali  $\bar{R} = R/I$  tale che l'applicazione canonica  $\pi : R \rightarrow \bar{R}$  che manda  $a$  in  $\bar{a} = a + I$  sia un omomorfismo.
- (b) Il nucleo di  $\pi$  è  $I$ .

*Dimostrazione.* Questa dimostrazione è stata già sviluppata nel caso speciale in cui  $R$  è l'anello degli interi (cap. 2, § 9). Vogliamo introdurre in  $\bar{R}$  una struttura di anello con le proprietà richieste, e per l'addizione la dimostrazione è stata già data [cap. 2 (10.5)]. Resta da definire la moltiplicazione. Siano  $x, y \in \bar{R}$ , diciamo  $x = \bar{a} = a + I$  e  $y = \bar{b} = b + I$ . Vorremmo definire il prodotto nel modo seguente:  $xy = \bar{ab} = ab + I$ . A differenza del prodotto di classi laterali in un gruppo [cap. 2 (10.1)], l'insieme dei prodotti

$$P = \{rs \mid r \in a + I, s \in b + I\}$$

non è sempre una classe laterale di  $I$ . Tuttavia, come accade nel caso dell'anello degli interi, l'insieme  $P$  è sempre contenuto nella classe laterale  $ab + I$ . Infatti, se scriviamo  $r = a + u$  e  $s = b + v$ , con  $u, v \in I$ , allora

$$(a + u)(b + v) = ab + (av + bu + uv),$$

e poiché  $I$  è un ideale,  $av + bu + uv \in I$ . Questo è tutto ciò che serve per definire la classe laterale prodotto: essa è la classe che contiene l'insieme  $P$ . Questa classe laterale è unica, poiché le classi laterali formano una partizione di  $R$ . La dimostrazione delle rimanenti asserzioni segue da vicino l'argomentazione sviluppata nel capitolo 2 (§ 10). ■

Procedendo in modo analogo a quello illustrato nel capitolo 6 (8.4) e nel capitolo 2 (10.9), si può dimostrare il risultato seguente:

(4.2) PROPOSIZIONE Sia  $f : R \rightarrow R'$  un omomorfismo di anelli con nucleo  $I$  e sia  $J$  un ideale contenuto in  $I$ . Indichiamo l'anello quoziante  $R/J$  con  $\bar{R}$ .

- (a) (Proprietà di rappresentazione degli anelli quoziante) Esiste uno e un solo omomorfismo  $\bar{f} : \bar{R} \rightarrow R'$  tale che  $\bar{f}\pi = f$ :

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \pi \searrow & \nearrow \bar{f} & \\ & \bar{R} = R/J & \end{array} .$$

- (b) (Primo teorema di isomorfismo) Se  $J = I$ , allora  $\bar{f}$  manda, mediante un isomorfismo,  $\bar{R}$  nell'immagine di  $f$ . ■

Desriveremo ora la relazione fondamentale tra gli ideali in un anello quoziante  $R/J$  e gli ideali nell'anello di partenza  $R$ .

(4.3) PROPOSIZIONE (Teorema di corrispondenza) *Sia  $\bar{R} = R/J$  e sia  $\pi$  l'applicazione canonica  $R \rightarrow \bar{R}$ .*

(a) *Esiste una corrispondenza biunivoca tra l'insieme degli ideali di  $R$  che contengono  $J$  e l'insieme di tutti gli ideali di  $\bar{R}$ , data da*

$$I \mapsto \pi(I) \quad e \quad \bar{I} \mapsto \pi^{-1}(\bar{I}).$$

(b) *Se  $I \subset R$  corrisponde a  $\bar{I} \subset \bar{R}$ , allora  $R/I$  e  $\bar{R}/\bar{I}$  sono anelli isomorfi.*

La seconda parte di questa proposizione è chiamata spesso il *terzo teorema di isomorfismo*. (Esiste anche un *secondo teorema di isomorfismo*; cfr. cap. 6, esercizio 7, p. 281).

*Dimostrazione.* Per dimostrare (a), dobbiamo verificare i punti seguenti:

- (i) Se  $I$  è un ideale di  $R$  che contiene  $J$ , allora  $\pi(I)$  è un ideale di  $\bar{R}$ .
- (ii) Se  $\bar{I}$  è un ideale di  $\bar{R}$ , allora  $\pi^{-1}(\bar{I})$  è un ideale di  $R$ .
- (iii)  $\pi^{-1}(\pi(I)) = I$  e  $\pi(\pi^{-1}(\bar{I})) = \bar{I}$ .

Sappiamo che l'immagine di un sottogruppo è un sottogruppo [cap. 2 (4.4)]. Pertanto per far vedere che  $\pi(I)$  è un ideale di  $\bar{R}$ , dobbiamo unicamente dimostrare che è chiuso rispetto alla moltiplicazione per elementi di  $\bar{R}$ . Sia  $\bar{r} \in \bar{R}$  e sia  $\bar{x} \in \pi(I)$ , sicché  $\bar{r} = \pi(r)$  per qualche  $r \in R$ , e  $\bar{x} = \pi(x)$  per qualche  $x \in I$ . Allora  $\bar{r}\bar{x} = \pi(rx)$  e  $rx \in I$ , e quindi  $\bar{r}\bar{x} \in \pi(I)$ . Si noti che questa dimostrazione vale per tutti gli ideali  $I$  di  $R$ ; in questo punto non è necessaria l'ipotesi che  $I \supset J$ . Tuttavia, il fatto che l'applicazione  $\pi$  è suriettiva è essenziale.

Successivamente, denotiamo l'omomorfismo  $\bar{R} \rightarrow \bar{R}/\bar{I}$  con  $\varphi$ , e consideriamo l'omomorfismo composto  $R \xrightarrow{\pi} \bar{R} \xrightarrow{\varphi} \bar{R}/\bar{I}$ . Poiché  $\pi$  e  $\varphi$  sono omomorfismi suriettivi, tale risulta  $\varphi \circ \pi$ . Inoltre, il nucleo di  $\varphi \circ \pi$  è l'insieme degli elementi  $r \in R$  tali che  $\pi(r) \in \bar{I} = \ker \varphi$ . Per definizione, questo insieme è  $\pi^{-1}(\bar{I})$ . Pertanto  $\pi^{-1}(\bar{I})$ , essendo il nucleo di un omomorfismo, è un ideale di  $R$ . Ciò prova (ii). Inoltre, applicando il primo teorema di isomorfismo all'omomorfismo  $\varphi \circ \pi$ , si ottiene che  $R/\pi^{-1}(\bar{I})$  è isomorfo a  $\bar{R}/\bar{I}$ , il che prova la parte (b) della proposizione.

Resta da provare (iii); si ricordi che  $\pi^{-1}$  di solito non è un'applicazione. Le relazioni di inclusione  $\pi^{-1}(\pi(I)) \supset I$  e  $\pi(\pi^{-1}(\bar{I})) \subset \bar{I}$  valgono in generale per qualunque applicazione tra insiemi e per tutti i sottoinsiemi. Inoltre, l'uguaglianza  $\pi(\pi^{-1}(\bar{I})) = \bar{I}$  vale per una qualsiasi applicazione suriettiva tra insiemi. (Omettiamo le verifiche di questi fatti.) Il punto finale, ossia la verifica della relazione  $\pi^{-1}(\pi(I)) \subset I$ , è quello che richiede che  $I \supset J$ . Sia  $x \in \pi^{-1}(\pi(I))$ . Allora

$\pi(x) \in \pi(I)$ , cioè esiste un elemento  $y \in I$  tale che  $\pi(y) = \pi(x)$ . Poiché  $\pi$  è un omomorfismo,  $\pi(x - y) = 0$  e  $x - y \in J = \ker \pi$ , e dato che  $y \in I$  e  $J \subset I$ , si ha  $x \in I$ , come richiesto. ■

La costruzione dell'anello quoziante ha un'interpretazione importante in termini di relazioni tra gli elementi in un anello  $R$ . Immaginiamo di effettuare una successione di operazioni  $+, -, \times$  su alcuni elementi di  $R$  per ottenere un nuovo elemento  $a$ . Se  $a$  è zero, si dice che gli elementi assegnati sono legati dall'equazione

$$(4.4) \quad a = 0.$$

Per esempio, gli elementi 2, 3, 6 dell'anello  $\mathbb{Z}$  sono legati dall'equazione  $2 \times 3 - 6 = 0$ .

Ora, se l'elemento  $a$  è diverso da zero, possiamo chiederci se è possibile modificare  $R$  in modo tale che (4.4) diventi vera. Possiamo pensare a questo procedimento come all'aggiunta di una nuova relazione, che farà rimpicciolire l'anello. Per esempio, la relazione  $3 \times 4 - 5 = 0$  non vale in  $\mathbb{Z}$ , perché  $3 \times 4 - 5 = 7$ . Ma noi possiamo imporre la relazione  $7 = 0$  sugli interi; ciò equivale a lavorare modulo 7.

A questo punto possiamo dimenticare il procedimento che ha condotto all'elemento particolare  $a$  e supporre che sia un qualunque elemento di  $R$ . Ora, quando modifichiamo  $R$  per imporre la relazione  $a = 0$ , vogliamo conservare le operazioni  $+$  e  $\times$ . Dovremo allora accettare alcune conseguenze di questa relazione: per esempio, moltiplicando entrambi i membri di  $a = 0$  per  $r \in R$  si ottiene  $ra = 0$ , mentre sommando  $b \in R$  si ha  $b + a = b$ . Effettuando queste operazioni una dopo l'altra, si ottiene

$$(4.5) \quad b + ra = b.$$

Se vogliamo porre  $a = 0$ , dobbiamo porre anche  $b + ra = b$  per ogni  $b, r \in R$ . Il teorema (4.1) assicura che ciò è sufficiente, che non vi sono cioè altre conseguenze di (4.4). Per verificarlo osserviamo che, se fissiamo un elemento  $b$ , ma lasciamo variare  $r$ , l'insieme  $\{b + ra\}$  è la classe laterale  $b + (a)$ , dove  $(a) = aR$  è l'ideale principale generato da  $a$ . Porre  $b + ra = b$  per ogni  $r$  equivale a uguagliare gli elementi di questa classe laterale. Ciò è precisamente quello che avviene passando da  $R$  all'anello quoziante  $\bar{R} = R/(a)$ . Gli elementi di  $\bar{R}$  sono le classi laterali  $\bar{b} = b + (a)$ , e l'applicazione canonica  $\pi : R \rightarrow \bar{R}$  manda tutti gli elementi  $b + ra$  di una classe laterale nello stesso elemento  $\bar{b} = \pi(b)$ . Pertanto  $\bar{R}$  è stato rimpicciolito esattamente nella misura giusta. Inoltre,  $\bar{a} = 0$ , poiché  $a$  è un elemento dell'ideale  $(a)$ , il quale è il nucleo di  $\pi$ . Pertanto è ragionevole considerare  $\bar{R} = R/(a)$  come l'anello ottenuto introducendo la relazione  $a = 0$  in  $R$ .

Se l'elemento  $a$  in questione era stato ottenuto da altri elementi mediante una successione di operazioni, come abbiamo supposto in (4.4), allora il fatto che  $\pi$

è un omomorfismo implica che la stessa successione di operazioni dà 0 in  $\bar{R}$ . Pertanto, se  $uv + w = a$  per qualche  $u, v, w \in R$ , allora in  $\bar{R}$  vale la relazione

$$(4.6) \quad \bar{u}\bar{v} + \bar{w} = 0.$$

Infatti, poiché  $\pi$  è un omomorfismo,  $\bar{u}\bar{v} + \bar{w} = \overline{uv + w} = \bar{a} = 0$ .

Un buon esempio di questa costruzione è la relazione  $n = 0$  nell'anello degli interi  $\mathbb{Z}$ : l'anello che così si ottiene è  $\mathbb{Z}/n\mathbb{Z}$ .

Più in generale, possiamo introdurre un numero arbitrario di relazioni  $a_1 = \dots = a_n = 0$ , prendendo l'ideale  $I$  generato da  $a_1, \dots, a_n$  (3.15), che è l'insieme delle combinazioni lineari  $\{r_1a_1 + \dots + r_na_n \mid r_i \in R\}$ . L'anello quoziante  $\bar{R} = R/I$  può essere considerato come l'anello ottenuto introducendo in  $R$  le  $n$  relazioni  $a_1 = 0, \dots, a_n = 0$ . Poiché  $a_i \in I$ , le classi resto  $\bar{a}_i$  sono nulle. Due elementi  $b, b'$  di  $R$  hanno la stessa immagine in  $\bar{R}$  se e soltanto se  $b' - b \in I$ , ossia  $b' = b + r_1a_1 + \dots + r_na_n$ , con  $r_i \in R$ . Pertanto

$$(4.7) \quad b + r_1a_1 + \dots + r_na_n = b$$

sono le uniche conseguenze di  $a_1 = \dots = a_n = 0$ .

Dal terzo teorema di isomorfismo (4.3b) discende che se si introducono le relazioni una alla volta, oppure tutte insieme, si ottengono anelli isomorfi. Per essere precisi, siano  $a, b$  elementi di un anello  $R$ , e sia  $\bar{R} = R/(a)$  l'anello ottenuto introducendo la relazione  $a = 0$  in  $R$ . Introducendo la relazione  $\bar{b} = 0$  nell'anello  $\bar{R}$ , si ottiene l'anello quoziante  $\bar{R}/(\bar{b})$ , e quest'ultimo è isomorfo all'anello quoziante  $R/(a, b)$ , ottenuto a partire dalle relazioni  $a = b = 0$ , poiché  $(a, b)$  e  $(\bar{b})$  sono ideali corrispondenti [cfr. (4.3)].

Più relazioni si aggiungono in  $R$ , più si rimpicciolisce l'anello quoziante  $\bar{R}$ . Aggiungendo relazioni alla rinfusa può accadere al limite che l'ideale  $I$  ottenuto sia uguale a  $R$  e  $\bar{R} = 0$ . In tal caso tutte le relazioni  $a = 0$  sono vere.

L'introduzione di relazioni porterà, nella maggior parte dei casi, a un nuovo anello. Ma in alcuni casi semplici è possibile, mediante il primo teorema di isomorfismo mettere in relazione l'anello ottenuto con un anello più familiare. Ecco due esempi in proposito.

Sia  $R = \mathbb{Z}[i]$  l'anello degli interi di Gauss, e sia  $\bar{R}$  l'anello ottenuto introducendo la relazione  $1 + 3i = 0$ . Pertanto  $\bar{R} = R/I$ , dove  $I$  è l'ideale principale generato da  $1 + 3i$ . Cominciamo a lavorare con la relazione, andando alla ricerca di conseguenze riconoscibili. Moltiplicando ambo i membri della relazione  $-1 = 3i$  per  $-i$ , otteniamo  $i = 3$ . Pertanto in  $\bar{R}$  si ha  $i = 3$ . D'altra parte, in  $R$ , e quindi anche in  $\bar{R}$ ,  $i^2 = -1$ . Ne segue che in  $\bar{R}$   $3^2 = -1$ , ossia  $10 = 0$ . Poiché in  $\bar{R}$   $i = 3$  e  $10 = 0$ , è ragionevole ipotizzare che  $\bar{R}$  sia isomorfo a  $\mathbb{Z}/(10) = \mathbb{Z}/10\mathbb{Z}$ .

(4.8) PROPOSIZIONE L'anello  $\mathbb{Z}[i]/(1 + 3i)$  è isomorfo all'anello  $\mathbb{Z}/10\mathbb{Z}$  degli interi modulo 10.

**Dimostrazione.** Consideriamo l'omomorfismo  $\varphi : \mathbb{Z} \rightarrow \bar{R}$  (3.9). In base al primo teorema di isomorfismo,  $\text{im } \varphi \approx \mathbb{Z}/(\ker \varphi)$ . Quindi per ottenere la tesi basta dimostrare che  $\varphi$  è suriettivo e che  $\ker \varphi = 10\mathbb{Z}$ . Ora ogni elemento di  $\bar{R}$  è la classe resto di un intero di Gauss  $a + bi$ . Poiché  $i = 3$  in  $\bar{R}$ , la classe resto di  $a + bi$  è uguale alla classe resto dell'intero  $a + 3b$ . Ciò mostra che  $\varphi$  è suriettivo. Inoltre, sia  $n$  un elemento di  $\ker \varphi$ . Utilizzando il fatto che  $\bar{R} = R/I$ , si ha che  $n$  deve appartenere all'ideale  $I$ , ossia che  $n$  è divisibile per  $1 + 3i$  nell'anello degli interi di Gauss. Pertanto possiamo scrivere  $n = (a + bi)(1 + 3i) = (a - 3b) + (3a + b)i$ , essendo  $a, b$  interi opportuni. Poiché  $n$  è intero, si ha  $3a + b = 0$ , ossia,  $b = -3a$ . Ne segue che  $n = a(1 - 3i)(1 + 3i) = 10a$ , e ciò prova che  $\ker \varphi \subset 10\mathbb{Z}$ . D'altra parte, abbiamo già visto che  $10 \in \ker \varphi$ . Pertanto  $\ker \varphi = 10\mathbb{Z}$ , come richiesto. ■

Un altro modo possibile per determinare il quoziante  $R/I$  è quello di trovare un anello  $R'$  e un omomorfismo  $\varphi : R \rightarrow R'$  il cui nucleo sia  $I$ . Per illustrare ciò, consideriamo l'anello  $\bar{R} = \mathbb{C}[x, y]/(xy)$ . In questo caso, possiamo usare il fatto che  $xy$  è un prodotto per trovare l'applicazione  $\varphi$ .

(4.9) PROPOSIZIONE L'anello  $\mathbb{C}[x, y]/(xy)$  è isomorfo al sottoanello dell'anello prodotto  $\mathbb{C}[x] \times \mathbb{C}[y]$  costituito dalle coppie  $(p(x), q(y))$  tali che  $p(0) = q(0)$ .

**Dimostrazione.** Possiamo determinare facilmente l'anello  $\mathbb{C}[x, y]/(y)$ , poiché l'ideale principale  $(y)$  è il nucleo dell'omomorfismo di sostituzione  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x]$  che manda  $y$  in 0. Per il primo teorema di isomorfismo,  $\mathbb{C}[x, y]/(y) \approx \mathbb{C}[x]$ . Similmente,  $\mathbb{C}[x, y]/(x) \approx \mathbb{C}[y]$ . È naturale quindi considerare l'omomorfismo  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x] \times \mathbb{C}[y]$  definito da  $f(x, y) \mapsto (f(x, 0), f(0, y))$ . Il nucleo di  $\varphi$  è l'intersezione dei nuclei:  $\ker \varphi = (y) \cap (x)$ . Un polinomio che appartiene a questa intersezione deve essere divisibile sia per  $y$  che per  $x$ , ossia deve essere divisibile per  $xy$ . Pertanto  $\ker \varphi = (xy)$ . Per il primo teorema di isomorfismo,  $\bar{R} = \mathbb{C}[x, y]/(xy)$  è isomorfo all'immagine di  $\varphi$ , e questa è il sottoanello definito nell'enunciato. ■

A parte il primo teorema di isomorfismo, non esistono metodi generali per determinare un anello quoziante, che di solito non sarà un anello familiare. Per esempio, l'anello  $\mathbb{C}[x, y]/(y^2 - x^3 + x)$  è profondamente diverso da ogni altro anello incontrato finora.

## 5 Aggiunzione di elementi

In questo paragrafo studieremo un procedimento che è strettamente collegato con l'introduzione di relazioni, e che consiste nell'aggiungere a un anello nuovi elementi. Il modello è dato dalla costruzione del campo dei numeri complessi a partire dai numeri reali. Ci si ottiene da  $\mathbb{R}$  aggiungendo  $i$ , e la costruzione è

puramente formale; in altre parole il numero immaginario  $i$  non ha altre proprietà all'infuori di quelle che derivano dalla relazione

$$(5.1) \quad i^2 = -1.$$

Siamo ora in grado di comprendere il principio generale che è alla base di questa costruzione. Partiamo da un anello  $R$  e consideriamo il problema di costruire un anello più grande contenente gli elementi di  $R$  e in più un nuovo elemento, che denotiamo con  $\alpha$ . Probabilmente richiederemo che  $\alpha$  soddisfi ad alcune relazioni, quale ad esempio (5.1). Un anello  $R'$  contenente  $R$  come sottoanello è chiamato *estensione di anelli* di  $R$ ; quindi stiamo cercando una estensione opportuna.

Può darsi che l'elemento  $\alpha$  appartenga a un'estensione di anelli  $R'$  che già conosciamo; in tal caso, la soluzione del problema è data dal sottoanello di  $R'$  generato da  $R$  e da  $\alpha$ . Questo sottoanello si denota con  $R[\alpha]$ . Lo abbiamo già descritto nel paragrafo 1, nel caso in cui  $R = \mathbb{Z}$  e  $R' = \mathbb{C}$ . Tale descrizione vale anche in generale:  $R[\alpha]$  è costituito dagli elementi di  $R'$  esprimibili nella forma polinomiale:

$$r_n\alpha^n + \cdots + r_1\alpha + r_0,$$

con coefficienti  $r_i$  in  $R$ . D'altra parte, come accade nella costruzione di  $\mathbb{C}$  a partire da  $\mathbb{R}$ , potremmo non conoscere ancora un'estensione contenente  $\alpha$ . Allora dobbiamo costruirla in modo astratto. In effetti, abbiamo già fatto ciò, costruendo l'anello dei polinomi  $R[x]$ .

L'anello dei polinomi  $R[x]$  è un'estensione di  $R$  ed è generata da  $R$  e da  $x$ . (La notazione  $R[x]$  è dunque in accordo con quella introdotta sopra.) Inoltre, il principio di sostituzione (3.4) afferma che l'anello dei polinomi è la *soluzione universale* del problema dell'aggiunzione di un nuovo elemento. Precisamente, se  $\alpha$  è un elemento di un'estensione di anelli  $R'$  di  $R$ , allora esiste un'unica applicazione  $R[x] \rightarrow R'$  che sia l'identità su  $R$  e che mandi  $x$  in  $\alpha$ . L'immagine di questa applicazione sarà il sottoanello  $R[\alpha]$ .

Consideriamo ora il problema delle relazioni che vogliamo che siano soddisfatte dal nuovo elemento. La variabile  $x$  nell'anello dei polinomi  $R[x]$  non soddisfa alcuna relazione all'infuori di quelle (come  $0x = 0$ ) che sono conseguenze degli assiomi di anello (questo è un altro modo di enunciare la proprietà universale dell'anello dei polinomi). Possiamo invece richiedere che siano soddisfatte alcune relazioni non banali. Ma avendo a disposizione l'anello  $R[x]$ , possiamo aggiungere ad esso delle relazioni a piacere con il procedimento dato nel paragrafo 4. Possiamo cioè utilizzare la costruzione del quoziente *sull'anello dei polinomi*  $R[x]$ . Il fatto che  $R$  venga sostituito da  $R[x]$  nella costruzione complica le cose dal punto di vista delle notazioni, ma, a parte ciò, non cambia nulla.

Per esempio, possiamo costruire i numeri complessi formalmente, introducendo la relazione  $x^2 + 1 = 0$  nell'anello dei polinomi a coefficienti reali  $R[x] = P$ . Per fare ciò, formiamo l'anello quoziente  $\bar{P} = P/(x^2 + 1)$ . La classe resto di  $x$

diventa l'elemento  $i$ . Si noti che la relazione  $\overline{x^2 + 1} = \overline{x}^2 + \overline{1} = 0$  vale in  $\bar{P}$ , perché l'applicazione  $\pi : P \rightarrow \bar{P}$  è un omomorfismo e perché  $x^2 + 1 \in \ker \pi$ . Ora, poiché  $\bar{1}$  è l'elemento unità in  $\bar{P}$ , la notazione standard per l'elemento unità lascia cadere  $\bar{1}$  e la barra. Pertanto  $\bar{P}$  si ottiene da  $P$  aggiungendo un elemento  $\bar{x}$  soddisfacente alla relazione  $\bar{x}^2 + 1 = 0$ . In altre parole,  $\bar{P} \approx \mathbb{C}$ , come richiesto.

Il fatto che il quoziente  $R[x]/(x^2 + 1)$  è isomorfo a  $\mathbb{C}$  segue anche dal primo teorema di isomorfismo (4.2b). Precisamente, la sostituzione (3.4) di  $x$  con  $i$  definisce un omomorfismo suriettivo  $\varphi : R[x] \rightarrow \mathbb{C}$ , il cui nucleo è l'insieme dei polinomi a coefficienti reali aventi  $i$  come radice. Ora, se  $i$  è una radice di un polinomio reale  $p(x)$ , anche  $-i$  è una radice di  $p(x)$ . Pertanto  $x - i$  e  $x + i$  dividono entrambi  $p(x)$ , e quindi il nucleo è l'insieme dei polinomi a coefficienti reali divisibili per  $(x - i)(x + i) = x^2 + 1$ , cioè l'ideale principale  $(x^2 + 1)$ . In base al primo teorema di isomorfismo,  $\mathbb{C}$  è isomorfo a  $R[x]/(x^2 + 1)$ .

Un altro esempio semplice di aggiunzione di un elemento è stato illustrato nel capitolo 8 (§ 6), dove, per calcolare i vettori tangenti, è stato introdotto un elemento infinitesimo formale soddisfacente alla relazione:

$$(5.2) \quad \epsilon^2 = 0.$$

Un elemento di un anello  $R$  è chiamato *infinitesimo* o *nilpotente* se qualche sua potenza è nulla, e il nostro procedimento permette di aggiungere elementi infinitesimi a un anello. Pertanto, aggiungendo a un anello  $R$  un elemento  $\epsilon$  soddisfacente alla relazione (5.2), si ottiene l'anello quoziente  $R' = R[x]/(\epsilon^2)$ . La classe resto di  $x$  è l'elemento infinitesimo  $\epsilon$ . In questo anello, la relazione  $\epsilon^2 = 0$  riduce ogni espressione polinomiale in  $\epsilon$  a una di grado  $< 2$ , sicché gli elementi di  $R'$  hanno la forma  $a + b\epsilon$ , con  $a, b \in R$ . Ma la regola della moltiplicazione [cap. 8 (6.5)] è diversa dalla regola della moltiplicazione per i numeri complessi.

In generale, se vogliamo aggiungere a un anello  $R$  un elemento  $\alpha$  soddisfacente a una o più relazioni polinomiali della forma:

$$(5.3) \quad f(\alpha) = c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0,$$

la soluzione è  $R' = R[x]/I$ , dove  $I$  è l'ideale di  $R[x]$  generato dai polinomi  $f(x)$ . Se  $\alpha$  denota la classe resto  $\bar{x}$  di  $x$  in  $R'$ , allora risulta

$$(5.4) \quad 0 = \overline{f(x)} = \overline{c_n}\bar{x}^n + \cdots + \overline{c_0} = \overline{c_n}\alpha^n + \cdots + \overline{c_0},$$

dove  $\overline{c}_i$  è l'immagine in  $R'$  del polinomio costante  $c_i$ . Pertanto  $\alpha$  soddisfa alla relazione in  $R'$  che corrisponde alla relazione (5.3) in  $R$ . L'anello ottenuto in questo modo sarà denotato spesso con  $R[\alpha]$ :

$$(5.5) \quad R[\alpha] = \text{anello ottenuto aggiungendo } \alpha \text{ a } R.$$

Osserviamo che più elementi  $\alpha_1, \dots, \alpha_m$  possono essere aggiunti ripetendo questo procedimento, oppure introducendo tutte insieme le relazioni opportune nell'anello dei polinomi in  $m$  variabili,  $R[x_1, \dots, x_m]$ .

Uno dei casi più importanti è quello in cui si richiede che il nuovo elemento  $\alpha$  soddisfi a una sola equazione *monica* di grado  $n > 0$ . Supponiamo che venga soddisfatta la relazione  $f(\alpha) = 0$ , dove  $f$  è il polinomio monico:

$$(5.6) \quad f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0.$$

Non è difficile descrivere con precisione l'anello  $R[\alpha]$  in questo caso speciale.

(5.7) PROPOSIZIONE *Sia  $R$  un anello e sia  $f(x)$  un polinomio monico di grado positivo  $n$ , a coefficienti in  $R$ . Si denoti con  $R[\alpha]$  l'anello ottenuto aggiungendo un elemento  $\alpha$  soddisfacente alla relazione  $f(\alpha) = 0$ . Gli elementi di  $R[\alpha]$  sono in corrispondenza biunivoca con i vettori  $(r_0, \dots, r_{n-1}) \in R^n$ : ogni vettore corrisponde alla combinazione lineare:*

$$r_0 + r_1\alpha + r_2\alpha^2 + \dots + r_{n-1}\alpha^{n-1}, \quad \text{con } r_i \in R.$$

Tale proposizione dice che le potenze  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  formano una *base* di  $R[\alpha]$  su  $R$ . Per moltiplicare due combinazioni lineari in  $R[\alpha]$  usiamo le regole della moltiplicazione tra polinomi e dividiamo il prodotto per  $f$ . Il resto è la combinazione lineare di  $1, \alpha, \dots, \alpha^{n-1}$  che rappresenta il prodotto. Pertanto, sebbene l'addizione in  $R'$  dipenda soltanto dal grado, la moltiplicazione dipende fortemente dal polinomio particolare  $f$ .

Per esempio, sia  $R'$  l'anello ottenuto aggiungendo a  $Z$  un elemento  $\alpha$  soddisfacente alla relazione  $\alpha^3 + 3\alpha + 1 = 0$ . Allora  $R' = Z[x]/(x^3 + 3x + 1)$  e gli elementi di  $R'$  sono combinazioni lineari  $r_0 + r_1\alpha + r_2\alpha^2$ , dove gli  $r_i$  sono interi. L'addizione di due combinazioni lineari è l'addizione di polinomi, per esempio:  $(2+\alpha-\alpha^2)+(1+\alpha)=3+2\alpha-\alpha^2$ . Per moltiplicare, calcoliamo il prodotto utilizzando la moltiplicazione di polinomi:  $(2+\alpha-\alpha^2)(1+\alpha)=2+3\alpha-\alpha^3$ . Dividiamo poi per  $1+3\alpha+\alpha^3$ , ottenendo  $2+3\alpha-\alpha^3=(1+3\alpha+\alpha^3)(-1)+(3+6\alpha)$ . Poiché in  $R'$ ,  $1+3\alpha+\alpha^3=0$ , il resto  $3+6\alpha$  è la combinazione lineare che rappresenta il prodotto.

Sia  $R'$  l'anello ottenuto aggiungendo a  $F_5$  un elemento  $\alpha$ , con la relazione  $\alpha^2 - 3 = 0$ ; sia cioè  $R' = F_5[x]/(x^2 - 3)$ . Qui  $\alpha$  rappresenta formalmente una radice quadrata di 3. Gli elementi di  $R'$  sono le 25 espressioni lineari in  $\alpha$ :  $a + b\alpha$ , con  $a, b \in F_5$ . Questo anello è un campo, per dimostrarlo verifichiamo che ogni elemento non nullo  $a + b\alpha$  di  $R'$  è invertibile. Si noti che  $(a + b\alpha)(a - b\alpha) = a^2 - 3b^2 \in F_5$ . Inoltre, l'equazione  $x^2 = 3$  non ha soluzioni in  $F_5$ , e ciò implica che  $a^2 - 3b^2 \neq 0$ . Pertanto  $a^2 - 3b^2$  è invertibile in  $F_5$  e in  $R'$ . Ciò dimostra che anche  $a + b\alpha$  è invertibile: il suo inverso è  $(a^2 - 3b^2)^{-1}(a - b\alpha)$ .

D'altra parte, applicando lo stesso procedimento a  $F_{11}$  non si ottiene un campo. Il motivo è che  $x^2 - 3 = (x + 5)(x - 5)$  in  $F_{11}[x]$ . Pertanto, se  $\alpha$  denota la classe resto di  $x$  in  $R' = F_{11}[x]/(x^2 - 3)$ , allora  $(\alpha + 5)(\alpha - 5) = 0$ . Ciò può essere spiegato intuitivamente, osservando che abbiamo costruito  $R'$  aggiungendo una radice quadrata di 3 a  $F_{11}$ , quando quel campo già contiene le due radici quadrate  $\pm 5$ . A prima vista, ci si potrebbe aspettare di riottenere  $F_{11}$  con questo procedimento. Ma non abbiamo precisato se  $\alpha$  è uguale a 5 oppure a -5. Abbiamo detto soltanto che il suo quadrato è 3. La relazione  $(\alpha + 5)(\alpha - 5) = 0$  riflette questa ambiguità.

*Dimostrazione della proposizione (5.7).* Poiché  $R[\alpha]$  è un quoziente dell'anello dei polinomi  $R[x]$ , ogni elemento in  $R[\alpha]$  è la classe resto di un polinomio. Ciò significa che esso può essere scritto nella forma  $g(\alpha)$  per qualche  $g(x) \in R[x]$ . La relazione  $f(\alpha) = 0$  può essere usata per sostituire ogni polinomio  $g(\alpha)$  di grado  $\geq n$  con uno di grado più basso. Precisamente, effettuiamo la divisione con resto del polinomio  $g(x)$  per  $f(x)$ , ottenendo un'espressione della forma:  $g(x) = f(x)q(x) + r(x)$ , come nella (3.19). Poiché  $f(\alpha) = 0$ ,  $g(\alpha) = r(\alpha)$ . Pertanto ogni elemento di  $R[\alpha]$  può essere scritto come un polinomio in  $\alpha$  di grado  $< n$ .

Mostriamo ora che l'ideale principale generato da  $f(x)$  non contiene elementi di grado  $< n$ , cosicché  $g(\alpha) \neq 0$  per ogni polinomio non nullo  $g(x)$  di grado  $< n$ . Ne seguirà che l'espressione di grado  $< n$  di un elemento di  $R[\alpha]$  è unica. L'ideale principale generato da  $f(x)$  è l'insieme di tutti i multipli  $hf$  di  $f$ . Sia  $h(x) = b_mx^m + \dots + b_0$ , con  $b_m \neq 0$ . Allora il termine di grado più alto di  $h(x)f(x)$  è  $b_mx^{m+n}$ , e quindi  $hf$  ha grado  $m+n \geq n$ . Ciò completa la dimostrazione della proposizione (5.7). ■

È più difficile analizzare la struttura dell'anello ottenuto aggiungendo un elemento che soddisfi a una relazione polinomiale non monica. Uno dei casi più semplici e più importanti si ottiene aggiungendo ad un anello un inverso moltiplicativo di un suo elemento. Se un elemento  $a \in R$  ha un inverso  $\alpha$ , allora  $\alpha$  soddisfa alla relazione:

$$(5.8) \quad a\alpha - 1 = 0.$$

Possiamo dunque aggiungere l'inverso di un elemento  $a$  formando l'anello quoziente  $R' = R[x]/(ax - 1)$ . La classe resto di  $x$  diventa l'inverso  $\alpha$  di  $a$ . Questo anello non ha nessuna base del tipo descritto nella proposizione (5.7), tuttavia può essere descritto abbastanza facilmente, poiché ogni elemento di  $R'$  ha la forma  $\alpha^k r$ , dove  $r \in R$  e  $k$  è un intero non negativo. Se, diciamo,  $\beta = r_0 + r_1\alpha + \dots + r_{n-1}\alpha^{n-1}$ , con  $r_i \in R$ , allora, poiché  $a\alpha = 1$ , possiamo anche scrivere  $\beta = \alpha^{n-1}(r_0a^{n-1} + r_1a^{n-2} + \dots + r_{n-1})$ .

Un esempio interessante si ottiene nel caso in cui  $R$  è esso stesso un anello di polinomi, diciamo  $R = F[t]$ , e aggiungiamo l'inverso della variabile  $t$ . Allora

$R' = F[t, x]/(xt - 1)$ . Questo anello si identifica in modo naturale con l'anello  $F[t, t^{-1}]$  dei polinomi di Laurent in  $t$ . Un polinomio di Laurent è un polinomio in  $t$  e  $t^{-1}$  del tipo

$$(5.9) \quad f(t) = \sum_{-n}^n a_i t^i = a_{-n} t^{-n} + \cdots + a_{-1} t^{-1} + a_0 + a_1 t + \cdots + a_n t^n.$$

La costruzione dell'isomorfismo  $F[t, x]/(xt - 1) \approx F[t, t^{-1}]$  è lasciata come esercizio.

Dobbiamo ora considerare un punto che è stato tralasciato nella precedente trattazione dell'aggiunzione di elementi, cioè: aggiungendo a un anello  $R$  un elemento  $\alpha$  e imponendo alcune relazioni, l'anello  $R$  di partenza risulterà un sottoanello dell'anello  $R[\alpha]$  che così si ottiene? Sappiamo che  $R$  è contenuto nell'anello dei polinomi  $R[x]$ , come il sottoanello dei polinomi costanti. Pertanto la restrizione dell'applicazione canonica  $\pi : R[x] \rightarrow R[x]/I = R[\alpha]$  ai polinomi costanti fornisce un omomorfismo  $\psi : R \rightarrow R[\alpha]$ , che è l'applicazione  $r \mapsto \bar{r}$  considerata sopra. Il nucleo dell'applicazione  $\psi : R \rightarrow R[\alpha] = R[x]/I$  è facile da determinare, in linea di principio. Esso è l'insieme dei polinomi costanti nell'ideale  $I$ :

$$(5.10) \quad \ker \psi = R \cap I.$$

Dalla proposizione (5.7) segue che  $\psi$  è iniettiva, e quindi che  $\ker \psi = 0$ , quando si richiede che  $\alpha$  soddisfi a un'equazione monica. Ma  $\psi$  non è sempre iniettiva.

Per esempio, faremmo meglio a non aggiungere un inverso di 0 a un anello. Dall'equazione  $0\alpha = 1$  possiamo concludere che  $0 = 1$ . L'elemento 0 è invertibile soltanto nell'anello nullo, sicché se insistiamo a voler aggiungere un inverso di 0, otteniamo necessariamente alla fine l'anello nullo.

Più in generale, se  $a, b$  sono due elementi di un anello  $R$  il cui prodotto  $ab$  è uguale a zero, allora  $a$  non è invertibile, a meno che  $b = 0$ . Infatti, se esiste  $a^{-1}$  in  $R$ , allora  $b = a^{-1}ab = a^{-1}0 = 0$ . Ne segue che, se  $ab$  è uguale a zero, allora, aggiungendo a  $R$  un inverso di  $a$ , si ottiene  $\bar{b} = 0$  in  $\bar{R}$ . Ciò si può vedere anche direttamente. Infatti, l'ideale di  $R[x]$  generato da  $ax - 1$  contiene  $-b(ax - 1) = b$ , e quindi la classe resto di  $b$  nell'anello  $R[x]/(ax - 1)$  è uguale a zero.

Per esempio,  $\bar{2} \cdot \bar{3} = 0$  nell'anello  $\mathbb{Z}/(6)$ . Se aggiungiamo l'inverso di  $\bar{3}$  a questo anello, otteniamo necessariamente  $\bar{2} = 0$ . Così facendo,  $\mathbb{Z}/(6)$  si contrae in  $\mathbb{Z}/(2) = \mathbb{F}_2$ . Poiché  $\bar{3} = \bar{1}$  è invertibile in  $\mathbb{F}_2$ , non occorre fare nient'altro, e  $R' = (\mathbb{Z}/(6))[x]/(\bar{3}x - \bar{1}) \approx \mathbb{F}_2$ . Ciò può essere verificato direttamente, anche questa volta. Per fare ciò, osserviamo che l'anello  $R'$  è isomorfo a  $\mathbb{Z}[x]/(6, 3x - 1)$ , e analizziamo le due relazioni  $6 = 0$  e  $3x - 1 = 0$ . Da esse segue che  $6x = 0$  e  $6x - 2 = 0$ , sicché  $2 = 0$ . Allora si ha anche  $2x = 0$  e ciò, insieme con  $3x - 1 = 0$ , implica che  $x - 1 = 0$ . Pertanto l'ideale  $(6, 3x - 1)$  di  $\mathbb{Z}[x]$  contiene gli elementi  $2, x - 1$ . D'altra parte,  $6$  e  $3x - 1$  appartengono all'ideale  $(2, x - 1)$ . Ne segue che i due ideali sono uguali, e  $R'$  è isomorfo a  $\mathbb{Z}[x]/(2, x - 1) \approx \mathbb{F}_2$ .

Un elemento  $a$  di un anello è chiamato *divisore dello zero* se esiste un elemento non nullo  $b$  tale che  $ab = 0$ . Per esempio, la classe resto di 3 è un divisore dello zero nell'anello  $\mathbb{Z}/(6)$ . Il termine “divisore dello zero” è entrato nell'uso, ma non è molto felice, poiché in realtà ogni elemento  $a \in R$  divide lo zero:  $0 = a0$ .

## 6 Domini di integrità e campi di frazioni

La differenza tra gli anelli e i campi è che gli elementi non nulli di un anello non hanno necessariamente un inverso. In questo paragrafo tratteremo il problema dell'immersione di un anello assegnato  $R$  come sottoanello in un campo. Abbiamo visto nell'ultimo paragrafo che non possiamo aggiungere l'inverso di un divisore dello zero senza annullare qualche elemento. Pertanto un anello che contiene divisori dello zero non può essere immerso in un campo.

(6.1) DEFINIZIONE *Un dominio di integrità  $R$  è un anello non nullo privo di divisori dello zero. In altre parole,  $1 \neq 0$  in  $R$ , e se  $a, b \in R$ ,  $ab = 0$ , allora  $a = 0$  oppure  $b = 0$ .*

Per esempio, ogni sottoanello di un campo è un dominio di integrità.

In un dominio di integrità vale la *legge di cancellazione*:

(6.2) *Se  $ab = ac$  e  $a \neq 0$ , allora  $b = c$ .*

Infatti, da  $ab = ac$  possiamo dedurre:  $a(b - c) = 0$ . Allora, poiché  $a \neq 0$ , segue che  $b - c = 0$ . ■

(6.3) PROPOSIZIONE *Sia  $R$  un dominio di integrità. Allora l'anello dei polinomi  $R[x]$  è un dominio di integrità.*

(6.4) PROPOSIZIONE *Un dominio di integrità con un numero finito di elementi è un campo.*

Le dimostrazioni di queste proposizioni sono lasciate come esercizi. ■

(6.5) TEOREMA *Sia  $R$  un dominio di integrità. Allora esiste un'immersione di  $R$  in un campo, ossia un omomorfismo iniettivo  $R \rightarrow F$ , dove  $F$  è un campo.*

Potremmo costruire il campo aggiungendo gli inversi di tutti gli elementi non nulli di  $R$ , utilizzando il procedimento descritto nell'ultimo paragrafo. Ma in questo caso è molto più semplice costruire  $F$  con le frazioni. Il nostro modello è la costruzione dell'insieme  $\mathbb{Q}$  dei numeri razionali come frazioni di interi, e una volta avanzata l'idea di usare le frazioni, la costruzione segue molto da vicino la costruzione dei numeri razionali.

Sia  $R$  un dominio di integrità. Una frazione sarà un simbolo  $a/b$  dove  $a, b \in R$  e  $b \neq 0$ . Due frazioni  $a_1/b_1, a_2/b_2$  si dicono *equivalenti*, e si scrive  $a_1/b_1 \approx a_2/b_2$ , se

$$a_1 b_2 = a_2 b_1.$$

Verifichiamo la transitività di questa relazione, dopo aver osservato che la proprietà riflessiva e la proprietà simmetrica sono chiaramente soddisfatte (cfr. cap. 2, §5). Supponiamo che  $a_1/b_1 \approx a_2/b_2$  e che  $a_2/b_2 \approx a_3/b_3$ . Allora  $a_1 b_2 = a_2 b_1$  e  $a_2 b_3 = a_3 b_2$ . Moltiplicando per  $b_3$  e per  $b_1$  si ottiene:

$$a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_2 b_1.$$

Cancellando  $b_2$ , si ha  $a_3 b_1 = a_1 b_3$ . Pertanto  $a_1/b_1 \approx a_3/b_3$ .

Il campo delle frazioni (o campo dei quozienti)  $F$  di  $R$  è l'insieme delle classi di equivalenza di frazioni. Così come facciamo con i numeri razionali, diremo che due frazioni  $a_1/b_1, a_2/b_2$  sono elementi uguali di  $F$  se sono frazioni equivalenti. Precisamente,  $a_1/b_1 = a_2/b_2$  in  $F$  significa che  $a_1 b_2 = a_2 b_1$ . L'addizione e la moltiplicazione di frazioni si definiscono come in aritmetica:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Qui occorre verificare che queste regole producono risultati equivalenti se  $a/b$  e  $c/d$  sono sostituite da frazioni equivalenti. Inoltre devono essere verificati gli assiomi di un campo. Tutte queste verifiche si effettuano in modo diretto e sono lasciate come esercizi. ■

Si noti che  $R$  è contenuto in  $F$ , purché identifichiamo un elemento  $a \in R$  con la frazione  $a/1$ , poiché  $a/1 \approx b/1$  se e soltanto se  $a = b$ . L'applicazione  $a \mapsto a/1$  è l'omomorfismo iniettivo citato nel teorema (6.5).

Come esempio, consideriamo l'anello dei polinomi  $K[x]$ , dove  $K$  è un campo. Questo anello è un dominio di integrità; il suo campo delle frazioni è chiamato il campo delle *funzioni razionali* in  $x$ , a coefficienti in  $K$  e si indica di solito con

$$(6.6) \quad K(x) = \left\{ \begin{array}{l} \text{classi di equivalenza di frazioni } f/g, \text{ dove } f, g \\ \text{sono polinomi e } g \text{ è diverso dal polinomio nullo} \end{array} \right\}.$$

Se  $K = \mathbb{R}$  una funzione razionale  $f(x)/g(x)$  individua una funzione reale di variabile reale, definita su tutti gli  $x \in \mathbb{R}$  tali che  $g(x) \neq 0$ . Tuttavia, come abbiamo visto per i polinomi, dovremmo distinguere tra le funzioni razionali definite formalmente, che sono quozienti di polinomi, e le funzioni vere e proprie che essi definiscono in ogni punto  $x$  in cui  $g(x) \neq 0$ .

Il campo delle frazioni è una soluzione universale del problema dell'immersione di un dominio di integrità in un campo, come mostra la proposizione seguente:

## 7 | Ideali massimali

(6.7) PROPOSIZIONE Sia  $R$  un dominio di integrità, con campo delle frazioni  $F$ , e sia  $\varphi : R \rightarrow K$  un omomorfismo iniettivo di  $R$  in un campo  $K$ . Allora la legge

$$\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$$

definisce l'unica estensione di  $\varphi$  a un omomorfismo  $\Phi : F \rightarrow K$ .

*Dimostrazione.* Dobbiamo verificare che tale estensione è ben definita. Innanzitutto, poiché il denominatore di una frazione è necessariamente diverso da zero e poiché  $\varphi$  è iniettivo,  $\varphi(b) \neq 0$  per ogni frazione  $a/b$ . Pertanto  $\varphi(b)$  è invertibile in  $K$ , e  $\varphi(a)\varphi(b)^{-1}$  è un elemento di  $K$ . Verifichiamo ora che frazioni equivalenti hanno la stessa immagine. Se  $a_2/b_2 \approx a_1/b_1$ , cioè  $a_2 b_1 = a_1 b_2$ , ne segue che  $\varphi(a_2)\varphi(b_1) = \varphi(a_1)\varphi(b_2)$  e  $\Phi(a_2/b_2) = \varphi(a_2)\varphi(b_2)^{-1} = \varphi(a_1)\varphi(b_1)^{-1} = \Phi(a_1/b_1)$ , come richiesto. Da ciò segue facilmente che  $\Phi$  è un omomorfismo ed è l'unica estensione di  $\varphi$ . ■

## 7 Ideali massimali

In questo paragrafo studieremo gli omomorfismi suriettivi

$$(7.1) \quad \varphi : R \rightarrow F$$

da un anello  $R$  a un campo  $F$ . Dato un omomorfismo siffatto, il primo teorema di isomorfismo ci dice che  $F$  è isomorfo a  $R/\ker \varphi$ . Pertanto possiamo ricostruire  $F$  e  $\varphi$ , a meno di isomorfismi, a partire dal nucleo. Per classificare tali omomorfismi, dobbiamo determinare gli ideali  $M$  tali che  $R/M$  sia un campo.

In base al teorema di corrispondenza (4.3), gli ideali di  $\bar{R} = R/M$  corrispondono agli ideali di  $R$  che contengono  $M$ . Inoltre, i campi sono caratterizzati dalla proprietà di avere esattamente due ideali (3.16). Pertanto, se  $\bar{R}$  è un campo, vi sono esattamente due ideali che contengono  $M$ , ossia  $M$  e  $R$ . Un ideale  $M$  con questa proprietà è chiamato *ideale massimale*.

(7.2) DEFINIZIONE Un ideale  $M$  si dice massimale se  $M \neq R$  e  $M$  non è contenuto in alcun ideale diverso da  $M$  e da  $R$ .

## (7.3) COROLLARIO

(a) Un ideale  $M$  di un anello  $R$  è massimale se e solo se  $\bar{R} = R/M$  è un campo.

(b) L'ideale nullo di  $R$  è massimale se e solo se  $R$  è un campo.

La proposizione seguente è conseguenza del fatto che tutti gli ideali di  $\mathbb{Z}$  sono principali:

(7.4) PROPOSIZIONE *Gli ideali massimali dell'anello  $\mathbb{Z}$  degli interi sono gli ideali principali generati dai numeri primi.* ■

Anche gli ideali massimali dell'anello  $\mathbb{C}[x]$  dei polinomi in una variabile a coefficienti complessi possono essere descritti in modo molto semplice:

(7.5) PROPOSIZIONE *Gli ideali massimali dell'anello dei polinomi  $\mathbb{C}[x]$  sono gli ideali principali generati dai polinomi lineari  $x - a$ . L'ideale  $M_a$  generato da  $x - a$  è il nucleo dell'omomorfismo di sostituzione  $s_a : \mathbb{C}[x] \rightarrow \mathbb{C}$ , che manda  $f(x)$  in  $f(a)$ . Pertanto esiste una corrispondenza biunivoca tra gli ideali massimali  $M_a$  e i numeri complessi  $a$ .*

*Dimostrazione.* Proviamo innanzitutto che ogni ideale massimale è generato da un polinomio lineare  $x - a$ . Sia  $M$  un ideale massimale. In base alla proposizione (3.21),  $M$  è un ideale principale, generato dal polinomio monico  $f \in M$  di grado minimo. Poiché ogni polinomio complesso di grado positivo ha una radice,  $f$  è divisibile per qualche polinomio lineare  $x - a$ . Allora  $f$  appartiene all'ideale principale  $(x - a)$ , e quindi  $M \subset (x - a)$ . Poiché  $M$  è massimale,  $M = (x - a)$ .

Dimostriamo ora che il nucleo dell'omomorfismo di sostituzione  $s_a$  è generato da  $x - a$ . Un polinomio  $g$  appartiene al nucleo di  $s_a$  se e solo se  $a$  è una radice di  $g$ , ossia  $x - a$  divide  $g$ . Pertanto  $x - a$  genera  $\ker s_a$ . Poiché l'immagine di  $s_a$  è un campo, ciò prova anche che  $(x - a)$  è un ideale massimale. ■

L'estensione della proposizione (7.5) al caso di più variabili costituisce uno dei teoremi più importanti relativi agli anelli di polinomi:

(7.6) TEOREMA DEGLI ZERI DI HILBERT *Gli ideali massimali dell'anello dei polinomi  $\mathbb{C}[x_1, \dots, x_n]$  sono in corrispondenza biunivoca con i punti dello spazio complesso di dimensione  $n$ . Un punto  $a = (a_1, \dots, a_n)$  in  $\mathbb{C}^n$  corrisponde al nucleo dell'omomorfismo di sostituzione  $s_a : \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}$  che manda  $f(x)$  in  $f(a)$ . Il nucleo  $M_a$  di tale omomorfismo è l'ideale generato dai polinomi lineari*

$$x_1 - a_1, \dots, x_n - a_n.$$

*Dimostrazione.* Sia  $a = (a_1, \dots, a_n)$  un punto di  $\mathbb{C}^n$ , e sia  $M_a$  il nucleo dell'omomorfismo di sostituzione  $s_a$ . Poiché  $s_a$  è suriettivo e  $\mathbb{C}$  è un campo,  $M_a$  è un ideale massimale. Verifichiamo che  $M_a$  è generato dai polinomi lineari, come asserito. Per fare ciò, sviluppiamo un polinomio  $f \in \mathbb{C}[x_1, \dots, x_n]$  con la formula di Taylor centrata nel punto  $a = (a_1, \dots, a_n)$  e otteniamo:

$$f(x) = f(a) + \sum_i c_i(x_i - a_i) + \sum_{i,j} c_{ij}(x_i - a_i)(x_j - a_j) + \dots,$$

ove  $c_i = \frac{\partial f}{\partial x_i}(a)$  e così via.

Si noti che ogni termine a secondo membro, ad eccezione di  $f(a)$ , è divisibile per almeno uno dei polinomi  $(x_i - a_i)$ . Pertanto, se  $f$  appartiene al nucleo di  $s_a$ , ossia, se  $f(a) = 0$ , allora  $f(x)$  appartiene all'ideale generato da  $x_1 - a_1, \dots, x_n - a_n$ . Ciò prova che i polinomi  $x_i - a_i$  generano  $M_a$ .

Più difficile è dimostrare che ogni ideale massimale è della forma  $M_a$  per qualche punto  $a \in \mathbb{C}^n$ . Sia  $M$  un ideale massimale arbitrario, e si denoti con  $K$  il campo  $\mathbb{C}[x_1, \dots, x_n]/M$ . Consideriamo la restrizione dell'applicazione canonica (4.1)  $\pi : \mathbb{C}[x_1, \dots, x_n] \rightarrow K$  al sottoanello  $\mathbb{C}[x_1]$  dei polinomi in una variabile:

$$\pi_1 : \mathbb{C}[x_1] \rightarrow K.$$

(7.7) LEMMA *Il nucleo di  $\pi_1$  è l'ideale nullo oppure è un ideale massimale.*

*Dimostrazione.* Supponiamo che il nucleo sia diverso da zero, e sia  $f$  un elemento non nullo in  $\ker \pi_1$ . Poiché  $K$  non è l'anello nullo,  $\ker \pi_1$  è diverso dall'intero anello. Pertanto  $f$  non è una costante, quindi  $f$  è divisibile per un polinomio lineare  $x_1 - a_1$ , e si può scrivere  $f = (x_1 - a_1)g$ . Allora  $\pi_1(x_1 - a_1)\pi_1(g) = \pi_1(f) = 0$  in  $K$ . Poiché  $K$  è un campo, si ha  $\pi_1(x_1 - a_1) = 0$  oppure  $\pi_1(g) = 0$ . Pertanto uno dei due elementi  $x_1 - a_1$ ,  $g$  appartiene a  $\ker \pi_1$ . Procedendo per induzione sul grado di  $f$ , si ha che  $\ker \pi_1$  contiene un polinomio lineare, ed è quindi un ideale massimale [cfr. (7.5)]. ■

Passiamo ora a dimostrare che  $\ker \pi_1$  non è l'ideale nullo. Ne seguirà che  $M$  contiene un polinomio lineare della forma  $x_1 - a_1$ . La stessa argomentazione si può ripetere per  $x_i$ ,  $i = 2, \dots, n$ , e quindi possiamo concludere che  $M$  contiene un polinomio lineare  $x_i - a_i$  per ogni  $i = 1, \dots, n$ . Allora  $M$  è contenuto nell'ideale generato da  $x_1 - a_1, \dots, x_n - a_n$ , ed essendo massimale è uguale a tale ideale. Perciò  $M$  è il nucleo dell'omomorfismo di sostituzione  $f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$ , come asserito.

Supponiamo dunque, per assurdo, che  $\ker \pi_1 = (0)$ . Allora  $\pi_1$  manda mediante un isomorfismo  $\mathbb{C}[x_1]$  nella sua immagine, che è un sottoanello di  $K$ . In base alla proposizione (6.7), questa applicazione può essere estesa al campo delle frazioni di  $\mathbb{C}[x]$ , e quindi  $K$  contiene un campo isomorfo al campo delle funzioni razionali  $\mathbb{C}(x)$  [cfr. 3.17].

Ora i monomi  $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$  formano una base di  $\mathbb{C}[x_1, \dots, x_n]$  come spazio vettoriale su  $\mathbb{C}$  (cfr. § 2). Pertanto  $\mathbb{C}[x_1, \dots, x_n]$  ha una base numerabile (app., § 1). Poiché  $K$  è un quoziente di  $\mathbb{C}[x_1, \dots, x_n]$ , esiste un insieme numerabile che genera  $K$  come spazio vettoriale su  $\mathbb{C}$ ; precisamente, le classi resto dei monomi generano tale campo. D'altra parte, dimostreremo che esiste un insieme non numerabile di elementi linearmente indipendenti in  $\mathbb{C}(x)$ . Ne seguirà [lemma (7.9)] che  $\mathbb{C}(x)$  non può essere isomorfo ad un sottospazio di  $K$ . Questa contraddizione proverà che  $\ker \pi_1 \neq (0)$ .

Abbiamo bisogno qui del fatto che gli elementi del campo complesso  $\mathbb{C}$  non formano un insieme numerabile [app. (1.7)]. Utilizzando questo fatto, i due lemmi seguenti concluderanno la dimostrazione:

(7.8) LEMMA *L'insieme non numerabile delle funzioni razionali  $(x - \alpha)^{-1}$ , con  $\alpha \in \mathbb{C}$ , è linearmente indipendente.*

*Dimostrazione.* Una funzione razionale  $f/g$  definisce una funzione complessa, mediante la valutazione, in tutti i punti del piano complesso in cui  $g \neq 0$ . La funzione razionale  $(x - \alpha)^{-1}$  ha un polo in  $\alpha$ , cioè  $\lim_{x \rightarrow \infty} |(x - \alpha)^{-1}| = +\infty$ ; in particolare,  $(x - \alpha)^{-1}$  non è limitata in un intorno di  $\alpha$ , mentre lo è in un intorno di ogni altro punto. Consideriamo una combinazione lineare della forma:

$$\sum_{i=1}^n \frac{c_i}{x - \alpha_i},$$

dove  $\alpha_1, \dots, \alpha_n$  sono numeri complessi distinti e dove qualche coefficiente, diciamo  $c_1$ , è diverso da zero. Il primo termine di questa somma non è limitato in un intorno di  $\alpha_1$ , ma gli altri termini sono ivi limitati. Ne segue che la combinazione lineare non definisce la funzione nulla, e quindi è diversa da zero. ■

(7.9) LEMMA *Sia  $V$  uno spazio vettoriale generato da un insieme numerabile  $\{v_1, v_2, \dots\}$  di vettori. Allora ogni insieme  $L$  di vettori linearmente indipendenti in  $V$  è finito o numerabile.*

*Dimostrazione.* Sia  $L$  un sottoinsieme linearmente indipendente di  $V$ , sia  $V_n$  il sottospazio di  $V$  generato dai primi  $n$  vettori  $v_1, \dots, v_n$  e sia  $L_n = L \cap V_n$ . Allora  $L_n$  è un insieme linearmente indipendente in uno spazio vettoriale di dimensione finita  $V_n$ , e quindi è un insieme finito [cap. 3 (3.16)]. Inoltre,  $L$  è l'unione di tutti gli  $L_n$ . Ma l'unione di un'infinità numerabile di insiemi finiti è un insieme finito o numerabile, da cui la tesi. ■

## 8 Geometria algebrica

La geometria algebrica mi sembra algebra con una marcia in più.

Solomon Lefschetz

Sia  $V$  un sottoinsieme dello spazio complesso  $\mathbb{C}^n$  di dimensione  $n$ . Se  $V$  può essere definito come l'insieme degli zeri comuni di un numero finito di polinomi in  $n$  variabili, allora si dice che  $V$  è una *varietà algebrica*, o, più brevemente, una *varietà*. (Non conosco l'origine di questo termine così poco attraente). Per esempio, una retta complessa in  $\mathbb{C}^2$  è, per definizione, l'insieme delle soluzioni di un'equazione lineare  $ax+by+c=0$ , ed è quindi una varietà. Anche un punto è una varietà: il punto  $(a, b)$  è l'insieme degli zeri comuni dei due polinomi  $x-a$  e  $y-b$ .

Abbiamo già incontrato altre varietà interessanti; ad esempio, il gruppo  $SL_2(\mathbb{C})$ , essendo il luogo delle soluzioni dell'equazione polinomiale  $x_{11}x_{22} - x_{12}x_{21} - 1 = 0$ , è una varietà in  $\mathbb{C}^4$ .

Il teorema degli zeri di Hilbert fornisce un legame importante tra l'algebra e la geometria. Esso afferma che gli ideali massimali nell'anello dei polinomi  $\mathbb{C}[x] = \mathbb{C}[x_1, \dots, x_n]$  corrispondono ai punti in  $\mathbb{C}^n$ . Tale corrispondenza può essere usata inoltre per mettere in relazione le varietà algebriche con gli anelli quoziente dell'anello dei polinomi.

(8.1) TEOREMA *Siano  $f_1, \dots, f_r$  polinomi in  $\mathbb{C}[x_1, \dots, x_n]$ , e sia  $V$  la varietà definita dal sistema di equazioni  $f_1(x) = 0, \dots, f_r(x) = 0$ . Sia  $I$  l'ideale  $(f_1, \dots, f_r)$  generato dai polinomi assegnati. Allora gli ideali massimali dell'anello quoziente  $R = \mathbb{C}[x]/I$  sono in corrispondenza biunivoca con i punti di  $V$ .*

*Dimostrazione.* Gli ideali massimali di  $R$  corrispondono agli ideali massimali di  $\mathbb{C}[x]$  che contengono  $I$  [teorema di corrispondenza (4.3)]. Inoltre un ideale contiene  $I$  se e soltanto se contiene i generatori  $f_1, \dots, f_r$  di  $I$ . D'altra parte, l'ideale massimale  $M_a$  che corrisponde a un punto  $a \in \mathbb{C}^n$  è il nucleo dell'omomorfismo di sostituzione  $f(x) \mapsto f(a)$ . Pertanto  $f_i \in M_a$  se e soltanto se  $f_i(a) = 0$ , il che equivale a dire che  $a \in V$ . ■

Questo teorema mostra che le proprietà algebriche dell'anello  $R$  sono strettamente collegate con la geometria di  $V$ . In linea di principio, tutte le proprietà del sistema di equazioni polinomiali

$$(8.2) \quad f_1(x) = \dots = f_r(x) = 0$$

si riflettono nella struttura dell'anello  $R = \mathbb{C}[x]/(f_1, \dots, f_r)$ . La teoria che studia tali legami è quel ramo della matematica che viene chiamato *geometria algebrica*. Non approfondiremo qui l'argomento: la cosa importante da ricordare è che le proprietà geometriche della varietà forniscono informazioni sull'anello, e viceversa.

La domanda più semplice riguardante un insieme è se esso sia vuoto o meno. Potremmo dunque chiederci se è possibile che un anello non abbia alcun ideale massimale. Ebbene, ciò accade soltanto per l'anello nullo:

(8.3) TEOREMA *Sia  $R$  un anello. Ogni ideale  $I$  di  $R$  diverso dall'ideale unità è contenuto in un ideale massimale.*

(8.4) COROLLARIO *L'unico anello  $R$  privo di ideali massimali è l'anello nullo.*

Il teorema (8.3) può essere dimostrato utilizzando l'*assioma della scelta* o il *lemma di Zorn* [app. (1.9)]. Tuttavia, per i quozienti di anelli di polinomi, esso è una conseguenza del teorema della base di Hilbert, che dimostreremo più avanti [cap. 12 (5.18)].

Se mettiamo insieme il teorema (8.1) e il teorema (8.3), otteniamo un altro corollario importante:

(8.5) COROLLARIO Siano  $f_1, \dots, f_r$  polinomi in  $\mathbb{C}[x_1, \dots, x_n]$ . Se il sistema di equazioni  $f_1 = \dots = f_r = 0$  non ha soluzioni in  $\mathbb{C}^n$ , allora 1 può essere espresso come combinazione lineare degli  $f_i$ :

$$1 = \sum_i g_i f_i,$$

dove i coefficienti  $g_i$  sono polinomi.

Infatti, se il sistema non ha soluzioni, il teorema (8.1) ci dice che non esiste alcun ideale massimale contenente l'ideale  $I = (f_1, \dots, f_r)$ . Pertanto, in base al teorema (8.3),  $I$  è l'ideale unità. ■

Nella maggior parte dei casi, tre polinomi  $f_1, f_2, f_3$  in due variabili  $x, y$  non hanno soluzioni comuni. Ne segue che, di solito, possiamo esprimere 1 come una combinazione lineare:  $1 = p_1 f_1 + p_2 f_2 + p_3 f_3$ , dove i coefficienti  $p_i$  sono polinomi. Ciò non è ovvio. Per esempio, l'ideale generato da

$$(8.6) \quad f_1 = x^2 + y^2 - 1, \quad f_2 = x^2 - y + 1, \quad f_3 = xy - 1$$

è l'ideale unità. Per dimostrarlo basta verificare che il sistema  $f_1 = f_2 = f_3 = 0$  non ha soluzioni in  $\mathbb{C}^2$ . Se non avessimo il teorema degli zeri, però, ci vorrebbe un po' di tempo per scoprire che possiamo scrivere 1 come una combinazione lineare del tipo suddetto.

Il teorema degli zeri è stato riformulato in molti modi, e in effetti l'enunciato dato nell'ultimo paragrafo non è quello originario, il quale ha la forma seguente:

(8.7) TEOREMA (Forma classica del teorema degli zeri) Siano  $f_1, \dots, f_r$  e  $g$  polinomi in  $\mathbb{C}[x_1, \dots, x_n]$ . Sia  $V$  la varietà degli zeri di  $f_1, \dots, f_r$ , e sia  $I$  l'ideale generato da questi polinomi. Se  $g = 0$  identicamente su  $V$ , allora qualche potenza di  $g$  appartiene all'ideale  $I$ .

*Dimostrazione.* Consideriamo l'anello ottenuto invertendo il polinomio  $g$  mediante l'equazione  $gy = 1$ . Supponiamo che  $g$  si annulli identicamente su  $V$ . Consideriamo gli  $r+1$  polinomi  $f_1(x), \dots, f_r(x), gy - 1$  nelle variabili  $x_1, \dots, x_n, y$ . L'ultimo di essi è l'unico in cui compare la variabile  $y$ . Si noti che questi  $r+1$  polinomi non hanno zeri comuni in  $\mathbb{C}^{n+1}$ . Infatti, se  $f_1, \dots, f_r$  si annullassero in un punto  $(a_1, \dots, a_n, b) \in \mathbb{C}^{n+1}$ , in quel punto, dato che per ipotesi  $g$  è nulla,  $gy - 1$  assumerebbe il valore  $-1$ . Applicando il corollario (8.5), si ha che i polinomi  $f_1, \dots, f_r, gy - 1$  generano l'ideale unità in  $\mathbb{C}[x, y]$ . Possiamo dunque scrivere

$$1 = \sum_i p_i(x, y) f_i(x) + q(x, y)(gy - 1).$$

Sostituendo  $y = 1/g$  in tale equazione, otteniamo

$$1 = \sum_i p_i(x, g^{-1}) f_i(x).$$

Eliminiamo ora i denominatori in  $p_i(x, g^{-1})$  moltiplicando ambo i membri dell'equazione per una potenza sufficientemente grande di  $g$ . Ciò fornisce l'espressione polinomiale richiesta:

$$g(x)^N = \sum_i h_i(x) f_i(x),$$

$$\text{dove } h_i(x) = g(x)^N p_i(x, g^{-1}). \blacksquare$$

Non è facile immaginare com'è fatta una varietà algebrica generica in  $\mathbb{C}^n$ , ma la forma generale di una varietà in  $\mathbb{C}^2$  può essere descritta in modo abbastanza semplice.

(8.8) PROPOSIZIONE Due polinomi non nulli in due variabili  $f(x, y), g(x, y)$  hanno soltanto un numero finito di zeri comuni, a meno che non abbiano un polinomio non costante come fattore comune.

Se i gradi di  $f, g$  sono rispettivamente  $m, n$ , il numero degli zeri comuni è al più  $mn$ . Tale valore è chiamato il *numero di Bézout*. Per esempio, due coniche si incontrano al più in quattro punti. È alquanto più difficile dimostrare l'esistenza di tale limitazione piuttosto che la semplice finitezza, e pertanto ometteremo la dimostrazione.

*Dimostrazione della proposizione (8.8).* Supponiamo che  $f, g$  non abbiano un fattore comune non costante. Denotiamo con  $F$  il campo delle funzioni razionali in  $x$ , ossia il campo delle frazioni dell'anello  $\mathbb{C}[x]$ . È utile considerare  $f, g$  come elementi dell'anello dei polinomi in una variabile  $F[y]$ , poiché possiamo usare il fatto che ogni ideale di  $F[y]$  è principale. Denotiamo con  $I$  l'ideale generato da  $f, g$  in  $F[y]$ . Esso è un ideale principale, generato dal massimo comune divisore  $h$  di  $f, g$  in  $F[y]$  (3.22). Se  $f, g$  non hanno fattori comuni non costanti in  $F[y]$ , allora  $I$  è l'ideale unità.

La nostra ipotesi è che  $f, g$  non hanno fattori comuni in  $\mathbb{C}[x, y]$ , non che essi non hanno fattori comuni in  $F[y]$ , sicché dobbiamo mettere in relazione queste due proprietà. La fattorizzazione dei polinomi è uno degli argomenti del prossimo capitolo, e pertanto enunciamo il risultato di cui abbiamo bisogno qui, rinviandone la dimostrazione [cfr. cap. 11 (3.9)].

(8.9) LEMMA Siano  $f, g \in \mathbb{C}[x, y]$ , e sia  $F$  il campo delle funzioni razionali in  $x$ . Se  $f, g$  hanno un fattore comune in  $F[y]$  che non è un elemento di  $F$ , allora hanno un fattore comune non costante in  $\mathbb{C}[x, y]$ .

Ritorniamo alla dimostrazione della proposizione. Poiché i due polinomi  $f, g$  non hanno fattori comuni in  $\mathbb{C}[x, y]$ , essi sono primi tra loro in  $F[y]$ , sicché l'ideale  $I$  da essi generato in  $F[y]$  è l'ideale unità. Pertanto possiamo scrivere  $1 = rf + sg$ , dove  $r, s$  sono elementi di  $F[y]$ . Allora  $r, s$  hanno denominatori che sono polinomi nella sola  $x$ , e che possiamo eliminare, moltiplicando ambo i membri dell'equazione per un opportuno polinomio  $p(x)$ . Si ottiene così un'equazione della forma:

$$p(x) = u(x, y)f(x, y) + v(x, y)g(x, y),$$

dove  $u, v \in \mathbb{C}[x, y]$ . Da questa equazione segue che uno zero comune di  $f, g$  deve essere anche uno zero di  $p$ . Ma  $p$  è un polinomio nella sola  $x$ , e un polinomio in una variabile ha soltanto un numero finito di radici. Pertanto ci sono solo un numero finito di valori della  $x$  che annullano contemporaneamente  $f$  e  $g$ . Lo stesso vale per la variabile  $y$ . Ne segue che gli zeri comuni di  $f, g$  formano un insieme finito. ■

Questa proposizione mostra che le varietà più interessanti in  $\mathbb{C}^2$  sono quelle che sono definite come gli zeri di un solo polinomio  $f(x, y)$ . Tali varietà sono chiamate *curve algebriche* o *superfici di Riemann*, e la loro struttura geometrica può essere abbastanza complicata. Una superficie di Riemann ha dimensione due, sicché chiamarla curva algebrica potrebbe sembrare poco appropriato. Questo uso del termine "curva" si riferisce al fatto che essa può essere descritta analiticamente, nell'intorno di un punto, mediante un solo parametro *complesso*.

Passiamo ora a dare una descrizione sommaria di una curva algebrica, nel caso in cui  $f$  è irriducibile. (Un polinomio si dice irriducibile se non è il prodotto di due polinomi non costanti.) Consideriamo  $f(x, y)$  come un polinomio in  $y$  i cui coefficienti sono polinomi in  $x$ :

$$(8.10) \quad f(x, y) = u_n(x)y^n + \dots + u_1(x)y + u_0(x),$$

con  $u_i(x) \in \mathbb{C}[x]$ .

(8.11) PROPOSIZIONE *Sia  $f(x, y)$  un polinomio irriducibile in  $\mathbb{C}[x, y]$ , che non sia un polinomio nella sola  $x$ , e sia  $S$  il luogo degli zeri di  $f$  in  $\mathbb{C}^2$ . Indichiamo con  $n$  il grado di  $f$  come polinomio in  $y$ .*

- (a) *Per ogni valore  $a$  della variabile  $x$ , vi sono al più  $n$  punti di  $S$  aventi  $a$  come prima coordinata.*
- (b) *Esiste un insieme finito  $\Delta$  di valori di  $x$  tale che, se  $a \notin \Delta$ , vi sono esattamente  $n$  punti di  $S$  aventi  $a$  come prima coordinata.*

**Dimostrazione.** Sia  $a \in \mathbb{C}$ , e consideriamo il polinomio  $f(a, y)$ . I punti  $(a, b) \in S$  sono i punti tali che  $b$  è una radice di  $f(a, y)$ . Tale polinomio non è identicamente nullo, altrimenti  $x - a$  dividerebbe ciascuno dei coefficienti  $u_i(x)$ , e quindi dividerebbe  $f$ . Ma, per ipotesi,  $f$  è irriducibile. Inoltre, il grado di  $f(a, y)$  in  $y$  è al più  $n$ , e pertanto  $f(a, y)$  ha al più  $n$  radici. Avrà meno di  $n$  radici se:

- (8.12) (i) *ha grado minore di  $n$ ;*  
oppure
- (ii) *ha grado  $n$ , ma ha una radice multipla.*

Il caso (i) si presenta quando il coefficiente direttore  $u_n(x)$  si annulla in  $a$ , ossia quando  $a$  è una radice di  $u_n(x)$ . Poiché  $u_n$  è un polinomio in  $x$ , ha un numero finito di radici.

Ora un numero complesso  $b$  è una radice multipla di un polinomio  $h(y)$  [ossia  $(y - b)^2$  divide  $h(y)$ ] se e soltanto se  $b$  è una radice sia di  $h(y)$  che della sua derivata  $h'(y)$ . La dimostrazione di questo fatto è lasciata come esercizio. Nella situazione attuale,  $h(y) = f(a, y)$ . La prima variabile è fissata, sicché la derivata è la derivata parziale rispetto a  $y$ . Dunque il caso (ii) si presenta nei punti  $(a, b)$  che sono zeri comuni di  $f$  e  $\partial f / \partial y$ . Si noti che  $f$  non divide la derivata parziale  $\partial f / \partial y$ , poiché il grado della derivata parziale in  $y$  è  $n - 1$ , che è minore del grado di  $f$  in  $y$ . Poiché per ipotesi  $f$  è irriducibile,  $f$  e  $\partial f / \partial y$  non hanno fattori non costanti in comune. Allora la proposizione (8.8) assicura che esiste un numero finito di zeri comuni. ■

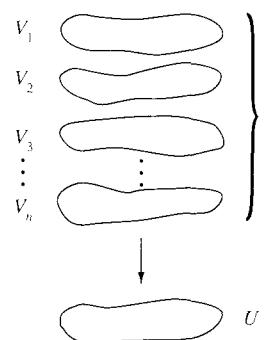
La proposizione (8.11) si può riassumere dicendo che  $S$  è un rivestimento a  $n$  fogli del piano complesso  $P$  della variabile  $x$ . Poiché esiste un insieme finito  $\Delta$  sul quale  $S$  ha meno di  $n$  fogli, esso è chiamato rivestimento ramificato. Per esempio, consideriamo il luogo di equazione  $x^2 + xy^2 - 1 = 0$ . Tale equazione ha due soluzioni in  $y$  per ogni valore di  $x$ , ad eccezione di  $x = 0, \pm 1$ . Per  $x = 0$  non vi è nessuna soluzione, e per  $x = 1$  o  $-1$  vi è una sola soluzione. Pertanto questo luogo è un rivestimento doppio ramificato di  $P$ .

Diamo ora la definizione precisa di rivestimento ramificato:

(8.13) DEFINIZIONE *Un rivestimento ramificato a  $n$  fogli del piano complesso  $P$  è uno spazio topologico  $S$  insieme con un'applicazione continua  $\pi : S \rightarrow P$ , tale che:*

- (a)  *$\pi$  è un'applicazione  $n - 1$  sul complementare di un insieme finito  $\Delta$  in  $P$ ;*
- (b) *per ogni punto  $x_0 \in P - \Delta$ , esiste un intorno aperto  $U$  di  $x_0$ , tale che  $\pi^{-1}(U)$  è costituito da  $n$  sottoinsiemi disgiunti:  $\pi^{-1}(U) = V_1 \cup \dots \cup V_n$ , dove ciascun  $V_i$  è aperto in  $S$ , e  $\pi$  manda  $V_i$  in  $U$  mediante un omeomorfismo.*

(8.14)

Parte di un rivestimento a  $n$  fogli.

(8.15) COROLLARIO Sia  $f(x, y)$  un polinomio irriducibile in  $\mathbb{C}[x, y]$  avente grado  $n > 0$  nella variabile  $y$ . La superficie di Riemann di  $f(x, y)$  è un rivestimento ramificato a  $n$  fogli del piano.

*Dimostrazione.* La proposizione (8.11) assicura che la superficie di Riemann  $S$  di  $f$  possiede la prima proprietà di un rivestimento ramificato. Resta dunque da verificare la proprietà (8.13b). Consideriamo un punto  $x_0$  in cui  $f(x_0, y)$  ha  $n$  radici  $y_1, \dots, y_n$ . Allora  $(\partial f / \partial y)(x_0, y_1) \neq 0$ , poiché  $y_1$  non è una radice multipla di  $f(x_0, y_1)$ . Applicando il teorema delle funzioni implicite [app. (4.1)], si ha che l'equazione (8.2) può essere risolta per  $y = \alpha_1(x)$ , come una funzione continua di  $x$  in un intorno  $U$  di  $x_0$ , in modo tale che  $y_1 = \alpha_1(x_0)$ . Similmente, possiamo risolvere per  $y = \alpha_i(x)$  in modo tale che  $y_i = \alpha_i(x_0)$ . Riducendo eventualmente l'ampiezza di  $U$  possiamo supporre che ciascuna funzione  $\alpha_i(x)$  sia definita su  $U$ . Poiché  $y_1, \dots, y_n$  sono tutti distinti e le funzioni  $\alpha_i(x)$  sono continue, esse non hanno valori comuni, purché si prenda  $U$  sufficientemente piccolo.

Consideriamo i grafici delle  $n$  funzioni continue  $\alpha_i$ :

$$(8.16) \quad V_i = \{(x, \alpha_i(x)) \mid x \in U\}.$$

Essi sono disgiunti poiché le funzioni  $\alpha_i(x)$  non hanno valori comuni su  $U$ . L'applicazione  $V_i \rightarrow U$  è un omeomorfismo, poiché ha la funzione inversa continua  $U \mapsto V_i$ . La funzione inversa manda  $x$  in  $(x, \alpha_i(x))$ . Inoltre,

$$\pi^{-1}(U) = V_1 \cup \dots \cup V_n,$$

poiché  $S$  ha al più  $n$  punti sopra ogni  $x$ , e gli  $n$  punti sono stati descritti come  $(x, \alpha_i(x)) \in V_i$ . Ciascuno degli insiemi  $V_i$  è chiuso in  $U \times \mathbb{C}$ , poiché è l'insieme degli zeri della funzione continua  $y - \alpha_i(x)$ . Allora  $V_i$  è chiuso anche nel sottoinsieme  $\pi^{-1}(U)$  di  $U \times \mathbb{C}$ . Ne segue che  $V_1$  è aperto in  $\pi^{-1}(U)$ , poiché è il complementare del sottoinsieme chiuso  $V_2 \cup \dots \cup V_n$ . Poiché  $U$  è aperto in  $\mathbb{C}$ , la sua immagine

inversa  $\pi^{-1}(U)$  è aperta in  $S$ . Pertanto  $V_1$  è aperto in un sottoinsieme aperto di  $S$ , ciò che prova che  $V_i$  è aperto anche in  $S$ . Similmente,  $V_i$  è aperto per ogni  $i$ . ■

Riprenderemo lo studio di questi luoghi nel capitolo 13.

Aiutando la geometria, l'algebra moderna aiuta innanzitutto se stessa.

Oskar Zariski

### Esercizi

#### I Definizione di anello

1. Dimostrare le seguenti identità in un anello arbitrario  $R$ :

(a)  $0a = 0$ ; (b)  $-a = (-1)a$ ; (c)  $(-a)b = -(ab)$ .

2. Descrivere esplicitamente il più piccolo sottoanello del campo dei numeri complessi che contiene la radice cubica reale di 2.

3. Dimostrare che gli elementi di  $\mathbb{Z}[\alpha]$ , con  $\alpha = \frac{1}{2}i$ , formano un sottoinsieme denso del piano complesso.

4. Dimostrare che  $7 + \sqrt[3]{2}$  e  $\sqrt{3} + \sqrt{-5}$  sono numeri algebrici.

5. Dimostrare che, per ogni intero  $n$ ,  $\cos(2\pi/n)$  è un numero algebrico.

6. Si denoti con  $\mathbb{Q}[\alpha, \beta]$  il più piccolo sottoanello di  $\mathbb{C}$  contenente  $\mathbb{Q}$ ,  $\alpha = \sqrt{2}$ ,  $\beta = \sqrt{3}$ , e si ponga  $\gamma = \alpha + \beta$ . Dimostrare che  $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$ .

7. Sia  $S$  un sottoanello di  $\mathbb{R}$  che risulti un insieme discreto nel senso illustrato nel capitolo 5 (4.3). Dimostrare che  $S = \mathbb{Z}$ .

8. In ciascuno dei casi seguenti, stabilire se  $S$  è un sottoanello di  $R$ :

(a)  $S$  è l'insieme di tutti i numeri razionali della forma  $a/b$ , dove  $b$  è un intero non divisibile per 3, e  $R = \mathbb{Q}$ .

(b)  $S$  è l'insieme delle funzioni che sono combinazioni lineari delle funzioni  $\{1, \cos nt, \sin nt \mid n \in \mathbb{Z}\}$ , e  $R$  è l'insieme di tutte le funzioni  $\mathbb{R} \rightarrow \mathbb{R}$ .

(c) (caso non commutativo)  $S$  è l'insieme delle matrici reali della forma  $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ , e  $R$  è l'insieme di tutte le matrici reali  $2 \times 2$ .

9. In ciascuno dei casi seguenti, stabilire se la struttura assegnata risulta un anello. In caso negativo, determinare gli assiomi di un anello che valgono e quelli che non valgono:

(a)  $U$  è un insieme arbitrario e  $R$  è l'insieme dei sottoinsiemi di  $U$ . L'addizione e la moltiplicazione tra elementi di  $R$  sono definite mediante le regole:  $A+B = A \cup B$  e  $A \cdot B = A \cap B$ .

(b)  $U$  è un insieme arbitrario e  $R$  è l'insieme dei sottoinsiemi di  $U$ . L'addizione e la moltiplicazione tra elementi di  $R$  sono definite mediante le regole:  $A+B = (A \cup B) - (A \cap B)$  e  $A \cdot B = A \cap B$ .

- (c)  $R$  è l'insieme delle funzioni continue  $\mathbb{R} \rightarrow \mathbb{R}$ . L'addizione e la moltiplicazione sono definite mediante le regole:  $[f+g](x) = f(x) + g(x)$  e  $[f \cdot g](x) = f(g(x))$ .
10. Determinare tutti gli anelli che contengono l'anello nullo come sottoanello.
11. Descrivere il gruppo delle unità in ciascuno degli anelli seguenti:
- $\mathbb{Z}/12\mathbb{Z}$ ; (b)  $\mathbb{Z}/7\mathbb{Z}$ ; (c)  $\mathbb{Z}/8\mathbb{Z}$ ; (d)  $\mathbb{Z}/n\mathbb{Z}$ .
12. Dimostrare che le unità nell'anello degli interi di Gauss sono  $\{\pm 1, \pm i\}$ .
13. Un elemento  $x$  di un anello  $R$  si dice *nilpotente* se qualche potenza di  $x$  è zero. Dimostrare che se  $x$  è nilpotente  $1+x$  è un'unità in  $R$ .
14. Dimostrare che l'insieme prodotto  $R \times R'$  di due anelli è un anello con l'addizione e la moltiplicazione definite componente per componente:
- $$(a, a') + (b, b') = (a+b, a'+b') \quad \text{e} \quad (a, a')(b, b') = (ab, a'b').$$
- Tale anello è chiamato l'*anello prodotto*.
- 2 Costruzione formale degli interi e dei polinomi
1. Dimostrare che ogni numero naturale  $n$  diverso da 1 è della forma  $m'$  per qualche numero naturale  $m$ .
2. Dimostrare le seguenti proprietà dei numeri naturali:
- la proprietà commutativa dell'addizione;
  - la proprietà associativa della moltiplicazione;
  - la proprietà distributiva;
  - la proprietà di cancellazione relativa all'addizione:  
se  $a+b=a+c$ , allora  $b=c$ ;
  - la proprietà di cancellazione relativa alla moltiplicazione:  
se  $ab=ac$ , allora  $b=c$ .
3. La relazione  $<$  su  $\mathbb{N}$  può essere definita mediante la regola:  $a < b$ , se  $b = a+n$  per qualche  $n$ . Supponiamo che le proprietà elementari dell'addizione siano state dimostrate.
- Dimostrare che, se  $a < b$ , allora  $a+n < b+n$  per ogni  $n$ .
  - Dimostrare che la relazione  $<$  è transitiva.
  - Dimostrare che, se  $a, b$  sono numeri naturali, allora vale una ed una sola delle relazioni seguenti:  
 $a < b$ ,  $a = b$ ,  $b < a$ .
  - Dimostrare che, se  $n \neq 1$ , allora  $a < an$ .

- **Dimostrare il principio di *induzione completa*:** Sia  $S$  un sottoinsieme di  $\mathbb{N}$  avente la seguente proprietà: se  $n$  è un numero naturale tale che  $m \in S$  per ogni  $m < n$ , allora  $n \in S$ . Allora risulta:  $S = \mathbb{N}$ .
5. Definire l'insieme  $\mathbb{Z}$  di tutti i numeri interi, utilizzando due copie di  $\mathbb{N}$  e un elemento che rappresenta lo zero, definire l'addizione e la moltiplicazione, e dedurre il fatto che  $\mathbb{Z}$  è un anello dalle proprietà dell'addizione e della moltiplicazione dei numeri naturali.
6. Sia  $R$  un anello. L'insieme di tutte le serie formali di potenze  $p(t) = a_0 + a_1t + a_2t^2 + \dots$ , con  $a_i \in R$ , forma un anello che si denota di solito con  $R[[t]]$ . (Col termine *serie formale di potenze* si intende una serie di potenze per cui non si richiede la convergenza).
- Dimostrare che le serie formali di potenze formano un anello.
  - Dimostrare che una serie di potenze  $p(t)$  è invertibile, se e soltanto se,  $a_0$  è un'unità di  $R$ .
7. Dimostrare che le unità dell'anello dei polinomi  $\mathbb{R}[x]$  sono i polinomi costanti non nulli.
- 3 Omomorfismi e ideali
1. Dimostrare che l'inverso di un isomorfismo di anelli  $\varphi : R \rightarrow R'$  è un isomorfismo.
2. È vero che, se un ideale  $I$  contiene un'unità, allora  $I$  è l'ideale unità?
3. Per quali interi  $n$  il polinomio  $x^2 + x + 1$  divide  $x^4 + 3x^3 + x^2 + 6x + 10$  in  $\mathbb{Z}/n\mathbb{Z}[x]$ ?
4. Dimostrare che nell'anello  $\mathbb{Z}[x]$  risulta:  $(2) \cap (x) = (2x)$ .
5. Dimostrare l'equivalenza delle due definizioni di ideale (3.11) e (3.12).
6. È vero che l'insieme dei polinomi  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  tali che  $2^{k+1}$  divide  $a_k$  per ogni  $k = 1, \dots, n$  è un ideale in  $\mathbb{Z}[x]$ ?
7. Dimostrare che ogni ideale non nullo nell'anello degli interi di Gauss contiene un intero diverso da zero.
8. Descrivere il nucleo dei seguenti omomorfismi:
- $\mathbb{R}[x, y] \rightarrow \mathbb{R}$  definito da  $f(x, y) \mapsto f(0, 0)$ ;
  - $\mathbb{R}[x] \rightarrow \mathbb{C}$  definito da  $f(x) \mapsto f(2+i)$ .
9. Descrivere il nucleo dell'omomorfismo  $f : \mathbb{Z}[x] \rightarrow \mathbb{R}$  definito da  $f(x) \mapsto f(1 + \sqrt{2})$ .
10. Descrivere il nucleo dell'omomorfismo  $\varphi : \mathbb{C}[x, y, z] \rightarrow \mathbb{C}[t]$  definito da  $\varphi(x) = t$ ,  $\varphi(y) = t^2$ ,  $\varphi(z) = t^3$ .
11. (a) Dimostrare che il nucleo dell'omomorfismo  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$  definito da  $x \mapsto t^2$ ,  $y \mapsto t^3$  è l'ideale principale generato dal polinomio  $y^2 - x^3$ .  
(b) Determinare esplicitamente l'immagine di  $\varphi$ .
12. Dimostrare l'esistenza dell'omomorfismo (3.8).
13. Enunciare e dimostrare un risultato analogo alla proposizione (3.8), sostituendo  $\mathbb{R}$  con un campo infinito arbitrario.

14. Dimostrare che, se due anelli  $R, R'$  sono isomorfi, tali risultano gli anelli di polinomi  $R[x]$  e  $R'[x]$ .
15. Sia  $R$  un anello e sia  $f(y) \in R[y]$  un polinomio in una variabile a coefficienti in  $R$ . Dimostrare che l'applicazione  $R[x, y] \rightarrow R[x, y]$  definita da  $x \mapsto x + f(y)$ ,  $y \mapsto y$  è un automorfismo di  $R[x, y]$ .
16. Dimostrare che un polinomio  $f(x) = \sum a_i x^i$  può essere sviluppato in serie di potenze di  $x - a$ :  $f(x) = \sum c_i (x - a)^i$ , e che i coefficienti  $c_i$  sono polinomi nei coefficienti  $a_i$ .
17. Siano  $R, R'$  due anelli, e sia  $R \times R'$  il loro prodotto. Quali delle seguenti applicazioni sono omomorfismi di anelli?
- $R \rightarrow R \times R'$ ,  $r \mapsto (r, 0)$ ;
  - $R \rightarrow R \times R$ ,  $r \mapsto (r, r)$ ;
  - $R \times R' \rightarrow R$ ,  $(r_1, r_2) \mapsto r_1$ ;
  - $R \times R \rightarrow R$ ,  $(r_1, r_2) \mapsto r_1 r_2$ ;
  - $R \times R \rightarrow R$ ,  $(r_1, r_2) \mapsto r_1 + r_2$ .
18. (a) È vero che  $\mathbb{Z}/(10)$  è isomorfo a  $\mathbb{Z}/(2) \times \mathbb{Z}/(5)$ ?  
(b) È vero che  $\mathbb{Z}/(8)$  è isomorfo a  $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$ ?
19. Sia  $R$  un anello di caratteristica  $p$ . Dimostrare che l'applicazione  $R \rightarrow R$  definita da  $x \mapsto x^p$  è un omomorfismo di anelli. Tale applicazione è chiamata l'*omomorfismo di Frobenius*.
20. Determinare tutti gli automorfismi dell'anello  $\mathbb{Z}[x]$ .
21. Dimostrare che l'applicazione  $\mathbb{Z} \rightarrow R$  definita in (3.9) è compatibile con la moltiplicazione tra interi positivi.
22. Dimostrare che la caratteristica di un campo è zero oppure un numero primo.
23. Sia  $R$  un anello di caratteristica  $p$ . Dimostrare che se  $a$  è nilpotente,  $1+a$  è *unipotente*, ossia qualche potenza di  $1+a$  è uguale a 1.
24. (a) Il *nilradicale*  $N$  di un anello  $R$  è l'insieme dei suoi elementi nilpotenti. Dimostrare che  $N$  è un ideale.  
(b) Determinare il nilradicale degli anelli  $\mathbb{Z}/(12)$ ,  $\mathbb{Z}/(n)$  e  $\mathbb{Z}$ .
25. (a) Dimostrare il corollario (3.20).  
(b) Dimostrare il corollario (3.22).
26. Determinare tutti gli ideali dell'anello  $\mathbb{R}[[t]]$  delle serie formali di potenze a coefficienti reali.
27. Trovare un ideale nell'anello dei polinomi in due variabili  $F[x, y]$  che non sia principale.
- \*28. Sia  $R$  un anello, e sia  $I$  un ideale dell'anello dei polinomi  $R[x]$ . Supponiamo che il grado minimo di un elemento non nullo di  $I$  sia  $n$  e che  $I$  contenga un polinomio monico di grado  $n$ . Dimostrare che  $I$  è un ideale principale.

29. Siano  $I, J$  ideali di un anello  $R$ . Mostrare con un esempio che  $I \cup J$  non è necessariamente un ideale, mentre  $I + J = \{r \in R \mid r = x + y, \text{ con } x \in I, y \in J\}$  lo è. Tale ideale è chiamato la *somma* degli ideali  $I, J$ .
30. (a) Siano  $I, J$  ideali di un anello  $R$ . Dimostrare che  $I \cap J$  è un ideale.  
(b) Mostrare con un esempio che l'insieme dei prodotti  $\{xy \mid x \in I, y \in J\}$  non è necessariamente un ideale e dimostrare tuttavia che l'insieme delle somme finite  $\sum x_\nu y_\nu$  di prodotti di elementi di  $I$  e  $J$  è un ideale. Tale ideale è chiamato l'*ideale prodotto*.  
(c) Dimostrare che  $IJ \subset I \cap J$ .  
(d) Mostrare con un esempio che  $IJ$  e  $I \cap J$  non sono necessariamente uguali.
31. Siano  $I, J, J'$  ideali in un anello  $R$ . È vero che  $I(J + J') = IJ + IJ'$ ?
- \*32. Se  $R$  è un anello non commutativo, si definisce *ideale* di  $R$  un sottoinsieme  $I$  di  $R$  che è chiuso rispetto all'addizione ed è tale che, se  $r \in R$  e  $x \in I$ , allora sia  $rx$  che  $xr$  appartengono a  $I$ . Dimostrare che l'anello non commutativo delle matrici reali  $n \times n$  non ha ideali propri.
33. È vero che, se in un anello  $R$   $a^2 = a$  per ogni  $a$ , allora  $R$  ha caratteristica 2?
34. Un elemento  $e$  di un anello  $S$  si dice *idempotente*, se  $e^2 = e$ . Si noti che in un prodotto di anelli  $R \times R'$  l'elemento  $e = (1, 0)$  è idempotente. L'obiettivo di questo esercizio è quello di dimostrare una proprietà inversa.
- Dimostrare che, se  $e$  è idempotente, allora anche  $e' = 1 - e$  è idempotente.
  - Sia  $e$  un elemento idempotente di un anello  $S$ . Dimostrare che l'ideale principale  $eS$  è un anello, con identità  $e$ . In generale non sarà un sottoanello di  $S$ , poiché non conterrà 1, a meno che non sia  $e = 1$ .
  - Sia  $e$  idempotente, e si ponga  $e' = 1 - e$ . Dimostrare che  $S$  è isomorfo all'anello prodotto  $(eS) \times (e'S)$ .
- #### 4 Anelli quoziente e relazioni in un anello
- Dimostrare che l'immagine dell'omomorfismo  $\varphi$  studiato nella proposizione (4.9) è il sottoanello descritto nella proposizione.
  - Determinare la struttura dell'anello  $\mathbb{Z}[x]/(x^2 + 3, p)$ , nei casi seguenti:
    - $p = 3$ ;
    - $p = 5$ .
  - Descrivere ciascuno dei seguenti anelli:
    - $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$ ;
    - $\mathbb{Z}[i]/(2 + i)$ .
  - Dimostrare la proposizione (4.2).
  - Sia  $R'$  l'anello ottenuto da un anello  $R$  introducendo la relazione  $\alpha = 0$ , e sia  $\psi : R \rightarrow R'$  l'applicazione canonica. Dimostrare la seguente *proprietà universale* relativa a tale costruzione: Sia  $\varphi : R \rightarrow \tilde{R}$  un omomorfismo di anelli, e supponiamo che  $\varphi(\alpha) = 0$  in  $\tilde{R}$ . Allora esiste un unico omomorfismo  $\varphi' : R' \rightarrow \tilde{R}$  tale che  $\varphi' \circ \psi = \varphi$ .

6. Siano  $I, J$  ideali di un anello  $R$ . Dimostrare che la classe resto di un elemento arbitrario di  $I \cap J$  in  $R/IJ$  è nilpotente.
7. Siano  $I, J$  ideali di un anello  $R$  tali che  $I + J = R$ .
- Dimostrare che  $IJ = I \cap J$ .
  - Dimostrare il *teorema cinese dei resti*, il quale afferma che per ogni coppia  $a, b$  di elementi di  $R$ , esiste un elemento  $x$  tale che  $x \equiv a$  (modulo  $I$ ) e  $x \equiv b$  (modulo  $J$ ). [La notazione  $x \equiv a$  (modulo  $I$ ) significa che  $x - a \in I$ ].
8. Siano  $I, J$  ideali di un anello  $R$  tali che  $I + J = R$  e  $IJ = 0$ .
- Dimostrare che  $R$  è isomorfo al prodotto  $(R/I) \times (R/J)$ .
  - Descrivere gli idempotenti corrispondenti a tale decomposizione in un prodotto (cfr. l'esercizio 34, § 3).
- 5 Aggiunzione di elementi**
- Descrivere l'anello ottenuto da  $\mathbb{Z}$  aggiungendo un elemento  $\alpha$  soddisfacente alle due relazioni:  $2\alpha - 6 = 0$ ,  $\alpha - 10 = 0$ .
  - Supponiamo di aggiungere a  $\mathbb{R}$  un elemento  $\alpha$  soddisfacente alla relazione  $\alpha^2 = 1$ . Dimostrare che l'anello che così si ottiene è isomorfo all'anello prodotto  $\mathbb{R} \times \mathbb{R}$ , e trovare l'elemento di  $\mathbb{R} \times \mathbb{R}$  che corrisponde ad  $\alpha$ .
  - Descrivere l'anello ottenuto dall'anello prodotto  $\mathbb{R} \times \mathbb{R}$  invertendo l'elemento  $(2, 0)$ .
  - Dimostrare che gli elementi  $1, t - \alpha, (t - \alpha)^2, \dots, (t - \alpha)^{n-1}$  formano una base per lo spazio vettoriale complesso  $\mathbb{C}[t]/((t - \alpha)^n)$ .
  - Si denoti con  $\alpha$  la classe resto di  $x$  nell'anello  $R' = \mathbb{Z}[x]/(x^4 + x^3 + x^2 + x + 1)$ . Calcolare le espressioni di  $(\alpha^3 + \alpha^2 + \alpha)(\alpha + 1)$  e  $\alpha^5$  mediante la base  $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ .
  - In ciascuno dei casi seguenti, descrivere l'anello ottenuto da  $\mathbb{F}_2$  aggiungendo un elemento  $\alpha$  soddisfacente alla relazione assegnata:
    - $\alpha^2 + \alpha + 1 = 0$ ;
    - $\alpha^2 + 1 = 0$ .
  - Studiare l'anello ottenuto da  $\mathbb{Z}$  aggiungendo un elemento  $\alpha$  soddisfacente alle due relazioni:  $\alpha^3 + \alpha^2 + 1 = 0$ ,  $\alpha^2 + \alpha = 0$ .
  - Sia  $a$  un elemento di  $R$ . Se aggiungiamo un elemento  $\alpha$  soddisfacente alla relazione  $\alpha = a$ , ci aspettiamo di ottenere un anello isomorfo a  $R$ . Dimostrare che ciò è vero.
  - Descrivere l'anello ottenuto da  $\mathbb{Z}/12\mathbb{Z}$  aggiungendo un inverso di 2.
  - Determinare la struttura dell'anello  $R'$  ottenuto da  $\mathbb{Z}$  aggiungendo un elemento  $\alpha$  soddisfacente, rispettivamente, ad uno dei seguenti insiemi di relazioni:
    - $2\alpha = 6$ ,  $6\alpha = 15$ ;
    - $2\alpha = 6$ ,  $6\alpha = 18$ ;
    - $2\alpha = 6$ ,  $6\alpha = 8$ .
  - Determinare la struttura dell'anello ottenuto da  $R = \mathbb{Z}/(10)$  aggiungendo un elemento  $\alpha$  soddisfacente, rispettivamente, ad una delle relazioni seguenti:
    - $2\alpha - 6 = 0$ ;
    - $2\alpha - 5 = 0$ .
  - Sia  $a$  un'unità in un anello  $R$ . Descrivere l'anello  $R' = R[x]/(ax - 1)$ .

13. (a) Dimostrare che l'anello ottenuto invertendo  $x$  nell'anello dei polinomi  $R[x]$  è isomorfo all'anello dei polinomi di Laurent, come asserito in (5.9).
- (b) È vero che le serie formali di Laurent  $\sum_{-\infty}^{\infty} a_n x^n$  formano un anello?
14. Sia  $a$  un elemento di un anello  $R$ , e sia  $R' = R[x]/(ax - 1)$  l'anello ottenuto aggiungendo a  $R$  un inverso di  $a$ . Dimostrare che il nucleo dell'omomorfismo  $R \rightarrow R'$  è l'insieme degli elementi  $b \in R$  tali che  $a^n b = 0$  per qualche  $n > 0$ .
15. Sia  $a$  un elemento di un anello  $R$ , e sia  $R'$  l'anello ottenuto da  $R$  aggiungendo un inverso di  $a$ . Dimostrare che  $R'$  è l'anello nullo se e soltanto se  $a$  è nilpotente.
16. Sia  $F$  un campo. Dimostrare che gli anelli  $F[x]/(x^2)$  e  $F[x]/(x - 1)^2$  sono isomorfi se e soltanto se  $F$  ha caratteristica 2.
17. Si ponga:  $\bar{R} = \mathbb{Z}[x]/(2x)$ . Dimostrare che ogni elemento di  $\bar{R}$  ha un'unica espressione della forma  $a_0 + a_1 x + \dots + a_n x^n$ , dove gli  $a_i$  sono interi e  $a_1, \dots, a_n$  sono uguali a 0 o a 1.
- 6 Domini di integrità e campi di frazioni**
- Dimostrare che un sottoanello di un dominio di integrità è un dominio di integrità.
  - Dimostrare che un dominio di integrità con un numero finito di elementi è un campo.
  - Sia  $R$  un dominio di integrità. Dimostrare che l'anello dei polinomi  $R[x]$  è un dominio di integrità.
  - Sia  $R$  un dominio di integrità. Dimostrare che gli elementi invertibili dell'anello dei polinomi  $R[x]$  sono le unità in  $R$ .
  - Esiste un dominio di integrità contenente esattamente 10 elementi?
  - Dimostrare che il campo delle frazioni dell'anello delle serie formali di potenze  $F[[x]]$  sopra un campo  $F$  si ottiene invertendo il solo elemento  $x$  ed esprimere gli elementi di tale campo come opportune serie di potenze con esponenti negativi.
  - Verificare che le classi di equivalenza di frazioni ottenute da un dominio di integrità formano un campo.
  - Un semigruppo  $S$  è un insieme con una legge di composizione associativa avente un elemento neutro. Sia  $S$  un semigruppo commutativo soddisfacente alla proprietà di cancellazione:  $ab = ac$  implica  $b = c$ . Utilizzare le frazioni per dimostrare che  $S$  può essere immerso in un gruppo.
  - Un sottoinsieme  $S$  di un dominio di integrità  $R$  chiuso rispetto alla moltiplicazione e non contenente 0 è chiamato *insieme moltiplicativo*. Dato un insieme moltiplicativo  $S$ , definiamo *S-frazioni* gli elementi della forma  $a/b$ , con  $b \in S$ . Dimostrare che le classi di equivalenza di *S-frazioni* formano un anello.
- 7 Ideali massimali**
- Dimostrare che gli ideali massimali dell'anello degli interi sono gli ideali principali generati dai numeri primi.

2. Determinare gli ideali massimali di ciascuno dei seguenti anelli:  
 (a)  $\mathbb{R} \times \mathbb{R}$ ; (b)  $\mathbb{R}[x]/(x^2)$ ; (c)  $\mathbb{R}[x]/(x^2 - 3x + 2)$ ; (d)  $\mathbb{R}[x]/(x^2 + x + 1)$ .
3. Dimostrare che l'ideale  $(x+y^2, y+x^2 + 2xy^2 + y^4)$  in  $\mathbb{C}[x, y]$  è un ideale massimale.
4. Sia  $R$  un anello e sia  $I$  un ideale di  $R$ . Sia  $M$  un ideale di  $R$  contenente  $I$  e sia  $\overline{M} = M/I$  il corrispondente ideale di  $\overline{R}$ . Dimostrare che  $M$  è massimale se e soltanto se  $\overline{M}$  è massimale.
5. Sia  $I$  l'ideale principale di  $\mathbb{C}[x, y]$  generato dal polinomio  $y^2 + x^3 - 17$ . Quali dei seguenti insiemi generano ideali massimali nell'anello quoziante  $R = \mathbb{C}[x, y]/I$ ?  
 (a)  $(x-1, y-4)$ ; (b)  $(x+1, y+4)$ ; (c)  $(x^3 - 17, y^2)$ .
6. Dimostrare che l'anello  $\mathbb{F}_5[x]/(x^2 + x + 1)$  è un campo.
7. Dimostrare che l'anello  $\mathbb{F}_2[x]/(x^3 + x + 1)$  è un campo, ma che  $\mathbb{F}_3[x]/(x^3 + x + 1)$  non lo è.
8. Sia  $R = \mathbb{C}[x_1, \dots, x_n]/I$  un quoziante di un anello di polinomi a coefficienti in  $\mathbb{C}$  e sia  $M$  un ideale massimale di  $R$ . Dimostrare che  $R/M$  è isomorfo a  $\mathbb{C}$ .
9. Definire una corrispondenza biunivoca tra gli ideali massimali di  $\mathbb{R}[x]$  e i punti del semipiano superiore (incluso l'asse  $x$ ).
10. Sia  $R$  un anello e sia  $M$  un ideale di  $R$ . Supponiamo che ogni elemento di  $R$  che non appartenga a  $M$  sia un'unità di  $R$ . Dimostrare che  $M$  è un ideale massimale e inoltre che esso è l'unico ideale massimale di  $R$ .
11. Sia  $P$  un ideale di un anello  $R$ . Dimostrare che  $\overline{R} = R/P$  è un dominio di integrità se e soltanto se  $P \neq R$  e inoltre  $P$  verifica la seguente proprietà: se  $a, b \in R$  e  $ab \in P$ , allora  $a \in P$  oppure  $b \in P$ . (Un ideale  $P$  soddisfacente a tali condizioni è chiamato un *ideale primo*).
12. Sia  $\varphi : R \rightarrow R'$  un omomorfismo di anelli e sia  $P'$  un ideale primo di  $R'$ .
  - (a) Dimostrare che  $\varphi^{-1}(P')$  è un ideale primo di  $R$ .
  - (b) Dare un esempio in cui  $P'$  è un ideale massimale, ma  $\varphi^{-1}(P')$  non è massimale.
- \*13. Sia  $R$  un dominio di integrità e  $F$  il suo campo delle frazioni, e sia  $P$  un ideale primo di  $R$ . Sia  $R_P$  il sottoinsieme di  $F$  definito da:  

$$R_P = \{a/d \mid a \in R, d \notin P\}.$$

Tale sottoinsieme è chiamato la *localizzazione di  $R$  in  $P$* .

  - (a) Dimostrare che  $R_P$  è un sottoanello di  $F$ .
  - (b) Determinare tutti gli ideali massimali di  $R_P$ .
14. Trovare un esempio di un “anello privo di elemento unità” con un ideale non contenuto in un ideale massimale.

## 8 Geometria algebrica

1. In ciascuno dei casi seguenti, determinare i punti di intersezione delle due curve piane complesse:

- (a)  $y^2 - x^3 + x^2 = 1, \quad x + y = 1$ ;
- (b)  $x^2 + xy + y^2 = 1, \quad x^2 + 2y^2 = 1$ ;
- (c)  $y^2 = x^3, \quad xy = 1$ ;
- (d)  $x + y + y^2 = 0, \quad x - y + y^2 = 0$ ;
- (e)  $x + y^2 = 0, \quad y + x^2 + 2xy + y^4 = 0$ .
2. Dimostrare che due polinomi di secondo grado  $f, g$  in due variabili hanno al più quattro zeri comuni, a meno che non abbiano un fattore non costante in comune.
3. Dedurre il teorema degli zeri di Hilbert dalla sua forma classica (8.7).
4. Siano  $U, V$  varietà in  $\mathbb{C}^n$ . Dimostrare che  $U \cup V$  e  $U \cap V$  sono varietà.
5. Siano  $f_1, \dots, f_r; g_1, \dots, g_s$  polinomi in  $\mathbb{C}[x_1, \dots, x_n]$ , e siano  $U, V$  gli insiemi degli zeri di  $\{f_1, \dots, f_r\}, \{g_1, \dots, g_s\}$ , rispettivamente. Dimostrare che, se  $U \cap V = \emptyset$ , allora l'ideale  $(f_1, \dots, f_r; g_1, \dots, g_s)$  è l'ideale unità.
6. Siano dati  $f = f_1 \cdot \dots \cdot f_m$  e  $g = g_1 \cdot \dots \cdot g_n$ , dove  $f_i, g_j$  sono polinomi irriducibili in  $\mathbb{C}[x, y]$ . Siano  $S_i = \{f_i = 0\}$  e  $T_j = \{g_j = 0\}$  le superfici di Riemann definite da tali polinomi, e sia  $V$  la varietà  $f = g = 0$ . Descrivere  $V$  mediante  $S_i$  e  $T_j$ .
7. Dimostrare che la varietà definita da un insieme di polinomi  $\{f_1, \dots, f_r\}$  dipende soltanto dall'ideale  $(f_1, \dots, f_r)$  che essi generano.
8. Sia  $R$  un anello contenente  $\mathbb{C}$  come sottoanello.
  - (a) Verificare esplicitamente che  $R$  risulta uno spazio vettoriale su  $\mathbb{C}$ .
  - (b) Supponiamo che  $R$  sia uno spazio vettoriale di dimensione finita su  $\mathbb{C}$  e che  $R$  contenga un solo ideale massimale  $M$ . Dimostrare che  $M$  è il *nilradicale* di  $R$ , ossia, che  $M$  è costituito precisamente dai suoi elementi nilpotenti.
9. Dimostrare che la conica complessa  $xy = 1$  è omeomorfa al piano privato di un punto.
10. Dimostrare che ogni varietà in  $\mathbb{C}^2$  è l'unione di un numero finito di punti e di curve algebriche.
11. I tre polinomi  $f_1 = x^2 + y^2 - 1$ ,  $f_2 = x^2 - y + 1$  e  $f_3 = xy - 1$  generano l'ideale unità in  $\mathbb{C}[x, y]$ . Dimostrare ciò in due modi: (i) provando che essi non hanno zeri comuni, e (ii) scrivendo 1 come una combinazione lineare di  $f_1, f_2, f_3$ , con polinomi come coefficienti.
12. (a) Determinare i punti di intersezione della curva algebrica  $S$ :  $y^2 = x^3 - x^2$  con la retta  $L$ :  $y = \lambda x$ .  
 (b) Parametrizzare i punti di  $S$  in funzione di  $\lambda$ .  
 (c) Utilizzando tale parametrizzazione, mettere in relazione  $S$  con il piano complesso nella variabile  $\lambda$ .
- \*13. Il *radicale* di un ideale  $I$  è l'insieme degli elementi  $r \in R$  tali che qualche potenza di  $r$  appartiene a  $I$ .
  - (a) Dimostrare che il radicale di  $I$  è un ideale.
  - (b) Dimostrare che le varietà definite da due insiemi di polinomi  $\{f_1, \dots, f_r\}$ ,

$\{g_1, \dots, g_s\}$  sono uguali se e soltanto se i due ideali  $(f_1, \dots, f_r), (g_1, \dots, g_s)$  hanno lo stesso radicale.

- \*14. Si consideri l'anello  $R = \mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_m)$  e sia  $A$  un anello contenente  $\mathbb{C}$  come sottoanello. Stabilire una corrispondenza biunivoca tra i seguenti insiemi:

- (i) gli omomorfismi  $\varphi : R \rightarrow A$  che si restringono all'identità su  $\mathbb{C}$ ,
- (ii) le  $n$ -uple  $a = (a_1, \dots, a_n)$  di elementi di  $A$  che sono soluzioni del sistema di equazioni  $f_1 = \dots = f_m = 0$ , ossia tali che  $f_i(a) = 0$  per  $i = 1, \dots, m$ .

### Esercizi vari

1. Sia  $F$  un campo e si denoti con  $K$  lo spazio vettoriale  $F^2$ . Definiamo la moltiplicazione mediante la legge:  $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$ .

- (a) Dimostrare che  $K$  risulta un anello rispetto a tale moltiplicazione e all'addizione tra vettori.
  - (b) Dimostrare che  $K$  è un campo se e soltanto se non esiste nessun elemento in  $F$  il cui quadrato è  $-1$ .
  - (c) Supponiamo che  $-1$  sia un quadrato in  $F$  e che  $F$  non abbia caratteristica 2. Dimostrare che  $K$  è isomorfo all'anello prodotto  $F \times F$ .
2. (a) È possibile definire la derivata di un polinomio  $f(x)$  a coefficienti in un anello  $R$  mediante la formula studiata in analisi:  $(a_n x^n + \dots + a_1 x + a_0)' = n a_n x^{n-1} + \dots + a_1$ , dove i coefficienti interi vengono interpretati in  $R$  utilizzando l'omomorfismo (3.9). Dimostrare la formula del prodotto:  $(fg)' = f'g + fg'$  e la regola di derivazione delle funzioni composte:  $(f \circ g)' = (f' \circ g)g'$ .
- (b) Sia  $f(x)$  un polinomio a coefficienti in un campo  $F$  e sia  $\alpha$  un elemento di  $F$ . Dimostrare che  $\alpha$  è una radice multipla di  $f$  se e solo se  $\alpha$  è una radice comune di  $f$  e della sua derivata  $f'$ .
  - (c) Posto  $F = \mathbb{F}_5$ , stabilire se i seguenti polinomi hanno radici multiple in  $F$ :  $x^{15} - x - 15 - 2x^5 + 1$ .

3. Sia  $R$  un insieme con due leggi di composizione soddisfacenti a tutti gli assiomi di un anello, ad eccezione della proprietà commutativa dell'addizione. Dimostrare che tale proprietà vale, sviluppando il prodotto  $(a+b)(c+d)$  in due modi utilizzando la proprietà distributiva.

4. Sia  $R$  un anello. Determinare le unità nell'anello dei polinomi  $R[x]$ .

5. Si denoti con  $R$  l'insieme delle successioni  $a = (a_1, a_2, a_3, \dots)$  di numeri reali che risultano costanti da un certo punto in poi:  $a_n = a_{n+1} = \dots$  per  $n$  abbastanza grande. In  $R$  l'addizione e la moltiplicazione sono definite componente per componente, ossia l'addizione è l'addizione tra vettori e  $ab = (a_1 b_1, a_2 b_2, \dots)$ .

- (a) Dimostrare che  $R$  è un anello.
  - (b) Determinare gli ideali massimali di  $R$ .
6. (a) Classificare gli anelli  $R$  che contengono  $\mathbb{C}$  e risultano spazi vettoriali di dimensione 2 su  $\mathbb{C}$ .
- (b) Risolvere lo stesso problema per la dimensione 3.

7. Si consideri l'applicazione  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x] \times \mathbb{C}[y] \times \mathbb{C}[t]$  definita da:  $f(x, y) \mapsto (f(x, 0), f(0, y), f(t, t))$ . Determinare esplicitamente l'immagine di  $\varphi$ .

8. Sia  $S$  un sottoanello di un anello  $R$ . Il *conduttore*  $C$  di  $S$  in  $R$  è l'insieme degli elementi  $\alpha \in R$  tali che  $\alpha S \subset C$ .

- (a) Dimostrare che  $C$  è un ideale di  $R$  ed è anche un ideale di  $S$ .
- (b) Dimostrare che  $C$  è il più grande ideale di  $S$  che sia anche ideale di  $R$ .
- (c) Determinare il conduttore in ciascuno dei tre casi seguenti:

- (i)  $R = \mathbb{C}[t]$ ,  $S = \mathbb{C}[t^2, t^3]$ ;
- (ii)  $R = \mathbb{Z}[\zeta]$ ,  $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ ,  $S = \mathbb{Z}[\sqrt{-3}]$ ;
- (iii)  $R = \mathbb{C}[t, t^{-1}]$ ,  $S = \mathbb{C}[t]$ .

9. Una retta in  $\mathbb{C}^2$  è il luogo delle soluzioni di un'equazione lineare  $L$ :  $ax + by + c = 0$ . Dimostrare che esiste una e una sola retta passante per due punti distinti  $(x_0, y_0)$ ,  $(x_1, y_1)$ , e inoltre che esiste un'unica retta passante per un punto  $(x_0, y_0)$  con una direzione tangente assegnata  $(u_0, v_0)$ .

10. Una curva algebrica  $C$  in  $\mathbb{C}^2$  si dice *irriducibile* se è il luogo degli zeri di un polinomio irriducibile  $f(x, y)$ , ossia un polinomio che non può essere espresso come un prodotto di polinomi non costanti. Un punto  $p \in C$  si dice un *punto singolare* della curva se  $\partial f / \partial x = \partial f / \partial y = 0$  in  $p$ . Altrimenti  $p$  è un punto *non singolare*. Dimostrare che una curva irriducibile ha soltanto un numero finito di punti singolari.

11. Sia  $L$ :  $ax + by + c = 0$  una retta e sia  $C$ :  $\{f = 0\}$  una curva in  $\mathbb{C}^2$ . Supponiamo che  $b \neq 0$ . Allora è possibile utilizzare l'equazione della retta per eliminare  $y$  dall'equazione  $f(x, y) = 0$  di  $C$ , ottenendo un polinomio  $g(x)$  in  $x$ . Dimostrare che le sue radici sono le ascisse dei punti di intersezione.

12. Con le notazioni introdotte nel problema precedente, si definisce *molteplicità di intersezione* di  $L$  e  $C$  in un punto  $p = (x_0, y_0)$  la molteplicità di  $x_0$  come radice di  $g(x)$ . La retta  $L$  si dice *retta tangente* a  $C$  in  $p$  se la molteplicità di intersezione è almeno 2. Dimostrare che, se  $p$  è un punto non singolare di  $C$ , allora esiste un'unica retta tangente in  $(x_0, y_0)$ , e determinare tale retta.

13. Dimostrare che, se  $p$  è un punto singolare di una curva  $C$ , la molteplicità di intersezione di ogni retta passante per  $p$  è almeno 2.

14. Si definisce *grado* di una curva irriducibile  $C$ :  $\{f = 0\}$  il grado  $d$  del polinomio irriducibile  $f$ .

- (a) Dimostrare che una retta  $L$  incontra  $C$  in al più  $d$  punti, a meno che  $C = L$ .
- (b) Dimostrare che esistono rette che incontrano  $C$  esattamente in  $d$  punti.

15. Determinare i punti singolari della curva  $C$ :  $x^3 + y^3 - 3xy = 0$ .

16. Dimostrare che una cubica irriducibile può avere al più un solo punto singolare.

17. Un punto non singolare  $p$  di una curva  $C$  si dice *punto di flesso* se la retta tangente  $L$  a  $C$  in  $p$  ha molteplicità di intersezione almeno 3 con  $C$  in  $p$ .

- (a) Dimostrare che i punti di flesso sono i punti non singolari di  $C$  in cui si annulla il determinante *hessiano*:

$$\det \begin{bmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial f}{\partial x} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} & f \end{bmatrix}.$$

- (b) Determinare i punti di flesso delle cubiche di equazione:  $y^2 - x^3 = 0$ ,  $y^2 - x^3 + x^2 = 0$ .
- \*18. Sia  $C$  una cubica irriducibile e sia  $L$  una retta congiungente due punti di flesso di  $C$ . Dimostrare che, se  $L$  incontra  $C$  in un terzo punto, allora tale punto è anch'esso un punto di flesso.
19. Siano  $U = \{f_i(x_1, \dots, x_m) = 0\}$ ,  $V = \{g_j(y_1, \dots, y_n) = 0\}$  due varietà. Dimostrare che la varietà definita dalle equazioni  $\{f_i(x) = 0, g_j(y) = 0\}$  in  $\mathbb{C}^{m+n}$  è l'insieme prodotto  $U \times V$ .
20. Dimostrare che il luogo di punti in  $\mathbb{R}^2$  definito dall'equazione  $y = \sin x$  non è contenuto in nessuna curva algebrica.
- \*21. Siano  $f, g$  polinomi in  $\mathbb{C}[x, y]$  privi di fattori comuni. Dimostrare che l'anello  $R = \mathbb{C}[x, y]/(f, g)$  è uno spazio vettoriale di dimensione finita su  $\mathbb{C}$ .
22. (a) Denotiamo con  $s, c$  le funzioni  $\sin x, \cos x$  sulla retta reale. Dimostrare che l'anello  $\mathbb{R}[s, c]$  da esse generato è un dominio di integrità.  
(b) Denotiamo con  $K = \mathbb{R}(s, c)$  il campo delle frazioni di  $\mathbb{R}[s, c]$ . Dimostrare che il campo  $K$  è isomorfo al campo delle funzioni razionali  $\mathbb{R}(x)$ .
- \*23. Siano  $f(x), g(x)$  polinomi a coefficienti in un anello  $R$ , con  $f \neq 0$ . Dimostrare che, se il prodotto  $f(x)g(x)$  è zero, esiste un elemento  $c \neq 0$  in  $R$  tale che  $cg(x) = 0$ .
- \*24. Sia  $R$  l'anello delle funzioni continue  $[0, 1] \rightarrow \mathbb{R}$ .
- (a) Dimostrare che una funzione  $f$  che non si annulla in nessun punto di  $[0, 1]$  è invertibile in  $R$ .  
(b) Siano  $f_1, \dots, f_n$  funzioni prive di zeri comuni su  $[0, 1]$ . Dimostrare che l'ideale generato da tali funzioni è l'ideale unità. (Suggerimento: si consideri  $f_1^2 + \dots + f_n^2$ )  
(c) Stabilire una corrispondenza biunivoca tra gli ideali massimali di  $R$  e i punti dell'intervallo  $[0, 1]$ .  
(d) Dimostrare che gli ideali massimali che contengono una funzione  $f$  corrispondono ai punti dell'intervallo in cui  $f = 0$ .  
(e) Estendere tali risultati alle funzioni continue su un insieme compatto  $X$  in  $\mathbb{R}^k$ .  
(f) Descrivere la situazione nel caso delle funzioni continue  $\mathbb{R} \rightarrow \mathbb{R}$ .

## Capitolo 11

### Fattorizzazione

È bello solo ciò che è vero.  
Hermann Minkowski

#### 1 Fattorizzazione di interi e polinomi

Questo capitolo è dedicato allo studio della divisione negli anelli. Poiché il modello fondamentale sono i numeri interi, cominceremo col passare in rassegna le loro proprietà. Alcune di esse sono state usate senza commento nei capitoli precedenti del libro, e qualcuna è stata già dimostrata.

La proprietà che è alla base di tutte le altre è la divisione con resto. Precisamente, se  $a, b$  sono interi e  $a \neq 0$ , esistono interi  $q, r$  tali che:

$$(1.1) \quad b = aq + r,$$

con  $0 \leq r < |a|$ . Questa proprietà viene enunciata spesso soltanto per interi positivi, ma essa vale anche se  $a$  e  $b$  assumono valori negativi. Ecco perché si usa il valore assoluto  $|a|$  per limitare il resto. La dimostrazione dell'esistenza di (1.1) è una semplice argomentazione per induzione.

Abbiamo già visto alcune delle conseguenze più importanti della divisione con resto; tuttavia le richiamiamo. Nel capitolo 10, abbiamo visto che ogni sottogruppo di  $\mathbb{Z}$  è un ideale e che ogni ideale di  $\mathbb{Z}$  è principale, ossia, ha la forma  $d\mathbb{Z}$  per qualche intero  $d \geq 0$ . Com'è stato dimostrato nel capitolo 2 (2.6), ciò implica che due interi  $a, b$  hanno un massimo comune divisore che è una combinazione lineare a coefficienti interi di  $a$  e  $b$ . Se  $a$  e  $b$  non hanno fattori in comune diversi da  $\pm 1$ , allora 1 è una combinazione lineare di  $a$  e  $b$  con coefficienti interi:

$$(1.2) \quad ra + sb = 1,$$

con  $r, s \in \mathbb{Z}$ . Ciò implica la proprietà fondamentale dei numeri primi, che è stata dimostrata nel capitolo 3 (2.8), e che qui rienunciamo:

(1.3) PROPOSIZIONE *Sia  $p$  un numero primo, e siano  $a, b$  interi. Se  $p$  divide il prodotto  $ab$ , allora  $p$  divide  $a$  oppure  $p$  divide  $b$ .* ■

(1.4) TEOREMA FONDAMENTALE DELL'ARITMETICA  
sare scomposto in un prodotto:

$$a = cp_1 \cdots p_k,$$

dove  $c = \pm 1$ , i  $p_i$  sono numeri primi, e  $k \geq 0$ . Tale espressione è unica a meno dell'ordine dei fattori primi.

*Dimostrazione.* Innanzitutto dimostriamo l'esistenza di una fattorizzazione mediante numeri primi; basterà considerare il caso  $a > 1$ . Procedendo per induzione per ogni intero positivo  $b < a$ . Ora, o  $a$  è primo, nel qual caso il prodotto in questione ha un solo fattore, oppure esiste un divisore proprio  $b \neq a$ . Allora  $a = bb'$  e inoltre  $b' \neq a$ . Sia  $b$  che  $b'$  sono più piccoli di  $a$ , e per l'ipotesi induttiva possono essere fattorizzati in prodotti di primi. Scrivendo tali fattorizzazioni l'una accanto all'altra, si ottiene una fattorizzazione di  $a$ .

In secondo luogo, la fattorizzazione è unica. Supponiamo che si abbia:

$$\pm p_1 \cdots p_n = a = \pm q_1 \cdots q_m.$$

Allora i segni certamente coincidono. Applichiamo poi (1.3), con  $p = p_1$ . Poiché  $p_1$  divide il prodotto  $q_1 \cdots q_m$ , esso divide qualche fattore  $q_i$ , diciamo  $q_1$ . Poiché  $q_1$  è primo, si ha:  $p_1 = q_1$ . A questo punto, cancelliamo  $p_1$  e procediamo per induzione. ■

La struttura dell'anello degli interi ha fortissime analogie con quella di un anello di polinomi in una variabile  $F[x]$  a coefficienti in un campo. Ogni volta che ricaviamo una proprietà di uno di questi anelli, dovremmo cercare di trovare la proprietà analoga nell'altro anello. Abbiamo già trattato la divisione con resto tra polinomi nel capitolo 10, e abbiamo visto che ogni ideale dell'anello dei polinomi  $F[x]$  è principale [cap. 10 (3.21)].

Un polinomio  $p(x)$  a coefficienti in un campo  $F$  si dice *irriducibile* se non è costante e se i suoi unici divisori di grado più basso in  $F[x]$  sono delle costanti. Ciò significa che l'unico modo di scrivere  $p$  come un prodotto di due polinomi è  $p = cp_1$  dove  $c$  è una costante. I polinomi irriducibili sono l'analogo dei numeri primi. Di solito, essi valgono normalizzati dividendoli per i loro coefficienti direttori, sicché diventano monici.

La dimostrazione del teorema seguente è simile a quella degli analoghi enunciati per l'anello degli interi:

(1.5) TEOREMA Sia  $F$  un campo, e sia  $F[x]$  l'anello dei polinomi in una variabile a coefficienti in  $F$ .

Se due polinomi  $f, g$  non hanno fattori comuni non costanti, allora esistono due polinomi  $r, s \in F[x]$  tali che  $rf + sg = 1$ .

(b) Se un polinomio irriducibile  $p \in F[x]$  divide un prodotto  $fg$ , allora  $p$  divide uno dei fattori  $f$  o  $g$ .

(c) Ogni polinomio non nullo  $f \in F[x]$  si può scomporre in un prodotto:

$$f = cp_1 \cdots p_k,$$

dove  $c$  è una costante non nulla, i  $p_i$  sono polinomi irriducibili monici in  $F[x]$ , e  $k \geq 0$ . Tale fattorizzazione è unica, a meno dell'ordine dei fattori. ■

Il fattore costante  $c$  che compare nell'enunciato (c) è analogo al fattore  $\pm 1$  in (1.4). Essi sono le unità nei rispettivi anelli. I fattori invertibili sono presenti poiché abbiamo normalizzato i numeri primi in modo che siano positivi, e i polinomi irriducibili in modo che siano monici. Possiamo considerare anche primi negativi o polinomi irriducibili non monici, se vogliamo (allora il fattore invertibile può essere assorbito, se  $k > 0$ ), ma ciò complica leggermente l'enunciato relativo all'unicità.

### (1.6) Esempi

Nell'anello  $C[x]$  ogni polinomio di grado positivo ha una radice  $\alpha$  e quindi ha un divisore della forma  $x - \alpha$ . Pertanto, i polinomi irriducibili sono lineari, e la fattorizzazione di un polinomio in fattori irriducibili ha la forma

$$(1.7) \quad f(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

dove gli  $\alpha_i$  sono le radici di  $f(x)$ , eventualmente ripetute. L'unicità di tale fattorizzazione non è sorprendente.

Quando  $F = R$ , vi sono due classi di polinomi irriducibili: i polinomi lineari e i polinomi quadratici irriducibili. Un polinomio quadratico reale  $x^2 + bx + c$  è irriducibile se e soltanto se il suo discriminante  $b^2 - 4c$  è negativo, nel qual caso ha due radici complesse coniugate. Il fatto che ogni polinomio irriducibile su  $C$  è lineare implica che nessun polinomio di grado maggiore di 2 è irriducibile su  $R$ . Supponiamo che un polinomio  $f(x)$  abbia coefficienti reali  $a_i$  e che  $\alpha$  sia una radice complessa, non reale di  $f(x)$ . Allora il numero complesso coniugato  $\bar{\alpha}$  è diverso da  $\alpha$  ed è anch'esso una radice. Infatti, poiché  $f$  è un polinomio reale, i suoi coefficienti  $a_i$  soddisfano la relazione  $a_i = \bar{a}_i$ . Allora risulta:

$$f(\bar{\alpha}) = a_n \bar{\alpha}^n + \cdots + a_1 \bar{\alpha} + a_0 = \bar{a}_n \bar{\alpha}^n + \cdots + \bar{a}_1 \bar{\alpha} + \bar{a}_0 = \overline{f(\alpha)} = \bar{0} = 0.$$

Il polinomio quadratico  $g(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$  ha coefficienti reali  $-(\alpha + \bar{\alpha})$  e  $\alpha\bar{\alpha}$ , e i suoi fattori lineari compaiono entrambi nella fattorizzazione complessa (1.7) di  $f(x)$ . Ne segue che  $g(x)$  divide  $f(x)$ . Pertanto la fattorizzazione

di  $f(x)$  in polinomi irriducibili reali si ottiene raggruppando le coppie coniugate nella fattorizzazione complessa. ■

Nel caso dei polinomi a coefficienti razionali, la fattorizzazione è più complicata di quella dei polinomi reali o complessi: in  $\mathbb{Q}[x]$  infatti vi sono polinomi irriducibili di qualunque grado: per esempio,  $x^5 - 3x^4 + 3$ . Vedremo ancora altri esempi nel paragrafo 4. Né la forma della fattorizzazione in polinomi irriducibili né la sua unicità sono immediate, per i polinomi a coefficienti razionali.

Avremo più volte occasione, in seguito, di fare riferimento alla seguente proprietà elementare:

(1.8) PROPOSIZIONE *Sia  $F$  un campo, e sia  $f(x)$  un polinomio di grado  $n$  a coefficienti in  $F$ . Allora  $f$  ha al più  $n$  radici in  $F$ .*

*Dimostrazione.* Un elemento  $\alpha \in F$  è una radice di  $f$  se e soltanto se  $x - \alpha$  divide  $f$  [cap. 10 (3.20)]. In tal caso, possiamo scrivere  $f(x) = (x - \alpha)q(x)$ , dove  $q(x)$  è un polinomio di grado  $n - 1$ . Se  $\beta$  è un'altra radice di  $f$ , allora  $f(\beta) = (\beta - \alpha)q(\beta) = 0$ . Poiché  $F$  è un campo, il prodotto di elementi non nulli di  $F$  è diverso da zero. Pertanto uno dei due elementi  $\beta - \alpha$ ,  $q(\beta)$  è uguale a zero. Nel primo caso,  $\beta = \alpha$ , e nel secondo caso,  $\beta$  è una delle radici di  $q(x)$ . Procedendo per induzione su  $n$ , possiamo supporre che  $q(x)$  ha al più  $n - 1$  radici in  $F$ . Allora vi sono al più  $n$  possibilità per  $\alpha$ . ■

Il fatto che  $F$  sia un campo è essenziale per la validità del teorema (1.5) e della proposizione (1.8), come mostra l'esempio seguente. Sia  $R$  l'anello  $\mathbb{Z}/8\mathbb{Z}$ . Allora nell'anello dei polinomi  $R[x]$  si ha:

$$x^2 - 1 = (x + 1)(x - 1) = (x + 3)(x - 3).$$

Il polinomio  $x^2 - 1$  ha quattro radici modulo 8, e la sua fattorizzazione in polinomi irriducibili non è unica.

## 2 Domini a fattorizzazione unica, domini a ideali principali, domini euclidei

Abbiamo visto che la fattorizzazione negli interi ha un analogo negli anelli di polinomi, ed è quindi naturale chiedersi se altri anelli abbiano questa proprietà. L'anello degli interi di Gauss è un esempio interessante, e ce ne sono relativamente pochi altri. In questo paragrafo vedremo in che modo si possono estendere varie parti della teoria fin qui svolta.

Cominciamo a introdurre la terminologia usata nello studio della fattorizzazione. È naturale supporre che l'anello  $R$  assegnato sia un dominio di integrità, cosicché si possa applicare la legge di cancellazione; questa ipotesi verrà fatta in tutto il paragrafo. Si dice che un elemento  $a$  divide un altro elemento  $b$  (e si scrive  $a \mid b$ ).

$b = aq$  per qualche  $q \in R$ . L'elemento  $a$  è un divisore proprio di  $b$  se  $b = aq$  per qualche  $q \in R$  e inoltre né  $a$  né  $q$  sono unità. Un elemento non nullo  $a$  di  $R$  si dice irriducibile se non è un'unità e se non ha divisori propri. Due elementi  $a, a'$  si dicono associati se ciascuno di essi divide l'altro. Si vede facilmente che  $a, a'$  sono associati se e soltanto se  $a' = ua$  per qualche unità  $u$ .

I concetti di divisore, unità, elementi associati possono essere interpretati utilizzando gli ideali principali generati dagli elementi. Ricordiamo che un ideale  $I$  si dice principale se è generato da un solo elemento:

$$(2.1) \quad I = (a).$$

Teniamo presente che l'ideale  $(a)$  è costituito da tutti gli elementi che sono multipli di  $a$ , ossia, che sono divisibili per  $a$ . Allora di ha:

$$u \text{ è un'unità} \Leftrightarrow (u) = (1)$$

$$a \text{ e } a' \text{ sono associati} \Leftrightarrow (a) = (a')$$

$$(2.2) \quad a \text{ divide } b \Leftrightarrow (a) \supset (b)$$

$$a \text{ è un divisore proprio di } b \Leftrightarrow (1) > (a) > (b).$$

La dimostrazione di queste equivalenze è immediata e pertanto viene omessa.

Volendo stabilire in un dominio di integrità  $R$  un teorema analogo al teorema fondamentale dell'aritmetica, si può pensare di dividere il relativo enunciato in due parti: la prima riguarda l'esistenza della rappresentazione di un dato elemento  $a$  come prodotto di elementi irriducibili, la seconda l'unicità di tale rappresentazione.

Consideriamo la prima parte. Supponiamo anzitutto che l'elemento assegnato  $a$  sia diverso da zero e non sia un'unità, altrimenti sarebbe impossibile scriverlo come prodotto di elementi irriducibili. Per fattorizzarlo procediamo come segue. Se  $a$  stesso è irriducibile, non vi è nulla da aggiungere. Se non lo è, allora possiede un divisore proprio, e pertanto si scomponete in un prodotto, diciamo  $a = a_1 b_1$ , dove né  $a_1$  né  $b_1$  sono unità. Proseguiamo fattorizzando  $a_1$  e  $b_1$ , se possibile, e via di questo passo, nella speranza ovviamente che il procedimento abbia termine, e cioè che dopo un numero finito di passi tutti i fattori siano irriducibili. Quest'ultima condizione può essere descritta in modo conciso in termini di ideali principali:

(2.3) PROPOSIZIONE *Sia  $R$  un dominio di integrità. Le seguenti condizioni sono equivalenti:*

(a) *Per ogni elemento non nullo  $a$  di  $R$  che non sia un'unità, il procedimento di fattorizzazione termina dopo un numero finito di passi e dà luogo ad una fattorizzazione  $a = b_1 \cdots b_k$  di  $a$  in elementi irriducibili di  $R$ .*

(b)  $R$  non contiene una catena ascendente infinita di ideali principali:

$$(a_1) < (a_2) < (a_3) < \dots$$

**Dimostrazione.** Supponiamo che  $R$  contenga una successione crescente infinita  $(a_1) < (a_2) < \dots$ . Allora  $(a_n) < (1)$  per ogni  $n$ , perché  $(a_n) < (a_{n+1}) \subseteq (1)$ . Poiché  $(a_{n-1}) < (a_n)$ ,  $a_n$  è un divisore proprio di  $a_{n-1}$ , diciamo  $a_{n-1} = a_n b_n$ , dove  $a_n, b_n$  non sono unità. Ciò fornisce una successione infinita di fattorizzazioni di  $a_1$ :  $a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2 \dots$ . Viceversa, una successione infinita di fattorizzazioni fornisce una catena ascendente infinita di ideali. ■

La condizione (2.3b) è chiamata spesso la *condizione della catena ascendente* per gli ideali principali. Tuttavia, per mettere in evidenza la fattorizzabilità, diremo che in  $R$  esiste una fattorizzazione se sono soddisfatte le condizioni equivalenti della proposizione (2.3).

È facile descrivere domini in cui non si possono fattorizzare gli elementi. Un esempio si ottiene aggiungendo all'anello dei polinomi  $F[x_1]$  tutte le radici  $2^k$ -esime di  $x_1$ :

$$(2.4) \quad R = F[x_1, x_2, x_3, \dots],$$

con le relazioni:  $x_2^2 = x_1$ ,  $x_3^2 = x_2$ ,  $x_4^2 = x_3$ , e così via. In questo anello, possiamo fattorizzare indefinitamente l'elemento  $x_1$ , e corrispondentemente si ottiene una catena ascendente infinita  $(x_1) < (x_2) < \dots$  di ideali principali.

In realtà abbiamo bisogno di un anello con infiniti generatori per ottenere un esempio come quello appena descritto, sicché incontreremo raramente anelli siffatti. In pratica, è la seconda parte del teorema fondamentale, quella sull'unicità, a dare le maggiori difficoltà. Di solito, una fattorizzazione in elementi irriducibili sarà possibile, ma non sarà necessariamente unica.

Le unità in un anello complicano l'enunciato relativo all'unicità. È chiaro che i fattori invertibili dovrebbero essere trascurati, poiché non vi è nessun limite alla possibilità di aggiungere tali fattori a coppie  $uu^{-1}$ . Per lo stesso motivo, i fattori associati dovrebbero essere considerati equivalenti. Le unità nell'anello degli interi sono  $\pm 1$ , e in questo anello è stato naturale normalizzare gli elementi irriducibili (i numeri primi) prendendoli positivi; analogamente possiamo normalizzare i polinomi irriducibili, richiedendo che essi siano monici. Non esiste un metodo universale per normalizzare gli elementi di un dominio di integrità arbitrario; quindi saremo costretti ad ammettere qualche ambiguità. In effetti è più chiaro fare riferimento agli *ideali principali* che agli elementi. Per esempio, elementi associati generano lo stesso ideale principale. Tuttavia, non è troppo scomodo utilizzare qui gli elementi, e noi continueremo a farlo. L'importanza degli ideali diventerà chiara nei paragrafi successivi di questo capitolo.

Diremo che un dominio di integrità  $R$  è un *dominio a fattorizzazione unica*, se esso ha le seguenti proprietà:

(2.5)

- (i) In  $R$  esiste una fattorizzazione degli elementi. In altre parole, il procedimento di scomposizione in fattori di un qualunque elemento non nullo  $a$  di  $R$  che non sia un'unità termina dopo un numero finito di passi e dà luogo a una scrittura del tipo:  $a = p_1 \cdots p_m$  dove ciascun  $p_i$  è irriducibile.
- (ii) La fattorizzazione di ogni elemento in fattori irriducibili è unica, nel senso che, date due fattorizzazioni diverse,  $a = p_1 \cdots p_m = q_1 \cdots q_n$ , risulta  $m = n$  e inoltre, a meno di un eventuale riordinamento dei fattori,  $p_i$  e  $q_i$  sono associati per ogni  $i$ .

Pertanto, nell'enunciato relativo all'unicità, fattorizzazioni associate sono considerate equivalenti.

Ecco un esempio in cui non vale l'unicità della fattorizzazione. L'anello è il **dominio di integrità**:

$$(2.6) \quad R = \mathbb{Z}[\sqrt{-5}].$$

Esso è costituito da tutti i numeri complessi della forma  $a + b\sqrt{-5}$ , dove  $a, b \in \mathbb{Z}$ . Le unità in questo anello sono  $\pm 1$ , e l'intero 6 possiede due fattorizzazioni in  $R$  essenzialmente diverse:

$$(2.7) \quad 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Non è difficile dimostrare che tutti e quattro i termini  $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$  sono elementi irriducibili di  $R$ . Poiché le unità sono  $\pm 1$ , gli elementi associati a 2 sono 2 e  $-2$ . Pertanto 2 non è associato a  $1 \pm \sqrt{-5}$ , il che prova che le due fattorizzazioni sono essenzialmente diverse e quindi che  $R$  non è un dominio a fattorizzazione unica.

La proprietà fondamentale dei numeri primi è che, se un primo divide un prodotto, allora divide uno dei fattori. Diremo che un elemento  $p$  di un dominio di integrità  $R$  è *primo* se possiede tali proprietà, ossia se  $p$  è non nullo e non è un'unità, e inoltre, se  $p$  divide un prodotto di elementi di  $R$ , allora divide uno dei fattori. Queste sono le proprietà da cui discende l'unicità della fattorizzazione.

(2.8) PROPOSIZIONE Sia  $R$  un dominio di integrità. Supponiamo che esista in  $R$  una fattorizzazione in elementi irriducibili. Allora  $R$  è un dominio a fattorizzazione unica se e soltanto se ogni elemento irriducibile è primo.

La dimostrazione è una semplice estensione delle argomentazioni utilizzate in (1.3) e (1.4), ed è lasciata come esercizio. ■

È importante fare distinzione tra i due concetti di elemento irriducibile ed elemento primo. Essi sono equivalenti nei domini a fattorizzazione unica, ma la maggior parte degli anelli contengono elementi irriducibili che non sono primi. Per esempio, nell'anello  $R = \mathbb{Z}[\sqrt{-5}]$  considerato prima, l'elemento 2 non ha fattori propri e pertanto è irriducibile. Tuttavia non è primo, poiché, sebbene divida il prodotto  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , non divide nessuno dei fattori.

Poiché gli elementi irriducibili in un dominio a fattorizzazione unica sono primi, le espressioni *fattorizzazione in elementi irriducibili* e *fattorizzazione in elementi primi* sono sinonime. Possiamo usarle indifferentemente quando lavoriamo in un dominio a fattorizzazione unica, ma non negli altri casi.

In un dominio a fattorizzazione unica, per stabilire se un elemento  $a$  divide un altro elemento  $b$ , basta considerare le rispettive fattorizzazioni in elementi irriducibili (o primi):

(2.9) PROPOSIZIONE *Sia  $R$  un dominio a fattorizzazione unica e siano  $a = p_1 \cdots p_r$ ,  $b = q_1 \cdots q_s$  fattorizzazioni in elementi primi di due elementi di  $R$ . Allora  $a$  divide  $b$  in  $R$  se e soltanto se  $s \geq r$ , e a meno di un eventuale riordinamento dei fattori di  $b$ ,  $p_i$  e  $q_i$  sono associati per  $i = 1, \dots, r$ .* ■

(2.10) COROLLARIO *Sia  $R$  un dominio a fattorizzazione unica, e siano  $a, b$  elementi di  $R$  non entrambi nulli. Allora esiste un massimo comune divisore  $d$  di  $a, b$ , con le seguenti proprietà:*

- (i)  $d$  divide  $a, b$ ;
  - (ii) se un elemento  $e$  di  $R$  divide  $a, b$ , allora  $e$  divide  $d$ .
- 

Dalla seconda condizione segue immediatamente che due massimi comuni divisori arbitrari di  $a, b$  sono associati. Tuttavia, *il massimo comune divisore non ha necessariamente la forma  $ra+sb$* . Per esempio, dimostreremo nel prossimo paragrafo [cfr. (3.8)] che l'anello dei polinomi a coefficienti interi  $\mathbb{Z}[x]$  è un dominio a fattorizzazione unica. In questo anello, gli elementi 2 e  $x$  hanno massimo comune divisore 1, ma 1 non è una loro combinazione lineare a coefficienti polinomi interi.

Un'altra proprietà importante dell'anello degli interi è che ogni ideale di  $\mathbb{Z}$  è principale. Un dominio di integrità in cui ogni ideale è principale è chiamato *dominio a ideali principali*.

### (2.11) PROPOSIZIONE

- (a) *In un dominio di integrità, un elemento primo è irriducibile.*
- (b) *In un dominio a ideali principali, un elemento irriducibile è primo.*

Le dimostrazioni di (2.9-2.11) sono lasciate come esercizi. ■

### (2.12) TEOREMA *Un dominio a ideali principali è un dominio a fattorizzazione unica.*

**Dimostrazione.** Supponiamo che  $R$  sia un dominio a ideali principali. Allora ogni elemento irriducibile di  $R$  è primo; quindi, in base alla proposizione (2.8), dobbiamo dimostrare soltanto l'esistenza in  $R$  di una fattorizzazione in elementi irriducibili. In virtù della proposizione (2.3), ciò equivale a dimostrare che  $R$  non contiene catene ascendenti infinite di ideali principali. Infatti, supponendo per assurdo che  $(a_1) < (a_2) < (a_3) < \dots$  sia una catena siffatta, otterremo una contraddizione.

### (2.13) LEMMA *Sia $R$ un anello arbitrario. L'unione di una catena ascendente di ideali $I_1 \subset I_2 \subset I_3 \subset \dots$ è un ideale.*

**Dimostrazione.** Denotiamo con  $I$  l'unione degli ideali della catena. Se  $u, v$  appartengono a  $I$ , essi appartengono a  $I_n$  per qualche  $n$ . Pertanto  $u+v$  e  $ru$  (con  $r \in R$ ) appartengono anch'essi a  $I_n$ , e quindi appartengono a  $I$ . ■

Applichiamo questo lemma all'unione  $I$  della catena di ideali principali in esame e utilizziamo l'ipotesi che  $R$  è un dominio a ideali principali per concludere che  $I$  è principale, diciamo  $I = (b)$ . Ora, poiché  $b$  appartiene all'unione degli ideali  $(a_n)$ ,  $b$  appartiene ad uno di questi ideali. Ma se  $b \in (a_n)$ , allora  $(b) \subset (a_n)$ , e d'altra parte  $(a_n) \subset (a_{n+1}) \subset (b)$ . Pertanto  $(a_n) = (a_{n+1}) = (b)$ . Ciò contraddice l'ipotesi che  $(a_n) < (a_{n+1})$ , e tale contraddizione completa la dimostrazione. ■

L'inverso del teorema (2.12) non vale. Per esempio, l'anello  $\mathbb{Z}[x]$  dei polinomi a coefficienti interi è un dominio a fattorizzazione unica [cfr. (3.8)], ma non è un dominio a ideali principali.

### (2.14) PROPOSIZIONE

- (a) *Sia  $p$  un elemento non nullo di un dominio a ideali principali  $R$ . Allora  $R/(p)$  è un campo se e soltanto se  $p$  è irriducibile.*
- (b) *Gli ideali massimali di un dominio a ideali principali sono gli ideali principali generati dagli elementi irriducibili.*

**Dimostrazione.** Poiché un ideale  $M$  è massimale se e soltanto se  $R/M$  è un campo, le due parti dell'enunciato sono equivalenti. Dimostreremo la seconda parte. Un ideale principale  $(a)$  contiene un altro ideale principale  $(b)$  se e soltanto se  $a$  divide  $b$ . Gli unici divisori di un elemento irriducibile  $p$  sono le unità e gli associati di  $p$ . Pertanto gli unici ideali principali che contengono  $(p)$  sono  $(p)$  e  $(1)$ . Poiché ogni ideale di  $R$  è principale, ciò prova che un elemento irriducibile genera un ideale massimale. Viceversa, sia  $b$  un elemento avente una fattorizzazione propria  $b = aq$ , dove né  $a$  né  $q$  sono unità. Allora  $(b) < (a) < (1)$ , e ciò prova che  $(b)$  non è massimale. ■

Passiamo ora a estendere, da un punto di vista generale, il procedimento della divisione con resto. Per fare ciò, abbiamo bisogno di una nozione di *grandezza* di un elemento di un anello. Grandezze appropriate sono ad esempio:

- |                               |   |
|-------------------------------|---|
| valore assoluto,              | se $R = \mathbb{Z}$ ,                                   |
| (2.15) grado di un polinomio, | se $R = F[x]$ ,   |
|                               | $(\text{valore assoluto})^2$ , se $R = \mathbb{Z}[i]$ . |

In generale, una *funzione di grandezza* su un dominio di integrità  $R$  è una funzione

$$(2.16) \quad \sigma : R - \{0\} \rightarrow \{0, 1, 2, \dots\}$$

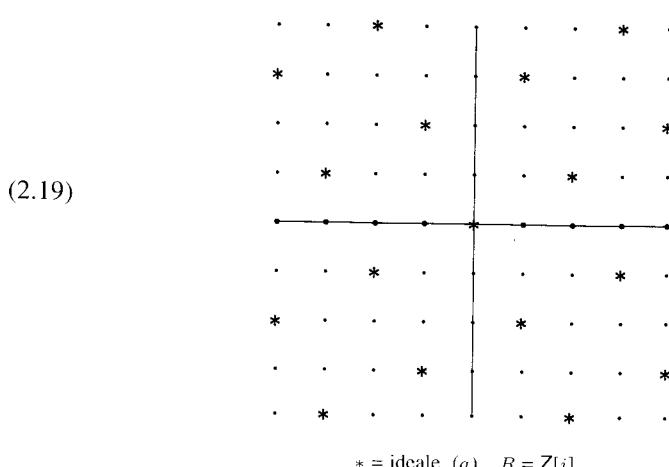
dall'insieme degli elementi non nulli di  $R$  all'insieme degli interi non negativi. Un dominio di integrità  $R$  è un *dominio euclideo* se esiste una funzione di grandezza  $\sigma$  su  $R$  tale che valga l'algoritmo della divisione con resto:

- (2.17) Siano  $a, b \in R$  e supponiamo che  $a \neq 0$ . Allora esistono elementi  $q, r \in R$  tali che  $b = aq + r$ , e inoltre  $r = 0$  oppure  $\sigma(r) < \sigma(a)$ .

Non richiediamo che gli elementi  $q, r$  siano determinati univocamente da  $a$  e  $b$ .

(2.18) PROPOSIZIONE Gli anelli  $\mathbb{Z}$ ,  $F[x]$ ,  $\mathbb{Z}[i]$  sono domini euclidei.

L'anello degli interi e l'anello dei polinomi sono stati già studiati. Dimostriamo ora che l'anello degli interi di Gauss è un dominio euclideo, avente come funzione di misura la funzione  $\sigma = |\cdot|^2$ . Gli elementi di  $\mathbb{Z}[i]$  formano un reticolo quadrato nel piano complesso, e i multipli di un elemento  $a$  assegnato formano un *reticolo simile*, precisamente l'ideale  $(a) = Ra$ . Se scriviamo  $a = re^{i\theta}$ , allora  $(a)$  si ottiene mediante una rotazione di un angolo  $\theta$  seguita da una "dilatazione" determinata dal fattore  $r = |a|$ :



Sappiamo che, per ogni numero complesso  $b$ , esiste almeno un punto del reticolo  $(a)$  alla distanza da  $b$ , elevata al quadrato, è  $\leq \frac{1}{2}|a|^2$ . Sia  $aq$  quel punto, e poniamo  $r^2 = b - aq$ . Allora  $|r|^2 \leq \frac{1}{2}|a|^2 < |a|^2$ , come richiesto. Si noti che, poiché l'elemento  $aq$  può essere scelto in più modi, questa divisione con resto non è unica.

Potremmo procedere anche algebricamente. Dividiamo il numero complesso  $b$  per  $a$ , sicché  $b = aw$ , dove  $w = x + yi$  non è necessariamente un intero di Gauss. Allora scegliamo il punto a coordinate intere  $(m, n)$  più vicino a  $(x, y)$ , scrivendo  $x = m + x_0$ ,  $y = n + y_0$ , dove  $m, n$  sono interi e  $x_0, y_0$  sono numeri reali tali che  $-\frac{1}{2} \leq x_0, y_0 < \frac{1}{2}$ . Allora  $(m+ni)a$  è il punto richiesto di  $Ra$ . Infatti,  $|x_0 + y_0 i|^2 < \frac{1}{2}$  e

$$|b - (m+ni)a|^2 = |a(x_0 + y_0 i)|^2 < \frac{1}{2}|a|^2. \blacksquare$$

Si può copiare la trattazione della fattorizzazione degli interi con qualche piccola variazione per dimostrare la proposizione seguente:

(2.20) PROPOSIZIONE Un dominio euclideo è un dominio a ideali principali, e quindi è un dominio a fattorizzazione unica. ■

(2.21) COROLLARIO Gli anelli  $\mathbb{Z}$ ,  $\mathbb{Z}[i]$ ,  $F[x]$  (essendo  $F$  un campo) sono domini a ideali principali e domini a fattorizzazione unica. ■

Nell'anello  $\mathbb{Z}[i]$  degli interi di Gauss l'elemento 3 è irriducibile, dunque primo, ma 2 e 5 non sono irriducibili, poiché

$$(2.22) \quad 2 = (1+i)(1-i) \quad \text{e} \quad 5 = (2+i)(2-i).$$

Queste sono le fattorizzazioni in fattori primi di 2 e 5 in  $\mathbb{Z}[i]$ .

Nell'anello  $\mathbb{Z}[i]$  vi sono quattro unità, precisamente  $\{\pm 1, \pm i\}$ , e pertanto ogni elemento non nullo  $\alpha$  ha quattro associati, precisamente gli elementi  $\pm \alpha$ ,  $\pm i\alpha$ . Per esempio, gli associati di  $2+i$  sono:

$$2+i, -2-i, -1+2i, 1-2i.$$

Non vi è nessun modo davvero naturale per normalizzare gli elementi primi in  $\mathbb{Z}[i]$ , anche se, in caso di necessità, sceglieremmo l'unico associato che sta nel primo quadrante e non appartiene all'asse immaginario. Tutto sommato, è meglio accettare l'ambiguità della (2.5), oppure lavorare con gli ideali principali.

### 3 Il lemma di Gauss

Il teorema (1.5) si applica, in particolare, all'anello  $\mathbb{Q}[x]$  dei polinomi a coefficienti razionali: ogni polinomio  $f(x) \in \mathbb{Q}[x]$  può essere espresso in modo unico nella forma  $cp_1 \cdots p_k$ , dove  $c \in \mathbb{Q}$  e i  $p_i$  sono polinomi monici irriducibili su  $\mathbb{Q}$ . Supponiamo ora che un polinomio  $f(x)$  abbia coefficienti interi, ossia  $f(x) \in \mathbb{Z}[x]$ ; è possibile fattorizzare  $f$  in  $\mathbb{Z}[x]$ ? Dimostreremo che ciò è possibile, e che  $\mathbb{Z}[x]$  è un dominio a fattorizzazione unica.

Ecco un esempio di fattorizzazione in fattori primi in  $\mathbb{Z}[x]$ :

$$6x^3 + 9x^2 + 9x + 3 = 3(2x+1)(x^2+x+1).$$

Come si vede in questo esempio, le scomposizioni in fattori irriducibili sono leggermente più complicate in  $\mathbb{Z}[x]$  che in  $\mathbb{Q}[x]$ . Innanzitutto, i numeri primi sono elementi irriducibili di  $\mathbb{Z}[x]$ , e pertanto essi possono comparire nella scomposizione in fattori primi di un polinomio. In secondo luogo, il fattore  $2x+1$  non è monico. Se vogliamo restare con i coefficienti interi, non possiamo richiedere fattori monici.

I fattori interi di un polinomio  $f(x) = a_n x^n + \dots + a_0$  in  $\mathbb{Z}[x]$  sono divisori comuni dei suoi coefficienti  $a_0, \dots, a_n$ . Un polinomio  $f(x)$  si dice *primitivo*, se i suoi coefficienti  $a_0, \dots, a_n$  non hanno divisori interi comuni diversi dalle unità  $\pm 1$  e se il suo coefficiente direttore  $a_n$  è positivo.

(3.1) LEMMA *Ogni polinomio non nullo  $f(x) \in \mathbb{Q}[x]$  può essere scritto in modo unico come un prodotto:*

$$f(x) = cf_0(x),$$

where  $c$  è un numero razionale e  $f_0(x)$  è un polinomio primitivo in  $\mathbb{Z}[x]$ . Il polinomio  $f$  ha coefficienti interi se e soltanto se  $c$  è un intero. In tal caso,  $|c|$  è il massimo comune divisore dei coefficienti di  $f$ , e il segno di  $c$  è il segno del coefficiente direttore di  $f$ .

Il numero razionale  $c$  che compare in questo lemma è chiamato il *contenuto* di  $f(x)$ . Se  $f$  ha coefficienti interi, il contenuto divide  $f$  in  $\mathbb{Z}[x]$ . Inoltre,  $f$  è primitivo se e soltanto se il suo contenuto è 1.

*Dimostrazione.* Per trovare  $f_0$ , innanzitutto moltiplichiamo  $f$  per un intero per eliminare i denominatori nei suoi coefficienti. Ciò fornirà un polinomio  $f_1$  a coefficienti interi. Mettiamo poi in evidenza il massimo comune divisore dei coefficienti di  $f_1$  e cambiamo eventualmente il segno del coefficiente direttore. Il polinomio  $f_0$  così ottenuto è primitivo, e  $f = cf_0$  per qualche numero razionale  $c$ .

Per dimostrare l'unicità, supponiamo che  $cf_0(x) = dg_0(x)$ , dove  $c, d \in \mathbb{Q}$  e  $f_0, g_0$  sono polinomi primitivi. Proveremo che  $c = d$  e  $f_0 = g_0$ . Eliminando i denominatori, ci riduciamo al caso in cui  $c$  e  $d$  sono interi. Denotiamo con  $\{a_i\}, \{b_i\}$ ,

rispettivamente, i coefficienti di  $f_0, g_0$ . Allora  $ca_i = db_i$  per ogni  $i$ . Poiché il massimo comune divisore di  $\{a_0, \dots, a_n\}$  è 1,  $c$  è il massimo comune divisore di  $\{ca_0, \dots, ca_n\}$ . Similmente,  $d$  è il massimo comune divisore di  $\{db_0, \dots, db_n\} = \{ca_0, \dots, ca_n\}$ . Ne segue che  $c = \pm d$  e  $f_0 = \pm g_0$ . Poiché  $f_0$  e  $g_0$  hanno coefficienti direttori positivi,  $f_0 = g_0$  e  $c = d$ . Se  $f$  ha coefficienti interi, non occorre eliminare i denominatori; pertanto  $c$  è un intero e, a meno eventualmente del segno, esso è il massimo comune divisore dei coefficienti, come enunciato. ■

Come abbiamo già osservato, il principio di sostituzione fornisce un omomorfismo

$$(3.2) \quad \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x],$$

dove  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  è il campo con  $p$  elementi. Tale omomorfismo manda un polinomio  $f(x) = a_m x^m + \dots + a_0$  nel suo resto (modulo  $p$ )  $\bar{f}(x) = \bar{a}_m x^m + \dots + \bar{a}_0$ . Utilizzeremo ciò per dimostrare il lemma di Gauss.

(3.3) TEOREMA (Lemma di Gauss) *Un prodotto di polinomi primitivi in  $\mathbb{Z}[x]$  è primitivo.*

*Dimostrazione.* Siano  $f, g$  due polinomi primitivi, e sia  $h = fg$  il loro prodotto. Poiché i coefficienti direttori di  $f$  e  $g$  sono positivi, tale risulta anche il coefficiente direttore di  $h$ . Per dimostrare che  $h$  è primitivo, basterà provare che nessun primo  $p$  divide tutti i coefficienti di  $h(x)$ . Ne seguirà che il contenuto di  $h$  è 1. Consideriamo l'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$  definito sopra. Dobbiamo dimostrare che  $\bar{h} \neq 0$ . Poiché  $f$  è primitivo, i suoi coefficienti non sono tutti divisibili per  $p$ . Pertanto  $\bar{f} \neq 0$ . Similmente  $\bar{g} \neq 0$ . Poiché l'anello dei polinomi  $\mathbb{F}_p[x]$  è un dominio di integrità,  $\bar{h} = \bar{f}\bar{g} \neq 0$ , come richiesto. ■

#### (3.4) PROPOSIZIONE

- (a) *Siano  $f, g$  polinomi in  $\mathbb{Q}[x]$ , e siano  $f_0, g_0$  i polinomi primitivi associati in  $\mathbb{Z}[x]$ . Se  $f$  divide  $g$  in  $\mathbb{Q}[x]$ , allora  $f_0$  divide  $g_0$  in  $\mathbb{Z}[x]$ .*
- (b) *Sia  $f$  un polinomio primitivo in  $\mathbb{Z}[x]$ , e sia  $g$  un qualsiasi polinomio a coefficienti interi. Supponiamo che  $f$  divida  $g$  in  $\mathbb{Q}[x]$ , diciamo  $g = fq$ , con  $q \in \mathbb{Q}[x]$ . Allora  $q \in \mathbb{Z}[x]$ , e quindi  $f$  divide  $g$  in  $\mathbb{Z}[x]$ .*
- (c) *Siano  $f, g$  polinomi in  $\mathbb{Z}[x]$ . Se essi hanno un fattore comune non costante in  $\mathbb{Q}[x]$ , allora essi hanno un fattore comune non costante anche in  $\mathbb{Z}[x]$ .*

*Dimostrazione.* Per dimostrare (a), possiamo eliminare i denominatori in modo tale che  $f$  e  $g$  diventino primitivi. Allora (a) è una conseguenza di (b). Per dimostrare (b), applichiamo (3.1) per scrivere il quoziente nella forma  $q = cq_0$ , dove  $q_0$  è un polinomio primitivo e  $c \in \mathbb{Q}$ . In base al lemma di Gauss,  $f q_0$  è

primitivo, e l'espressione  $g = cfq_0$  prova che esso è il polinomio primitivo  $g_0$  associato a  $g$ . Pertanto  $g = cq_0$  è l'espressione per  $g$  fornita dal lemma (3.1), e  $c$  è il contenuto di  $g$ . Poiché  $g \in \mathbb{Z}[x]$ , ne segue che  $c \in \mathbb{Z}$ , e quindi che  $q \in \mathbb{Z}[x]$ . Infine, per dimostrare (c), supponiamo che  $f, g$  abbiano un fattore comune  $h$  in  $\mathbb{Q}[x]$ . Possiamo supporre che  $h$  sia primitivo, e allora da (b) segue che  $h$  divide sia  $f$  che  $g$  in  $\mathbb{Z}[x]$ . ■

(3.5) COROLLARIO *Se un polinomio non costante è irriducibile in  $\mathbb{Z}[x]$  è irriducibile anche in  $\mathbb{Q}[x]$ .* ■

(3.6) PROPOSIZIONE *Sia  $f$  un polinomio a coefficienti interi con coefficiente direttore positivo. Allora  $f$  è irriducibile in  $\mathbb{Z}[x]$  se e soltanto se  $f$  soddisfa ad una delle seguenti condizioni:*

- (i)  $f$  è un numero primo, oppure
- (ii)  $f$  è un polinomio primitivo che è irriducibile in  $\mathbb{Q}[x]$ .

*Dimostrazione.* Supponiamo che  $f$  sia irriducibile. In base al lemma (3.1), possiamo scrivere  $f = cf_0$ , dove  $f_0$  è primitivo. Poiché  $f$  è irriducibile, non possono esistere fattori propri. Pertanto o  $c$  o  $f_0$  è uguale a 1. Se  $f_0 = 1$ , allora  $f$  è costante, e un polinomio costante irriducibile è necessariamente un numero primo. Se  $c = 1$ , allora  $f$  è primitivo, ed è irriducibile in  $\mathbb{Q}[x]$  in virtù del corollario precedente. Il viceversa, ossia il fatto che i numeri primi e i polinomi irriducibili primitivi sono elementi irriducibili di  $\mathbb{Z}[x]$ , è chiaro. ■

(3.7) PROPOSIZIONE *Ogni elemento irriducibile di  $\mathbb{Z}[x]$  è un elemento primo.*

*Dimostrazione.* Sia  $f$  irriducibile in  $\mathbb{Z}[x]$ , e supponiamo che  $f$  divida  $gh$ , dove  $g, h \in \mathbb{Z}[x]$ .

*Caso 1:*  $f = p$  è un numero primo. Scriviamo, in base a (3.1),  $g = cq_0$  e  $h = dq_0$ . Allora  $g_0h_0$  è primitivo, e pertanto qualche coefficiente, diciamo  $a$ , di  $g_0h_0$  non è divisibile per  $p$ . Ma poiché  $p$  divide  $gh$ , il coefficiente corrispondente, che è  $eda$ , è divisibile per  $p$ . Ne segue che  $p$  divide  $c$  o  $d$ , e quindi  $p$  divide  $g$  o  $h$ .

*Caso 2:*  $f$  è un polinomio primitivo che è irriducibile in  $\mathbb{Q}[x]$ . In base a (2.11b),  $f$  è un elemento primo di  $\mathbb{Q}[x]$ . Pertanto  $f$  divide  $g$  o  $h$  in  $\mathbb{Q}[x]$ . In virtù di (3.4),  $f$  divide  $g$  o  $h$  in  $\mathbb{Z}[x]$ . ■

(3.8) TEOREMA *L'anello dei polinomi  $\mathbb{Z}[x]$  è un dominio a fattorizzazione unica. Ogni polinomio non nullo  $f(x) \in \mathbb{Z}[x]$ , diverso da  $\pm 1$ , si può scomporre in un prodotto*

$$f(x) = \pm p_1 \cdots p_m q_1(x) \cdots q_n(x),$$

*se i  $p_i$  sono numeri primi e i  $q_i(x)$  sono polinomi primitivi irriducibili. Tale espressione è unica a meno di un riordinamento dei fattori.*

*L'esistenza di una fattorizzazione si dimostra facilmente per  $\mathbb{Z}[x]$ , e pertanto questo teorema segue dalle proposizioni (3.7) e (2.8).* ■

Sia ora  $R$  un dominio a fattorizzazione unica, e sia  $F$  il suo campo delle frazioni [cap. 10 (6.5)]. Allora  $R[x]$  è un sottoanello di  $F[x]$ , e i risultati di questo paragrafo possono essere generalizzati, sostituendo dappertutto  $\mathbb{Z}$  con  $R$  e  $\mathbb{Q}$  con  $F$ . L'unico cambiamento da fare è che, invece di normalizzare i polinomi primitivi è meglio accettare l'ambiguità dovuta ai fattori invertibili, come nel paragrafo precedente. I risultati principali sono i seguenti:

(3.9) TEOREMA *Sia  $R$  un dominio a fattorizzazione unica con campo delle frazioni  $F$ .*

- (a) *Siano  $f, g$  polinomi in  $F[x]$ , e siano  $f_0, g_0$  i polinomi primitivi associati in  $R[x]$ . Se  $f$  divide  $g$  in  $F[x]$ , allora  $f_0$  divide  $g_0$  in  $R[x]$ .*
- (b) *Sia  $f$  un polinomio primitivo in  $R[x]$ , e sia  $g$  un polinomio arbitrario in  $R[x]$ . Supponiamo che  $f$  divida  $g$  in  $F[x]$ , cioè che ad esempio  $g = fq$ , con  $q \in F[x]$ . Allora  $q \in R[x]$ , e quindi  $f$  divide  $g$  in  $R[x]$ .*
- (c) *Siano  $f, g$  polinomi in  $R[x]$ . Se essi hanno un fattore comune non costante in  $F[x]$ , allora essi hanno un fattore comune non costante anche in  $R[x]$ .*
- (d) *Se un polinomio non costante  $f$  è irriducibile in  $R[x]$ , allora esso è irriducibile in  $F[x]$ .*
- (e)  *$R[x]$  è un dominio a fattorizzazione unica.*

La dimostrazione ricalca quella data per l'anello  $\mathbb{Z}[x]$ , e pertanto viene omessa. ■

Poiché  $R[x_1, \dots, x_n] \approx R[x_1, \dots, x_{n-1}][x_n]$ , si ottiene il seguente corollario:

(3.10) COROLLARIO *Gli anelli di polinomi  $\mathbb{Z}[x_1, \dots, x_n]$  e  $F[x_1, \dots, x_n]$ , dove  $F$  è un campo, sono domini a fattorizzazione unica.* ■

Pertanto l'anello  $\mathbb{C}[x, y]$  dei polinomi complessi in due variabili è un dominio a fattorizzazione unica. Tuttavia, a differenza di ciò che accade nel caso di una variabile, in cui ogni polinomio complesso è un prodotto di fattori lineari, i polinomi complessi in due variabili sono spesso irriducibili, e quindi primi.

L'irriducibilità di un polinomio  $f(x, y)$  può essere dimostrata talvolta studiando il luogo  $W = \{f(x, y) = 0\}$  in  $\mathbb{C}^2$ . Supponiamo che  $f$  si fattorizzi in  $\mathbb{C}[x, y]$ :

$$f(x, y) = g(x, y)h(x, y),$$

dove  $g, h$  sono polinomi non costanti. Allora  $f(x, y) = 0$  se e soltanto se è soddisfatta una delle due equazioni  $g(x, y) = 0$  oppure  $h(x, y) = 0$ . Pertanto, se denotiamo con  $U = \{g(x, y) = 0\}$ ,  $V = \{h(x, y) = 0\}$  le due varietà corrispondenti in  $\mathbb{C}^2$ , risulta:

$$W = U \cup V.$$

Talvolta si vede geometricamente che  $W$  non si può scomporre in questo modo. Per esempio, possiamo usare questo metodo per dimostrare che il polinomio

$$f(x, y) = x^2 + y^2 - 1$$

è irriducibile. Poiché il grado totale di  $f$  è 2, ogni divisore proprio di  $f$  deve essere lineare, ossia della forma  $ax+by+c$ . Ora le soluzioni di un'equazione lineare giacciono su una retta, mentre  $\{f=0\}$  è una circonferenza. Naturalmente, quando parliamo di rette e circonferenze, parliamo in realtà dei luoghi reali in  $\mathbb{R}^2$ . Pertanto, questa argomentazione prova che  $f$  è irriducibile in  $\mathbb{R}[x, y]$ . Ma di fatto, il luogo reale di una circonferenza ha abbastanza punti per provare l'irriducibilità anche in  $\mathbb{C}[x, y]$ . Supponiamo che  $f = gh$  in  $\mathbb{C}[x, y]$ , dove  $g$  e  $h$  sono polinomi lineari come in precedenza. Allora ogni punto della circonferenza reale  $x^2 + y^2 - 1 = 0$  giace su uno dei due luoghi complessi  $U, V$ . Pertanto almeno uno di questi luoghi contiene due punti reali. Esiste una ed una sola retta complessa (essendo una retta il luogo delle soluzioni di un'equazione lineare  $ax + by + c = 0$ ) che passa per due punti assegnati, e se questi punti sono reali, l'equazione lineare che definisce la retta è anch'essa reale, a meno di un fattore costante. Ciò si dimostra scrivendo esplicitamente l'equazione di una retta per due punti. Pertanto, se  $f$  ha un fattore lineare, allora  $f$  ha un fattore lineare reale. Ma la circonferenza non contiene una retta.

Si può dimostrare anche algebricamente che  $x^2 + y^2 - 1$  è irriducibile, utilizzando il metodo dei coefficienti indeterminati (cfr. § 4, esercizio 18).

#### 4 Fattorizzazione esplicita dei polinomi

Ci poniamo ora il problema di determinare i fattori di un dato polinomio a coefficienti interi:

$$(4.1) \quad f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Ciò che cerchiamo sono i fattori irriducibili in  $\mathbb{Q}[x]$ , e in base al corollario (3.5), ciò equivale a determinare i fattori irriducibili in  $\mathbb{Z}[x]$ . I fattori lineari si possono trovare abbastanza facilmente. Se  $b_1 x + b_0$  divide  $f(x)$ , allora  $b_1$  divide  $a_n$  e  $b_0$  divide  $a_0$ . Gli interi che dividono  $a_n$  e  $a_0$  sono in numero finito, sicché possiamo esaminare tutti i casi possibili. In ciascun caso, effettuiamo la divisione

cerchiamo se il resto è zero. Oppure possiamo sostituire il numero razionale  $-b_0/b_1$  in  $f(x)$  per vedere se è una radice.

Sebbene la situazione non sia tanto chiara per i fattori di grado più alto, Kronecker dimostrò che i fattori possono essere determinati mediante un numero finito di operazioni. Il suo metodo è basato sulla formula di interpolazione di Lagrange. Purtroppo è poco pratico, poiché richiede troppi passi, tranne che per fattori di grado basso. Sul problema dell'efficienza dei calcoli si è lavorato molto. Uno dei metodi più utili è il calcolo modulo  $p$ , che utilizza l'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$ . Se il polinomio  $f(x)$  si fattorizza in  $\mathbb{Z}[x]$ :  $f = gh$ , allora anche il suo resto  $\bar{f}(x)$  modulo  $p$  si fattorizza:  $\bar{f} = \bar{g}\bar{h}$ . Inoltre, poiché in  $\mathbb{F}_p[x]$  i polinomi di un qualsiasi grado sono in numero finito, tutte le fattorizzazioni in  $\mathbb{F}_p[x]$  possono essere effettuate in un numero finito di passi.

(4.2) PROPOSIZIONE Sia  $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$  un polinomio a coefficienti interi, e sia  $p$  un numero primo che non divida  $a_n$ . Se il resto  $\bar{f}$  di  $f$  modulo  $p$  è irriducibile, allora  $f$  è irriducibile in  $\mathbb{Q}[x]$ .

*Dimostrazione.* Ciò segue da un esame attento dell'omomorfismo. Abbiamo bisogno dell'ipotesi che  $p$  non divida  $a_n$  allo scopo di escludere la possibilità che un fattore  $g$  di  $f$  possa ridursi ad una costante in  $\mathbb{F}_p[x]$ . Tale ipotesi si mantiene, se sostituiamo  $f$  con il polinomio primitivo associato. Pertanto possiamo supporre che  $f$  sia primitivo. Poiché  $p$  non divide  $a_n$ , i gradi di  $f$  e  $\bar{f}$  sono uguali. Se  $f$  si fattorizza in  $\mathbb{Q}[x]$ , allora esso si fattorizza anche in  $\mathbb{Z}[x]$ , in virtù del corollario (3.5). Sia  $f = gh$  una fattorizzazione propria in  $\mathbb{Z}[x]$ . Poiché  $f$  è primitivo,  $g$  e  $h$  hanno gradi positivi. Inoltre, poiché  $\deg f = \deg \bar{f}$  e  $\bar{f} = \bar{g}\bar{h}$ , ne segue che  $\deg g = \deg \bar{g}$  e  $\deg h = \deg \bar{h}$ , e quindi che  $\bar{f} = \bar{g}\bar{h}$  è una fattorizzazione propria, il che prova che  $\bar{f}$  è riducibile. ■

Se sospettiamo che un dato polinomio  $f(x) \in \mathbb{Z}[x]$  sia irriducibile, possiamo provare ad effettuare la riduzione modulo  $p$  per qualche numero primo piccolo, per esempio  $p = 2$  o  $3$ , e sperare che  $\bar{f}$  risulti un polinomio dello stesso grado e irriducibile. In tal caso, avremo dimostrato che anche  $f$  è irriducibile. Si noti inoltre che, poiché  $\mathbb{F}_p$  è un campo, i risultati del teorema (1.5) valgono per l'anello  $\mathbb{F}_p[x]$ .

Il metodo di riduzione modulo  $p$  funziona abbastanza spesso, ma non sempre; infatti esistono polinomi a coefficienti interi che sono irriducibili, sebbene essi possano essere fattorizzati modulo  $p$  per ogni primo  $p$ . Un esempio è dato dal polinomio  $x^4 - 10x^2 + 1$ .

I polinomi irriducibili in  $\mathbb{F}_p[x]$  si possono trovare con il metodo "del crivello". Il crivello di Eratostene è il nome dato al metodo seguente per la determinazione dei numeri primi minori di un numero  $n$  assegnato. Scriviamo in ordine gli interi da 2 a  $n$ . Il primo intero, 2, è primo poiché ogni fattore proprio di 2 deve essere più piccolo di 2, e non vi sono interi più piccoli nella nostra lista. Prendiamo

nota del fatto che 2 è primo e cancelliamo poi con un tratto di penna i multipli di 2 dalla nostra lista, i quali non sono primi. Il primo intero che rimane è 3, che è primo poiché non è divisibile per nessun primo più piccolo. Annotiamo il fatto che 3 è primo e cancelliamo poi con un tratto di penna i multipli di 3 dalla nostra lista. Di nuovo, il più piccolo intero che rimane, 5, è primo, e così via.

$$2 \ 3 \cancel{4} \ 5 \cancel{6} \ 7 \cancel{8} \ 9 \cancel{10} \ 11 \cancel{12} \ 13 \ 14 \cancel{15} \ 16 \ 17 \cancel{18} \ 19 \dots$$

Questo metodo permetterà di determinare anche i polinomi irriducibili in  $\mathbb{F}_p[x]$ . Elenchiamo tutti i polinomi, grado per grado, e poi cancelliamo con un tratto di penna i prodotti. Per esempio, i polinomi lineari in  $\mathbb{F}_2[x]$  sono  $x$  e  $x+1$ , e sono irriducibili. I polinomi di grado 2 sono  $x^2$ ,  $x^2+x$ ,  $x^2+1$ ,  $x^2+x+1$ . I primi tre sono divisibili per  $x$  o per  $x+1$ , sicché l'ultimo è l'unico polinomio irriducibile di grado 2 su  $\mathbb{F}_2$ .

(4.3) *I polinomi irriducibili di grado  $\leq 4$  su  $\mathbb{F}_2$  sono:*

$$\begin{aligned} &x, \ x+1; \quad x^2+x+1; \quad x^3+x^2+1, \ x^3+x+1; \\ &x^4+x^3+1, \ x^4+x+1, \ x^4+x^3+x^2+x+1. \end{aligned}$$

Facendo le prove con i polinomi di questa lista, possiamo fattorizzare tutti i polinomi di grado  $\leq 9$  in  $\mathbb{F}_2[x]$ .

Come esempio di applicazione di (4.2), il polinomio  $x^4 - 6x^3 + 12x^2 - 3x + 9$  è irriducibile in  $\mathbb{Q}[x]$ , poiché il suo resto in  $\mathbb{F}_2[x]$  è  $x^4+x+1$ .

(4.4) *I polinomi irriducibili monici di grado 2 su  $\mathbb{F}_3$  sono:*

$$x^2+1, \ x^2+x-1, \ x^2-x-1.$$

La riduzione modulo  $p$  può aiutare a descrivere la fattorizzazione di un polinomio, anche quando il resto è riducibile. Consideriamo ad esempio il polinomio  $f(x) = x^3 + 6x + 3$ , che, modulo 3, si riduce a  $x^3$ . Se  $f(x)$  fosse riducibile, diciamo  $(ax+b)(cx^2+dx+e) = x^3 + 6x + 3$ , allora  $ax+b$  dovrebbe dividere  $x^3$  in  $\mathbb{F}_3[x]$ , il che implicherebbe  $b \equiv 0$  (modulo 3). Analogamente, potremmo concludere che  $e \equiv 0$  (modulo 3). Ora queste due condizioni non possono essere entrambe soddisfatte, poiché  $be = 3$ ; quindi non esiste nessuna fattorizzazione, e  $f(x)$  è irriducibile.

Il principio utilizzato in questo esempio è chiamato *criterio di Eisenstein*.

(4.5) PROPOSIZIONE (Criterio di Eisenstein) *Sia  $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  un polinomio a coefficienti interi, e sia  $p$  un numero primo. Supponiamo che i coefficienti di  $f$  soddisfino alle seguenti condizioni:*

(i)  $p$  non divide  $a_n$ ;

**(ii)  $p$  divide gli altri coefficienti  $a_{n-1}, \dots, a_0$ ;**

**(iii)  $p^2$  non divide  $a_0$ .**

Allora  $f$  è irriducibile in  $\mathbb{Q}[x]$ . Se  $f$  è primitivo, è irriducibile anche in  $\mathbb{Z}[x]$ .

Per esempio,  $x^4 + 50x^2 + 30x + 20$  è irriducibile in  $\mathbb{Q}[x]$  e in  $\mathbb{Z}[x]$ .

**Dimostrazione.** Supponiamo che  $f$  soddisfi alle condizioni enunciate e sia  $\bar{f}$  il resto di  $f$  modulo  $p$ . Le ipotesi (i) e (ii) implicano che  $\bar{f} = \bar{a}_n x^n$  e che  $\bar{a}_n \neq 0$ . Se  $f$  è riducibile in  $\mathbb{Q}[x]$ , allora  $f$  si scomponga in  $\mathbb{Z}[x]$  in un prodotto di fattori di grado positivo, diciamo  $f = gh$ . Allora  $\bar{g}$  e  $\bar{h}$  dividono  $\bar{a}_n x^n$ , e quindi ciascuno di questi polinomi è un monomio; quindi tutti i coefficienti di  $g$  e di  $h$ , ad eccezione dei coefficienti direttori, sono divisibili per  $p$ . Siano  $b_0, c_0$ , rispettivamente, i termini noti di  $g, h$ , per cui il termine noto di  $f$  è  $a_0 = b_0 c_0$ . Poiché  $p$  divide  $b_0$  e  $c_0$ , ne segue che  $p^2$  divide  $a_0$ , il che contraddice (iii). Ciò prova che  $f$  è irriducibile. L'ultima asserzione segue dalla proposizione (3.6). ■

Una delle applicazioni più importanti del criterio di Eisenstein è la dimostrazione dell'irriducibilità del polinomio ciclotomico  $x^{p-1} + x^{p-2} + \dots + x + 1$ , le cui radici sono le radici  $p$ -esime dell'unità, ossia le potenze di  $\zeta = e^{2\pi i/p}$ :

(4.6) COROLLARIO *Sia  $p$  un numero primo. Il polinomio  $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$  è irriducibile in  $\mathbb{Q}[x]$ .*

**Dimostrazione.** Osserviamo innanzitutto che  $(x-1)f(x) = x^p - 1$ . Sostituendo in questo prodotto  $x = y+1$ , e otteniamo:

$$yf(y+1) = (y+1)^p - 1 = y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \dots + \binom{p}{p-1} y.$$

Si ha:  $\binom{p}{i} = p(p-1)\dots(p-i+1)/i!$ . Se  $i < p$ , allora il primo  $p$  non è un fattore di  $i!$ , e pertanto  $i!$  divide il prodotto  $(p-1)\dots(p-i+1)$  dei termini rimanenti nel numeratore dell'intero  $\binom{p}{i}$ . Ciò implica che  $\binom{p}{i}$  è divisibile per  $p$ . Dividendo lo sviluppo di  $yf(y+1)$  per  $y$ , si ha che  $f(y+1)$  soddisfa alle condizioni del criterio di Eisenstein, e quindi è un polinomio irriducibile. Ne segue che anche  $f(x)$  è irriducibile. ■

È istruttivo esaminare l'enunciato analogo al criterio di Eisenstein, ottenuto sostituendo l'anello degli interi con l'anello dei polinomi  $\mathbb{C}[t]$ . Allora  $\mathbb{Z}[x]$  viene sostituito da  $\mathbb{C}[t][x] \approx \mathbb{C}[t, x]$ , ossia l'anello dei polinomi in due variabili.

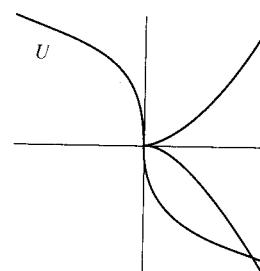
(4.7) PROPOSIZIONE Sia  $f(t, x)$  un elemento di  $\mathbb{C}[t, x]$ , scritto come un polinomio in  $x$  i cui coefficienti sono polinomi in  $t$ :  $f(t, x) = a_n(t)x^n + \dots + a_1(t)x + a_0(t)$ . Supponiamo che:

- (i)  $t$  non divide  $a_n(t)$ ;
- (ii)  $t$  divide  $a_{n-1}(t), \dots, a_0(t)$ ;
- (iii)  $t^2$  non divide  $a_0(t)$ .

Allora  $f(t, x)$  è irriducibile nell'anello  $\mathbb{C}(t)[x]$ . Inoltre, se  $f$  è primitivo, ossia se  $f$  non ha fattori che siano polinomi nella sola  $t$ , allora  $f$  è irriducibile in  $\mathbb{C}[t, x]$ .

Questa proposizione può essere dimostrata esattamente come la proposizione (4.5), sostituendo  $\mathbb{F}_p[x]$  con  $\mathbb{C}[x] = \mathbb{C}[t, x]/(t)$ . Tuttavia, esaminiamo la situazione dal punto di vista geometrico, considerando il luogo  $W = \{f(t, x) = 0\}$  nello spazio complesso di dimensione 2. Le condizioni (i) e (ii) di (4.7) implicano che  $f(0, x) = cx^n$ , dove  $c = a_n(0) \neq 0$ . Ne segue che l'unica soluzione di  $f(t, x) = 0$  con  $t = 0$  è  $t = x = 0$ , sicché la varietà  $W$  incontra l'asse  $x$  ( $t = 0$ ) soltanto nell'origine.

Supponiamo che  $f(t, x)$  sia riducibile:  $f(t, x) = g(t, x)h(t, x)$ . Allora  $W$  è l'unione delle due varietà  $U = \{g = 0\}$  e  $V = \{h = 0\}$ . Inoltre,  $cx^n = f(0, x) = g(0, x)h(0, x)$ . Ne segue che  $g(0, x)$  è il prodotto di una costante per  $x^r$ , e  $h(0, x)$  è il prodotto di una costante per  $x^{n-r}$ , dove  $r$  è il grado di  $g$  nella variabile  $x$ . Pertanto  $g$  e  $h$  si annullano entrambi nell'origine. Ne segue che l'origine è un punto singolare di  $W$ , ossia, le derivate parziali  $\partial f/\partial x$  e  $\partial f/\partial t$  si annullano entrambe in  $(0, 0)$ . Ciò si verifica derivando il prodotto  $gh$ . D'altra parte,  $\frac{\partial f}{\partial t}(0, 0) = \frac{da_0}{dt}(0)$ , e questo è il coefficiente lineare di  $a_0(t)$ . Se esso è nullo,  $t^2$  divide  $a_0(t)$ , il che contraddice l'ipotesi (4.7iii). ■



## 5 Primi nell'anello degli interi di Gauss

Abbiamo visto che l'anello degli interi di Gauss è un dominio euclideo. Le sue unità sono  $\{\pm 1, \pm i\}$ , e ogni elemento non nullo che non sia un'unità è un prodotto di elementi primi. In questo paragrafo studieremo questi elementi primi, chiamati *primi di Gauss*, e le loro relazioni con i numeri primi. Abbiamo considerato alcuni esempi nel paragrafo 2, dove abbiamo visto in particolare che il numero

5 si fattorizza in  $\mathbb{Z}[i]$ :  $5 = (2+i)(2-i)$ , mentre 3 non si fattorizza; 3 è un *numero di Gauss*. Ricordiamo che, poiché vi sono quattro unità, esistono quattro fattorizzazioni associate dell'intero 5, che sono equivalenti:

$$(2+i)(2-i) = (-2-i)(-2+i) = (1-2i)(1+2i) = (-1+2i)(-1-2i).$$

Dimostreremo ora che gli esempi dei numeri 3 e 5 rappresentano i due modi in cui i numeri primi si possono fattorizzare nell'anello  $\mathbb{Z}[i]$ . I risultati sono riassunti nel teorema seguente:

### (5.1) TEOREMA

- (a) Sia  $p$  un numero primo. Allora, o  $p$  è un primo di Gauss, o è il prodotto di due primi di Gauss complessi coniugati:  $p = \pi\bar{\pi}$ .
- (b) Sia  $\pi$  un primo di Gauss. Allora, o  $\pi\bar{\pi}$  è un numero primo, o è il quadrato di un numero primo.
- (c) I numeri primi che sono primi di Gauss sono quelli congrui a 3 modulo 4, ossia,  $p = 3, 7, 11, 19, \dots$
- (d) Sia  $p$  un numero primo. Le seguenti condizioni sono equivalenti:
  - (i)  $p$  è un prodotto di due primi di Gauss complessi coniugati;
  - (ii)  $p$  è una somma di quadrati di due interi:  $p = a^2 + b^2$ , con  $a, b \in \mathbb{Z}$ ;
  - (iii) la congruenza  $x^2 \equiv -1$  (modulo  $p$ ) ha una soluzione intera;
  - (iv)  $p \equiv 1$  (modulo 4), oppure  $p = 2$ ; ossia,  $p = 2, 5, 13, 17, \dots$

Ci vorrà un po' di tempo per dimostrare tutte le parti di questo teorema.

Il lemma seguente discende direttamente dalla definizione di intero di Gauss:

(5.2) LEMMA Un intero di Gauss che sia un numero reale è un intero ordinario. Un intero ordinario  $d$  divide un altro intero  $a$  in  $\mathbb{Z}[i]$  se e solo se  $d$  divide  $a$  in  $\mathbb{Z}$ . Inoltre,  $d$  divide un intero di Gauss  $a+bi$  se e solo se  $d$  divide sia  $a$  che  $b$ . ■

Ora, per dimostrare la parte (a) del teorema, sia  $p$  un numero primo. Allora  $p$  non è un'unità nell'anello  $\mathbb{Z}[i]$ . Ne segue che esso ha come divisore un primo di Gauss, diciamo  $\pi = a+bi$ , dove  $a, b \in \mathbb{Z}$ . Anche il complesso coniugato  $\bar{\pi} = a-bi$  divide  $p$ , poiché  $p = \bar{\pi}\pi$ , sicché  $\pi\bar{\pi} = a^2 + b^2$  divide  $p^2$  nell'anello degli interi di Gauss. Essendo un numero intero,  $\pi\bar{\pi}$  è un divisore intero di  $p^2$ . Vi sono due possibilità:  $\pi$  è un associato di  $p$ , oppure  $\pi$  è un divisore proprio di  $p$  nell'anello degli interi di Gauss. Nel primo caso,  $p$  è un primo di Gauss. Nel secondo caso,  $\pi\bar{\pi}$  è un divisore proprio di  $p^2$  nell'anello  $\mathbb{Z}$ , e pertanto, essendo  $\pi\bar{\pi}$  un intero positivo, risulta:  $\pi\bar{\pi} = p$ .

Possiamo adattare questa argomentazione per dimostrare la parte (b). Sia  $\pi$  un primo di Gauss. Allora  $\pi\bar{\pi}$  è un intero positivo, diciamo  $\pi\bar{\pi} = n$ . Fattorizziamo ora  $n$  in un prodotto di numeri primi nell'anello degli interi. Tale fattorizzazione sarà anche una fattorizzazione nell'anello degli interi di Gauss, anche se non necessariamente una fattorizzazione in elementi primi. Poiché  $\pi$  è un primo di Gauss che divide  $n$  in  $\mathbb{Z}[i]$ , esso divide uno dei numeri primi che sono fattori di  $n$ . Pertanto  $\pi$  divide un numero primo  $p$ . Allora  $\pi\bar{\pi}$  è un divisore intero di  $p^2$ , e quindi  $\pi\bar{\pi} = p$  oppure  $\pi\bar{\pi} = p^2$ .

Si noti che la parte (c) del teorema (5.1) è una conseguenza formale di (a) e dell'equivalenza delle condizioni (d)(i) e (d)(iv); passiamo dunque alla dimostrazione di (d). È facile vedere che gli enunciati (i) e (ii) sono equivalenti. Infatti, supponiamo che  $p = \pi\bar{\pi}$  per qualche primo di Gauss  $\pi = a + bi$ . Allora  $p = \pi\bar{\pi} = (a + bi)(a - bi) = a^2 + b^2$ , sicché  $p$  è una somma di quadrati di due interi. Viceversa, se  $p = a^2 + b^2$ , allora  $p = (a + bi)(a - bi)$  fornisce una fattorizzazione di  $p$  nell'anello degli interi di Gauss, la quale è una fattorizzazione in fattori primi, in virtù di (a).

L'equivalenza degli enunciati (d)(i) e (d)(iii) è più difficile da dimostrare. Torniamo indietro alla costruzione formale degli interi di Gauss: l'anello  $\mathbb{Z}[i]$  si ottiene dall'anello  $\mathbb{Z}$  aggiungendo un elemento  $i$  con la relazione  $i^2 + 1 = 0$ ; quindi vi è un isomorfismo:

$$(5.3) \quad \mathbb{Z}[x]/(x^2 + 1) \xrightarrow{\sim} \mathbb{Z}[i].$$

Denotiamo con  $(p)$  l'ideale principale generato da un numero primo  $p$  nell'anello degli interi di Gauss. I suoi elementi sono gli interi di Gauss  $a + bi$  tali che  $a$  e  $b$  sono entrambi divisibili per  $p$ . Denotiamo con  $R'$  l'anello quoziante  $\mathbb{Z}[i]/(p)$ ; allora  $R'$  può essere considerato anche come l'anello ottenuto introducendo le due relazioni:

$$(5.4) \quad x^2 + 1 = 0 \quad \text{e} \quad p = 0$$

nell'anello dei polinomi  $\mathbb{Z}[x]$ . Pertanto si ha un isomorfismo:

$$(5.5) \quad \mathbb{Z}[x]/(x^2 + 1, p) \xrightarrow{\sim} \mathbb{Z}[i]/(p) = R',$$

dove  $(x^2 + 1, p)$  denota l'ideale di  $\mathbb{Z}[x]$  generato dai due elementi.

(5.6) LEMMA *Sia  $p$  un numero primo. I seguenti enunciati sono equivalenti:*

- (i)  $p$  è un primo di Gauss;
- (ii) l'anello  $R' = \mathbb{Z}[i]/(p)$  è un campo;
- (iii)  $x^2 + 1$  è un polinomio irriducibile nell'anello  $\mathbb{F}_p[x]$ .

*Dimostrazione.* L'equivalenza dei primi due enunciati segue dalla proposizione (2.14). Ciò che stiamo davvero cercando è l'equivalenza di (i) e (iii), e a prima

occhio, non sembra affatto che questi due enunciati siano in relazione tra loro. È stato proprio per ottenere questa equivalenza che abbiamo introdotto l'anello auxiliario  $R'$ . La dimostrazione è basata sulla seguente osservazione elementare, ma particolarmente utile, conseguenza del terzo teorema di isomorfismo [cap. 10 (4.3b)]:

(5.7) *Per costruire l'anello  $R'$ , non importa quale delle due relazioni (5.4) è introdotta per prima nell'anello  $\mathbb{Z}[x]$ .*

Pertanto invertiamo l'ordine e cominciamo a mandare l'elemento  $p$  nello zero. Il principio di sostituzione ci dice quello che otterremo. Il nucleo dell'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$  è precisamente l'ideale  $p\mathbb{Z}[x]$ . Poiché tale applicazione è suriettiva, essa induce un isomorfismo

$$\mathbb{Z}[x]/p\mathbb{Z}[x] \xrightarrow{\sim} \mathbb{F}_p[x].$$

Introduciamo ora l'altra relazione  $x^2 + 1 = 0$  in questo anello, interpretando i coefficienti di questo polinomio come elementi di  $\mathbb{F}_p$ . Si ottiene così un isomorfismo:

$$(5.8) \quad \mathbb{F}_p[x]/(x^2 + 1) \xrightarrow{\sim} R'.$$

La proposizione (2.14), applicata all'anello  $\mathbb{F}_p[x]$ , prova che  $R'$  è un campo se e soltanto se  $x^2 + 1$  è irriducibile in  $\mathbb{F}_p[x]$ . ■

Siamo ora in grado di dimostrare l'equivalenza delle condizioni (d)(i) e (d)(iii) del teorema (5.1). Sappiamo dal lemma (5.6) che  $p$  è un primo di Gauss se e soltanto se  $x^2 + 1$  è un polinomio irriducibile nell'anello  $\mathbb{F}_p[x]$ . Poiché è un polinomio quadratico,  $x^2 + 1$  è riducibile se ha una radice in  $\mathbb{F}_p$  e irriducibile se non ha radici. Inoltre, la classe resto modulo  $p$  di un intero  $a$  è una radice di  $x^2 + 1$  se e soltanto se  $a^2 \equiv -1$  (modulo  $p$ ). Pertanto la congruenza  $x^2 \equiv -1$  (modulo  $p$ ) ha una soluzione se e soltanto se  $x^2 + 1$  è riducibile modulo  $p$ , il che accade se e soltanto se  $p$  non è un primo di Gauss. Ne segue l'equivalenza di (i) e (iii).

Resta da dimostrare l'equivalenza tra la condizione (iv) dell'enunciato (d) e una delle altre condizioni. Proveremo che essa è equivalente alla condizione (iii). La congruenza  $x^2 \equiv -1$  (modulo 2) ha la soluzione  $x = 1$ ; pertanto basta considerare gli altri primi, ossia, i primi dispari. Il lemma seguente risolve il nostro problema:

(5.9) LEMMA *Sia  $p$  un primo dispari, e si denoti con  $\bar{a}$  la classe resto di un intero  $a$  modulo  $p$ . Allora:*

- (a) *L'intero  $a$  è una soluzione della congruenza  $x^2 \equiv -1$  (modulo  $p$ ) se e solo se la sua classe resto  $\bar{a}$  è un elemento di ordine 4 nel gruppo moltiplicativo del campo  $\mathbb{F}_p$ .*

(b) Il gruppo moltiplicativo  $\mathbb{F}_p^*$  contiene un elemento di ordine 4 se e solo se  $p \equiv 1 \pmod{4}$ .

*Dimostrazione.* Esiste uno ed un solo elemento di ordine 2 in  $\mathbb{F}_p^*$ , precisamente la classe resto di  $-1$ . Infatti, un elemento di ordine 2 è una radice del polinomio  $x^2 - 1$ , e noi conosciamo le radici di questo polinomio, date da  $\pm 1$  in qualsiasi campo [cfr. (1.7)]. Se una classe resto  $\bar{a}$  ha ordine 4 in  $\mathbb{F}_p^*$ , allora  $\bar{a}^2$  ha ordine 2; ne segue che  $\bar{a}^2 = -1$ , cioè  $a^2 \equiv -1 \pmod{p}$ . Viceversa, se  $a^2 \equiv -1 \pmod{p}$ , allora  $\bar{a}$  ha ordine 4 in  $\mathbb{F}_p^*$ . Ciò prova la parte (a) del lemma.

Ora l'ordine del gruppo  $\mathbb{F}_p^*$  è  $p-1$ . Pertanto, se questo gruppo contiene un elemento di ordine 4, allora  $p-1$  è divisibile per 4, o equivalentemente,  $p \equiv 1 \pmod{4}$ . Viceversa, supponiamo che  $p-1$  sia divisibile per 4, e sia  $H$  il 2-sottogruppo di Sylow di  $\mathbb{F}_p^*$  il cui ordine è la più grande potenza  $2^r$  di 2 che divide  $p-1$ ; l'ordine di  $H$  è almeno 4, sicché esiste in  $H$  un elemento  $\bar{a}$  diverso da  $\pm 1$ . Tale elemento non ha ordine 2 e neppure ordine 1, ma poiché  $H$  è un 2-gruppo, l'ordine di  $\bar{a}$  è una potenza di 2. Pertanto qualche potenza di  $\bar{a}$  ha esattamente ordine 4.

Ciò completa la dimostrazione del teorema (5.1). ■

## 6 Interi algebrici

Nei prossimi paragrafi studieremo la fattorizzazione dei numeri algebrici nel caso semplice, ma importante, degli interi immaginari quadratici. L'anello degli interi di Gauss è qui il nostro modello. Gli ideali furono introdotti inizialmente proprio per estendere le proprietà della fattorizzazione degli interi ordinari ai numeri algebrici, e l'estensione è molto suggestiva.

A differenza della maggior parte degli argomenti che abbiamo studiato, l'aritmetica dei campi di numeri quadratici non ha un'importanza universale. Ha molte applicazioni in aritmetica, ma relativamente poche in altre aree della matematica. Il motivo per cui abbiamo inserito questo argomento, a parte la sua eleganza, è la sua importanza storica. Molti dei nostri strumenti algebrici furono inizialmente sviluppati per estendere le proprietà aritmetiche degli interi ai numeri algebrici.

Una tipica applicazione dei numeri algebrici all'aritmetica concerne la determinazione dei punti interi su un'ellisse di equazione:

$$(6.1) \quad x^2 + 5y^2 = p,$$

dove per semplicità supponiamo che  $p$  sia un numero primo. Per determinare i punti interi sulla circonferenza  $x^2 + 5y^2 = p$ , possiamo cominciare a fattorizzare il primo membro dell'equazione, ottenendo  $(x+iy)(x-iy) = p$ , e poi utilizzare l'aritmetica negli interi di Gauss per analizzare la fattorizzazione. Abbiamo fatto questo nella

dimostrazione del teorema (5.1). Il procedimento analogo per l'equazione (6.1) porta a

$$(x + \sqrt{-5}y)(x - \sqrt{-5}y) = p.$$

che possiamo provare ad analizzare nell'anello  $\mathbb{Z}[\sqrt{-5}]$ . Però, come abbiamo visto, la fattorizzazione non è unica in questo anello, sicché avremo qualche difficoltà.

Un altro esempio è dato dalla famosa equazione di Fermat:

$$(6.2) \quad x^3 + y^3 = z^3.$$

È stato dimostrato da Eulero che questa equazione non ha soluzioni intere, tranne le soluzioni banali in cui una delle variabili è zero. Per analizzare tale equazione, possiamo portare  $y^3$  al secondo membro e fattorizzare, ottenendo:

$$(6.3) \quad x^3 = (z-y)(z-\zeta y)(z-\bar{\zeta} y),$$

dove

$$(6.4) \quad \zeta = \frac{1}{2}(-1 + \sqrt{-3}) = e^{2\pi i/3}$$

è una radice cubica complessa di 1. Possiamo allora analizzare questa equazione utilizzando l'aritmetica nell'anello  $\mathbb{Z}[\zeta]$ , che è un dominio euclideo, e pertanto vale in esso la fattorizzazione unica. Purtroppo, la dimostrazione del fatto che l'equazione (6.2) non possiede soluzioni non banali è abbastanza complicata, e pertanto non verrà data.

Problemi di questo tipo, in cui si richiedono soluzioni intere di equazioni polinomiali, sono chiamati *problemis diofantei*. Analizzeremo alcuni di questi problemi più avanti (§ 12), quando avremo a disposizione gli strumenti necessari.

Un numero complesso  $\alpha$  si dice *algebrico* se è radice di un polinomio non nullo  $f(x)$  a coefficienti razionali (cap. 10, § 1). Naturalmente, possiamo eliminare i denominatori nei coefficienti del polinomio  $f(x)$ . Pertanto, se  $\alpha$  è un numero algebrico è radice anche di un polinomio a coefficienti interi. Il numero  $\alpha$  si dice *intero algebrico* se è radice di un polinomio *monico* a coefficienti interi, ossia un polinomio della forma:

$$(6.5) \quad f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \text{ con } a_i \in \mathbb{Z}.$$

Ad esempio, la radice cubica dell'unità  $\zeta$ , essendo una radice del polinomio  $x^3 - 1$ , è un intero algebrico.

Sia  $\alpha$  un numero algebrico. L'insieme di tutti i polinomi in  $\mathbb{Q}[x]$  che hanno  $\alpha$  come radice è il nucleo dell'omomorfismo di sostituzione:

$$\mathbb{Q}[x] \rightarrow \mathbb{C}, \text{ definito da } f(x) \mapsto f(\alpha).$$

Pertanto esso è un ideale principale, generato da un elemento irriducibile  $f(x)$  dell'anello dei polinomi, che è chiamato "il" *polinomio irriducibile di  $\alpha$  su  $\mathbb{Q}$* . (Perché  $f$  è irriducibile?) Esso è un polinomio di grado minimo che ha  $\alpha$  come radice ed è unico a meno di un fattore costante. Il grado del polinomio irriducibile di  $\alpha$  è chiamato anche il *grado* di  $\alpha$  su  $\mathbb{Q}$ .

Non è restrittivo supporre che il polinomio irriducibile  $f(x)$  di  $\alpha$  sia un polinomio *primitivo* in  $\mathbb{Z}[x]$ . Allora  $f(x)$  genera anche l'ideale di  $\mathbb{Z}[x]$  costituito da tutti i polinomi a coefficienti interi aventi  $\alpha$  come radice.

(6.6) PROPOSIZIONE *Il nucleo dell'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{C}$  che manda  $x$  in  $\alpha$  è l'ideale principale di  $\mathbb{Z}[x]$  generato dal polinomio irriducibile primitivo di  $\alpha$ .*

*Dimostrazione.* Sia  $f(x)$  il polinomio irriducibile primitivo di  $\alpha$ . Se  $g \in \mathbb{Z}[x]$  ha  $\alpha$  come radice,  $f$  divide  $g$  in  $\mathbb{Q}[x]$ , e quindi  $f$  divide  $g$  anche in  $\mathbb{Z}[x]$ , in virtù di (3.4). Pertanto  $g$  appartiene all'ideale principale di  $\mathbb{Z}[x]$  generato da  $f$ . ■

Si noti che il coefficiente direttore di un polinomio  $f(x)$  divide il coefficiente direttore di ogni multiplo di  $f(x)$  in  $\mathbb{Z}[x]$ . Pertanto dalla proposizione (6.6) segue che, se il polinomio irriducibile primitivo  $f(x)$  di  $\alpha$  non è monico, allora  $\alpha$  non è radice di nessun polinomio monico a coefficienti interi.

(6.7) PROPOSIZIONE *Un numero algebrico  $\alpha$  è un intero algebrico se e solo se il polinomio irriducibile primitivo di  $\alpha$  è monico. Ciò equivale a dire che  $\alpha$  è un intero algebrico se e solo se il polinomio irriducibile monico di  $\alpha$  in  $\mathbb{Q}[x]$  ha coefficienti interi.* ■

Il polinomio irriducibile primitivo della radice cubica dell'unità  $\zeta$  è  $x^2 + x + 1$ .

(6.8) COROLLARIO *Un numero razionale  $r$  è un intero algebrico se e soltanto se esso è un numero intero ordinario.*

Infatti, il polinomio irriducibile monico su  $\mathbb{Q}$  di un numero razionale  $r$  è  $x - r$ . ■

La proposizione (6.7) può essere usata per stabilire se un numero algebrico è o non è un intero algebrico, purché possiamo calcolare il suo polinomio irriducibile. Per esempio,  $\alpha = \frac{1}{2}(1 + \sqrt{2})$  è una radice di  $4x^2 - 4x - 1$ . Questo è il polinomio irriducibile primitivo di  $\alpha$ , quindi  $\alpha$  non è un intero algebrico.

Il concetto di intero algebrico è stata una delle scoperte più importanti della teoria dei numeri. Non è facile spiegare rapidamente come si sia giunti alla sua definizione, ma approssimativamente possiamo pensare al coefficiente direttore di  $f(x)$ , polinomio irriducibile primitivo di  $\alpha$ , come a un "denominatore". Se  $\alpha$  è una radice di un polinomio a coefficienti interi  $f(x) = dx^n + a_{n-1}x^{n-1} + \dots + a_0$ , allora

*è un intero algebrico, poiché è una radice del polinomio monico a coefficienti interi:*

$$(6.9) \quad x^n + a_{n-1}x^{n-1} + da_{n-2}x^{n-2} + \dots + d^{n-2}a_1x + d^{n-1}a_0.$$

Pertanto possiamo "eliminare il denominatore" in ogni numero algebrico  $\alpha$ , moltiplicandolo per un intero opportuno in modo da ottenere un intero algebrico. Tuttavia, il coefficiente direttore non è esattamente un denominatore. Così ad esempio, se  $\alpha = \frac{1}{2}(1 + \sqrt{2})$ , allora  $2\alpha$  è un intero algebrico, mentre il coefficiente direttore del suo polinomio irriducibile primitivo è 4.

In un'altra direzione, l'esempio dell'intero algebrico  $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$  mostra che non dobbiamo pervenire a conclusioni affrettate soltanto perché qualche espressione per un numero algebrico contiene denominatori.

Il calcolo esplicito con gli interi algebrici non è molto facile. Si dimostra che essi formano un sottoanello di  $\mathbb{C}$ , ossia che somme e prodotti di interi algebrici sono interi algebrici, ma ciò non è ovvio. Piuttosto che sviluppare una teoria generale, studieremo esplicitamente il caso delle estensioni quadratiche.

Un campo di numeri quadratico  $F = \mathbb{Q}[\sqrt{d}]$  è costituito da tutti i numeri complessi

$$(6.10) \quad a + b\sqrt{d}, \quad \text{con } a, b \in \mathbb{Q},$$

dove  $d$  è un intero fissato, positivo o negativo, che non è un quadrato. La notazione  $\sqrt{d}$  sta ad indicare la radice quadrata positiva se  $d > 0$ , e la radice quadrata immaginaria con coefficiente reale positivo se  $d < 0$ . Se  $d$  è divisibile per il quadrato di un intero, questo può essere portato fuori dal radicale e inglobato in  $b$ , senza cambiare il campo. Pertanto si suppone di solito che  $d$  sia *privò di quadrati*, ossia, che  $d = \pm p_1 \cdots p_r$ , dove i  $p_i$  sono primi distinti, oppure che  $d = -1$ . Pertanto i valori che consideriamo sono:

$$d = -1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \dots$$

Il campo  $F$  è chiamato *campo di numeri quadratico reale* se  $d > 0$ , oppure un *campo di numeri quadratico immaginario* se  $d < 0$ .

Passiamo ora a calcolare gli interi algebrici in  $F$ . Il calcolo per un valore particolare di  $d$  non è più semplice di quello relativo al caso generale. Tuttavia, procedendo nei calcoli, si può pensare di sostituire un valore, per esempio  $d = 5$ . Poniamo:

$$(6.11) \quad \delta = \sqrt{d}.$$

Quando  $d$  è negativo,  $\delta$  è un numero immaginario puro. Sia  $\alpha = a + b\delta$  un elemento di  $F$  che non appartenga a  $\mathbb{Q}$ , ossia tale che  $b \neq 0$ . Allora anche  $\alpha' = a - b\delta$

appartiene a  $F$ . Se  $d$  è negativo,  $\alpha'$  è il complesso coniugato di  $\alpha$ . Si noti che  $\alpha$  è una radice del polinomio

$$(6.12) \quad (x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha' = x^2 - 2ax + (a^2 - b^2d).$$

Questo polinomio ha i coefficienti razionali  $-2a$  e  $a^2 - b^2d$ . Poiché  $\alpha$  non è un numero razionale, non può essere la radice di un polinomio lineare. Pertanto il polinomio (6.12) è irriducibile e quindi è il polinomio irriducibile monico di  $\alpha$  su  $\mathbb{Q}$ . In base a (6.7),  $\alpha$  è un intero algebrico se e soltanto se il polinomio (6.12) ha coefficienti interi. Si ottiene così il corollario seguente:

(6.13) COROLLARIO *Il numero  $\alpha = a + b\delta$  è un intero algebrico se e soltanto se  $2a$  e  $a^2 - b^2d$  sono interi.* ■

Questo corollario vale anche quando  $b = 0$ , poiché se  $a^2$  è un intero, tale è anche  $a$ . Se vogliamo, possiamo usare le condizioni del corollario come definizione degli interi in  $F$ .

Le possibilità per  $a$  e  $b$  dipendono dalla classe di congruenza di  $d$  modulo 4. Si noti che, poiché si suppone che  $d$  sia privo di quadrati, il caso  $d \equiv 0$  (modulo 4) è stato scartato, sicché  $d \equiv 1, 2$ , o  $3$  (modulo 4).

(6.14) PROPOSIZIONE *Gli interi algebrici nel campo quadratico  $F = \mathbb{Q}[\sqrt{d}]$  hanno la forma  $\alpha = a + b\delta$ , dove:*

- (a) se  $d \equiv 2$  o  $3$  (modulo 4), allora  $a$  e  $b$  sono interi;
- (b) se  $d \equiv 1$  (modulo 4), allora o  $a, b \in \mathbb{Z}$  oppure  $a, b \in \mathbb{Z} + \frac{1}{2}$ .

La radice cubica dell'unità  $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$  è un esempio di un intero algebrico del secondo tipo. D'altra parte, poiché  $-1 \equiv 3$  (modulo 4), gli interi nel campo  $\mathbb{Q}[i]$  sono esattamente gli interi di Gauss.

*Dimostrazione.* Poiché i coefficienti del polinomio irriducibile di  $\alpha$  (6.12) sono  $2a$  e  $a^2 - b^2d$ , se  $a$  e  $b$  sono interi  $\alpha$  è certamente un intero algebrico. Supponiamo che  $d \equiv 1$  (modulo 4) e che  $a, b \in \mathbb{Z} + \frac{1}{2}$  (cioè  $a$  e  $b$  sono semi-interi). Allora  $2a \in \mathbb{Z}$ . Per dimostrare che  $a^2 - b^2d \in \mathbb{Z}$ , scriviamo  $a = \frac{1}{2}m$ ,  $b = \frac{1}{2}n$ , dove  $m, n$  sono interi dispari. Facendo i calcoli modulo 4, otteniamo:

$$m^2 - n^2d \equiv (\pm 1)^2 - (\pm 1)^2 \cdot 1 \equiv 0 \pmod{4}.$$

Ne segue che  $a^2 - b^2d = \frac{1}{4}(m^2 - n^2d) \in \mathbb{Z}$ , come richiesto.

Viceversa, supponiamo che  $\alpha$  sia un intero algebrico. Allora  $2a \in \mathbb{Z}$ , in base al corollario (6.13). Vi sono due casi possibili: o  $a \in \mathbb{Z}$ , o  $a \in \mathbb{Z} + \frac{1}{2}$ .

Caso 1:  $a \in \mathbb{Z}$ . In tal caso, anche  $b^2d \in \mathbb{Z}$ . Ora, se scriviamo  $b = m/n$ , dove  $m, n$  sono interi primi tra loro e  $n > 0$ , allora  $b^2d = m^2d/n^2$ . Poiché  $d$  è privo di quadrati,  $d$  non può cancellare un quadrato al denominatore. Pertanto  $n = 1$ . Se  $a$  è un intero, anche  $b$  deve essere un intero.

Caso 2:  $a \in \mathbb{Z} + \frac{1}{2}$  è un semi-intero, diciamo  $a = \frac{1}{2}m$  come prima. Allora  $4a^2 \in \mathbb{Z}$ , e la condizione  $a^2 - b^2d \in \mathbb{Z}$  implica che  $4b^2d \in \mathbb{Z}$ , ma  $b^2d \notin \mathbb{Z}$ . Pertanto anche  $b$  è un semi-intero, diciamo  $b = \frac{1}{2}n$ , dove  $n$  è dispari. Imponendo la condizione:  $a^2 - b^2d \in \mathbb{Z}$ , deve risultare:  $m^2 - n^2d \equiv 0 \pmod{4}$ . Sviluppando i calcoli modulo 4, otteniamo che  $d \equiv 1$  (modulo 4). ■

Un modo conveniente per scrivere tutti gli interi nel caso  $d \equiv 1$  (modulo 4) si ottiene introducendo l'intero algebrico

$$(6.15) \quad \eta = \frac{1}{2}(1 + \delta),$$

che è una radice del polinomio monico a coefficienti interi:

$$(6.16) \quad x^2 - x + \frac{1}{4}(1 - d).$$

(6.17) PROPOSIZIONE *Supponiamo che  $d \equiv 1$  (modulo 4). Allora gli interi algebrici in  $F = \mathbb{Q}[\sqrt{d}]$  sono i numeri della forma  $a + b\eta$ , dove  $a, b \in \mathbb{Z}$ .* ■

È facile dimostrare mediante un calcolo esplicito che gli interi in  $F$  formano in ogni caso un anello  $R$ , chiamato l'*anello degli interi in  $F$* . I calcoli in  $R$  possono essere effettuati utilizzando l'algebra della scuola media.

Il *discriminante* di  $F$  è, per definizione, il discriminante del polinomio  $x^2 - d$  nel caso in cui  $R = \mathbb{Z}[\delta]$ , e il discriminante del polinomio  $x^2 - x + \frac{1}{4}(1 - d)$  se  $R = \mathbb{Z}[\eta]$ . Tale discriminante sarà denotato con  $D$ . Pertanto

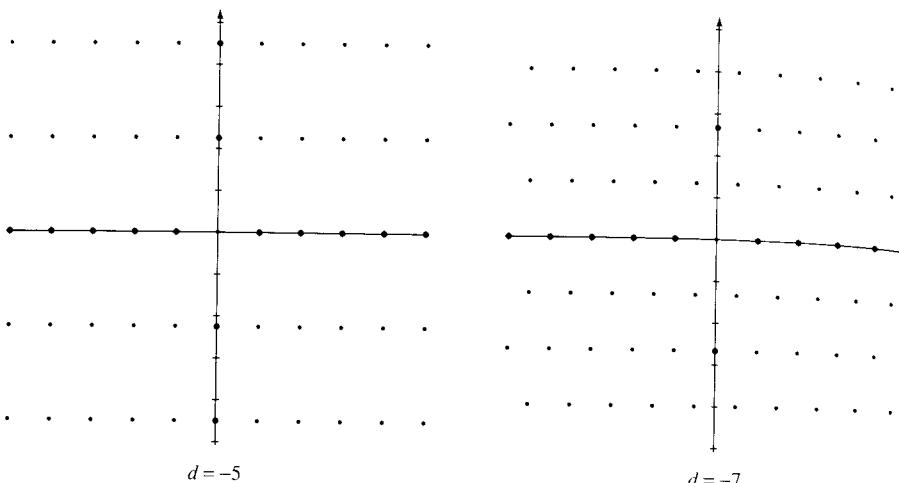
$$(6.18) \quad D = \begin{cases} 4d, & \text{se } d \equiv 2, 3 \\ d, & \text{se } d \equiv 1 \end{cases} \pmod{4}.$$

Poiché  $D$  può essere calcolato per mezzo di  $d$ , non è molto importante introdurre una notazione separata per il discriminante. Tuttavia, alcune formule diventano indipendenti dalla classe di congruenza, quando vengono espresse per mezzo di  $D$  anziché di  $d$ .

Il caso quadratico immaginario  $d < 0$  è leggermente più facile da trattare del caso reale, sicché ci concentreremo su di esso nei prossimi paragrafi. Nel caso immaginario, l'anello  $R$  forma un reticolo nel piano complesso, che è rettangolare se  $d \equiv 2, 3$  (modulo 4), e "triangolare isoscele", se  $d \equiv 1$  (modulo 4). Quando

$d = -1$ ,  $R$  è l'anello degli interi di Gauss, e il reticolo è quadrato. Quando  $d = -3$ , il reticolo è triangolare equilatero. Altri due esempi sono illustrati qui sotto.

(6.19)



Interi in alcuni campi quadratici immaginari.

La proprietà di essere un reticolo è una proprietà davvero speciale per gli anelli come quelli che stiamo considerando, e useremo la geometria per analizzarli. Pensare a  $R$  come un reticolo è anche utile per l'intuizione.

Nel seguito sarà utile avere un esempio specifico di riferimento. A tale scopo, utilizzeremo il caso  $d = -5$ . Poiché  $-5 \equiv 3 \pmod{4}$ , l'anello degli interi forma un reticolo rettangolare, e  $R = \mathbb{Z}[\delta]$ , dove  $\delta = \sqrt{-5}$ .

## 7 Fattorizzazione nei campi quadratici immaginari

Sia  $R$  l'anello degli interi di un campo di numeri quadratico immaginario  $F = \mathbb{Q}[\delta]$ . Se  $\alpha = a + b\delta$  è un elemento di  $R$ , lo è anche il suo complesso coniugato  $\bar{\alpha} = a - b\delta$ . Si chiama *norma* di  $\alpha$  l'intero

$$(7.1) \quad N(\alpha) = \alpha\bar{\alpha},$$

che è anche uguale ad  $a^2 - b^2d$  e a  $|\alpha|^2$ , ed è il termine noto del polinomio irriducibile di  $\alpha$  su  $\mathbb{Q}$ . Pertanto  $N(\alpha)$  è un intero positivo, tranne che per  $\alpha = 0$ . Si noti che

$$(7.2) \quad N(\beta\gamma) = N(\beta)N(\gamma).$$

Questa formula ci permette di controllare un po' i possibili fattori di un elemento  $\alpha$  di  $R$ . Supponiamo che  $\alpha = \beta\gamma$ . Allora entrambi i fattori nel secondo membro di (7.2) sono interi positivi. Pertanto, per cercare i fattori di  $\alpha$ , basta considerare gli elementi  $\beta$  la cui norma divide  $N(\alpha)$ ; questo non è un lavoro troppo grosso, se  $\alpha$  e  $\beta$  sono ragionevolmente piccoli.

In particolare, cerchiamo le unità di  $R$ :

### (7.3) PROPOSIZIONE

- (a) Un elemento  $\alpha$  di  $R$  è un'unità se e solo se  $N(\alpha) = 1$ .
- (b) Le unità di  $R$  sono  $\{\pm 1\}$ , a meno che  $d = -1$  oppure  $-3$ . Se  $d = -1$ , sicché  $R$  è l'anello degli interi di Gauss, le unità sono  $\{\pm 1, \pm i\}$ , e se  $d = -3$  esse sono le potenze della radice sesta dell'unità  $\frac{1}{2}(1 + \sqrt{-3})$ .

*Dimostrazione.* Se  $\alpha$  è un'unità, allora  $N(\alpha)N(\alpha^{-1}) = N(1) = 1$ . Poiché  $N(\alpha)$  e  $N(\alpha^{-1})$  sono interi positivi, essi sono entrambi uguali a 1. Viceversa, se  $N(\alpha) = N(\alpha^{-1})$ , allora  $\bar{\alpha} = \alpha^{-1}$ . Pertanto  $\alpha^{-1} \in R$ , e  $\alpha$  è un'unità. Dunque  $\alpha$  è un'unità se e solo se appartiene alla circonferenza unitaria nel piano complesso. La seconda asserzione segue dalla configurazione del reticolo  $R$  [cfr. figura (6.19)]. ■

Passiamo poi a studiare la fattorizzazione di un elemento  $\alpha \in R$  in fattori irriducibili.

### (7.4) PROPOSIZIONE In $R$ esiste una fattorizzazione.

*Dimostrazione.* Se  $\alpha = \beta\gamma$  è una fattorizzazione propria in  $R$ , allora  $\beta, \gamma$  non sono unità. Pertanto, in virtù della proposizione (7.3),  $N(\alpha) = N(\beta)N(\gamma)$  è una fattorizzazione propria nell'anello degli interi. A questo punto l'esistenza di una fattorizzazione in fattori irriducibili in  $R$  segue dall'esistenza della fattorizzazione in  $\mathbb{Z}$ . ■

Tuttavia, nella maggior parte dei casi, la fattorizzazione in elementi irriducibili non sarà unica. Abbiamo già visto (§ 2) un esempio semplice con  $d = -5$ :

$$(7.5) \quad 6 = 2 \cdot 3 = (1 + \delta)(1 - \delta),$$

dove  $\delta = \sqrt{-5}$ . Per esempio, per dimostrare che  $1 + \delta$  è irriducibile, osserviamo che la sua norma è  $(1 + \delta)(1 - \delta) = 6$ . Un fattore proprio deve avere norma 2 o 3, ossia valore assoluto  $\sqrt{2}$  o  $\sqrt{3}$ , e nel reticolo  $R$  non ci sono punti siffatti.

Lo stesso metodo fornisce esempi per altri valori di  $d$ :

### (7.6) PROPOSIZIONE L'unico anello $R$ con $d \equiv 3 \pmod{4}$ che sia un dominio a fattorizzazione unica è l'anello degli interi di Gauss.

*Dimostrazione.* Supponiamo che  $d \equiv 3 \pmod{4}$ , ma che  $d \neq -1$ . Allora

$$1-d = 2\left(\frac{1-d}{2}\right) \quad \text{e} \quad 1-d = (1+\delta)(1-\delta),$$

cioè ci sono due fattorizzazioni di  $1-d$  in  $R$ . L'elemento 2 è irriducibile perché  $N(2) = 4$  è il più piccolo valore  $> 1$  assunto da  $N(\alpha)$ . [Gli unici punti di  $R$  all'interno della circonferenza di centro l'origine e raggio 2 sono 0, 1, -1, quando  $d = -5, -13, -17, \dots$ . Vedi fig. (6.19)]. Pertanto, se  $R$  fosse un dominio a fattorizzazione unica, 2 dovrebbe dividere  $1+\delta$  oppure  $1-\delta$  in  $R$ , il che non è possibile perché  $\frac{1}{2} \pm \frac{1}{2}\delta$  non appartiene a  $R$  quando  $d \equiv 3 \pmod{4}$ . ■

Si noti che questo ragionamento non funziona se  $d \equiv 1 \pmod{4}$ ; infatti in tal caso, 2 divide  $1+\delta$ , poiché  $\frac{1}{2} + \frac{1}{2}\delta \in R$ . Vi sono più casi di fattorizzazione unica quando  $d \equiv 1 \pmod{4}$ . Il teorema seguente è molto profondo, e non verrà dimostrato:

(7.7) TEOREMA Sia  $R$  l'anello degli interi nel campo quadratico immaginario  $\mathbb{Q}(\sqrt{d})$ . Allora  $R$  è un dominio a fattorizzazione unica se e soltanto se  $d$  è uno degli interi seguenti:  $-1, -2, -3, -7, -11, -19, -43, -67, -163$ .

Gauss dimostrò che, per questi valori di  $d$ ,  $R$  è un dominio a fattorizzazione unica, e congetturò anche che non ve ne fossero altri. Questa parte molto più difficile del teorema fu dimostrata finalmente da Baker e Stark nel 1966, dopo che il problema era stato studiato per oltre 150 anni.

Gli ideali furono introdotti per salvare l'unicità della fattorizzazione. Come sappiamo (2.12),  $R$  deve contenere qualche ideale non principale, a meno che non sia un dominio a fattorizzazione unica. Vedremo nel prossimo paragrafo come questi ideali non principali possano sostituire gli elementi.

Si noti che ogni ideale non nullo  $A$  è un sottoreticolo di  $R$ . Infatti è un sottogruppo rispetto all'addizione, ed è discreto poiché  $R$  è discreto. Inoltre, se  $\alpha$  è un elemento non nullo di  $A$ , allora anche  $\alpha\delta$  appartiene ad  $A$ , e  $\alpha, \alpha\delta$  sono linearmente indipendenti su  $R$ . Tuttavia, non tutti i sottoreticoli sono ideali.

(7.8) PROPOSIZIONE Se  $d \equiv 2$  o  $3 \pmod{4}$ , gli ideali non nulli di  $R$  sono i sottoreticoli chiusi rispetto alla moltiplicazione per  $\delta$ . Se  $d \equiv 1 \pmod{4}$ , essi sono i sottoreticoli chiusi rispetto alla moltiplicazione per  $\eta = \frac{1}{2}(1+\delta)$ .

*Dimostrazione.* Affinché sia un ideale, un sottoinsieme  $A$  deve essere chiuso rispetto all'addizione e rispetto alla moltiplicazione per gli elementi di  $R$ . Ogni reticolo è chiuso rispetto all'addizione e rispetto alla moltiplicazione per gli interi. Pertanto, se esso è chiuso anche rispetto alla moltiplicazione per  $\delta$ , allora è chiuso

anche rispetto alla moltiplicazione per un elemento della forma  $a+b\delta$ , con  $a, b \in \mathbb{Z}$ . Ciò include tutti gli elementi di  $R$  se  $d \equiv 2, 3 \pmod{4}$ . La dimostrazione nel caso in cui  $d \equiv 1 \pmod{4}$  è simile. ■

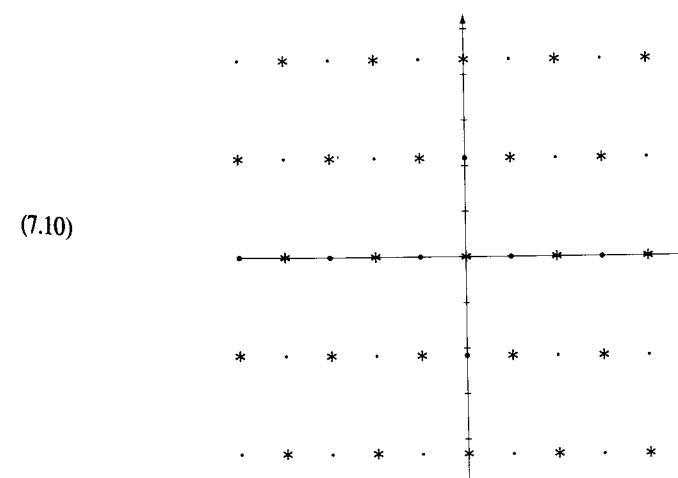
Allo scopo di imparare a conoscere le varie possibilità, descriveremo gli ideali dell'anello  $R = \mathbb{Z}[\sqrt{-5}]$  prima di andare avanti. Gli ideali più interessanti sono quelli che non sono principali.

(7.9) PROPOSIZIONE Sia  $R = \mathbb{Z}[\delta]$ , dove  $\delta = \sqrt{-5}$ , e sia  $A$  un ideale non nullo di  $R$ . Sia  $\alpha$  un elemento non nullo di  $A$  avente valore assoluto minimo  $|\alpha|$ . Allora vi sono due casi possibili:

Caso 1:  $A$  è l'ideale principale  $(\alpha)$ , che ha come base del reticolo i due elementi  $(\alpha, \alpha\delta)$ .

Caso 2:  $A$  ha come base del reticolo  $\left(\alpha, \frac{1}{2}(\alpha + \alpha\delta)\right)$ , e non è un ideale principale.

Il secondo caso può presentarsi soltanto se  $\frac{1}{2}(\alpha + \alpha\delta)$  è un elemento di  $R$ . Un esempio è dato dall'ideale  $A = (2, 1+\delta)$  rappresentato nella figura seguente.



L'ideale  $(2, 1+\delta)$  nell'anello  $\mathbb{Z}[\delta]$ ,  $\delta = \sqrt{-5}$ .

L'enunciato della proposizione (7.9) si può interpretare geometricamente. Si noti che la base di reticolo  $(\alpha, \alpha\delta)$  dell'ideale principale  $(\alpha)$  è ottenuta dalla base di reticolo  $(1, \delta)$  di  $R$  mediante la moltiplicazione per  $\alpha$ . Se scriviamo  $\alpha = re^{i\theta}$ , allora l'effetto della moltiplicazione per  $\alpha$  è quello di ruotare il piano complesso

di un angolo  $\theta$  e poi di "dilatarlo" mediante il fattore  $r$ . Pertanto  $(\alpha)$  e  $R$  sono figure geometriche simili, come abbiamo osservato nel paragrafo 2. Analogamente, la base  $\left(\alpha, \frac{1}{2}(\alpha + \alpha\delta)\right)$  è ottenuta dalla base  $(2, 1 + \delta)$  mediante la moltiplicazione per  $\frac{1}{2}\alpha$ . Pertanto gli ideali che compaiono nel caso 2 sono figure simili a quella rappresentata nella figura (7.10). Le classi di similitudine di ideali sono chiamate *classi di ideali*, e il loro numero è chiamato *numero di classe* di  $R$ . Così, ad esempio, la proposizione (7.9) implica che il numero di classe di  $\mathbb{Z}[\sqrt{-5}]$  è 2. Studieremo le classi di ideali per altri campi quadratici immaginari nel paragrafo 10.

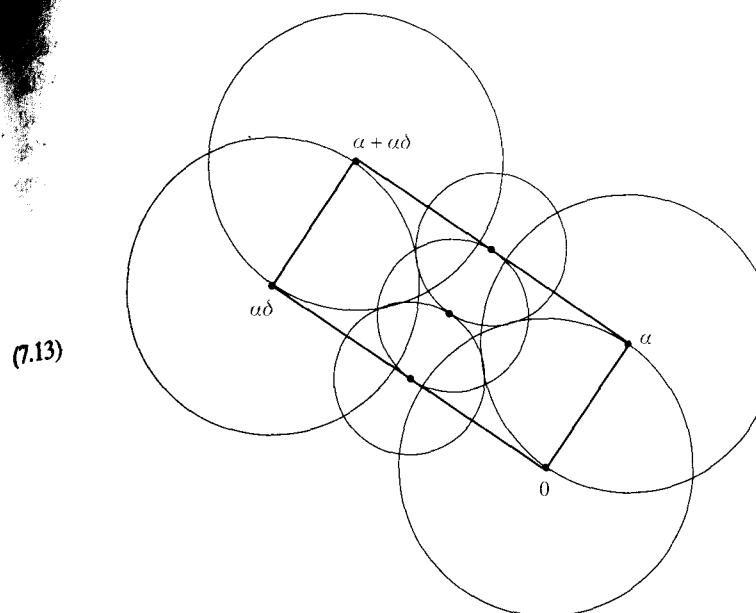
La dimostrazione della proposizione (7.9) è basata sul lemma seguente, che riguarda i reticolati nel piano complesso:

(7.11) LEMMA *Sia  $r$  il minimo valore assoluto degli elementi non nulli di un reticolo  $A$ , sia  $\gamma$  un elemento di  $A$ , e sia  $n$  un intero positivo. Sia  $D$  il disco di raggio  $\frac{1}{n}r$  intorno al punto  $\frac{1}{n}\gamma$ . Allora non vi è nessun punto di  $A$  all'interno di  $D$ , eccetto, al più, il suo centro  $\frac{1}{n}\gamma$ .*

*Dimostrazione.* Sia  $\beta$  un punto all'interno di  $D$ . Allora dalla definizione del disco segue che  $\left|\beta - \frac{1}{n}\gamma\right| < \frac{1}{n}r$ , ossia  $|n\beta - \gamma| < r$ . Se  $\beta \in A$ , allora anche  $n\beta - \gamma \in A$ . In questo caso,  $n\beta - \gamma$  è un elemento di  $A$  con valore assoluto minore di  $r$ , il che implica  $n\beta - \gamma = 0$ , e quindi  $\beta = \frac{1}{n}\gamma$ . ■

*Dimostrazione del teorema (7.9).* Sia  $\alpha$  un elemento in  $A$  avente valore assoluto minimo  $r$ . L'ideale principale  $(\alpha) = R\alpha$  è costituito dai numeri complessi  $(a+b\delta)\alpha$ , con  $a, b \in \mathbb{Z}$ . Pertanto esso ha come base del reticolo  $(\alpha, \alpha\delta)$ , come asserito nella proposizione. Poiché  $A$  contiene  $\alpha$ , esso contiene anche l'ideale principale  $(\alpha)$ , e se  $A = (\alpha)$  siamo nel caso 1.

Supponiamo che  $A > (\alpha)$ , e sia  $\beta$  un elemento di  $A$  che non appartenga a  $(\alpha)$ . Possiamo scegliere  $\beta$  appartenente al rettangolo i cui quattro vertici sono  $0, \alpha, \alpha\delta, \alpha + \alpha\delta$  [cfr. cap. 5 (4.14)]. La figura (7.13) mostra un disco di raggio  $r$  intorno ai quattro vertici di questo rettangolo, e un disco di raggio  $\frac{1}{2}r$  intorno ai tre punti del semireticolo  $\frac{1}{2}\alpha\delta, \frac{1}{2}(\alpha + \alpha\delta), \alpha + \frac{1}{2}\alpha\delta$ . Si noti che le parti interne di questi dischi ricoprono il rettangolo. In base al lemma (7.11), gli unici punti delle parti interne che possono appartenere ad  $A$  sono i centri dei dischi. Poiché  $\beta$  non appartiene a  $(\alpha)$ , non è un vertice del rettangolo. Pertanto  $\beta$  deve essere uno dei punti del semireticolo  $\frac{1}{2}\alpha\delta, \frac{1}{2}(\alpha + \alpha\delta)$ , oppure  $\alpha + \frac{1}{2}\alpha\delta$ .



(7.13)

Ciò esaurisce le informazioni che possiamo ricavare dal fatto che  $A$  è un reticolo. Usiamo ora il fatto che  $A$  è un ideale per scartare i due punti  $\frac{1}{2}\alpha\delta$  e  $\alpha + \frac{1}{2}\alpha\delta$ . Supponiamo che  $\frac{1}{2}\alpha\delta \in A$ . Moltiplicando per  $\delta$ , otteniamo che anche  $\frac{1}{2}\alpha\delta^2 = \frac{5}{2}\alpha \in A$  e quindi, poiché  $\alpha \in A$ ,  $\frac{1}{2}\alpha \in A$ . Ciò contraddice la scelta fatta per  $\alpha$ . Successivamente osserviamo che, se  $\alpha + \frac{1}{2}\alpha\delta$  appartenesse ad  $A$ , allora anche  $\frac{1}{2}\alpha\delta$  apparrebbe ad  $A$ , eventualità che abbiamo appena scartato. L'unica possibilità che rimane è che  $\beta = \frac{1}{2}(\alpha + \alpha\delta)$ , e allora siamo nel caso 2. ■

## 8 Fattorizzazione degli ideali

Sia  $R$  l'anello degli interi in un campo quadratico immaginario. Per evitare confusione, denoteremo gli interi ordinari con lettere latine  $a, b, \dots$ , gli elementi di  $R$  con lettere greche  $\alpha, \beta, \dots$ , e gli ideali con lettere maiuscole  $A, B, \dots$ . Considereremo soltanto ideali non nulli di  $R$ .

La notazione  $A = (\alpha, \beta, \dots, \gamma)$  indica l'ideale generato dagli elementi  $\alpha, \beta, \dots, \gamma$ . Poiché un ideale è un reticolo piano, ha una base di reticolo costituita da due elementi. Ogni base del reticolo genera l'ideale, ma dobbiamo fare distinzione tra le nozioni di base di reticolo e insieme di generatori. Dobbiamo ricordare anche le relazioni (2.2) che collegano gli elementi con gli ideali principali da essi generati.

Dedekind estese la nozione di divisibilità agli ideali utilizzando la seguente definizione di moltiplicazione di ideali. Se  $A$  e  $B$  sono ideali in un anello  $R$ , vorremmo definire l'ideale prodotto  $AB$  come l'insieme di tutti i prodotti  $\alpha_i \beta_j$ , dove  $\alpha_i \in A$  e  $\beta_j \in B$ , ma purtroppo questo insieme di prodotti di solito non è un ideale, perché non è chiuso rispetto alla somma. Per ottenere un ideale, dobbiamo mettere in  $AB$  tutte le *somme finite di prodotti*:

$$(8.1) \quad \sum_i \alpha_i \beta_i, \quad \text{dove } \alpha_i \in A \text{ e } \beta_i \in B.$$

L'insieme di tali somme è il più piccolo ideale di  $R$  che contiene tutti i prodotti  $\alpha\beta$ , e questo *ideale prodotto* si denota con  $AB$ . (L'uso di questa notazione per il prodotto è diverso dall'uso fatto in teoria dei gruppi [cap. 2 (8.5)]). La definizione di moltiplicazione di ideali non è così semplice come potevamo sperare, ma ha delle proprietà abbastanza buone.

Si noti che la moltiplicazione di ideali è commutativa e associativa, e che  $R$  è un elemento unità. Ecco perché  $R = (1)$  è chiamato spesso l'ideale unità:

$$(8.2) \quad AR = RA = A, \quad AB = BA, \quad (AB)C = A(BC).$$

### (8.3) PROPOSIZIONE

(a) *Il prodotto di ideali principali è principale. Precisamente, se  $A = (\alpha)$  e  $B = (\beta)$ , allora  $AB = (\alpha\beta)$ .*

(b) *Supponiamo che  $A = (\alpha)$  sia principale, ma  $B$  sia arbitrario. Allora*

$$AB = \alpha B = \{\alpha\beta \mid \beta \in B\}.$$

(c) *Siano  $\alpha_1, \dots, \alpha_m$  e  $\beta_1, \dots, \beta_n$  generatori per gli ideali  $A$  e  $B$  rispettivamente. Allora  $AB$  è generato come ideale dagli  $mn$  prodotti  $\alpha_i\beta_j$ .*

La dimostrazione della proposizione è lasciata come esercizio. ■

In analogia con la divisibilità tra elementi di un anello, si dice che un ideale  $A$  divide un altro ideale  $B$ , se esiste un ideale  $C$  tale che  $B = AC$ .

Per vedere come la moltiplicazione di ideali può essere usata, torniamo all'esempio  $d = -5$ , in cui  $2 \cdot 3 = (1+\delta)(1-\delta)$ . Se valesse l'unicità della fattorizzazione in  $R = \mathbb{Z}[\delta]$ , potremmo concludere che esiste un elemento  $\rho$  divisore sia di 2 che di  $1+\delta$ ; in questo caso 2 e  $1+\delta$  apparterrebbero all'ideale principale  $(\rho)$ , ma non esiste alcun elemento in  $R$  che divide sia 2 che  $1+\delta$ . Tuttavia, esiste un ideale non principale che contiene 2 e  $1+\delta$ , precisamente l'ideale generato da questi due elementi. Tale ideale  $A = (2, 1+\delta)$  è rappresentato nella figura (7.10). Utilizzando i fattori di 6, possiamo costruire altri tre ideali:

$$\bar{A} = (2, 1-\delta), \quad B = (3, 1+\delta), \quad \bar{B} = (3, 1-\delta).$$

Il primo di questi ideali è denotato con  $\bar{A}$ , poiché è il complesso coniugato dell'ideale  $A$ :

$$(8.4) \quad \bar{A} = \{\bar{\alpha} \mid \alpha \in A\}.$$

Come reticolo,  $\bar{A}$  si ottiene mediante una riflessione del reticolo  $A$  intorno all'asse reale. Si vede facilmente che il complesso coniugato di un ideale è un ideale. In realtà, il nostro ideale  $A$  risulta uguale al suo complesso coniugato  $\bar{A}$ , poiché  $1-\delta = 2 - (1+\delta) \in A$ . Si tratta di una simmetria casuale del reticolo  $A$ , infatti ad esempio gli ideali  $B$  e  $\bar{B}$  non sono uguali tra loro.

Calcoliamo ora i prodotti di questi ideali. In base alla proposizione (8.3c), l'ideale  $A\bar{A}$  è generato dai quattro prodotti dei generatori  $(2, 1+\delta)$  e  $(2, 1-\delta)$  di  $A$  e  $\bar{A}$ :

$$A\bar{A} = (4, 2+2\delta, 2-2\delta, 6).$$

Ciascuno di questi quattro generatori è divisibile per 2, sicché  $A\bar{A} \subset (2)$ . D'altra parte,  $2 = 6 - 4$  appartiene ad  $A\bar{A}$ . Pertanto  $(2) \subset A\bar{A}$ , e quindi  $A\bar{A} = (2)!$  [La notazione (2) è ambigua, poiché può denotare sia  $2R$  che  $2\mathbb{Z}$ . Qui essa sta a indicare  $2R$ ]. Inoltre, il prodotto  $AB$  è generato dai quattro prodotti:

$$AB = (6, 2+2\delta, 3+3\delta, -4+2\delta).$$

Ciascuno di questi quattro elementi è divisibile per  $1+\delta$ . Poiché  $1+\delta$  appartiene ad  $AB$ , si ha che  $AB = (1+\delta)$ . Analogamente,  $\bar{A}\bar{B} = (1-\delta)$  e  $B\bar{B} = (3)$ .

Ne segue che l'ideale principale (6) è il prodotto dei quattro ideali:

$$(8.5) \quad (6) = (2)(3) = (A\bar{A})(B\bar{B}) = (AB)(\bar{A}\bar{B}) = (1+\delta)(1-\delta).$$

Non è straordinario? La fattorizzazione di ideali  $(6) = A\bar{A}B\bar{B}$  ha fornito un raffinamento comune delle due fattorizzazioni (2.7).

Il resto del paragrafo è dedicato alla dimostrazione della fattorizzazione unica degli ideali nell'anello degli interi di un campo di numeri quadratico immaginario. Seguiremo la fattorizzazione degli elementi il più strettamente possibile.

La prima cosa da fare è trovare, per gli ideali, una nozione analoga a quella di elemento primo:

**(8.6) PROPOSIZIONE** Sia  $P$  un ideale di un anello  $R$ , diverso dall'ideale unità. Le seguenti condizioni sono equivalenti:

- (i) Se  $\alpha, \beta$  sono elementi di  $R$  tali che  $\alpha\beta \in P$ , allora  $\alpha \in P$  oppure  $\beta \in P$ .
- (ii) Se  $A, B$  sono ideali in  $R$  tali che  $AB \subset P$ , allora  $A \subset P$  oppure  $B \subset P$ .
- (iii) L'anello quoziante  $R/P$  è un dominio di integrità.

Un ideale che soddisfi una di queste condizioni è chiamato *ideale primo*.

Per esempio, ogni ideale massimale è primo, poiché se  $M$  è massimale, allora  $R/M$  è un campo, e un campo è un dominio di integrità. L'ideale nullo di un anello  $R$  è primo se e soltanto se  $R$  è un dominio di integrità.

*Dimostrazione della proposizione.* Le condizioni affinché  $\bar{R} = R/P$  sia un dominio di integrità sono che  $\bar{R} \neq 0$  e che  $\bar{\alpha}\bar{\beta} = 0$  implica che  $\bar{\alpha} = 0$  oppure  $\bar{\beta} = 0$ . Queste condizioni si traducono, in  $R$ , nelle condizioni:  $P \neq R$  e  $\alpha, \beta \in P$  implica che  $\alpha \in P$  oppure  $\beta \in P$ . Pertanto (i) e (iii) sono equivalenti. Il fatto che (ii) implica (i) si vede prendendo  $A = (\alpha)$  e  $B = (\beta)$ . L'unica implicazione sorprendente è che (i) implica (ii). Supponiamo che valga la condizione (i), e siano  $A, B$  ideali tali che  $AB \subset P$ . Se  $A$  non è contenuto in  $P$ , esiste qualche elemento  $\alpha \in A$  che non appartiene a  $P$ . Se  $\beta$  è un elemento di  $B$ , allora  $\alpha\beta \in AB$ , e quindi  $\alpha\beta \in P$ . In virtù di (i),  $\beta \in P$ . Poiché ciò è vero per tutti gli elementi di  $B$ , si ha che  $B \subset P$ , come richiesto. ■

Ritorniamo ora allo studio dei campi di numeri quadratici immaginari.

(8.7) LEMMA *Siano  $A \subset B$  reticolati in  $\mathbb{R}^2$ . Esiste soltanto un numero finito di reticolati  $L$  compresi tra  $A$  e  $B$ , ossia, tali che  $A \subset L \subset B$ .*

*Dimostrazione.* Sia  $(\alpha_1, \alpha_2)$  una base di reticolo per  $A$ , e sia  $P$  il parallelogramma con vertici  $0, \alpha_1, \alpha_2, \alpha_1 + \alpha_2$ . Esiste un numero finito di elementi di  $B$  contenuti in  $P$  [cap. 5 (4.12)], sicché se  $L$  è un reticolo compreso tra  $A$  e  $B$  esiste un numero finito di possibilità per l'insieme  $L \cap P$ . Chiamiamo  $S$  tale insieme. La dimostrazione sarà completata provando che  $S$  ed  $A$  determinano il reticolo  $L$ . Per provare ciò, sia  $\gamma$  un elemento di  $L$ . Allora esiste un elemento  $\alpha \in A$  tale che  $\gamma - \alpha$  appartiene a  $P$ , e quindi a  $S$ . [Vedi la dimostrazione di (4.14) nel cap. 5]. In simboli, si ha:  $L = S + A$ . Ciò descrive  $L$  per mezzo di  $S$  e di  $A$ , come richiesto. ■

(8.8) PROPOSIZIONE *Sia  $R$  l'anello degli interi in un campo di numeri quadratici immaginario.*

- (a) *Sia  $B$  un ideale non nullo di  $R$ . Allora esiste un numero finito di ideali compresi tra  $B$  e  $R$ .*
- (b) *Ogni ideale proprio di  $R$  è contenuto in un ideale massimale [cfr. cap. 10 (8.3)].*
- (c) *Gli ideali primi non nulli di  $R$  sono gli ideali massimali.*

*Dimostrazione.*

- (a) Segue dal lemma (8.7).
- (b) Sia  $B$  un ideale proprio. Allora  $B$  è contenuto soltanto in un numero finito di ideali. Possiamo trovare tra di essi un ideale massimale.

(c) Abbiamo già osservato che gli ideali massimali sono primi. Viceversa, sia  $P$  un ideale primo non nullo. Allora  $P$  ha indice finito in  $R$ . Pertanto  $R/P$  è un dominio di integrità finito, e quindi è un campo [cap. 10 (6.4)]. Ciò prova che  $P$  è un ideale massimale. ■

(8.9) TEOREMA *Sia  $R$  l'anello degli interi in un campo quadratico immaginario  $F$ . Ogni ideale non nullo di  $R$  che non sia l'intero anello è un prodotto di ideali primi. Tale fattorizzazione è unica, a meno dell'ordine dei fattori.*

Questo risultato notevole può essere esteso ad altri anelli di interi algebrici, ma è una proprietà molto particolare di questi anelli. La maggior parte degli anelli non possiedono la fattorizzazione unica degli ideali. Parecchie cose possono non valere in un anello qualsiasi, e noi vogliamo prendere in considerazione esplicitamente una di esse. Sappiamo che un ideale principale  $(\alpha)$  contiene un altro ideale principale  $(\beta)$  se e soltanto se  $\alpha$  divide  $\beta$  nell'anello. Pertanto la definizione di un elemento primo  $\pi$  può essere rientrata nel modo seguente: se  $(\pi) \supset (\alpha\beta)$ , allora  $(\pi) \supset (\alpha)$  oppure  $(\pi) \supset (\beta)$ . La seconda delle definizioni equivalenti (8.6) di un ideale primo è l'enunciato analogo per gli ideali: se  $P \supset AB$ , allora  $P \supset A$  oppure  $P \supset B$ . Pertanto, se l'inclusione di ideali fosse equivalente alla divisibilità, la dimostrazione dell'unicità della fattorizzazione si generalizzerebbe al caso degli ideali. Purtroppo la definizione poco agevole dell'ideale prodotto dà luogo a delle difficoltà. Nella maggior parte degli anelli, l'inclusione  $A \supset B$  non implica che  $A$  divide  $B$ . Ciò rende più debole l'analogia tra gli ideali primi e gli elementi primi. Sarà importante stabilire l'equivalenza dell'inclusione e della divisibilità negli anelli particolari che stiamo studiando. Ciò verrà fatto più avanti, nella proposizione (8.11).

Passiamo ora a dimostrare il teorema (8.9). Per il resto del paragrafo,  $R$  denoterà l'anello degli interi in un campo di numeri quadratici immaginario. La dimostrazione è basata sul lemma seguente:

(8.10) LEMMA FONDAMENTALE *Sia  $R$  l'anello degli interi in un campo di numeri quadratici immaginario. Il prodotto di un ideale non nullo e del suo coniugato è un ideale principale di  $R$  generato da un intero ordinario:*

$$A\bar{A} = (n), \quad \text{per qualche } n \in \mathbb{Z}.$$

Il punto più importante qui è che per ogni ideale  $A$  esiste qualche ideale  $B$  tale che  $AB$  sia principale. Il fatto che  $\bar{A}$  risponda allo scopo e il fatto che l'ideale prodotto sia generato da un intero ordinario sono fatti secondari.

Dimostreremo il lemma alla fine del paragrafo. Supponiamolo vero per ora e ricaviamo alcune conseguenze relative alla moltiplicazione di ideali. Poiché tali

conseguenze dipendono dal Lemma fondamentale, esse non valgono per anelli arbitrari.

(8.11) PROPOSIZIONE *Sia  $R$  l'anello degli interi in un campo di numeri quadratico immaginario.*

- (a) (Legge di cancellazione) *Siano  $A, B, C$  ideali non nulli di  $R$ . Se  $AB \supseteq AC$ , allora  $B \supseteq C$ . Se  $AB = AC$ , allora  $B = C$ .*
- (b) *Se  $A$  e  $B$  sono ideali non nulli di  $R$ , allora  $A \supseteq B$  se e solo se  $A$  divide  $B$  ossia, se e solo se  $B = AC$  per qualche ideale  $C$ .*
- (c) *Sia  $P$  un ideale primo non nullo di  $R$ . Se  $P$  divide un prodotto  $AB$  di ideali, allora  $P$  divide uno dei fattori  $A$  o  $B$ .*

*Dimostrazione.* (a) Supponiamo che  $AB \supseteq AC$ . Se  $A = (\alpha)$  è principale, allora  $AB = \alpha B$  e  $AC = \alpha C$  (8.3). Considerando questi insiemi come sottoinsiemi di  $C$ , moltiplichiamo la relazione  $\alpha B \supseteq \alpha C$  a sinistra per  $\alpha^{-1}$  per concludere che  $B \supseteq C$ . Pertanto l'asserzione è vera quando  $A$  è principale. In generale, se  $AB \supseteq AC$ , allora moltiplicando ambo i membri per  $\bar{A}$  e applicando il Lemma fondamentale, si ha:  $nB = \bar{A}AB \supseteq \bar{A}AC = nC$ . Applicando ciò che è già stato dimostrato, si ottiene la tesi. Il caso in cui  $AB = AC$  si dimostra nello stesso modo.

(b) L'implicazione non immediata è che se  $A$  contiene  $B$ , allora  $A$  divide  $B$ . Verificheremo innanzitutto ciò quando  $A = (\alpha)$  è principale. In questo caso, dire che  $(\alpha) \supseteq B$  significa dire che  $\alpha$  divide ogni elemento  $\beta$  di  $B$ . Sia  $C = \alpha^{-1}B$  l'insieme dei quozienti, ossia, l'insieme degli elementi  $\alpha^{-1}\beta$ , con  $\beta = \alpha\gamma \in B$ . Si può verificare che  $C$  è un ideale e che  $\alpha C = B$ . Ne segue che  $B = AC$  in questo caso. Sia ora  $A$  un ideale arbitrario (non nullo), e supponiamo che  $A \supseteq B$ . Allora  $(n) = \bar{A}A \supseteq \bar{A}B$ . Per quanto è stato già dimostrato, esiste un ideale  $C$  tale che  $nC = \bar{A}B$ , ossia  $\bar{A}AC = \bar{A}B$ . In base alla legge di cancellazione, si ha:  $AC = B$ .

(c) Per dimostrare l'enunciato (c), applichiamo la parte (b) per tradurre la divisibilità nell'inclusione. Allora (c) segue dalla definizione di ideale primo. ■

*Dimostrazione del teorema (8.9).* Occorre dimostrare due cose. Innanzitutto, dobbiamo provare che ogni ideale (non nullo) proprio  $A$  è un prodotto di ideali primi. Se  $A$  non è primo, allora certamente non è massimale, sicché possiamo trovare un ideale proprio  $A_1$  strettamente più grande di  $A$ . Allora  $A_1$  divide  $A$  (8.11b), e pertanto possiamo scrivere  $A = A_1B_1$ . Ne segue che  $A \subset B_1$ . Inoltre, se avessimo  $A = B_1$ , la legge di cancellazione implicherebbe che  $R = A_1$ , contraddicendo il fatto che  $A_1$  è un ideale proprio. Dunque  $A < B_1$ . Similmente,  $A < A_1$ . Poiché vi è soltanto un numero finito di ideali compresi tra  $A$  e  $R$ , questo processo di fattorizzazione di un ideale termina dopo un numero finito di passi, quando tutti i fattori sono massimali, e quindi primi. Pertanto ogni ideale proprio  $A$  può essere fattorizzato in un prodotto di ideali primi.

Ora, per dimostrare l'unicità della fattorizzazione, applichiamo la proprietà (8.11c) degli ideali primi, secondo cui, se  $P_1 \cdots P_r = Q_1 \cdots Q_s$ , con  $P_i, Q_j$  ideali primi, allora  $P_1$  divide  $Q_1 \cdots Q_s$ , e quindi divide uno dei fattori, diciamo  $Q_1$ . Poiché  $Q_1$  è massimale, si ha  $P_1 = Q_1$ . A questo punto, cancellando mediante (8.11a) e procedendo per induzione su  $r$ , si ottiene la tesi. ■

(8.12) TEOREMA *L'anello degli interi  $R$  è un dominio a fattorizzazione unica se e solo se è un dominio a ideali principali. In tal caso, le fattorizzazioni degli elementi e degli ideali corrispondono tra loro in modo naturale.*

*Dimostrazione.* Già sappiamo che un dominio a ideali principali è un dominio a fattorizzazione unica (2.12). Viceversa, supponiamo che  $R$  sia un dominio a fattorizzazione unica, e sia  $P$  un ideale primo non nullo di  $R$ . Allora  $P$  contiene un elemento irriducibile, diciamo  $\pi$ . Infatti, ogni elemento non nullo  $\alpha$  di  $P$  è un prodotto di elementi irriducibili e, in base alla definizione di ideale primo,  $P$  contiene uno dei suoi fattori irriducibili. D'altra parte (cfr. (2.8)), un elemento irriducibile  $\pi$  è primo, ossia  $(\pi)$  è un ideale primo. Allora, in virtù di (8.8),  $(\pi)$  è massimale. Poiché  $(\pi) \subset P$ , ne segue che  $(\pi) = P$ , e quindi che  $P$  è principale. In base al teorema (8.9), ogni ideale non nullo  $A$  è un prodotto di ideali primi, e pertanto è principale (8.3a). Dunque  $R$  è un dominio a ideali principali. L'ultima asserzione del teorema segue da (2.2). ■

*Dimostrazione del lemma fondamentale (8.10).* Siano  $\alpha$  e  $\beta$  due generatori di  $A$  come reticolo. Allora  $\alpha$  e  $\beta$  sicuramente generano  $A$  anche come ideale, e inoltre  $\bar{\alpha}$  e  $\bar{\beta}$  generano  $\bar{A}$ . Quindi i quattro prodotti  $\alpha\bar{\alpha}$ ,  $\alpha\bar{\beta}$ ,  $\bar{\alpha}\beta$ ,  $\bar{\beta}\beta$  generano l'ideale  $A\bar{A}$ . I tre elementi  $\alpha\bar{\alpha}$ ,  $\beta\bar{\beta}$ ,  $\alpha\bar{\beta} + \bar{\alpha}\beta$  di  $A\bar{A}$  sono uguali ai propri coniugati e quindi sono numeri razionali. Poiché sono anche interi algebrici, risultano interi ordinari. Sia  $n$  il loro massimo comune divisore in  $\mathbb{Z}$ . Allora  $n$  è una combinazione lineare di  $\alpha\bar{\alpha}$ ,  $\beta\bar{\beta}$ ,  $\alpha\bar{\beta} + \bar{\alpha}\beta$  a coefficienti interi. Ne segue che  $n$  appartiene all'ideale prodotto  $A\bar{A}$ , e quindi  $A\bar{A} \supseteq (n)$ . Se dimostriamo che  $n$  divide ciascuno dei quattro generatori dell'ideale  $A\bar{A}$  in  $R$ , ne seguirà che  $(n) \supseteq A\bar{A}$ , e quindi che  $(n) = A\bar{A}$ , ossia la tesi.

Ora, per costruzione,  $n$  divide  $\alpha\bar{\alpha}$  e  $\beta\bar{\beta}$  in  $\mathbb{Z}$ , e quindi in  $R$ . Pertanto dobbiamo dimostrare che  $n$  divide  $\alpha\bar{\beta}$  e  $\bar{\alpha}\beta$  in  $R$ . Gli elementi  $(\alpha\bar{\beta})/n$  e  $(\bar{\alpha}\beta)/n$  sono radici del polinomio  $x^2 - rx + s$ , dove

$$r = \frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{n} \quad \text{e} \quad s = \frac{\alpha\bar{\alpha}}{n} \frac{\beta\bar{\beta}}{n}.$$

In base alla definizione di  $n$ , questi elementi  $r, s$  sono interi, e pertanto questa è un'equazione monica in  $\mathbb{Z}[x]$ . Ne segue che  $(\alpha\bar{\beta})/n$  e  $(\bar{\alpha}\beta)/n$  sono interi algebrici, come richiesto. ■

**Osservazione.** Questo è l'unico punto dove la definizione di intero algebrico è usata direttamente. Il lemma sarebbe falso se prendessimo un anello più piccolo di  $R$ , per esempio se non considerassimo gli elementi con coefficienti semi-interni, quando  $d \equiv 1$  (modulo 4).

### 9 La relazione tra gli ideali primi di $R$ e i numeri primi

Abbiamo visto nel paragrafo 5 in che modo i primi nell'anello degli interi di Gauss sono in relazione con i numeri primi. Un'analisi simile può essere fatta per l'anello  $R$  degli interi in un campo di numeri quadratico. La differenza fondamentale è che  $R$ , di solito, non è un dominio a ideali principali, e pertanto dovremmo parlare di ideali primi piuttosto che di elementi primi. Ciò rende complicata l'estensione degli enunciati (c) e (d) del teorema (5.1), e noi non ci occuperemo qui di questo problema. [Tuttavia, si veda (12.10)].

(9.1) **PROPOSIZIONE** *Sia  $P$  un ideale primo non nullo di  $R$ . Allora esiste un numero primo  $p$  tale che o  $P = (p)$  oppure  $P\bar{P} = (p)$ . Viceversa, sia  $p$  un numero primo. Allora esiste un ideale primo  $P$  di  $R$  tale che o  $P = (p)$  oppure  $P\bar{P} = (p)$ .*

La dimostrazione segue da vicino quella delle parti (a) e (b) del teorema (5.1). ■

Il secondo caso di (9.1) spesso è suddiviso in due sottocasi, a seconda che  $P$  e  $\bar{P}$  siano uguali oppure no. Si usa di solito la terminologia seguente. Se  $(p)$  è un ideale primo si dice che  $p$  rimane primo in  $R$ . Se  $P\bar{P} = (p)$  si dice che  $p$  si spezza in  $R$ , a meno che  $P = \bar{P}$ , nel qual caso si dice che  $p$  si ramifica in  $R$ .

Analizziamo ulteriormente il comportamento dei numeri primi. Supponiamo che  $d \equiv 2$  o  $3$  (modulo 4). In questo caso,  $R = \mathbb{Z}[\delta]$  è isomorfo a  $\mathbb{Z}[x]/(x^2 - d)$ . Ricordiamo che gli ideali primi contenenti l'ideale  $(p)$  corrispondono agli ideali primi dell'anello  $R/(p)$  [cap. 10 (4.3)]. Si noti che:

$$(9.2) \quad R/(p) \approx \mathbb{Z}[x]/(x^2 - d, p).$$

Scambiando l'ordine delle due relazioni  $x^2 - d = 0$  e  $p = 0$ , come nella dimostrazione del teorema (5.1), otteniamo la prima parte della proposizione enunciata qui sotto. La seconda parte si ottiene nello stesso modo, utilizzando il polinomio (6.16).

### (9.3) PROPOSIZIONE

- (a) *Supponiamo che  $d \equiv 2$  o  $3$  (modulo 4). Un numero primo  $p$  rimane primo in  $R$  se e solo se il polinomio  $x^2 - d$  è irriducibile su  $\mathbb{F}_p$ .*
- (b) *Supponiamo che  $d \equiv 1$  (modulo 4). Allora  $p$  rimane primo se e solo se il polinomio  $x^2 - x + \frac{1}{4}(1-d)$  è irriducibile su  $\mathbb{F}_p$ . ■*

### 10 Classi di ideali nei campi quadratici immaginari

Come s'è detto,  $R$  denota l'anello degli interi in un campo di numeri quadratico immaginario. Allo scopo di analizzare fino a che punto l'unicità della fattorizzazione degli elementi viene a mancare in  $R$ , introduciamo una relazione di equivalenza tra ideali che sia compatibile con la moltiplicazione di ideali e tale che gli ideali principali formino una sola classe di equivalenza. Diremo che due ideali  $A, B$  sono simili, e scriveremo  $A \sim B$ , se esistono elementi non nulli  $\sigma, \tau \in R$  tali che:

$$(10.1) \quad \sigma B = \tau A.$$

Questa è una relazione di equivalenza. Le classi di equivalenza rispetto a tale relazione sono chiamate *classi di ideali*, e la classe di ideali di  $A$  sarà denotata con  $\langle A \rangle$ .

Potremmo anche prendere l'elemento  $\lambda = \sigma^{-1}\tau$  del campo di numeri quadratico  $F = \mathbb{Q}[\delta]$  e dire che  $A$  e  $B$  sono simili se

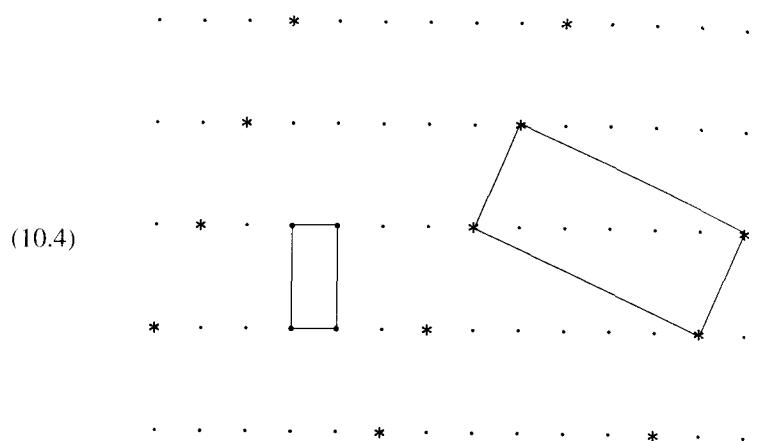
$$(10.2) \quad B = \lambda A, \quad \text{per qualche } \lambda \in \mathbb{Q}[\delta].$$

La relazione di similitudine ha un'elegante interpretazione geometrica. Due ideali  $A$  e  $B$  sono simili se e soltanto se i reticolati che li rappresentano nel piano complesso sono figure geometriche simili, mediante una similitudine che conserva l'orientazione. Per verificare ciò, osserviamo che un reticolo appare con la stessa forma in tutti i suoi punti, quindi possiamo supporre che una similitudine metta in relazione l'elemento  $0$  di  $A$  con l'elemento  $0$  di  $B$ . Allora essa sarà descritta come una rotazione seguita da una dilatazione o da una contrazione, ossia come la moltiplicazione per un numero complesso  $\lambda$ . Poiché la moltiplicazione per  $\lambda$  porta un elemento non nullo  $\alpha \in A$  in un elemento  $\lambda\alpha = \beta \in B$ ,  $\lambda = \beta\alpha^{-1}$  appartiene automaticamente al campo  $F$ .

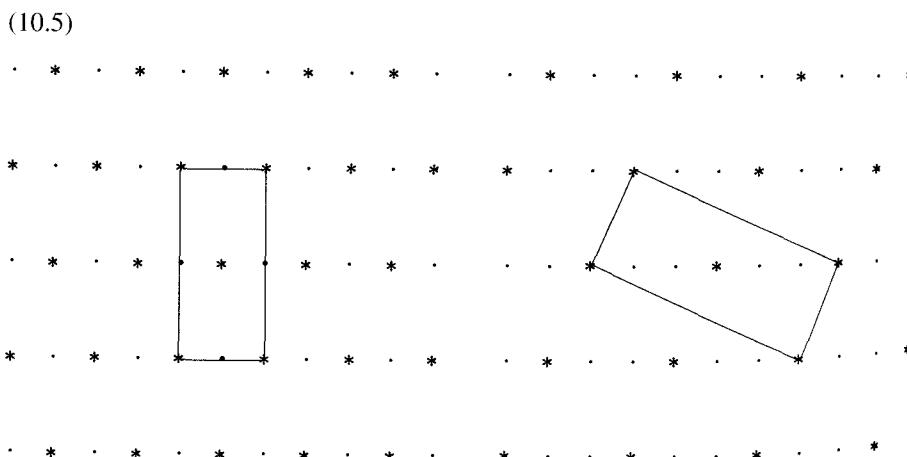
Un ideale  $B$  è simile all'ideale unità  $R$  se e solo se  $B = \lambda R$  per qualche elemento  $\lambda$  del campo. Allora  $\lambda$  è un elemento di  $B$ , e quindi di  $R$ . In questo caso,  $B$  è l'ideale principale  $(\lambda)$ . Pertanto vale il risultato seguente:

(10.3) **PROPOSIZIONE** *La classe di ideali  $\langle R \rangle$  è costituita dagli ideali principali. ■*

La figura (10.4) rappresenta l'ideale principale  $(1 + \delta)$  nell'anello  $\mathbb{Z}[\delta]$ , dove  $\delta = -5$ .

L'ideale principale  $(1 + \delta)$ .

Abbiamo visto in (7.9) che vi sono due classi di ideali. Ciascuno degli ideali  $A = (2, 1 + \delta)$  e  $B = (3, 1 + \delta)$ , per esempio, rappresenta la classe degli ideali non principali. In questo caso,  $2B = (1 + \delta)A$ . Questi ideali sono illustrati nella figura (10.5).

Gli ideali  $(2, 1 + \delta)$  e  $(3, 1 + \delta)$ .

(10.6) PROPOSIZIONE Le classi di ideali formano un gruppo abeliano  $\mathcal{C}$  rispetto alla legge di composizione indotta dalla moltiplicazione di ideali:

$$\langle A \rangle \langle B \rangle = \text{classe di } AB = \langle AB \rangle;$$

la classe degli ideali principali è l'identità:  $\langle R \rangle = \langle 1 \rangle$ .

**Dimostrazione.** Se  $A \sim A'$  e  $B \sim B'$ , allora per definizione  $A' = \lambda A$  e  $B' = \mu B$ , con  $\lambda, \mu \in F = \mathbb{Q}[\delta]$ ; ne segue che  $A'B' = \lambda\mu AB$ . Ciò prova che  $\langle AB \rangle = \langle A'B' \rangle$ , e quindi questa legge di composizione è ben definita. Inoltre è commutativa e associativa poiché tale è la moltiplicazione di ideali, e la classe di  $R$  è l'identità (8.2). Infine,  $A\bar{A} = (n)$  è principale, in base al lemma fondamentale (8.10). Poiché la classe dell'ideale principale  $(n)$  è l'identità in  $\mathcal{C}$ , si ha:  $\langle A \rangle \langle \bar{A} \rangle = \langle R \rangle$ , sicché  $\langle \bar{A} \rangle = \langle A \rangle^{-1}$ . ■

(10.7) COROLLARIO Sia  $R$  l'anello degli interi in un campo di numeri quadratico immaginario. Le seguenti affermazioni sono equivalenti:

- (i)  $R$  è un dominio a ideali principali;
- (ii)  $R$  è un dominio a fattorizzazione unica;
- (iii) il gruppo delle classi di ideali  $\mathcal{C}$  di  $R$  è il gruppo banale.

Infatti, dire che  $\mathcal{C}$  è banale equivale a dire che ogni ideale è simile all'ideale unità, il che, in base alla proposizione (10.3), significa che ogni ideale è principale. In virtù del teorema (8.12), ciò accade se e soltanto se  $R$  è un dominio a fattorizzazione unica. ■

Alla luce del corollario (10.7), è naturale contare le classi di ideali e considerare il risultato, chiamato il *numero di classe*, come una misura della non unicità della fattorizzazione degli elementi in  $R$ . Informazioni più precise si ottengono dalla struttura di  $\mathcal{C}$  come gruppo. Come abbiamo visto (7.9), vi sono due classi di ideali nell'anello  $\mathbb{Z}[\sqrt{-5}]$ ; pertanto il suo gruppo delle classi di ideali è un gruppo ciclico di ordine 2 e il suo numero di classe è 2.

Dimostreremo ora che il gruppo delle classi di ideali  $\mathcal{C}$  è sempre un gruppo finito. La dimostrazione è basata su un famoso lemma di Minkowski relativo ai punti di un reticolo in una regione convessa. Un sottoinsieme limitato  $S$  del piano  $\mathbb{R}^2$  si dice *convesso* e *simmetrico rispetto all'origine*, se possiede le seguenti proprietà:

- (10.8) (a) Convessità: Se  $p, q \in S$ , allora il segmento di retta che congiunge  $p$  e  $q$  è contenuto in  $S$ .  
 (b) Simmetria rispetto all'origine: Se  $p \in S$ , allora  $-p \in S$ .

Si noti che queste condizioni implicano che  $0 \in S$ , a meno che  $S$  non sia vuoto.

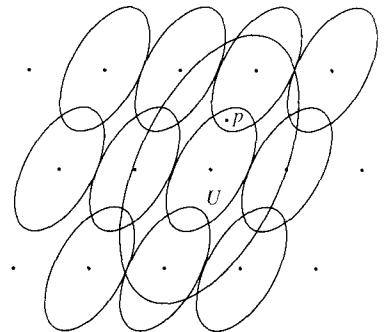
(10.9) LEMMA DI MINKOWSKI Sia  $L$  un reticolo in  $\mathbb{R}^2$ , e sia  $S$  un sottoinsieme di  $\mathbb{R}^2$  convesso e simmetrico rispetto all'origine. Si denoti con  $\Delta(L)$  l'area del parallelogramma generato da una base del reticolo  $L$ . Se si ha:

$$\text{Area}(S) > 4 \Delta(L),$$

allora  $S$  contiene un punto del reticolo diverso da 0.

**Dimostrazione.** Definiamo  $U$  come l'insieme convesso simile a  $S$ , ma avente la dimensione lineare ridotta della metà. In altre parole, poniamo  $p \in U$  se  $2p \in S$ . Allora anche  $U$  è convesso e simmetrico rispetto all'origine, e risulta:  $\text{Area}(U) = \frac{1}{4} \text{Area}(S)$ . Pertanto la diseguaglianza in esame può essere riscritta nella forma:  $\text{Area}(U) > \Delta(L)$ .

(10.10)



(10.11) **LEMMA** Esiste un elemento  $\alpha \in L$  tale che  $U \cap (U + \alpha)$  non è vuoto.

**Dimostrazione.** Sia  $P$  il parallelogramma generato da una base del reticolo  $L$ . I parallelogrammi traslati  $P + \alpha$ , con  $\alpha \in L$ , ricoprono il piano senza sovrapporsi tranne che lungo i loro lati. Il motivo euristico per cui il lemma è vero è che vi è un solo traslato  $U + \alpha$  per ciascun traslato  $P + \alpha$ , e l'area di  $U$  è maggiore dell'area di  $P$ , sicché i traslati  $U + \alpha$  devono sovrapporsi. Per rendere preciso questo ragionamento, osserviamo che, poiché  $U$  è un insieme limitato, esso interseca un numero finito di traslati  $P + \alpha$ , diciamo  $P + \alpha_1, \dots, P + \alpha_k$ . Denotiamo con  $U_i$  l'insieme  $(P + \alpha_i) \cap U$ . Allora  $U$  è scomposto nei pezzi  $U_1, \dots, U_k$ , e inoltre

$$\text{Area}(U) = \sum \text{Area}(U_i).$$

Riportiamo indietro  $U_i$  in  $P$  sottraendo  $\alpha_i$ , ponendo  $V_i = U_i - \alpha_i$ , e osserviamo che  $V_i = P \cap (U - \alpha_i)$ . Pertanto  $V_i$  è un sottoinsieme di  $P$ , e inoltre  $\text{Area}(V_i) = \text{Area}(U_i)$ . Allora

$$\sum \text{Area}(V_i) = \text{Area}(U) > \Delta(L) = \text{Area}(P).$$

Ciò implica che due degli insiemi  $V_i$  devono sovrapporsi, ossia, che per qualche  $i \neq j$ ,  $(U - \alpha_i) \cap (U - \alpha_j)$  non è l'insieme vuoto. Aggiungendo  $\alpha_i$  e ponendo  $\alpha = \alpha_i - \alpha_j$ , si ottiene che anche  $U \cap (U + \alpha)$  è non vuoto. ■

Ritornando alla dimostrazione del lemma di Minkowski, scegliamo  $\alpha$  come nel lemma (10.11), e sia  $p$  un punto di  $U \cap (U + \alpha)$ . Poiché  $p \in U + \alpha$ , ne segue che  $p - \alpha \in U$ , e quindi, per simmetria, anche  $q = \alpha - p \in U$ . Il punto medio tra  $p$  e

$\alpha$ , che appartiene anch'esso a  $U$ , poiché  $U$  è convesso. Pertanto  $\alpha \in S$ , come dimostrato. ■

(10.12) **COROLLARIO** Ogni reticolo  $L$  in  $\mathbb{R}^2$  contiene un vettore non nullo  $\alpha$  tale che

$$|\alpha|^2 \leq 4 \Delta(L)/\pi.$$

**Dimostrazione.** Applichiamo il lemma di Minkowski, prendendo come  $S$  un cerchio di raggio  $r$  intorno all'origine. Il lemma garantisce l'esistenza di un punto del reticolo diverso da 0 in  $S$ , purché  $\pi r^2 > 4 \Delta(L)$ , ossia,  $r^2 > 4 \Delta(L)/\pi$ . Pertanto per ogni numero reale positivo  $\epsilon$ , esiste un punto  $\alpha$  del reticolo, con  $|\alpha|^2 < 4 \Delta(L)/\pi + \epsilon$ . Poiché vi sono soltanto un numero finito di punti del reticolo in una regione limitata e poiché  $\epsilon$  può essere arbitrariamente piccolo, esiste un punto del reticolo che soddisfa la diseguaglianza richiesta. ■

Ritorniamo ora agli ideali nell'anello  $R$  degli interi in un campo quadratico immaginario. Vi sono due misure per la grandezza di un ideale, che risultano coincidenti, come vedremo. La prima è l'indice in  $R$ . Poiché un ideale  $A$  è un sottoreticolo di  $R$ , esso ha indice finito:

$$[R : A] = \text{numero delle classi laterali additive di } A \text{ in } R.$$

Tale indice può venire espresso per mezzo dell'area del parallelogramma generato dai vettori di una base:

(10.13) **LEMMA** Siano  $(a_1, a_2)$  e  $(b_1, b_2)$  basi per i reticolati  $A \subset B$  in  $\mathbb{R}^2$ , e siano  $\Delta(A)$  e  $\Delta(B)$  le aree dei parallelogrammi generati da queste basi. Allora  $[B : A] = \Delta(A)/\Delta(B)$ .

La dimostrazione è lasciata come esercizio. ■

(10.14) **COROLLARIO**

- (a) **Sia**  $A$  **un reticolo piano.** L'area  $\Delta(A)$  è indipendente dalla base del reticolo  $A$ .
- (b) **Se**  $C \supset B \supset A$  sono reticolati, allora  $[C : A] = [C : B][B : A]$ . ■

È facile calcolare l'area  $\Delta(R)$  utilizzando la descrizione (6.14) dell'anello:

$$(10.15) \quad \Delta(R) = \frac{1}{2} \sqrt{|D|} = \begin{cases} \sqrt{|d|}, & \text{se } d \equiv 2, 3 \pmod{4} \\ \frac{1}{2} \sqrt{|d|}, & \text{se } d \equiv 1 \pmod{4} \end{cases}$$

dove  $D$  è il discriminante (6.18).

L'altra misura della grandezza di un ideale può essere ottenuta dal lemma fondamentale (8.10): scriviamo  $A\bar{A} = (n)$  e prendiamo l'intero  $n$  (positivo, naturalmente). Esso è analogo alla norma di un elemento (7.1) e pertanto è chiamato la *norma* dell'ideale:

$$(10.16) \quad N(A) = n, \quad \text{se } A\bar{A} = (n).$$

Essa ha la proprietà moltiplicativa:

$$(10.17) \quad N(AB) = N(A)N(B),$$

poiché  $AB\bar{AB} = A\bar{A}B\bar{B} = (nm)$ , se  $N(B) = m$ . Si noti inoltre che, se  $A$  è l'ideale principale  $(\alpha)$ , allora la sua norma è la norma di  $\alpha$ :

$$(10.18) \quad N((\alpha)) = \alpha\bar{\alpha} = N(\alpha) = |\alpha|^2,$$

poiché  $(\alpha)(\bar{\alpha}) = (\alpha\bar{\alpha})$ .

(10.19) LEMMA *Per ogni ideale non nullo  $A$  di  $R$ , si ha:*

$$[R : A] = N(A).$$

(10.20) COROLLARIO Proprietà moltiplicativa dell'indice: *Siano  $A$  e  $B$  ideali non nulli di  $R$ . Allora*

$$[R : AB] = [R : A][R : B]. \blacksquare$$

Rimandiamo la dimostrazione del lemma (10.19) e ricaviamo da esso la finitezza del numero di classe.

(10.21) TEOREMA *Poniamo  $\mu = 2\sqrt{|D|}/\pi$ . Ogni classe di ideali contiene un ideale  $A$  tale che  $N(A) \leq \mu$ .*

*Dimostrazione.* Sia  $A$  un ideale. Dobbiamo trovare un altro ideale  $A'$  nella classe di  $A$  che abbia norma non più grande di  $\mu$ . In virtù del corollario (10.12) esiste un elemento  $\alpha \in A$  tale che

$$N(\alpha) = |\alpha|^2 \leq 4\Delta(A)/\pi.$$

Allora  $A \supset (\alpha)$ . Ciò implica che  $A$  divide  $(\alpha)$ , ossia, che  $AC = (\alpha)$  per qualche ideale  $C$ . In base alla proprietà moltiplicativa delle norme (10.17) e a (10.18), si ha:

$$N(A)N(C) = N(\alpha) \leq 4\Delta(A)/\pi.$$

Utilizzando (10.13), (10.14) e (10.19), scriviamo

$$\Delta(A) = [R : A]\Delta(R) = \frac{1}{2}N(A)\sqrt{|D|}.$$

Sostituendo l'espressione ora trovata per  $\Delta(A)$  e cancellando  $N(A)$ , otteniamo  $N(C) \leq \mu$ .

Ora, poiché  $CA$  è un ideale principale, la classe  $\langle C \rangle$  è l'inversa di  $\langle A \rangle$ , ossia  $\langle C \rangle = \langle \bar{A} \rangle$ . Pertanto abbiamo dimostrato che  $\langle \bar{A} \rangle$  contiene un ideale la cui norma soddisfa la diseguaglianza richiesta. Scambiando i ruoli di  $A$  e  $\bar{A}$  si completa la dimostrazione. ■

La finitezza del numero di classe segue facilmente:

(10.22) TEOREMA *Il gruppo delle classi di ideali  $\mathcal{C}$  è finito.*

*Dimostrazione.* In virtù di (10.19) e (10.21), basta dimostrare che esiste un numero finito di ideali  $A$  con indice  $[R : A] \leq \mu$ , quindi basta far vedere che esiste soltanto un numero finito di sottoreticolari  $L \subset R$  con  $[R : L] \leq \mu$ . Scegliamo un intero  $n \leq \mu$ , e sia  $L$  un sottoreticolo tale che  $[R : L] = n$ . Allora  $R/L$  è un gruppo abeliano di ordine  $n$ , e pertanto la moltiplicazione per  $n$  è l'applicazione nulla su questo gruppo. Ciò si traduce in  $R$  nella relazione  $nR \subset L$ , ossia i sottoreticolari di indice  $n$  contengono  $nR$ . Dal lemma (8.7) segue che vi è un numero finito di reticolari  $L$  siffatti. Poiché vi è un numero finito di possibilità per  $n$ , la tesi è dimostrata. ■

Il gruppo delle classi di ideali può essere calcolato esplicitamente cercando i sottoreticolari  $L \subset R$  di indice  $\leq \mu$  che sono ideali, ma questo non è un metodo efficiente. È meglio cercare direttamente gli ideali primi. Denotiamo con  $[\mu]$  il più grande intero minore di  $\mu$ .

(10.23) PROPOSIZIONE *Il gruppo delle classi di ideali  $\mathcal{C}$  è generato dalle classi degli ideali primi  $P$  che dividono  $(p)$ , essendo  $p$  un numero primo  $\leq [\mu]$ .*

*Dimostrazione.* Sappiamo che ogni classe contiene un ideale  $A$  di norma  $N(A) \leq \mu$ , e poiché  $N(A)$  è un intero, si ha  $N(A) \leq [\mu]$ . Supponiamo che un ideale  $A$  con norma  $\leq \mu$  sia fattorizzato in un prodotto di ideali primi:  $A = P_1 \cdots P_k$ . Allora  $N(A) = N(P_1) \cdots N(P_k)$ , in virtù di (10.17). Ne segue che  $N(P_i) \leq [\mu]$  per ogni  $i$ , e quindi le classi degli ideali primi  $P$  di norma  $\leq [\mu]$  formano un insieme di generatori di  $\mathcal{C}$ , come asserito. ■

Per applicare questa proposizione, esaminiamo ciascun numero primo  $p \leq [\mu]$ . Se  $p$  rimane primo in  $R$ , allora l'ideale primo  $(p)$  è principale, e quindi la sua classe è banale. Scartiamo questi primi. Se  $p$  non rimane primo in  $R$ , allora

includiamo nel nostro insieme di generatori la classe di uno dei suoi due fattori dati da ideali primi,  $P$ . La classe dell'altro fattore primo è la sua inversa. Può ancora accadere che  $P$  sia un ideale principale, nel qual caso verrà scartato. Gli ideali primi che rimangono generano  $\mathcal{C}$ .

La tabella (10.24) riporta alcuni valori che illustrano vari gruppi.

$d$	$D$	$[\mu]$	Gruppo delle classi di ideali
(10.24)	-2	1	banale
	-5	2	ordine 2
	-13	4	ordine 2
	-14	4	ordine 4, ciclico
	-21	5	gruppo quadrinomio di Klein
	-23	3	ordine 3
	-26	6	ordine 6
	-47	4	ordine 5
	-71	5	ordine 7

Alcuni gruppi di classi di ideali.

### (10.25) Esempi

Per applicare la proposizione (10.23), fattorizziamo  $(p)$  in un prodotto di ideali primi, per ogni primo  $p \leq \mu$ .

- (a)  $d = -7$ . In questo caso  $[\mu] = 1$ . La proposizione (10.23) ci dice che il gruppo delle classi  $\mathcal{C}$  è generato dall'insieme vuoto di ideali primi. Pertanto  $\mathcal{C}$  è banale, e  $R$  è un dominio a fattorizzazione unica.
- (b)  $d = -67$ . In questo caso  $R = \mathbb{Z}[\eta]$ , dove  $\eta = \frac{1}{2}(1+\delta)$ , e  $[\mu] = 5$ . Il gruppo delle classi di ideali è generato dagli ideali primi che dividono  $(2), (3), (5)$ . In base alla proposizione (9.3), un numero primo  $p$  rimane primo in  $R$  se e solo se il polinomio  $x^2 - x + 17$  è irriducibile modulo  $p$ . Ciò è vero per ciascuno dei primi  $2, 3, 5$ . Pertanto gli ideali primi in questione sono principali, e il gruppo delle classi di ideali è banale.
- (c)  $d = -14$ . In questo caso  $[\mu] = 4$ , sicché  $\mathcal{C}$  è generato dagli ideali primi che dividono  $(2)$  e  $(3)$ . Il polinomio  $x^2 + 14$  è riducibile sia modulo 2 che modulo 3, e pertanto, in base a (9.3), nessuno di questi interi rimane primo in  $R$ . Allora si avrà, diciamo,  $(2) = P\bar{P}$  e  $(3) = Q\bar{Q}$ . Come abbiamo visto nel caso di  $\mathbb{Z}[\sqrt{-5}]$ , otteniamo che  $P = (2, \delta) = \bar{P}$ . La classe di ideali  $\langle P \rangle$  ha ordine 2 in  $\mathcal{C}$ .

Per calcolare l'ordine della classe  $\langle Q \rangle$ , possiamo calcolare esplicitamente le potenze dell'ideale e trovare la prima potenza il cui reticolo sia simile a  $R$ , ma questo metodo non è efficiente. È meglio calcolare le norme di alcuni ele-

menti piccoli di  $R$ , sperando di dedurre una relazione tra i generatori. Ovviamente, i primi elementi da prendere in considerazione sono  $\delta$  e  $1+\delta$ . Ma  $N(\delta) = 14$  e  $N(1+\delta) = 15$ , e quindi fanno intervenire i primi 7 e 5, i cui fattori non rientrano tra i nostri generatori. Preferiremmo non considerare questi altri primi. L'elemento  $2+\delta$  è migliore, poiché  $N(2+\delta) = (2+\delta)(2-\delta) = 2 \cdot 3 \cdot 3$ . Ciò fornisce la relazione tra ideali:

$$(2+\delta)(2-\delta) = P\bar{P}Q\bar{Q}Q\bar{Q} = P^2Q^2\bar{Q}^2.$$

Poiché  $2+\delta$  e  $2-\delta$  non sono associati, non generano lo stesso ideale, ma ideali coniugati. Tenendo conto di questi fatti, le sole fattorizzazioni possibili in fattori primi di  $(2+\delta)$  sono  $PQ^2$  e  $P\bar{Q}^2$ . Il caso in cui ci troviamo dipende da quale fattore di  $(3)$  viene contrassegnato con  $Q$ . Pertanto possiamo supporre che  $(2+\delta) = PQ^2$ . Allora, poiché  $(2+\delta)$  è un ideale principale,  $\langle P \rangle \langle Q \rangle^2 = \langle 1 \rangle$  in  $\mathcal{C}$ . Ne segue che  $\langle Q \rangle^2 = \langle P \rangle^{-1} = \langle P \rangle$ . Ciò prova che  $\mathcal{C}$  è il gruppo ciclico di ordine 4 generato da  $\langle Q \rangle$ .

(d)  $d = -23$ , e quindi  $R = \mathbb{Z}[\eta]$ , dove  $\eta = \frac{1}{2}(1+\delta)$ . Allora  $[\mu] = 3$ , sicché  $\mathcal{C}$  è generato dalle classi degli ideali primi che dividono  $(2)$  e  $(3)$ . Entrambi questi primi si spezzano in  $R$ , poiché il polinomio  $x^2 - x + 6$  è riducibile modulo 2 e modulo 3 (9.3). Infatti,  $(2) = P\bar{P}$ , dove  $P$  ha la base di reticolo  $(2, \eta)$  [cfr. (7.8)]. Questo non è un ideale principale.

Scriviamo poi  $(3) = Q\bar{Q}$ . Per determinare la struttura del gruppo delle classi di ideali, osserviamo che  $N(\eta) = 2 \cdot 3$  e  $N(1+\eta) = 2 \cdot 2 \cdot 2$ . Pertanto si ha:

$$(\eta)(\bar{\eta}) = P\bar{P}Q\bar{Q} \quad \text{e} \quad (1+\eta)(\bar{1+\eta}) = (8) = (2)^3 = P^3\bar{P}^3.$$

Scambiando i ruoli di  $P, \bar{P}$  e di  $Q, \bar{Q}$ , se necessario, otteniamo  $(\eta) = PQ$  e  $(1+\eta) = P^3$  oppure  $\bar{P}^3$ . Pertanto  $\langle P \rangle^3 = \langle 1 \rangle$  e  $\langle Q \rangle = \langle P \rangle^{-1}$  in  $\mathcal{C}$ . Il gruppo delle classi di ideali è un gruppo ciclico di ordine 3. ■

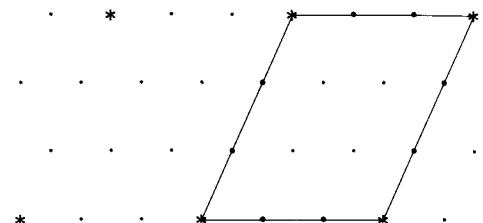
*Dimostrazione del lemma* (10.19). Questo lemma è vero per l'ideale unità  $R$ . Dimostreremo che  $[R : P] = N(P)$ , se  $P$  è un ideale primo e inoltre che, se  $P$  è un ideale primo e  $A$  è un ideale non nullo arbitrario, allora  $[R : AP] = [R : A][R : P]$ . Ne seguirà che, se  $[R : A] = N(A)$ , allora  $[R : AP] = N(AP)$ . Procedendo per induzione sulla lunghezza della fattorizzazione in primi di un ideale, si completerà la dimostrazione.

(10.26) LEMMA Sia  $n$  un intero ordinario, e sia  $A$  un ideale. Allora

$$[R : nA] = n^2[R : A].$$

*Dimostrazione.* Sappiamo che  $R \supset A \supset nA$ , e pertanto (10.14b)  $[R : nA] = [R : A][A : nA]$ . Dunque dobbiamo dimostrare che  $[A : nA] = n^2$ . Ora  $A$  è un reticolo, e  $nA$  è il sottoreticolo ottenuto mediante una dilatazione con fattore  $n$ :

(10.27)



$$3A = \{*\}.$$

Chiaramente,  $[A : nA] = n^2$ , come richiesto. ■

Ritorniamo alla dimostrazione del lemma (10.19). Vi sono due casi da considerare per l'ideale  $P$ . In base a (9.1), esiste un numero primo  $p$  tale che o  $P = (p)$  oppure  $P\bar{P} = (p)$ .

Nel primo caso,  $N(P) = p^2$ , e  $AP = pA$ . Possiamo usare il Lemma (10.26) due volte per concludere che  $[R : AP] = p^2[R : A]$  e  $[R : P] = p^2[R : R] = p^2$ . Pertanto  $[R : AP] = [R : A][R : P]$  e  $[R : P] = N(P)$ , come richiesto.

Nel secondo caso,  $N(P) = p$ . Consideriamo la catena di ideali  $A > AP > A\bar{P}$ . Dalla legge di cancellazione (8.11a) segue che questa è una catena strettamente decrescente di ideali, e quindi che

$$(10.28) \quad [R : A] < [R : AP] < [R : A\bar{P}].$$

Inoltre, poiché  $P\bar{P} = (p)$ , si ha:  $A\bar{P} = pA$ . Pertanto possiamo applicare di nuovo il lemma (10.26) e concludere che  $[R : A\bar{P}] = p^2[R : A]$ . Poiché ciascun indice in (10.28) è un divisore proprio del successivo, l'unica possibilità è che  $[R : AP] = p[R : A]$ . Applicando questo al caso in cui  $A = R$ , si ha che  $[R : P] = p = N(P)$ . Pertanto otteniamo di nuovo che  $[R : AP] = [R : A][R : P]$  e  $[R : P] = N(P)$ . Ciò completa la dimostrazione. ■

## 11 Campi quadratici reali

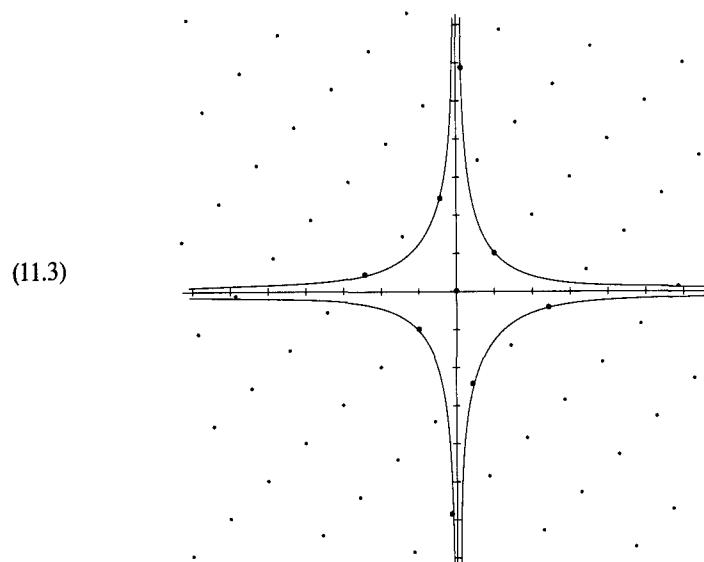
In questo paragrafo daremo un breve sguardo ai campi di numeri quadratici reali  $\mathbb{Q}[\delta]$ , dove  $\delta^2 = d > 0$ . Utilizzeremo come esempio il campo  $\mathbb{Q}[\sqrt{2}]$ . L'anello degli interi in questo campo è

$$(11.1) \quad R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Poiché  $\mathbb{Q}[\sqrt{d}]$  è un sottocampo del campo dei numeri reali, l'anello degli interi non è immerso come un reticolo nel piano complesso, tuttavia possiamo rappresentare  $R$  come un reticolo, usando i coefficienti  $(a, b)$  come coordinate. Una rappresentazione un po' più conveniente di  $R$  come un reticolo si ottiene associando all'intero algebrico  $a + b\sqrt{d}$  il punto  $(u, v)$ , dove

$$(11.2) \quad u = a + b\sqrt{d}, \quad v = a - b\sqrt{d}.$$

Il reticolo così ottenuto è raffigurato qui sotto nel caso  $d = 2$ :



Il reticolo  $\mathbb{Z}[\sqrt{2}]$ .

Poiché il sistema di coordinate  $(u, v)$  è collegato al sistema di coordinate  $(a, b)$  per mezzo della trasformazione lineare (11.2), non vi è una differenza sostanziale tra i due modi di rappresentare  $R$ , anche se, poiché la trasformazione non è ortogonale, la forma del reticolo è diversa nelle due rappresentazioni.

Ricordiamo che il campo  $\mathbb{Q}[\sqrt{d}]$  è isomorfo al campo costruito astrattamente:

$$(11.4) \quad F = \mathbb{Q}[x]/(x^2 - d).$$

Sostituendo  $\mathbb{Q}[\sqrt{d}]$  con  $F$  e denotiamo la classe resto di  $x$  in  $F$  con  $\delta$ . Pertanto questo elemento  $\delta$  è una radice quadrata astratta di  $d$ , piuttosto che la radice quadrata reale positiva. Allora le coordinate  $u, v$  rappresentano i due modi in cui il campo  $F$  definito astrattamente può essere immerso nel campo dei numeri reali; precisamente  $u$  manda  $\delta$  in  $\sqrt{d}$  e  $v$  manda  $\delta$  in  $-\sqrt{d}$ .

Dato un elemento  $\alpha = a + b\delta \in \mathbb{Q}[\delta]$ , denotiamo con  $\alpha'$  l'elemento "coniugato"  $a - b\delta$ . La *norma* di  $\alpha$  è definita ponendo:

$$(11.5) \quad N(\alpha) = \alpha\alpha' = a^2 - db^2,$$

in analogia col caso quadratico immaginario (7.1). Se  $\alpha$  è un intero algebrico, allora  $N(\alpha)$  è un intero, non necessariamente positivo, e inoltre

$$(11.6) \quad N(\alpha\beta) = \alpha\beta\alpha'\beta' = N(\alpha)N(\beta).$$

Con questa definizione di norma, si generalizza la dimostrazione della fattorizzazione unica degli ideali in un prodotto di ideali primi nei campi quadratici immaginari.

Vi sono due differenze notevoli tra i campi quadratici reali e i campi quadratici immaginari. La prima è che per i campi quadratici reali gli ideali appartenenti ad una stessa classe non sono figure geometriche simili, quando sono immersi come reticolati nel piano  $(u, v)$  mediante la trasformazione (11.2). In particolare, gli ideali principali non sono necessariamente simili al reticolo  $R$ . Il motivo è semplice, giacché la moltiplicazione per un elemento  $\alpha = a + b\delta$  altera la coordinata  $u$  per il fattore  $a + b\sqrt{d}$ , e la coordinata  $v$  per il fattore  $a - b\sqrt{d}$ . Questo fatto complica leggermente la geometria, ed è il motivo per cui abbiamo studiato per primo il caso quadratico immaginario. La teoria non cambia in modo essenziale: il numero di classe è ancora finito.

La seconda differenza è più importante: vi sono infinite unità nell'anello degli interi in un campo quadratico reale. Poiché la norma  $N(\alpha)$  di un intero algebrico è un intero ordinario, un'unità deve avere norma  $\pm 1$  come prima [cfr. (7.3)], e se  $N(\alpha) = \alpha\bar{\alpha} = \pm 1$ , allora  $\pm\alpha'$  è l'inverso di  $\alpha$ , sicché  $\alpha$  è un'unità. Per esempio,

$$(11.7) \quad \alpha = 1 + \sqrt{2}, \quad \alpha^2 = 3 + 2\sqrt{2}$$

sono unità nell'anello  $R = \mathbb{Z}[\sqrt{2}]$ . Le loro norme sono  $-1$  e  $1$  rispettivamente. L'elemento  $\alpha$  ha ordine infinito nel gruppo delle unità di  $R$ .

La condizione  $N(\alpha) = a^2 - db^2 = \pm 1$  per le unità si traduce nelle coordinate  $(u, v)$  in:

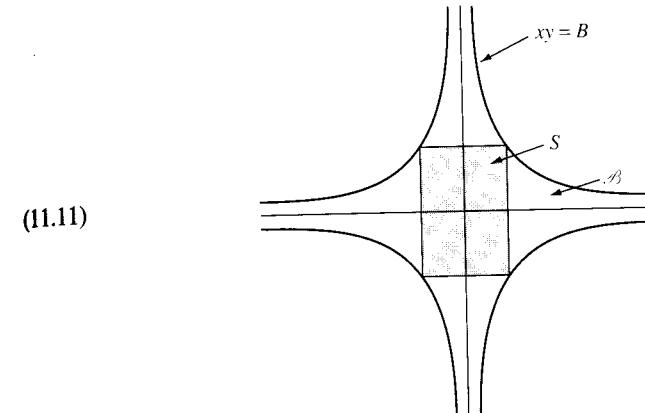
$$(11.8) \quad uv = \pm 1.$$

Le unità sono cioè i punti del reticolo che giacciono su una delle due iperboli  $uv = 1$  e  $uv = -1$ . Queste iperboli sono disegnate nella figura (11.3). È notevole il fatto che i campi quadratici reali hanno sempre infinite unità, o equivalentemente, che il reticolo degli interi contiene sempre infiniti punti sull'iperbole  $uv = 1$ . Questo fatto non è ovvio, né dal punto di vista algebrico, né geometrico.

(11.9) TEOREMA Sia  $R$  l'anello degli interi in un campo di numeri quadratici reali. Il gruppo delle unità in  $R$  è infinito.

(11.10) LEMMA Si denoti con  $\Delta$  l'area del parallelogramma generato da una base di reticolo di  $R$ , nella sua immersione nel piano  $(u, v)$ . Esistono infiniti elementi  $\beta$  di  $R$  la cui norma  $N(\beta)$  è limitata, e più precisamente, tali che  $|N(\beta)| \leq B$ , dove  $B$  è un qualunque numero reale  $> \Delta$ .

*Dimostrazione.* Nell'immersione nel piano  $(u, v)$ , gli elementi di norma  $r$  sono i punti del reticolo che giacciono sull'iperbole  $xy = r$ , e gli elementi la cui norma è limitata in valore assoluto da un numero positivo  $B$  sono quelli che appartengono alla regione  $\mathcal{B}$  limitata dai quattro rami delle iperboli  $xy = B$ ,  $xy = -B$ .



(11.11)

Scegliamo un numero reale positivo arbitrario  $u_0$ . Allora il rettangolo  $S$  i cui vertici sono  $(\pm u_0, \pm B/u_0)$  giace interamente nella regione  $\mathcal{B}$ , e l'area di questo rettangolo è  $4B$ . Pertanto, se  $B > \Delta$ , il lemma di Minkowski garantisce l'esistenza in  $S$  di un punto  $\alpha$  del reticolo diverso da zero. La norma di questo punto è limitata da  $B$ . Ciò è vero per tutti gli  $u_0$ , e se  $u_0$  è molto grande, il rettangolo  $S$  è molto stretto. D'altra parte, non vi sono punti del reticolo sull'asse  $u$ , poiché non vi sono elementi non nulli in  $R$  di norma zero. Pertanto nessun punto del reticolo è contenuto in tutti i rettangoli  $S$ . Ne segue che vi sono infiniti punti del reticolo in  $\mathcal{B}$ . ■

Poiché esiste soltanto un numero finito di interi  $r$  nell'intervallo  $-B \leq r \leq B$ , dal lemma (11.10) discende il seguente corollario:

(11.12) COROLLARIO Per qualche intero  $r$ , esistono infiniti elementi di  $R$  di norma  $r$ . ■

Sia  $r$  un intero. Diremo che due elementi  $\beta_1 = m_1 + n_1\delta$ ,  $\beta_2 = m_2 + n_2\delta$  di  $R$  sono congrui modulo  $r$  se  $r$  divide  $\beta_1 - \beta_2$  in  $R$ . Se  $d \equiv 2$  o  $3$  (modulo 4), ciò significa proprio che  $m_1 \equiv m_2$  e  $n_1 \equiv n_2$  (modulo  $r$ ).

(11.13) LEMMA Siano  $\beta_1, \beta_2$  elementi di  $R$  con la stessa norma  $r$  e congruenti modulo  $r$ . Allora  $\beta_1/\beta_2$  è un'unità di  $R$ .

*Dimostrazione.* Basta provare che  $\beta_1/\beta_2$  appartiene a  $R$ , poiché la stessa argomentazione proverà che  $\beta_2/\beta_1 \in R$ , e quindi che  $\beta_1/\beta_2$  è un'unità. Sia  $\beta'_i = m_i - n_i\delta$  il coniugato di  $\beta_i$ ,  $i = 1, 2$ . Allora  $\beta_1/\beta_2 = \beta_1\beta'_2/\beta_2\beta'_1 = \beta_1\beta'_2/r$ . Ma  $\beta'_2 \equiv \beta'_1$  (modulo  $r$ ), sicché  $\beta_1\beta'_2 \equiv \beta_1\beta'_1 = r$  (modulo  $r$ ). Pertanto  $r$  divide  $\beta_1\beta'_2$ , il che prova che  $\beta_1/\beta_2 \in R$ , come richiesto. ■

*Dimostrazione del teorema (11.9).* Sceglieremo  $r$  in modo tale che vi siano infiniti elementi  $\beta = m + n\delta$  di norma  $r$ . Consideriamo la partizione dell'insieme di questi elementi in classi di congruenza modulo  $r$ . Poiché vi è un numero finito di classi di congruenza, qualche classe contiene infiniti elementi; il quoziente di due elementi qualsiasi di questa classe è un'unità. ■

## 12 Alcune equazioni diofantee

Le equazioni diofantee sono equazioni polinomiali a coefficienti interi, che devono essere risolte in  $\mathbb{Z}$ . La più famosa è l'*equazione di Fermat*:

$$(12.1) \quad x^n + y^n = z^n.$$

L'“ultimo teorema” di Fermat afferma che, se  $n \geq 3$ , questa equazione non ha soluzioni intere  $x, y, z$ , tranne le soluzioni banali in cui una delle variabili è zero. Fermat scrisse questo teorema sul margine di un libro, asserendo che il margine non conteneva abbastanza spazio per la sua dimostrazione. Oggi non si conosce nessuna dimostrazione generale,\* sebbene il teorema sia stato dimostrato per ogni  $n < 10^5$ . Inoltre, un teorema di Faltings del 1983, applicabile a questa equazione così come a molte altre, mostra che esiste soltanto un numero finito di soluzioni intere per ogni valore assegnato di  $n$ .

Questo paragrafo contiene alcuni esempi di equazioni diofantee che possono essere risolte utilizzando l'aritmetica dei campi di numeri quadratici immaginari. Un lettore interessato dovrebbe consultare un testo di teoria dei numeri per una trattazione più organica.

Abbiamo a disposizione due metodi, precisamente l'aritmetica dei campi di numeri quadratici e le congruenze, e li useremo entrambi.

### (12.2) Esempio

Determinazione degli interi  $n$  tali che l'equazione

$$x^2 + y^2 = n$$

abbia una soluzione intera.

\* L'ultimo teorema di Fermat è stato dimostrato nel 1994 da A. Wiles.

Qui il problema è quello di determinare gli interi  $n$  che sono somme di quadrati, o equivalentemente, tali che esiste un punto con coordinate intere sulla circonferenza  $x^2 + y^2 = n$ . Il teorema (5.1) ci dice che, quando  $p$  è primo, l'equazione  $x^2 + y^2 = p$  ha una soluzione intera se e soltanto se  $p = 2$  oppure  $p \equiv 1 \pmod{4}$ . Non è difficile estendere questo risultato agli interi arbitrari. Per fare ciò, interpretiamo una somma di quadrati  $a^2 + b^2$  come la norma  $\alpha\bar{\alpha}$  dell'intero di Gauss  $\alpha = a + bi$ . Allora il problema è quello di stabilire quali sono gli interi  $n$  che risultano norme di interi di Gauss. Ora, se un intero di Gauss  $\alpha$  si fattorizza in un prodotto di primi di Gauss, diciamo  $\alpha = \pi_1 \cdots \pi_k$ , allora anche la sua norma si fattorizza:  $N(\alpha) = N(\pi_1) \cdots N(\pi_k)$ . Pertanto, se  $n$  è la norma di un intero di Gauss, allora esso è un prodotto di norme di primi di Gauss, e viceversa. Le norme dei primi di Gauss sono i primi  $p \equiv 1 \pmod{4}$ , i quadrati dei primi  $p \equiv 3 \pmod{4}$ , e il primo 2. Otteniamo così il teorema seguente:

(12.3) TEOREMA L'equazione  $x^2 + y^2 = n$  ha una soluzione intera se e solo se ogni primo  $p$  che è congruo a 3 modulo 4 ha un esponente pari nella fattorizzazione di  $n$ . ■

### (12.4) Esempio

Determinazione delle soluzioni intere dell'equazione:

$$y^2 + 13 = x^3.$$

Fattorizziamo il primo membro dell'equazione, ottenendo:

$$(y + \delta)(y - \delta) = x^3,$$

dove  $\delta = \sqrt{-13}$ . L'anello degli interi  $R = \mathbb{Z}[\delta]$  non è un dominio a fattorizzazione unica, e pertanto analizzeremo questa equazione utilizzando la fattorizzazione degli ideali.

(12.5) LEMMA Siano  $a, b$  interi, e sia  $R$  un anello contenente  $\mathbb{Z}$  come sottoanello. Se  $a$  e  $b$  sono contenuti in uno stesso ideale proprio  $A$  di  $R$ , allora hanno un fattore primo comune in  $\mathbb{Z}$ .

*Dimostrazione.* Supponiamo per assurdo che  $a, b$  non abbiano fattori primi comuni in  $\mathbb{Z}$ , sicché possiamo scrivere  $1 = ra + sb$ , con  $r, s \in \mathbb{Z}$ . Ne segue che, essendo per ipotesi  $a, b$  contenuti in un ideale proprio  $A$  di  $R$ , anche  $1 \in A$ . Ma un ideale proprio non può contenere un'unità. ■

(12.6) LEMMA Sia  $(x, y)$  una soluzione intera dell'equazione (12.4). Allora i due ideali  $(y + \delta)$  e  $(y - \delta)$  non hanno come fattori comuni ideali primi in  $R$ .

*Dimostrazione.* Sia  $P$  un ideale primo di  $R$  che contenga  $y + \delta$  e  $y - \delta$ . Allora  $2y \in P$  e  $2\delta \in P$ . Poiché  $P$  è un ideale primo, o  $2 \in P$ , oppure  $y \in P$  e  $\delta \in P$ .

Nel primo caso,  $2$  e  $y^2 + 13$  non sono interi primi tra loro, in virtù del lemma (12.5), e poiché  $2$  è primo, esso divide  $y^2 + 13$  in  $\mathbb{Z}$ . Ne segue che  $2$  divide  $x$  e che  $8$  divide  $y^2 + 13 = x^3$ . Pertanto  $y$  deve essere dispari. Allora  $y^2 \equiv 1$  (modulo 4), e quindi  $y^2 + 13 \equiv 2$  (modulo 4). Ciò contraddice il fatto che  $x^3 \equiv 0$  (modulo 8).

Supponiamo che  $y, \delta \in P$ . Allora  $13 \in P$ , e quindi  $13$  e  $y$  non sono relativamente primi in  $\mathbb{Z}$ , ossia  $13$  divide  $y$ . Pertanto  $13$  divide  $x$ , e leggendo l'equazione  $y^2 + 13 = x^3$  modulo  $13^2$ , otteniamo  $13 \equiv 0$  (modulo  $13^2$ ), il che è assurdo. Pertanto abbiamo dimostrato che  $y + \delta$  e  $y - \delta$  sono relativamente primi in  $R$ . ■

Interpretiamo ora l'equazione  $(y + \delta)(y - \delta) = (x)^3$  come un'uguaglianza di ideali principali di  $R$ , e fattorizziamo il secondo membro in primi, diciamo:

$$(y + \delta)(y - \delta) = (P_1 \cdots P_s)^3.$$

Ora, a destra abbiamo un cubo, e i due ideali a sinistra non hanno fattori primi comuni. Ne segue che ciascuno di questi ideali è anch'esso un cubo, diciamo  $(y + \delta) = A^3$  e  $(y - \delta) = \bar{A}^3$  per qualche ideale  $A$ . Osservando la nostra tabella delle classi di ideali (10.24), troviamo che il gruppo delle classi di ideali di  $R$  è ciclico di ordine 2. Pertanto le classi di ideali di  $A$  e  $A^3$  sono uguali. Poiché  $A^3$  è un ideale principale, tale è anche  $A$ , diciamo  $A = (u + v\delta)$ , con  $u, v$  interi. Siamo stati fortunati. Infatti, poiché le unità in  $R$  sono  $\pm 1$ ,  $(u + v\delta)^3 = \pm(y + \delta)$ . Cambiando segno, se necessario, possiamo supporre che  $(u + v\delta)^3 = y + \delta$ .

Completiamo ora l'analisi, studiando l'equazione  $y + \delta = (u + v\delta)^3$ . Sviluppiamo il secondo membro, ottenendo:

$$y + \delta = (u^3 - 39uv^2) + (3u^2v - 13v^3)\delta.$$

Pertanto  $y = u^3 - 39uv^2$  e  $1 = (3u^2 - 13v^2)v$ . Dalla seconda equazione segue che  $v = \pm 1$  e che  $3u^2 - 13 = \pm 1$ . Le uniche possibilità sono  $u = \pm 2$  e  $v = -1$ . Allora  $y = \pm 70$  e  $x = (u + v\delta)(u - v\delta) = 17$ . Questi valori forniscono soluzioni, sicché le soluzioni intere dell'equazione  $y^2 + 13 = x^3$  sono  $x = 17$  e  $y = \pm 70$ . ■

### (12.7) Esempio

Determinazione dei numeri primi  $p$  tali che l'equazione:

$$x^2 + 5y^2 = p$$

abbia una soluzione intera.

Poniamo  $\delta = \sqrt{-5}$  e  $R = \mathbb{Z}[\delta]$ . Sappiamo da (9.3a) che l'ideale principale  $(p)$  si spezza in  $R$  se e soltanto se la congruenza  $x^2 \equiv -5$  (modulo  $p$ ) ha una soluzione intera. Se  $(p) = P\bar{P}$  e se  $P$  è un ideale principale, diciamo  $P = (a + b\delta)$ , allora

$(a + b\delta)(a - b\delta) = (a^2 + 5b^2)$ . Poiché le uniche unità in  $R$  sono  $\pm 1$ ,  $a^2 + 5b^2 = \pm p$ ,

poiché  $a^2 + 5b^2$  è positivo, si ha  $a^2 + 5b^2 = p$ .

Purtroppo  $R$  non è un dominio a ideali principali. Pertanto è abbastanza probabile che  $(p) = P\bar{P}$ , ma che  $P$  non sia un ideale principale. Per analizzare meglio

la situazione, utilizziamo il fatto che vi sono esattamente due classi di ideali in

$\mathbb{Z}$ . Gli ideali principali formano una classe, e l'altra classe è rappresentata da un

ideale non principale arbitrario. L'ideale  $A = (2, 1 + \delta)$  è un ideale non principale, e

ricordiamo che per questo ideale,  $A^2 = A\bar{A} = (2)$ . Ora, poiché il gruppo delle classi

di ideali è ciclico di ordine 2, il prodotto di due ideali nella stessa classe è principale. Supponiamo che  $(p) = P\bar{P}$  e che  $P$  non sia un ideale principale. Ne segue

che  $AP$  è principale, diciamo  $AP = (a + b\delta)$ . Allora  $(a + b\delta)(a - b\delta) = AP\bar{A}P = (2p)$ .

Otteniamo così  $a^2 + 5b^2 = 2p$ .

(12.8) LEMMA Sia  $p$  un numero primo dispari. La congruenza  $x^2 \equiv -5$  (modulo  $p$ ) ha una soluzione se e solo se una delle due equazioni  $x^2 + 5y^2 = p$  o  $x^2 + 5y^2 = 2p$  ha una soluzione intera.

*Dimostrazione.* Se la congruenza ha una soluzione, allora  $(p) = P\bar{P}$ , e i due casi vengono discussi come sopra, a seconda che  $P$  sia o non sia principale. Viceversa, se  $a^2 + 5b^2 = p$ , allora  $(p)$  si spezza in  $R$ , e possiamo applicare (9.3a). Se  $a^2 + 5b^2 = 2p$ , allora  $(a + b\delta)(a - b\delta) = (2p) = A\bar{A}(p)$ . Dalla fattorizzazione unica degli ideali segue che anche  $(p)$  si spezza, e pertanto possiamo applicare ancora (9.3a). ■

Questo lemma non risolve il nostro problema originario, ma abbiamo fatto dei progressi. Nella maggior parte delle situazioni di questo tipo, non potremmo completare la nostra analisi. Ma qui siamo di nuovo fortunati, o meglio questo esempio era stato scelto poiché ammette una soluzione completa. Precisamente, possiamo distinguere i due casi mediante le congruenze. Se  $a^2 + 5b^2 = p$ , allora uno dei due interi  $a, b$  è dispari e l'altro è pari. Calcoliamo la congruenza modulo 4, trovando che  $a^2 + 5b^2 \equiv 1$  (modulo 4), e quindi che  $p \equiv 1$  (modulo 4), in questo caso. Se  $a^2 + 5b^2 = 2p$ , calcoliamo le congruenze modulo 8. Poiché  $p \equiv 1$  o 3 (modulo 4), sappiamo che  $2p \equiv 2$  o 6 (modulo 8). Ogni quadrato è congruo a 0, 1 o 4 (modulo 8). Ne segue che  $5b^2 \equiv 0, 5$  o 4 (modulo 8), il che prova che  $a^2 + 5b^2$  non può essere congruo a 2 (modulo 8). Dunque  $p \equiv 3$  (modulo 4) in questo caso. Abbiamo dimostrato pertanto il lemma seguente:

(12.9) LEMMA Sia  $p$  un numero primo dispari. Supponiamo che la congruenza  $x^2 \equiv -5$  (modulo  $p$ ) abbia una soluzione. Allora  $x^2 + 5y^2 = p$  ha una soluzione intera se  $p \equiv 1$  (modulo 4), e  $x^2 + 5y^2 = 2p$  ha una soluzione intera se  $p \equiv 3$  (modulo 4). ■

Rimane infine il problema di caratterizzare i numeri primi dispari  $p$  tali che la congruenza  $x^2 \equiv -5$  (modulo  $p$ ) abbia una soluzione. Questo viene risolto per mezzo della sorprendente *legge di reciprocità quadratica*, la quale assicura che  $x^2 \equiv 5$  (modulo  $p$ ) ha una soluzione se e solo se  $x^2 \equiv p$  (modulo 5) ne ha una! Inoltre la seconda congruenza ha una soluzione se e soltanto se  $p \equiv \pm 1$  (modulo 5). Mettendo insieme ciò con il lemma precedente e con il fatto che  $-1$  è un quadrato modulo 5, otteniamo:

(12.10) TEOREMA *Sia  $p$  un numero primo dispari. L'equazione  $x^2 + 5y^2 = p$  ha soluzioni intere se e soltanto se  $p \equiv 1$  (modulo 4) e  $p \equiv \pm 1$  (modulo 5).* ■

Ci sembra fuor di dubbio che ancora si nascondano, in questo campo, molte cose importanti sulle quali altri potrà esercitare il proprio ingegno.

Karl Friedrich Gauss

### Esercizi

#### 1 Fattorizzazione di interi e polinomi

1. Siano  $a, b$  interi positivi la cui somma sia un numero primo  $p$ . Dimostrare che il loro massimo comune divisore è 1.
2. Definire il massimo comune divisore di un insieme di  $n$  interi e dimostrarne l'esistenza.
3. Dimostrare che, se  $d$  è il massimo comune divisore di  $a_1, \dots, a_n$ , il massimo comune divisore di  $a_1/d, \dots, a_n/d$  è 1.
4. (a) Dimostrare che, se  $n$  è un intero positivo che non è il quadrato di un intero,  $\sqrt{n}$  non è un numero razionale.  
(b) Dimostrare l'enunciato analogo per le radici  $n$ -esime.
5. (a) Siano  $a, b$  interi con  $a \neq 0$  e scriviamo  $b = aq + r$ , dove  $0 \leq r < |a|$ . Dimostrare che i due massimi comuni divisori  $(a, b)$  e  $(a, r)$  sono uguali.  
(b) Descrivere un algoritmo, basato su (a), per calcolare il massimo comune divisore.  
(c) Utilizzare l'algoritmo trovato per calcolare il massimo comune divisore delle seguenti coppie di numeri:  
**(a)** 1456, 235; **(b)** 123456789, 135792468.
6. Calcolare il massimo comune divisore dei seguenti polinomi:  $x^3 - 6x^2 + x + 4$ ,  $x^5 - 6x + 1$ .
7. Dimostrare che, se due polinomi  $f, g$  a coefficienti in un campo  $F$  si spezzano in fattori lineari in  $F[x]$ , il loro massimo comune divisore è il prodotto dei loro fattori lineari comuni.
8. Scomporre i seguenti polinomi in fattori irriducibili in  $\mathbb{F}_p[x]$ :  
**(a)**  $x^3 + x + 1$ ,  $p = 2$ ; **(b)**  $x^2 - 3x - 3$ ,  $p = 5$ ; **(c)**  $x^2 + 1$ ,  $p = 7$ .
9. Euclide ha dimostrato che esistono infiniti numeri primi osservando che, se  $p_1, \dots, p_k$  sono primi, allora ogni fattore primo  $p$  di  $n = (p_1 \cdot \dots \cdot p_k) + 1$  deve essere diverso da tutti i  $p_i$ .

- (a) Adattare questa argomentazione per dimostrare che, per ogni campo  $F$ , esistono infiniti polinomi irriducibili monici in  $F[x]$ .
- (b) Spiegare perché l'argomentazione non vale per l'anello delle serie formali di potenze  $F[[x]]$ .

#### 10. Frazioni parziali per gli interi:

- (a) Scrivere la frazione  $r = 7/24$  nella forma  $r = a/8 + b/3$ .
- (b) Dimostrare che, se  $n = uv$ , dove  $u, v$  sono primi tra loro, ogni frazione  $r = m/n$  può essere scritta nella forma:  $r = a/u + b/v$ .
- (c) Sia  $n = n_1 n_2 \dots n_k$  la fattorizzazione di un numero intero  $n$  in potenze di primi distinti:  $n_i = p_i^{e_i}$ . Dimostrare che ogni frazione  $r = m/n$  può essere scritta nella forma:  $r = m_1/n_1 + \dots + m_k/n_k$ .

#### 11. Teorema cinese dei resti:

- (a) Siano  $m, n$  interi primi tra loro e siano  $a, b$  interi arbitrari. Dimostrare che esiste un intero  $x$  che è soluzione del sistema di congruenze:  $x \equiv a$  (modulo  $m$ ),  $x \equiv b$  (modulo  $n$ ).
- (b) Determinare tutte le soluzioni di queste due congruenze.

#### 12. Risolvere i seguenti sistemi di congruenze:

- (a)  $x \equiv 3$  (modulo 15),  $x \equiv 5$  (modulo 8),  $x \equiv 2$  (modulo 7).
- (b)  $x \equiv 13$  (modulo 43),  $x \equiv 7$  (modulo 71).

#### 13. Frazioni parziali per i polinomi:

- (a) Dimostrare che ogni funzione razionale in  $\mathbb{C}(x)$  può essere scritta come somma di un polinomio e di una combinazione lineare di funzioni della forma  $1/(x-a)^i$ .
- (b) Trovare una base per  $\mathbb{C}(x)$ , considerato come spazio vettoriale su  $\mathbb{C}$ .

#### \*14. Sia $F$ un sottocampo di $\mathbb{C}$ e sia $f \in F[x]$ un polinomio irriducibile. Dimostrare che $f$ non ha radici multiple in $\mathbb{C}$ .

15. Dimostrare che il massimo comune divisore di due polinomi  $f, g$  in  $\mathbb{Q}[x]$  è anche il loro massimo comune divisore in  $\mathbb{C}[x]$ .
16. Siano  $a, b$  interi primi tra loro. Dimostrare che esistono interi  $m, n$  tali che  $a^m + b^n \equiv 1$  (modulo  $ab$ ).

#### 2 Domini a fattorizzazione unica, domini a ideali principali, domini euclidei

1. Dimostrare o confutare le seguenti affermazioni:
  - (a) L'anello dei polinomi in due variabili  $\mathbb{R}[x, y]$  è un dominio euclideo.
  - (b) L'anello  $\mathbb{Z}[x]$  è un dominio a ideali principali.
2. Dimostrare che i seguenti anelli sono domini euclidei:
  - (a)  $\mathbb{Z}[\zeta]$ ,  $\zeta = e^{2\pi i/3}$ ;
  - (b)  $\mathbb{Z}[\sqrt{-2}]$ .
3. Dare un esempio che mostri che la divisione con resto non è necessariamente unica in un dominio euclideo.

4. Siano  $m, n$  due interi. Dimostrare che il loro massimo comune divisore in  $\mathbb{Z}$  è uguale al loro massimo comune divisore in  $\mathbb{Z}[i]$ .
5. Dimostrare che ogni elemento primo di un dominio di integrità è irriducibile.
6. Dimostrare la proposizione 2.8 secondo cui un dominio  $R$  in cui esiste una fattorizzazione è un dominio a fattorizzazione unica se e solo se ogni elemento irriducibile è primo.
7. Dimostrare che in un dominio a ideali principali  $R$  ogni coppia  $a, b$  di elementi, non entrambi nulli, ha un massimo comune divisore  $d$ , con le seguenti proprietà:
  - (i)  $d = ar + bs$ , con  $r, s \in R$ ;
  - (ii)  $d$  divide sia  $a$  che  $b$ ;
  - (iii) se  $e \in R$  divide  $a, b$ , allora  $e$  divide  $d$ .
 Inoltre,  $d$  è determinato a meno di un fattore invertibile.
8. Trovare il massimo comune divisore di  $11+7i$ ,  $18-i$  in  $\mathbb{Z}[i]$ .
9. (a) Dimostrare che  $2, 3, 1 \pm \sqrt{-5}$  sono elementi irriducibili dell'anello  $R = \mathbb{Z}[\sqrt{-5}]$  e che le unità di questo anello sono  $\pm 1$ .
   
(b) Dimostrare che in questo anello esiste una fattorizzazione.
10. Dimostrare che l'anello  $\mathbb{R}[[t]]$  delle serie formali di potenze a coefficienti reali è un dominio a fattorizzazione unica.
11. (a) Dimostrare che, se  $R$  è un dominio di integrità, allora due elementi  $a, b$  sono associati se e soltanto se differiscono per un fattore invertibile.
   
\*(b) Dare un esempio che mostri che (a) non vale, se  $R$  non è un dominio di integrità.
12. Sia  $R$  un dominio a ideali principali.
  - (a) Dimostrare che, dati due elementi  $a, b$  non entrambi nulli, esiste un *minimo comune multiplo*  $[a, b] = m$  tale che  $a$  e  $b$  dividono  $m$  e che, se  $a$  e  $b$  dividono un elemento  $r \in R$ , allora  $m$  divide  $r$ . Dimostrare che  $m$  è unico a meno di un fattore invertibile.
  - (b) Denotato con  $(a, b)$  il massimo comune divisore di  $a, b$ , dimostrare che  $(a, b)[a, b]$  è un associato di  $ab$ .
13. Se  $a$  e  $b$  sono interi e se  $a$  divide  $b$  nell'anello degli interi di Gauss, allora  $a$  divide  $b$  in  $\mathbb{Z}$ .
14. (a) Dimostrare che l'anello  $R$  (2.4) ottenuto aggiungendo le radici  $2^k$ -esime  $x_k$  di  $x$  ad un anello di polinomi è l'unione degli anelli di polinomi  $F[x_k]$ .
   
(b) Dimostrare che non esiste nessuna decomposizione di  $x_1$  in fattori irriducibili in  $R$ .
15. Per *raffinamento* di una fattorizzazione  $a = b_1 \cdot \dots \cdot b_k$  si intende l'espressione di  $a$  ottenuta fattorizzando i termini  $b_i$ . Si consideri l'anello  $R$  (2.4). Dimostrare che due fattorizzazioni diverse di uno stesso elemento  $a \in R$  hanno raffinamenti tali che tutti i loro fattori sono associati.

6. Sia  $R$  l'anello  $F[u, v, y, x_1, x_2, x_3, \dots]/(x_1y = uv, x_2^2 = x_1, x_3^2 = x_2, \dots)$ . Dimostrare che  $u$  e  $v$  sono elementi irriducibili in  $R$ , ma che il procedimento di fattorizzazione dell'elemento  $uv$  non ha necessariamente termine.
  17. Dimostrare la proposizione (2.9) e il corollario (2.10).
  18. Dimostrare la proposizione (2.11).
  19. Dimostrare che le fattorizzazioni (2.22) sono le decomposizioni in fattori primi in  $\mathbb{Z}[i]$ .
  20. Nello studio della fattorizzazione unica interviene soltanto l'operazione di moltiplicazione in  $R$ , sicché dovrebbe essere possibile estendere le definizioni. Sia  $S$  un semigruppo commutativo, ossia un insieme dotato di una legge di composizione associativa e commutativa con identità. Supponiamo che valga in  $S$  la legge di cancellazione: se  $ab = ac$ , allora  $b = c$ . Introdurre le definizioni opportune in modo da estendere la proposizione (2.8) in questo nuovo contesto.
  - \*21. Dati  $n$  elementi  $v_1, \dots, v_n$  in  $\mathbb{Z}^2$ , possiamo definire un semigruppo  $S$  come l'insieme di tutte le combinazioni lineari di  $(v_1, \dots, v_n)$  a coefficienti interi non negativi, rispetto all'operazione di *addizione*. Determinare quali di questi semigruppi hanno la proprietà della fattorizzazione unica.
- ### 3 Il lemma di Gauss
1. Siano  $a$  e  $b$  elementi di un campo  $F$ , con  $a \neq 0$ . Dimostrare che un polinomio  $f(x) \in F[x]$  è irriducibile se e solo se  $f(ax + b)$  è irriducibile.
  2. Sia  $F = \mathbb{C}(x)$  e siano  $f, g$  elementi di  $\mathbb{C}[x, y]$ . Dimostrare che se  $f$  e  $g$  hanno un fattore comune in  $F[y]$  hanno un fattore comune anche in  $\mathbb{C}[x, y]$ .
  3. Sia  $f$  un polinomio irriducibile in  $\mathbb{C}[x, y]$  e sia  $g$  un altro polinomio. Dimostrare che, se la varietà degli zeri di  $g$  in  $\mathbb{C}^2$  contiene la varietà degli zeri di  $f$ , allora  $f$  divide  $g$ .
  4. Dimostrare che due polinomi a coefficienti interi sono relativamente primi in  $\mathbb{Q}[x]$  se e soltanto se l'ideale che essi generano in  $\mathbb{Z}[x]$  contiene un intero.
  5. Dimostrare il lemma di Gauss senza ricorrere alla riduzione modulo  $p$ , nel modo seguente: Sia  $a_i$  il coefficiente di grado minimo  $i$  di  $f$  che non sia divisibile per  $p$ . Quindi  $p$  divide  $a_\nu$  se  $\nu < i$ , ma  $p$  non divide  $a_i$ . Analogamente, sia  $b_j$  il coefficiente di grado minimo di  $g$  che non sia divisibile per  $p$ . Dimostrare che il coefficiente di  $h$  di grado  $i+j$  non è divisibile per  $p$ .
  6. Enunciare e dimostrare il lemma di Gauss per i domini euclidei.
  - \*7. Il polinomio cubico  $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{C}[x]$  può essere descritto dal punto  $a = (a_0, a_1, a_2) \in \mathbb{C}^3$ . Dimostrare che il luogo dei punti che corrispondono ai polinomi cubici riducibili è una sottovarietà di  $\mathbb{C}^3$ .
  8. Dimostrare che un polinomio a coefficienti interi è primitivo, se e soltanto se, esso non è contenuto in nessuno dei nuclei delle applicazioni (3.2).
  9. Dimostrare che  $\det \begin{bmatrix} x & y \\ z & w \end{bmatrix}$  è irriducibile nell'anello dei polinomi  $\mathbb{C}[x, y, z, w]$ .

10. Dimostrare che il nucleo dell'omomorfismo  $\mathbb{Z}[x] \rightarrow \mathbb{R}$  che manda  $x$  in  $1 + \sqrt{2}$  è un ideale principale, e trovare un generatore per tale ideale.
11. (a) Si consideri l'applicazione  $\psi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$  definita da
- $$f(x, y) \mapsto f(t^2, t^3).$$
- Dimostrare che il suo nucleo è un ideale principale e che la sua immagine è l'insieme dei polinomi  $p(t)$  tali che  $p'(0) = 0$ .
- (b) Si consideri l'applicazione  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$  definita da
- $$f(x, y) \mapsto (t^2 - t, t^3 - t^2).$$
- Dimostrare che il suo nucleo è un ideale principale e che la sua immagine è l'insieme dei polinomi  $p(t)$  tali che  $p(0) = p(1)$ . Dare una spiegazione intuitiva di ciò mediante la geometria della varietà  $\{f = 0\}$  in  $\mathbb{C}^2$ .
- 4 Fattorizzazione esplicita dei polinomi**
1. Dimostrare che i seguenti polinomi sono irriducibili in  $\mathbb{Q}[x]$ :
- (a)  $x^2 + 27x + 213$ ; (b)  $x^3 + 6x + 12$ ; (c)  $8x^3 - 6x + 1$ ;
  - (d)  $x^3 + 6x^2 + 7$ ; (e)  $x^5 - 3x^4 + 3$ .
2. Scomporre il polinomio  $x^5 + 5x + 5$  in fattori irriducibili in  $\mathbb{Q}[x]$  e in  $\mathbb{F}_2[x]$ .
3. Scomporre  $x^3 + x + 1$  in fattori irriducibili in  $\mathbb{F}_p[x]$ , per  $p = 2, 3, 5$ .
4. Scomporre  $x^4 + x^2 + 1$  in fattori irriducibili in  $\mathbb{Q}[x]$ .
5. Supponiamo che un polinomio della forma  $x^4 + bx^2 + c$  sia un prodotto di due polinomi di secondo grado in  $\mathbb{Q}[x]$ . Che cosa si può dire sui coefficienti di tali fattori?
6. Dimostrare che i seguenti polinomi sono irriducibili:
- (a)  $x^2 + x + 1$  nel campo  $\mathbb{F}_2$ ; (b)  $x^2 + 1$  in  $\mathbb{F}_7$ ; (c)  $x^3 - 9$  in  $\mathbb{F}_{31}$ .
7. Decomporre i seguenti polinomi in fattori irriducibili in  $\mathbb{Q}[x]$ :
- (a)  $x^3 - 3x - 2$ ; (b)  $x^3 - 3x + 2$ ; (c)  $x^9 - 6x^6 + 9x^3 - 3$ .
8. Sia  $p$  un numero primo. Dimostrare che il polinomio  $x^n - p$  è irriducibile in  $\mathbb{Q}[x]$ .
9. Utilizzando la riduzione modulo 2, fattorizzare i seguenti polinomi in  $\mathbb{Q}[x]$ :
- (a)  $x^2 + 2345x + 125$ ; (b)  $x^3 + 5x^2 + 10x + 5$ ; (c)  $x^3 + 2x^2 + 3x + 1$ ;
  - (d)  $x^4 + 2x^3 + 2x^2 + 2x + 2$ ; (e)  $x^4 + 2x^3 + 3x^2 + 2x + 1$ ; (f)  $x^4 + 2x^3 + x^2 + 2x + 1$ ;
  - (g)  $x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$ .
10. Sia  $p$  un numero primo e sia  $f \in \mathbb{Z}[x]$  un polinomio di grado  $2n+1$ , cioè  $f(x) = a_{2n+1}x^{2n+1} + \dots + a_1x + a_0$ . Supponiamo che  $a_{2n+1} \not\equiv 0$  (modulo  $p$ ),  $a_0, a_1, \dots, a_n \equiv 0$  (modulo  $p^2$ ),  $a_{n+1}, \dots, a_{2n} \equiv 0$  (modulo  $p$ ),  $a_0 \not\equiv 0$  (modulo  $p^3$ ). Dimostrare che  $f$  è irriducibile in  $\mathbb{Q}[x]$ .
11. Sia  $p$  un numero primo e sia  $A \neq I$  una matrice  $n \times n$  ad elementi interi tale che  $A^p = I$ , ma  $A^{p-1} \neq I$ . Dimostrare che  $n \geq p-1$ .

Determinare i polinomi irriducibili monici di grado 3 su  $\mathbb{F}_3$ .

Determinare i polinomi irriducibili monici di grado 2 su  $\mathbb{F}_5$ .

**14 Formula di interpolazione di Lagrange:**

(a) Siano  $x_0, \dots, x_d$  numeri complessi distinti. Trovare un polinomio  $p(x)$  di grado  $d$  che si annulli in  $x_1, \dots, x_d$  e sia tale che  $p(x_0) = 1$ .

(b) Siano  $x_0, \dots, x_d; y_0, \dots, y_d$  numeri complessi e supponiamo che gli  $x_i$  siano distinti. Allora esiste uno ed un solo polinomio  $g(x) \in \mathbb{C}[x]$  di grado  $\leq d$ , tale che  $g(x_i) = y_i$  per  $i = 0, \dots, d$ . Dimostrare ciò determinando esplicitamente il polinomio  $g$  per mezzo di  $x_i, y_i$ .

\*15. Utilizzare la formula di interpolazione di Lagrange per dare un metodo per trovare tutti i fattori polinomiali a coefficienti interi di un polinomio a coefficienti interi in un numero finito di passi.

16. Sia  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  un polinomio monico a coefficienti interi e sia  $r \in \mathbb{Q}$  una radice razionale di  $f(x)$ . Dimostrare che  $r$  è un intero.

17. Dimostrare che il polinomio  $x^2 + y^2 - 1$  è un elemento irriducibile di  $\mathbb{C}[x, y]$  con il metodo dei coefficienti indeterminati, ossia studiando l'equazione  $(ax + by + c)(a'x + b'y + c') = x^2 + y^2 - 1$ , dove  $a, b, c, a', b', c'$  sono delle incognite.

### 5 Primi nell'anello degli interi di Gauss

1. Dimostrare che ogni primo di Gauss divide uno ed un solo numero primo.

2. Scomporre 30 in fattori primi in  $\mathbb{Z}[i]$ .

3. Scomporre i seguenti interi di Gauss in primi di Gauss:

(a)  $1 - 3i$ ; (b)  $10$ ; (c)  $6 + 9i$ .

4. Fare un disegno chiaro che raffiguri i primi nell'anello degli interi di Gauss aventi grandezza variabile in un intervallo ragionevolmente ampio.

5. Sia  $\pi$  un primo di Gauss. Dimostrare che  $\pi$  e  $\bar{\pi}$  sono associati se e soltanto se o  $\pi$  è associato ad un numero primo oppure  $\pi\bar{\pi} = 2$ .

6. Sia  $R$  l'anello  $\mathbb{Z}[\sqrt{3}]$ . Dimostrare che un numero primo  $p$  è un elemento primo di  $R$  se e solo se il polinomio  $x^2 - 3$  è irriducibile in  $\mathbb{F}_p[x]$ .

7. Descrivere l'anello quoziante  $\mathbb{Z}[i]/(p)$  in ciascuno dei casi seguenti:

(a)  $p = 2$ ; (b)  $p \equiv 1$  (modulo 4); (c)  $p \equiv 3$  (modulo 4).

\*8. Sia  $R = \mathbb{Z}[\zeta]$ , dove  $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$  è una radice cubica complessa di 1. Sia  $p$  un numero primo diverso da 3. Adattare la dimostrazione del teorema (5.1) per dimostrare quanto segue:

(a) Il polinomio  $x^2 + x + 1$  ha una radice in  $\mathbb{F}_p$  se e solo se  $p \equiv 1$  (modulo 3).

(b)  $(p)$  è un ideale primo di  $R$  se e solo se  $p \equiv -1$  (modulo 3).

(c)  $p$  si fattorizza in  $R$  se e solo se si può scrivere nella forma  $p = a^2 + ab + b^2$ , con  $a, b$  interi.

(d) Fare un disegno che raffiguri i primi di valore assoluto  $\leq 10$  in  $R$ .

## 6 Interi algebrici

1. È vero che  $\frac{1}{2}(1+\sqrt{3})$  è un intero algebrico?
2. Sia  $\alpha$  un intero algebrico il cui polinomio irriducibile monico su  $\mathbb{Z}$  sia  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ , e poniamo  $R = \mathbb{Z}[\alpha]$ . Dimostrare che  $\alpha$  è un'unità in  $R$  se e soltanto se  $a_0 = \pm 1$ .
3. Siano  $d$  e  $d'$  due numeri interi distinti privi di quadrati. Dimostrare che  $\mathbb{Q}(\sqrt{d})$  e  $\mathbb{Q}(\sqrt{d'})$  sono sottocampi distinti di  $\mathbb{C}$ .
4. Dimostrare che nell'anello degli interi in un campo di numeri quadratico immaginario esiste una fattorizzazione.
5. Sia  $\alpha$  la radice cubica reale di 10, e poniamo  $\beta = a + b\alpha + c\alpha^2$ , con  $a, b, c \in \mathbb{Q}$ . Allora  $\beta$  è una radice di un polinomio cubico monico  $f(x) \in \mathbb{Q}[x]$ . Il polinomio irriducibile di  $\alpha$  su  $\mathbb{Q}$  è  $x^3 - 10$ , e le sue tre radici sono  $\alpha$ ,  $\alpha' = \zeta\alpha$  e  $\alpha'' = \zeta^2\alpha$ , dove  $\zeta = e^{2\pi i/3}$ . Le tre radici di  $f$  sono  $\beta$ ,  $\beta' = a + b\zeta\alpha + c\zeta^2\alpha^2$  e  $\beta'' = a + b\zeta^2\alpha + c\zeta\alpha^2$ , sicché  $f(x) = (x - \beta)(x - \beta')(x - \beta'')$ .
  - (a) Determinare  $f(x)$  sviluppando il prodotto. (I termini contenenti  $\alpha$  e  $\alpha^2$  devono eliminarsi, sicché non occorre calcolarli).
  - (b) Determinare gli elementi  $\beta$  che risultano interi algebrici.
6. Dimostrare la proposizione (6.17).
7. Dimostrare che l'anello degli interi in un campo quadratico immaginario è un sottoanello massimale di  $\mathbb{C}$  rispetto alla proprietà di essere un reticolo nel piano complesso.
8. (a) Sia  $S = \mathbb{Z}[\alpha]$ , dove  $\alpha$  è una radice complessa di un polinomio monico di grado 2. Dimostrare che  $S$  è un reticolo nel piano complesso.
  - (b) Dimostrare il viceversa, ossia che un sottoanello  $S$  di  $\mathbb{C}$  che risulta un reticolo ha la forma data in (a).
9. Sia  $R$  l'anello degli interi nel campo  $\mathbb{Q}(\sqrt{d})$ .
  - (a) Determinare gli elementi  $\alpha \in R$  tali che  $R = \mathbb{Z}[\alpha]$ .
  - (b) Dimostrare che se  $R = \mathbb{Z}[\alpha]$  e se  $\alpha$  è una radice del polinomio  $x^2 + bx + c$  su  $\mathbb{Q}$ , il discriminante  $b^2 - 4c$  è  $D$  (6.18).

## 7 Fattorizzazione nei campi quadratici immaginari

1. Dimostrare la proposizione (7.3) usando l'aritmetica.
2. Dimostrare che gli elementi  $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$  sono irriducibili nell'anello  $\mathbb{Z}[\sqrt{-5}]$ .
3. Sia  $d = -5$ . Stabilire in quali dei seguenti casi il reticolo delle combinazioni lineari intere dei vettori assegnati risulta un ideale:
  - (a)  $(5, 1+\delta)$ ; (b)  $(7, 1+\delta)$ ; (c)  $(4 - 2\delta, 2 + 2\delta, 6 + 4\delta)$ .
4. Sia  $A$  un ideale dell'anello degli interi  $R$  in un campo quadratico immaginario. Dimostrare che esiste una base di reticolo per  $A$  tale che uno dei suoi elementi è un intero positivo.

**Sia  $R = \mathbb{Z}[\sqrt{-5}]$ .** Dimostrare che il reticolo generato da  $(3, 1+\sqrt{-5})$  è un ideale in  $R$ , determinare il suo elemento non nullo avente valore assoluto minimo e verificare che tale ideale ha la forma (7.9), Caso 2.

**6.** Con le notazioni introdotte in (7.9), dimostrare che se  $\alpha$  è un elemento di  $R$  tale che anche  $\frac{1}{2}(\alpha + \alpha\delta)$  appartiene a  $R$ , allora  $\left(\alpha, \frac{1}{2}(\alpha + \alpha\delta)\right)$  è una base di reticolo di un ideale.

**7.** Per ciascuno degli anelli  $R$  elencati, utilizzare il metodo della proposizione (7.9) per descrivere gli ideali in  $R$ . Fare un disegno che rappresenti le forme possibili dei reticolli in ciascuno dei casi corrispondenti:

- (a)  $R = \mathbb{Z}[\sqrt{-3}]$ ; (b)  $R = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ ; (c)  $R = \mathbb{Z}[\sqrt{-6}]$ ;
- (d)  $R = \mathbb{Z}[\sqrt{-7}]$ ; (e)  $R = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-7})\right]$ ; (f)  $R = \mathbb{Z}[\sqrt{-10}]$ .

**8.** Dimostrare che  $R$  non è un dominio a fattorizzazione unica, se  $d \equiv 2$  (modulo 4) e  $d < -2$ .

**9.** Sia  $d \leq -3$ . Dimostrare che 2 non è un elemento primo nell'anello  $\mathbb{Z}[\sqrt{d}]$ , ma che 2 è irriducibile in questo anello.

## 8 Fattorizzazione degli ideali

**1.** Sia  $R = \mathbb{Z}[\sqrt{-6}]$ . Fattorizzare esplicitamente l'ideale (6) in un prodotto di ideali primi.

**2.** Sia  $\delta = \sqrt{-3}$  e  $R = \mathbb{Z}[\delta]$ . (Questo non è l'anello degli interi nel campo di numeri quadratico immaginario  $\mathbb{Q}(\delta)$ ). Sia  $A$  l'ideale  $(2, 1+\delta)$ . Dimostrare che  $\overline{AA}$  non è un ideale principale e quindi che il lemma fondamentale non vale per questo anello.

**3.** Sia  $R = \mathbb{Z}[\sqrt{-5}]$ . È vero che 11 è un elemento irriducibile di  $R$ ? È vero che (11) è un ideale primo in  $R$ ?

**4.** Sia  $R = \mathbb{Z}[\sqrt{-6}]$ . Trovare una base di reticolo per l'ideale prodotto  $AB$ , dove  $A = (2, \delta)$  e  $B = (3, \delta)$ .

**5.** Dimostrare che se  $A \supset A'$  allora  $AB \supset A'B$ .

**6.** Fattorizzare esplicitamente l'ideale principale (14) in ideali primi nell'anello  $R = \mathbb{Z}[\delta]$ , dove  $\delta = \sqrt{-5}$ .

**7.** Sia  $P$  un ideale primo di un dominio di integrità  $R$ , e supponiamo che in  $R$  esista una fattorizzazione. Dimostrare che, se  $a \in P$ , allora qualche fattore irriducibile di  $a$  appartiene a  $P$ .

9 La relazione tra gli ideali primi di  $R$  e i numeri primi

**1.** Trovare basi di reticolo per i divisori primi di 2 e 3 nell'anello degli interi in:

- (a)  $\mathbb{Q}(\sqrt{-14})$ ; (b)  $\mathbb{Q}(\sqrt{-23})$ .

**2.** Sia  $d = -14$ . Per ciascuno dei seguenti primi  $p$ , stabilire se  $p$  si spezza o si ramifica in  $R$ , e in caso affermativo determinare una base di reticolo per un ideale primo che sia un fattore di  $(p)$ : 2, 3, 5, 7, 11, 13.

3. (a) Supponiamo che un numero primo  $p$  rimanga primo in  $R$ . Dimostrare che  $R/(p)$  risulta allora un campo con  $p^2$  elementi.  
 (b) Dimostrare che, se  $p$  si spezza in  $R$ , allora  $R/(p)$  è isomorfo all'anello prodotto  $\mathbb{F}_p \times \mathbb{F}_p$ .
4. Sia  $p$  un primo che si spezzi in  $R$ , diciamo  $(p) = P\bar{P}$ , e sia  $\alpha \in P$  un elemento non divisibile per  $p$ . Dimostrare che  $P$  è generato come ideale da  $p$  e  $\alpha$ .
5. Dimostrare la proposizione (9.3b).
6. Se  $d \equiv 2$  o  $3$  (modulo 4), allora in base alla proposizione (9.3a) un numero primo  $p$  rimane primo nell'anello degli interi di  $\mathbb{Q}[\sqrt{d}]$  se il polinomio  $x^2 - d$  è irriducibile modulo  $p$ .
  - (a) Dimostrare la stessa cosa nel caso in cui  $d \equiv 1$  (modulo 4) e  $p \neq 2$ .
  - (b) Che cosa accade in questo caso al primo  $p = 2$ ?
7. Supponiamo che  $d \equiv 2$  o  $3$  (modulo 4). Dimostrare che un numero primo  $p$  si ramifica in  $R$  se e solo se  $p = 2$  oppure  $p$  divide  $d$ .
8. Enunciare e dimostrare un problema analogo al precedente, nel caso in cui  $d \equiv 1$  (modulo 4).
9. Sia  $p$  un numero primo che si ramifichi in  $R$ , e sia  $(p) = P^2$ . Trovare una base di reticolo esplicita per  $P$ . In quali casi  $P$  è un ideale principale?
10. Un numero primo potrebbe essere della forma  $a^2 + b^2d$ , con  $a, b \in \mathbb{Z}$ . Esaminare accuratamente in che modo ciò è collegato alla fattorizzazione in ideali primi di  $(p)$  in  $R$ .
- \*11. Dimostrare la proposizione (9.1).

#### 10 Classi di ideali nei campi quadratici immaginari

1. Dimostrare che gli ideali  $A$  e  $A'$  sono simili se e soltanto se esiste un ideale non nullo  $C$  tale che  $AC$  e  $A'C$  siano ideali principali.
2. La stima del corollario (10.12) può essere migliorata da  $|\alpha|^2 \leq 2\Delta(L)/\sqrt{3}$ , studiando i punti del reticolo in un cerchio anziché in un qualunque insieme convesso simmetrico rispetto all'origine. Sviluppare la dimostrazione di questo risultato.
3. Sia  $R = \mathbb{Z}[\delta]$ , dove  $\delta^2 = -6$ .
  - (a) Dimostrare che i reticolati  $P = (2, \delta)$  e  $Q = (3, \delta)$  sono ideali primi di  $R$ .
  - (b) Fattorizzare esplicitamente l'ideale principale  $(6)$  in un prodotto di ideali primi di  $R$ .
  - (c) Dimostrare che le classi di ideali di  $P$  e  $Q$  sono uguali.
  - (d) Il limite di Minkowski per  $R$  è  $[\mu] = 3$ . Utilizzando questo fatto, determinare il gruppo delle classi di ideali di  $R$ .
4. In ciascuno dei casi seguenti, determinare il gruppo delle classi di ideali e disegnare le forme possibili dei reticolati corrispondenti:
  - (a)  $d = -10$ ; (b)  $d = -13$ ; (c)  $d = -14$ ; (d)  $d = -15$ ; (e)  $d = -17$ ; (f)  $d = -21$ .

Dimostrare che per ciascuno dei valori di  $d$  elencati nel teorema (7.7) vale l'unicità della fattorizzazione.

Dimostrare il lemma (10.13).

7. Dedurre il corollario (10.14) dal lemma (10.13).

8. Verificare la tabella (10.24).

#### 11 Campi quadratici reali

1. Sia  $R = \mathbb{Z}[\delta]$ , dove  $\delta = \sqrt{2}$ . Definire una funzione di grandezza  $\sigma$  su  $R$ , utilizzando l'immersione del reticolo (11.2):  $\sigma(a+b\delta) = a^2 - 2b^2$ . Dimostrare che con tale funzione di grandezza,  $R$  risulta un dominio euclideo.
2. Sia  $R$  l'anello degli interi in un campo di numeri quadratico reale, con  $d \equiv 2$  o  $3$  (modulo 4). In base a (6.14),  $R$  ha la forma  $\mathbb{Z}[x]/(x^2 - d)$ . Possiamo considerare inoltre l'anello  $R' = \mathbb{R}[x]/(x^2 - d)$ , che contiene  $R$  come sottoanello.
  - (a) Dimostrare che gli elementi di  $R'$  sono in corrispondenza biunivoca con i punti di  $\mathbb{R}^2$ , in modo tale che gli elementi di  $R$  corrispondono ai punti del reticolo.
  - (b) Determinare il gruppo delle unità di  $R'$ . Dimostrare che il sottoinsieme  $U'$  di  $R'$  costituito dai punti situati sulle due iperboli  $xy = \pm 1$  forma un sottogruppo del gruppo delle unità.
  - (c) Dimostrare che il gruppo delle unità  $U$  di  $R$  è un sottogruppo discreto di  $U'$ , e provare che il sottogruppo  $U_0$  di  $U$  costituito dalle unità che appartengono al primo quadrante è un gruppo ciclico infinito.
  - (d) Quali sono le strutture possibili del gruppo delle unità  $U$ ?
3. Si denoti con  $U_0$  il sottogruppo del gruppo delle unità  $U$  di  $R$  costituito dalle unità che appartengono al primo quadrante, nell'immersione (11.2). Trovare un generatore per  $U_0$  nei casi seguenti:
  - (a)  $d = 3$ ; (b)  $d = 5$ .
4. Dimostrare che, se  $d$  è un quadrato  $> 1$ , allora l'equazione  $x^2 - y^2d = 1$  non ha soluzioni intere, all'infuori di  $x = \pm 1$ ,  $y = 0$ .
5. Disegnare una figura che rappresenti le iperboli e le unità in un intervallo ragionevolmente ampio, per  $d = 3$ .

#### 12 Alcune equazioni diofantee

1. Determinare i numeri primi  $p$  tali che l'equazione  $x^2 + 5y^2 = 2p$  abbia una soluzione intera.
2. Esprimere l'enunciato del teorema (12.10) per mezzo della congruenza modulo 20.
3. Dimostrare che se la congruenza  $x^2 \equiv -5$  (modulo  $p$ ) ha una soluzione esiste un punto di coordinate intere su una delle due ellissi:  $x^2 + 5y^2 = p$  oppure  $2x^2 + 2xy + 3y^2 = p$ .
4. Determinare le condizioni sugli interi  $a, b, c$  tali che l'equazione diofantea lineare  $ax + by = c$  abbia una soluzione intera e, in tal caso, trovare tutte le soluzioni.

5. Determinare i numeri primi  $p$  tali che l'equazione  $x^2 + 2y^2 = p$  abbia una soluzione intera.
6. Determinare i numeri primi  $p$  tali che l'equazione  $x^2 + xy + y^2 = p$  abbia una soluzione intera.
7. Dimostrare che se la congruenza  $x^2 \equiv -10$  (modulo  $p$ ) ha una soluzione, l'equazione  $x^2 + 10y^2 = p^2$  ha una soluzione intera. Generalizzare tale risultato.
8. Trovare tutte le soluzioni intere dell'equazione  $x^2 + 2 = y^3$ .
9. Risolvere le seguenti equazioni diofantee:
  - (a)  $y^2 + 10 = x^3$ ; (b)  $y^2 + 1 = x^3$ ; (c)  $y^2 + 2 = x^3$ .

## Esercizi vari

1. Dimostrare che esistono infiniti numeri primi congrui a 1 modulo 4.
2. Dimostrare che esistono infiniti numeri primi congrui a  $-1$  modulo 6, studiando la fattorizzazione del numero intero  $p_1 p_2 \cdots p_r - 1$ , dove  $p_1, \dots, p_r$  sono i primi  $r$  numeri primi.
3. Dimostrare che esistono infiniti numeri primi congrui a  $-1$  modulo 4.
4. (a) Determinare gli ideali primi dell'anello dei polinomi in due variabili  $\mathbb{C}[x, y]$ .  
 (b) Dimostrare che nell'anello  $\mathbb{C}[x, y]$  non vale la fattorizzazione unica degli ideali.
5. Mettere in relazione le fattorizzazioni proprie degli elementi in un dominio di integrità con le fattorizzazioni proprie degli ideali principali. Utilizzando tale relazione, enunciare e dimostrare la proprietà di fattorizzazione unica degli ideali in un dominio a ideali principali.
6. Sia  $R$  un dominio di integrità e sia  $I$  un ideale che risulti un prodotto di ideali massimali distinti in due modi, diciamo  $I = P_1 \cdots P_r = Q_1 \cdots Q_s$ . Dimostrare che le due fattorizzazioni coincidono, a meno dell'ordine dei fattori.
7. Sia  $R$  un anello contenente  $\mathbb{Z}$  come sottoanello. Dimostrare che se due interi  $m, n$  sono contenuti in un ideale proprio di  $R$ , allora hanno un fattore intero comune  $> 1$ .
- \*8. (a) Sia  $\theta$  un elemento del gruppo  $\mathbb{R}/\mathbb{Z}$ . Utilizzare il principio delle gabbie dei piccioni [cfr. app. (1.6)] per dimostrare che per ogni intero  $n$  esiste un intero  $b \leq n$  tale che  $|b\theta| \leq 1/bn$ .  
 (b) Dimostrare che per ogni numero reale  $r$  e per ogni  $\epsilon > 0$  esiste una frazione  $m/n$  tale che  $|r - m/n| \leq \epsilon/n$ .  
 (c) Estendere tale risultato ai numeri complessi provando che per ogni numero complesso  $\alpha$  e per ogni numero reale  $\epsilon > 0$  esiste un elemento di  $\mathbb{Z}(i)$ , diciamo  $\beta = (a+bi)/n$ , con  $a, b, n \in \mathbb{Z}$  tale che  $|\alpha - \beta| \leq \epsilon/n$ .  
 (d) Sia  $\epsilon$  un numero reale positivo, e per ogni elemento  $\beta = (a+bi)/n$  di  $\mathbb{Q}(i)$ , con  $a, b, n \in \mathbb{Z}$ , si consideri il disco di raggio  $\epsilon/n$  intorno a  $\beta$ . Dimostrare che le parti interne di questi dischi ricoprono il piano complesso.  
 (e) Estendere il metodo della proposizione (7.9) per dimostrare che il numero di classi è finito per ogni campo quadratico immaginario.

- Esercizi**
- (a) Sia  $R$  l'anello delle funzioni che sono polinomi in  $\cos t$  e  $\sin t$ , a coefficienti reali. Dimostrare che  $R \approx \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ .
  - (b) Dimostrare che  $R$  non è un dominio a fattorizzazione unica.
  - \*(c) Dimostrare che  $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$  è un dominio a ideali principali e quindi un dominio a fattorizzazione unica.
  10. Nella definizione di dominio euclideo, si suppone che la funzione di grandezza  $\sigma$  abbia come codominio l'insieme degli interi non negativi. Potremmo generalizzarla, ammettendo come codominio qualche altro insieme ordinato. Sia dato ad esempio l'anello prodotto  $R = \mathbb{C}[x] \times \mathbb{C}[y]$ . Dimostrare che possiamo definire una funzione di grandezza  $R - \{0\} \rightarrow S$ , dove  $S$  è l'insieme ordinato  $\{0, 1, 2, 3, \dots; \omega, \omega + 1, \omega + 2, \omega + 3, \dots\}$ , in modo tale che in  $R$  valga l'algoritmo della divisione con resto.
  11. Sia  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$  un omomorfismo definito, diciamo, da  $x \mapsto x(t)$ ,  $y \mapsto y(t)$ . Dimostrare che, se  $x(t)$  e  $y(t)$  non sono entrambi delle costanti, allora  $\ker \varphi$  è un ideale principale non nullo.

omorfì a nessun modulo libero, pur essendo generati da un insieme finito di elementi.

Esaminiamo il concetto di modulo nel caso in cui  $R$  è l'anello degli interi  $\mathbb{Z}$ . Ogni gruppo abeliano  $V$ , con la sua legge di composizione denotata con  $+$ , può essere trasformato in un modulo su  $\mathbb{Z}$  in un unico modo, mediante le regole:

$$nv = v + \cdots + v = "n \text{ volte } v"$$

e  $(-n)v = -(nv)$ , per ogni intero positivo  $n$ . Queste regole sono le uniche compatibili con gli assiomi (1.1), a partire da  $1v = v$ , ed è intuitivamente plausibile che in tal modo  $V$  risulta uno  $\mathbb{Z}$ -modulo, cioè, gli assiomi (1.1) sono verificati. (Per dare una dimostrazione formale, dovremmo tornare indietro agli assiomi di Peano.) Viceversa, ogni  $\mathbb{Z}$ -modulo ha la struttura di un gruppo abeliano rispetto alla sua legge di composizione  $"+"$ . Dunque

### (1.2) I concetti di gruppo abeliano e di $\mathbb{Z}$ -modulo sono equivalenti.

Per far apparire naturale tale corrispondenza dobbiamo usare, nel gruppo abeliano, la notazione additiva.

L'anello degli interi fornisce esempi che mostrano che i moduli su un anello  $R$  non sono necessariamente liberi. Nessun gruppo abeliano finito, tranne il gruppo nullo, è isomorfo ad un modulo libero  $\mathbb{Z}^n$ , poiché  $\mathbb{Z}^n$  è infinito se  $n > 0$  e  $\mathbb{Z}^0 = 0$ .

Il resto del paragrafo estende ai moduli un po' di terminologia di base. Un sottomodulo di un  $R$ -modulo  $V$  è un sottoinsieme non vuoto che è chiuso rispetto all'addizione e alla moltiplicazione per uno scalare. Abbiamo già visto in un caso i sottomoduli, precisamente gli ideali.

### (1.3) PROPOSIZIONE I sottomoduli dell' $R$ -modulo $R^1$ sono gli ideali di $R$ .

*Dimostrazione.* Per definizione, un ideale è un sottoinsieme di  $R$  che è chiuso rispetto all'addizione e alla moltiplicazione per elementi di  $R$ . ■

La definizione di omomorfismo di  $R$ -moduli ricalca quella di applicazione lineare di spazi vettoriali. Un omomorfismo  $\varphi : V \rightarrow W$  di  $R$ -moduli è un'applicazione che è compatibile con le leggi di composizione, ossia tale che

$$(1.4) \quad \varphi(v + v') = \varphi(v) + \varphi(v') \quad \text{e} \quad \varphi(rv) = r\varphi(v),$$

per ogni  $v, v' \in V$  e per ogni  $r \in R$ . Un omomorfismo biiettivo è chiamato isomorfismo. Il nucleo di un omomorfismo  $\varphi : V \rightarrow W$  è un sottomodulo di  $V$ , e l'immagine di  $\varphi$  è un sottomodulo di  $W$ .

La dimostrazione data per gli spazi vettoriali [cap. 4 (2.1)] mostra che ogni omomorfismo  $\varphi : R^m \rightarrow R^n$  di moduli liberi è la moltiplicazione a sinistra per una matrice a elementi in  $R$ .

Sii saggio! Generalizza!  
"Piccayne Sentinel"

## 1 Definizione di modulo

Sia  $R$  un anello commutativo. Un  $R$ -modulo  $V$  è un gruppo abeliano con una legge di composizione, denotata con  $+$ , insieme con una moltiplicazione per uno scalare  $R \times V \rightarrow V$ , scritta nella forma:  $(r, v) \mapsto rv$ , la quale soddisfa ai seguenti assiomi:

- (1.1) (i)  $1v = v$ ,
- (ii)  $(rs)v = r(sv)$ ,
- (iii)  $(r + s)v = rv + sv$ ,
- (iv)  $r(v + v') = rv + rv'$ ,

per ogni  $r, s \in R$  e per ogni  $v, v' \in V$ . Si noti che questi sono esattamente gli assiomi di spazio vettoriale. Quando  $F$  è un campo, un  $F$ -modulo è proprio uno spazio vettoriale su  $F$ . Pertanto i moduli sono la generalizzazione naturale degli spazi vettoriali al caso degli anelli. Tuttavia il fatto che gli elementi di un anello non sono necessariamente invertibili rende lo studio dei moduli più complicato.

Gli esempi più semplici sono i moduli  $R^n$  di  $R$ -vettori, ossia vettori riga o colonna con elementi nell'anello. Le leggi di composizione per gli  $R$ -vettori sono le stesse leggi definite per i vettori con elementi in un campo:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}, \quad r \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ra_1 \\ \vdots \\ ra_n \end{bmatrix}.$$

I moduli così definiti sono chiamati *moduli liberi*. Tuttavia, se  $R$  non è un campo, non è più vero che questi sono gli "unici" moduli. Vi sono moduli che non sono

Abbiamo bisogno anche di estendere ai moduli il concetto di gruppo quoziante. Sia  $R$  un anello, e sia  $W$  un sottomodulo di un  $R$ -modulo  $V$ . Il quoziante  $V/W$  è il gruppo additivo delle classi laterali  $\bar{v} = v + W$  [cap. 2 (9.5)]. Diventa un  $R$ -modulo mediante la legge:

$$(1.5) \quad r\bar{v} = \bar{rv}.$$

Abbiamo già effettuato costruzioni simili più volte. Raccogliamo qui sotto i fatti di cui avremo bisogno.

### (1.6) PROPOSIZIONE

- (a) La legge (1.5) è ben definita, e dà a  $\bar{V} = V/W$  una struttura di  $R$ -modulo.
- (b) L'applicazione canonica  $\pi : V \rightarrow \bar{V}$  che manda  $v$  in  $\bar{v}$  è un omomorfismo suriettivo di  $R$ -moduli, e il suo nucleo è  $W$ .
- (c) (Proprietà di rappresentazione) Sia  $f : V \rightarrow V'$  un omomorfismo di  $R$ -moduli il cui nucleo contenga  $W$ . Allora esiste uno e un solo omomorfismo  $\bar{f} : \bar{V} \rightarrow V'$  tale che  $f = \bar{f}\pi$ .
- (d) (Primo teorema di isomorfismo) Se  $\ker f = W$ , allora  $\bar{f}$  è un isomorfismo da  $\bar{V}$  all'immagine di  $f$ .
- (e) (Teorema di corrispondenza) Esiste una corrispondenza biunivoca tra i sottomoduli  $\bar{S}$  di  $\bar{V}$  e i sottomoduli  $S$  di  $V$  che contengono  $W$ , definita da  $S = \pi^{-1}(\bar{S})$  e  $\bar{S} = \pi(S)$ . Se  $S$  e  $\bar{S}$  sono moduli corrispondenti, allora  $V/S$  è isomorfo a  $\bar{V}/\bar{S}$ .

Conosciamo già i fatti analoghi relativi ai gruppi e ai sottogruppi normali. Tutto ciò che resta da verificare in ciascun enunciato è che la moltiplicazione per uno scalare è ben definita, soddisfa agli assiomi di modulo ed è compatibile con le applicazioni. Tali verifiche seguono il modello dato in precedenza. ■

## 2 Matrici, moduli liberi, basi

Le matrici a elementi in un anello possono essere trattate esattamente come le matrici a elementi in un campo. Precisamente, le operazioni di addizione e di moltiplicazione di matrici sono definite come nel capitolo 1, e soddisfano a proprietà simili. Una matrice a elementi in un anello  $R$  è chiamata spesso una  $R$ -matrice.

Vediamo ora quali  $R$ -matrici sono invertibili. Il determinante di una  $R$ -matrice  $n \times n$   $A = (a_{ij})$  può essere calcolato mediante una qualsiasi delle vecchie regole. È conveniente usare lo sviluppo completo [cap. 1 (4.12)] che esprime il determinante come un polinomio negli  $n^2$  elementi della matrice. Pertanto scriviamo

$$(2.1) \quad \det A = \sum_p \pm a_{1p(1)} \cdots a_{np(n)},$$

ove la somma è estesa a tutte le permutazioni dell'insieme  $\{1, \dots, n\}$ , e il simbolo  $\pm$  sta a indicare il segno della permutazione. Applicando questa formula a una  $R$ -matrice, otteniamo un elemento di  $R$ . Le regole già viste per il determinante continuano a valere; in particolare

$$\det AB = (\det A)(\det B).$$

Abbiamo dimostrato questa regola quando gli elementi delle matrici sono in un campo [cap. 1 (3.16)], nel prossimo paragrafo faremo vedere che tali formule valgono anche nel caso degli anelli. Per ora prendiamole per buone.

Se  $A$  ha un'inversa moltiplicativa  $A^{-1}$  a elementi in  $R$ , allora

$$(\det A)(\det A^{-1}) = \det I = 1,$$

ciò mostra che il determinante di una  $R$ -matrice invertibile è un'unità dell'anello. Viceversa, sia  $A$  una  $R$ -matrice il cui determinante  $\delta$  sia un'unità. Allora possiamo trovare la sua inversa mediante la regola di Cramer:  $\delta I = A(\text{adj } A)$ , dove la matrice aggiunta si calcola a partire da  $A$  prendendo i determinanti dei minori [cap. 1 (5.4)]. Questa regola vale anche in un anello arbitrario. Pertanto, se  $\delta$  è un'unità, possiamo ricavare la matrice  $A^{-1}$  a elementi in  $R$ :

$$A^{-1} = \delta^{-1}(\text{adj } A).$$

**(2.2) COROLLARIO** Una matrice  $n \times n$  a elementi in  $R$  è invertibile se e solo se il suo determinante è un'unità. Le matrici invertibili formano un gruppo

$$GL_n(R) = \{R\text{-matrici } n \times n \text{ invertibili}\},$$

chiamato il gruppo lineare generale su  $R$ . ■

Il fatto che il determinante di una matrice invertibile deve essere un'unità è una condizione forte quando  $R$  ha poche unità. Per esempio, se  $R$  è l'anello degli interi, il determinante deve essere  $\pm 1$ . La maggior parte delle matrici ad elementi interi sono matrici reali invertibili, sicché esse appartengono a  $GL_n(\mathbb{R})$ . Ma, a meno che il determinante non sia  $\pm 1$ , gli elementi della matrice inversa non saranno interi, e pertanto le matrici inverse non appariranno a  $GL_n(\mathbb{Z})$ . Tuttavia, vi sono sempre abbastanza matrici invertibili, se  $n > 1$ , poiché le matrici elementari

$$I + ae_{ij} = \begin{bmatrix} 1 & & & \\ & \ddots & & a \\ & & \ddots & \\ & & & 1 \end{bmatrix}, \quad i \neq j, \quad a \in R,$$

hanno determinante 1. Queste matrici generano un gruppo abbastanza grande. Le altre matrici elementari, ossia quelle di trasposizione e le matrici

$$\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & u & \\ & & & \ddots \\ & & & & 1 \end{bmatrix}, \text{ dove } u \text{ è un'unità di } R.$$

sono anch'esse invertibili.

Ritorniamo ora allo studio degli  $R$ -moduli. I concetti di base e di indipendenza (cap. 3, § 3) si estendono senza cambiamenti dagli spazi vettoriali ai moduli. Precisamente, si dice che un insieme ordinato  $(v_1, \dots, v_k)$  di elementi di un modulo  $V$  genera  $V$ , se ogni elemento  $v \in V$  è una combinazione lineare

$$(2.3) \quad v = r_1 v_1 + \dots + r_k v_k, \quad \text{con } r_i \in R.$$

In tal caso gli elementi  $v_i$  sono chiamati *generatori*. Un modulo  $V$  si dice *finitamente generato* se ha un insieme finito di generatori. La maggior parte dei moduli che studieremo saranno finitamente generati. Uno  $\mathbb{Z}$ -modulo  $V$  è finitamente generato se e soltanto se è un gruppo abeliano finitamente generato nel senso definito nel capitolo 6 (§ 8).

Abbiamo visto nel paragrafo 1 che i moduli non sono necessariamente isomorfi a qualche modulo  $R^k$ . Tuttavia può accadere che un dato modulo lo sia; in tal caso, esso è chiamato ancora *modulo libero*. Dunque un modulo finitamente generato  $V$  è libero se per qualche  $n$  esiste un isomorfismo

$$\varphi : R^n \xrightarrow{\sim} V.$$

Per esempio, i reticolati in  $\mathbb{R}^2$  sono  $\mathbb{Z}$ -moduli liberi, mentre i gruppi abeliani finiti non nulli non sono liberi. Uno  $\mathbb{Z}$ -modulo libero è chiamato anche un *gruppo abeliano libero*. I moduli liberi formano una classe importante e naturale, e li studieremo per primi. Riprenderemo lo studio dei moduli, nel caso generale, a partire dal paragrafo 5.

Seguendo le definizioni date per gli spazi vettoriali, si dice che un insieme di elementi  $(v_1, \dots, v_n)$  di un modulo  $V$  è *indipendente*, se nessuna combinazione lineare non banale è nulla, ossia se vale la seguente condizione:

$$(2.4) \quad \text{Se } r_1 v_1 + \dots + r_n v_n = 0, \text{ con } r_i \in R, \text{ allora } r_i = 0 \text{ per } i = 1, \dots, n.$$

L'insieme è una *base*, se è sia indipendente che un insieme di generatori. La *base canonica*  $\mathbf{E} = (e_1, \dots, e_k)$  è una base di  $R^k$ . Esattamente come accade per gli spazi

vettoriali, un insieme  $(v_1, \dots, v_k)$  è una base se ogni elemento  $v \in V$  si esprime in modo unico come una combinazione lineare (2.3).

Possiamo parlare anche di combinazioni lineari e di indipendenza lineare di insiemi infiniti, utilizzando la terminologia introdotta nel capitolo 3 (§ 5).

Denotiamo l'insieme ordinato  $(v_1, \dots, v_n)$  con  $\mathbf{B}$ , come nel capitolo 3 (§ 3).

Allora la moltiplicazione per  $\mathbf{B}$ :

$$\mathbf{B}X = (v_1, \dots, v_n) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1 x_1 + \dots + v_n x_n.$$

definisce un omomorfismo di moduli, diciamo:

$$(2.5) \quad \mu : R^n \rightarrow V.$$

Questo omomorfismo è suriettivo se e solo se l'insieme  $(v_1, \dots, v_n)$  genera  $V$ , ed è iniettivo se e solo se esso è indipendente. Dunque l'omomorfismo  $\mu$  è biettivo se e solo se  $\mathbf{B}$  è una base di  $V$ , nel qual caso  $V$  è un modulo libero. Pertanto un modulo  $V$  ha una base se e solo se è libero. La maggior parte dei moduli non hanno base.

I calcoli con le basi per gli  $R$ -moduli liberi possono essere effettuati pressappoco come con le basi degli spazi vettoriali, utilizzando le matrici a elementi in  $R$ . In particolare, possiamo parlare del *vettore delle coordinate* di un elemento  $v \in V$  rispetto a una base  $\mathbf{B} = (v_1, \dots, v_n)$ : è l'unico vettore colonna  $X \in R^n$  tale che

$$v = \mathbf{B}X = v_1 x_1 + \dots + v_n x_n.$$

Date due basi  $\mathbf{B} = (v_1, \dots, v_n)$  e  $\mathbf{B}' = (v'_1, \dots, v'_r)$  di uno stesso modulo libero  $V$ , la matrice del cambiamento di base si ottiene come nel capitolo 3 (§ 4), scrivendo gli elementi  $v_j$  della prima base come combinazioni lineari della seconda base:  $\mathbf{B} = \mathbf{B}'P$ , ossia

$$(2.6) \quad v_j = \sum_{i=1}^r v'_i p_{ij}.$$

Così come accade per gli spazi vettoriali, due basi diverse di uno stesso modulo libero su un anello  $R$  hanno la stessa cardinalità, purché  $R$  non sia l'anello nullo; pertanto  $n = r$  nelle basi sopra assegnate. Questo si può dimostrare considerando la matrice inversa  $Q = (q_{ij})$ , la quale si ottiene scrivendo  $\mathbf{B}'$  per mezzo di  $\mathbf{B}$ :  $\mathbf{B}' = \mathbf{B}Q$ . Allora

$$\mathbf{B} = \mathbf{B}'P = \mathbf{B}'Q\mathbf{P}.$$

Poiché  $\mathbf{B}$  è una base, vi è un unico modo di scrivere  $v_j$  come una combinazione lineare di  $(v_1, \dots, v_n)$ , precisamente:  $v_j = 1v_j$ , ossia  $\mathbf{B} = \mathbf{B}I$ . Pertanto  $QP = I$ ,

e analogamente  $PQ = I$ . Dunque la matrice di un cambiamento di base è una  $R$ -matrice invertibile.

Ora  $P$  è una matrice  $r \times n$ , e  $Q$  è una matrice  $n \times r$ . Supponiamo che  $r > n$ . Allora possiamo rendere quadrate le matrici  $P$  e  $Q$ , aggiungendo degli zeri:

$$\begin{bmatrix} P \\ 0 \end{bmatrix} \begin{bmatrix} Q \\ 0 \end{bmatrix} = I.$$

Ciò non cambia il prodotto  $PQ$ . Ma i determinanti di queste matrici quadrate sono uguali a zero, sicché esse non sono invertibili, poiché  $R \neq 0$ . Ciò prova che  $r = n$ , come affermato.

È davvero sorprendente il fatto che esistono anelli *non commutativi*  $R$  per i quali i moduli  $R^n$ , per  $n = 1, 2, 3, \dots$ , sono tutti isomorfi (cfr. p. 578, esercizio 6): se gli elementi delle matrici non commutano tra loro, i determinanti non hanno un buon comportamento.

Purtroppo, la maggior parte dei concetti relativi agli spazi vettoriali hanno nomi differenti, quando vengono usati per i moduli sugli anelli, ed è troppo tardi per cambiarli. Il numero degli elementi di una base di un modulo libero  $V$  è chiamato il *rango* di  $V$ , anziché la dimensione.

Come abbiamo già osservato, ogni omomorfismo  $\varphi : R^n \rightarrow R^m$  tra vettori colonna è la moltiplicazione a sinistra per una matrice  $A$ . Se  $\varphi : V \rightarrow W$  è un omomorfismo di  $R$ -moduli liberi, con basi  $\mathbf{B} = (v_1, \dots, v_n)$  e  $\mathbf{C} = (w_1, \dots, w_m)$  rispettivamente, allora la *matrice* dell'omomorfismo è, per definizione, la matrice  $A = (a_{ij})$ , dove

$$(2.7) \quad \varphi(v_j) = \sum_i w_i a_{ij}$$

come in precedenza [cap. 4 (2.3)]. Un cambiamento delle basi  $\mathbf{B}, \mathbf{C}$  mediante  $R$ -matrici invertibili  $P, Q$  cambia la matrice  $A$  di  $\varphi$  in  $A' = QAP^{-1}$  [cap. 4 (2.7)].

### 3 Il principio di permanenza delle identità

In questo paragrafo consideriamo il seguente problema: perché le proprietà delle matrici a elementi in un campo continuano a valere quando gli elementi appartengono a un anello? In breve, il motivo è che esse sono *identità*, il che significa che valgono anche quando gli elementi delle matrici sono sostituiti da variabili. Per essere più precisi, supponiamo di voler dimostrare qualche identità, come la proprietà moltiplicativa dei determinanti:  $(\det A)(\det B) = \det(AB)$ , oppure la regola di Cramer. Supponiamo di aver già verificato l'identità per le matrici a elementi complessi. Non vogliamo fare la verifica di nuovo; e d'altra parte potremmo aver usato alcune proprietà speciali di  $\mathbb{C}$  (quali gli assiomi di un campo, il fatto che ogni polinomio a coefficienti complessi ha una radice, oppure il fatto che  $\mathbb{C}$  ha caratteristica zero), per verificare le identità in questione. Di

nel corso delle dimostrazioni abbiamo usato proprietà speciali e pertanto le dimostrazioni non varranno per gli anelli. Faremo ora vedere come sia possibile dedurre tali identità per tutti gli anelli a partire dalle stesse identità per i numeri complessi.

Il principio è molto generale, ma per focalizzare meglio l'attenzione, ci limitiamo a considerare l'identità  $(\det A)(\det B) = \det(AB)$ . Come prima cosa sostituiamo in essa gli elementi delle matrici con delle variabili, scrivendo

$$(\det X)(\det Y) = \det(XY),$$

dove  $X$  e  $Y$  denotano matrici  $n \times n$  aventi, come elementi, delle variabili. Dopodiché sostituiamo a queste variabili elementi appartenenti a un anello arbitrario  $R$ . Da un punto di vista formale, la sostituzione è definita per mezzo dell'anello dei polinomi a coefficienti interi  $\mathbb{Z}[\{x_{ij}\}, \{y_{kl}\}]$  nei  $2n^2$  elementi variabili delle matrici. Esiste un unico omomorfismo dall'anello degli interi ad un anello arbitrario  $R$  [cap. 10 (3.9)]. Date due matrici  $A = (a_{ij})$ ,  $B = (b_{kl})$  a elementi in  $R$ , esiste un omomorfismo

$$(3.1) \quad \mathbb{Z}[\{x_{ij}\}, \{y_{kl}\}] \rightarrow R,$$

il cosiddetto omomorfismo di sostituzione, il quale manda  $x_{ij}$  in  $a_{ij}$  e  $y_{kl}$  in  $b_{kl}$  [cap. 10 (3.4)]. Le nostre matrici variabili hanno elementi nell'anello dei polinomi, ed è naturale dire che l'omomorfismo manda  $X$  in  $A$  e  $Y$  in  $B$ , nel senso che gli elementi di  $X = (x_{ij})$  vengono mandati negli elementi di  $A = (a_{ij})$  e così via, mediante l'omomorfismo.

Il principio generale che abbiamo in mente è il seguente. Supponiamo di voler dimostrare un'identità i cui termini siano tutti polinomi a coefficienti interi negli elementi delle matrici; in tal caso i termini sono compatibili con gli omomorfismi di anelli. Per esempio, se un omomorfismo  $\varphi : R \rightarrow R'$  manda  $A$  in  $A'$  e  $B$  in  $B'$ , esso manda  $\det A$  in  $\det A'$ . Per verificarlo, osserviamo che lo sviluppo completo del determinante è

$$\det A = \sum_p \pm a_{1p(1)} \cdots a_{np(n)},$$

dove la somma è estesa a tutte le permutazioni  $p$ . Poiché  $\varphi$  è un omomorfismo, si ha:

$$\varphi(\det A) = \sum_p \pm \varphi(a_{1p(1)} \cdots a_{np(n)}) = \sum_p \pm a'_{1p(1)} \cdots a'_{np(n)} = \det A'.$$

Ovviamente, questo è un principio generale. Di conseguenza, se la nostra identità vale per le  $R$ -matrici  $A, B$ , allora essa vale anche per le  $R'$ -matrici  $A', B'$ .

Ora, per ogni coppia di matrici  $A, B$ , abbiamo l'omomorfismo (3.1) che manda  $X$  in  $A$  e  $Y$  in  $B$ . Sostituendo, nel principio appena descritto,  $R$  con  $\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$

e  $R'$  con  $R$ . Concludiamo che, se l'identità vale per le matrici variabili  $X, Y$  in  $\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$ , essa vale per ogni coppia di matrici in un anello arbitrario  $R$ :

(3.2) *Per dimostrare la nostra identità in generale, è sufficiente*

*dimostrarla per le matrici variabili  $X, Y$  nell'anello  $\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$ .*

Per dimostrare l'identità per le matrici variabili, consideriamo l'anello degli interi come un sottoanello del campo dei numeri complessi e notiamo l'inclusione degli anelli di polinomi:

$$\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}] \subset \mathbb{C}[\{x_{ij}\}, \{y_{ij}\}].$$

Possiamo anche verificare la nostra identità nell'anello più grande. Ora, per ipotesi, essa è equivalente all'uguaglianza di certi polinomi nelle variabili  $\{x_{ij}\}, \{y_{ij}\}, \dots$ . Scriviamo l'identità nella forma  $f(x_{ij}, y_{kl}) = 0$ . Il simbolo  $f$  sta a indicare eventualmente più polinomi.

Consideriamo ora la *funzione* polinomiale corrispondente al polinomio  $f(x_{ij}, y_{kl})$ , chiamiamola  $\tilde{f}(x_{ij}, y_{kl})$ . Se l'identità è stata dimostrata per tutte le matrici complesse, allora ne segue che  $\tilde{f}(x_{ij}, y_{kl})$  è la funzione nulla. Applichiamo il fatto [cap. 10 (3.8)] che un polinomio è determinato dalla funzione da esso definita, per concludere che  $f(x_{ij}, y_{kl}) = 0$ , e la tesi è dimostrata.

È possibile formalizzare la trattazione precedente e dimostrare un teorema ben preciso che riguarda la validità delle identità in un anello qualsiasi. Tuttavia, perfino i matematici, in qualche occasione, sono dell'avviso che non valga la pena di dare formulazioni precise e che sia più facile considerare i singoli casi man mano che si presentano. Questa è appunto una di quelle occasioni.

#### 4 Diagonalizzazione delle matrici intere

In questo paragrafo tratteremo la riduzione in forma diagonale di una matrice  $m \times n$  intera (ossia, ad elementi in  $\mathbb{Z}$ )  $A = (a_{ij})$  mediante una successione di operazioni elementari. Applicheremo in seguito questo procedimento per classificare i gruppi abeliani. Lo stesso metodo continuerà a valere per le matrici a elementi in un dominio euclideo e, con qualche modifica, per le matrici a elementi in un dominio a ideali principali.

I migliori risultati si ottengono operando al tempo stesso sia sulle righe che sulle colonne. Pertanto utilizzeremo le seguenti operazioni:

- (4.1) (i) aggiungere un multiplo intero di una riga a un'altra riga, oppure un multiplo intero di una colonna a un'altra colonna;  
(ii) scambiare tra loro due righe oppure due colonne;  
(iii) moltiplicare una riga o una colonna per un'unità.

ormalmente, le unità in  $\mathbb{Z}$  sono  $\pm 1$ . Ogni operazione può essere effettuata moltiplicando  $A$  a sinistra o a destra per un'opportuna matrice elementare intera. Il risultato di una sequenza di operazioni di questo tipo sarà una matrice della forma:

$$(4.2) \quad A' = QAP^{-1},$$

dove  $Q \in GL_m(\mathbb{Z})$  e  $P^{-1} \in GL_n(\mathbb{Z})$  sono prodotti di matrici elementari intere. È chiaro che potremmo cancellare in  $P$  il simbolo dell'inversione. L'abbiamo scritto poiché vogliamo interpretare poi l'operazione come un cambiamento di base. Su un campo, ogni matrice può essere trasformata nella forma a blocchi:

$$A' = \begin{bmatrix} I & \\ & 0 \end{bmatrix}$$

mediante operazioni di questo tipo [cap. 4 (2.9)]. Non possiamo sperare che tale risultato continui a valere per gli interi, infatti non vale neppure per le matrici  $1 \times 1$ . Tuttavia possiamo diagonalizzare:

(4.3) TEOREMA Sia  $A$  una matrice intera  $m \times n$ . Esistono prodotti  $Q, P$  di matrici elementari intere come sopra, tali che  $A' = QAP^{-1}$  è una matrice diagonale:

$$\begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{bmatrix}$$

dove gli elementi diagonali  $d_i$  sono non negativi e ciascun elemento diagonale divide il successivo:  $d_1 \mid d_2, d_2 \mid d_3, \dots$

Dimostrazione. La nostra strategia consistrà nell'effettuare una successione di operazioni, in modo da ottenere alla fine una matrice della forma:

$$(4.4) \quad \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & \left[ \begin{array}{c|c} & \\ \vdots & B \\ & \end{array} \right] \\ \vdots & & & \\ 0 & & & \end{bmatrix},$$

in cui  $d_1$  divide ogni elemento di  $B$ . A questo punto, lavoriamo su  $B$ . Il procedimento è basato su ripetute divisioni con resto. Descriveremo un metodo sistematico, che però, di solito, non è il più rapido.

Possiamo supporre che  $A \neq 0$ .

*Passo 1:* Permutando righe e colonne, spostiamo un elemento non nullo con valore assoluto minimo nell'angolo in alto a sinistra. Moltiplichiamo, se necessario, la prima riga per  $-1$ , in modo tale che il suddetto elemento  $a_{11}$  diventi positivo.

Cerchiamo ora di "svuotare" la prima riga e la prima colonna. Ogni volta che un'operazione produce nella matrice un elemento non nullo, in valore assoluto minore di  $a_{11}$ , torniamo indietro al passo 1 e ripartiamo da capo. Così facendo può accadere che il lavoro già fatto per eliminare elementi della matrice venga rovinato. Tuttavia, si saranno compiuti dei progressi, poiché ogni volta la grandezza di  $a_{11}$  si riduce. In ogni caso, non dovremo ritornare infinite volte al passo 1.

*Passo 2:* Scegliamo un elemento non nullo  $a_{i1}$  nella prima colonna, con  $i > 1$ , e dividiamo per  $a_{11}$ :

$$a_{i1} = a_{11}q + r,$$

dove  $0 \leq r < a_{11}$ . Sottraiamo  $q$  volte la prima riga dalla  $i$ -esima riga. Ciò muta  $a_{i1}$  in  $r$ .

Se  $r \neq 0$ , torniamo al passo 1. Se  $r = 0$ , abbiamo prodotto uno zero nella prima colonna. Applicando un numero finito di volte i passi 1 e 2, otteniamo una matrice in cui  $a_{i1} = 0$  per ogni  $i > 1$ . Similmente, possiamo usare l'analogo del passo 2 per le operazioni sulle colonne per svuotare la prima riga, ottenendo alla fine una matrice in cui l'unico elemento non nullo nella prima riga e nella prima colonna è  $a_{11}$ , come richiesto da (4.3). Tuttavia, può accadere che  $a_{11}$  non divida ancora ogni elemento della matrice  $B$  (4.4).

*Passo 3:* Supponiamo che  $a_{11}$  sia l'unico elemento non nullo nella prima riga e nella prima colonna, ma che qualche elemento  $b$  di  $B$  non sia divisibile per  $a_{11}$ . Aggiungiamo alla prima colonna la colonna di  $A$  che contiene  $b$ . Ciò produce un elemento  $b$  nella prima colonna.

Torniamo indietro al passo 2. La divisione con resto produrrà ora un elemento più piccolo nella matrice, rimandandoci indietro al passo 1. Una successione finita di questi passi produrrà una matrice della forma (4.4), il che ci permetterà di procedere per induzione. ■

#### (4.5) Esempio

Non seguiamo il metodo sistematico:

$$A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \xrightarrow[\text{sulle col.}]{\text{operaz.}} \begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \xrightarrow[\text{sulle col.}]{\text{operaz.}} \begin{bmatrix} 1 & 5 \\ 3 & 5 \end{bmatrix} \xrightarrow[\text{sulle righe}]{\text{operaz.}} \begin{bmatrix} 1 & 5 \\ 1 & 5 \end{bmatrix} = A'.$$

In questo caso, si ha

$$Q = \begin{bmatrix} 1 & \\ -3 & 1 \end{bmatrix} \quad \text{e} \quad P^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Si noti che l'ingrediente fondamentale in questa dimostrazione è l'algoritmo della divisione con resto. La stessa dimostrazione continuerà a valere in un dominio euclideo arbitrario.

**(4.6) TEOREMA** *Sia  $R$  un dominio euclideo, per esempio un anello di polinomi in una variabile  $F[t]$  su un campo. Sia  $A$  una matrice  $m \times n$  a elementi in  $R$ . Esistono prodotti  $Q, P$  di  $R$ -matrici elementari tali che  $A' = QAP^{-1}$  è diagonale e tali che ciascun elemento diagonale di  $A'$  divide il successivo:  $d_1 | d_2 | d_3 \dots$ . Se  $R = F[t]$ , possiamo normalizzare, richiedendo che i polinomi  $d_i$  siano monici.* ■

#### (4.7) Esempio

Diagonalizzazione di una matrice di polinomi:

$$\begin{aligned} A &= \begin{bmatrix} t^2 - 3t + 2 & t - 2 \\ (t-1)^3 & t^2 - 3t + 2 \end{bmatrix} \xrightarrow{\text{operaz.}} \begin{bmatrix} t^2 - 3t + 2 & t - 2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow{\text{operaz.}} \\ &\quad \begin{bmatrix} -t+1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow{\text{operaz.}} \begin{bmatrix} -1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow{\text{operaz.}} \\ &\quad \begin{bmatrix} -1 & 0 \\ (t-1)^2 & (t-1)^2(t-2) \end{bmatrix} \xrightarrow{\text{operaz.}} \begin{bmatrix} 1 & \\ & (t-1)^2(t-2) \end{bmatrix} = A'. \end{aligned}$$

In entrambi gli esempi, abbiamo ottenuto alla fine 1 nell'angolo in alto a sinistra. Ciò non è sorprendente: gli elementi delle matrici avranno spesso il massimo comune divisore uguale a 1.

La diagonalizzazione delle matrici intere può essere usata per descrivere gli omomorfismi tra i gruppi abeliani liberi. Come abbiamo già osservato (2.8), un omomorfismo  $\varphi : V \rightarrow W$  di gruppi abeliani liberi è descritto da una matrice, una volta che siano state scelte delle basi per  $V$  e  $W$ . Un cambiamento di base in  $V, W$  mediante matrici intere invertibili  $P, Q$  muta  $A$  in  $A' = QAP^{-1}$ . Abbiamo così dimostrato il teorema seguente:

**(4.8) TEOREMA** *Sia  $\varphi : V \rightarrow W$  un omomorfismo di gruppi abeliani liberi. Esistono basi di  $V$  e  $W$  tali che la matrice dell'omomorfismo abbia la forma diagonale (4.3).* ■

Nel resto del paragrafo analizzeremo il significato di questo teorema per due gruppi ausiliari associati ad un omomorfismo: il nucleo e l'immagine.

Il teorema (4.11) è veramente esplicito. Sia  $S$  il sottogruppo di  $\mathbb{Z}^m$  generato dalle colonne di una matrice  $A$ , e supponiamo che  $A' = QAP^{-1}$  sia diagonale. Per rappresentare  $S$  nella forma descritta nel teorema, riscriviamo tale equazione nella forma:

$$(4.13) \quad Q^{-1}A' = AP^{-1},$$

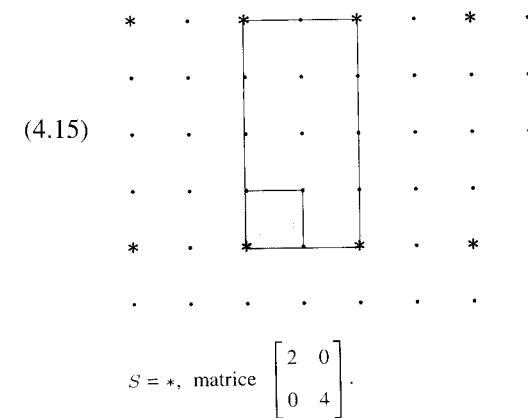
e la interpretiamo come segue. Le colonne della matrice  $AP^{-1}$  formano il nuovo insieme di generatori per  $S$ . Poiché la matrice  $A'$  è diagonale, la (4.13) ci dice che i nuovi generatori sono multipli delle colonne di  $Q^{-1}$ . Effettuiamo un cambiamento di base in  $\mathbb{Z}^m$ , dalla base canonica alla base formata dalle colonne di  $Q^{-1}$ . La matrice di questo cambiamento di base è  $Q$  [cfr. cap. 3 (4.21)]. Allora i nuovi generatori sono multipli dei nuovi elementi della base.

Per esempio, sia  $S$  il reticolo in  $\mathbb{R}^2$  generato dalle due colonne della matrice  $A$  dell'esempio (4.5). Allora si ha:

$$(4.14) \quad Q^{-1}A' = \begin{bmatrix} 1 & \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 5 \end{bmatrix} = \begin{bmatrix} 1 & \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = AP^{-1}.$$

La nuova base di  $\mathbb{Z}^2$  è  $(w'_1, w'_2) = \left( \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$ , e i nuovi generatori di  $S$  sono  $(u'_1, u'_2) = (u_1, u_2)P^{-1} = (w'_1, 5w'_2)$ .

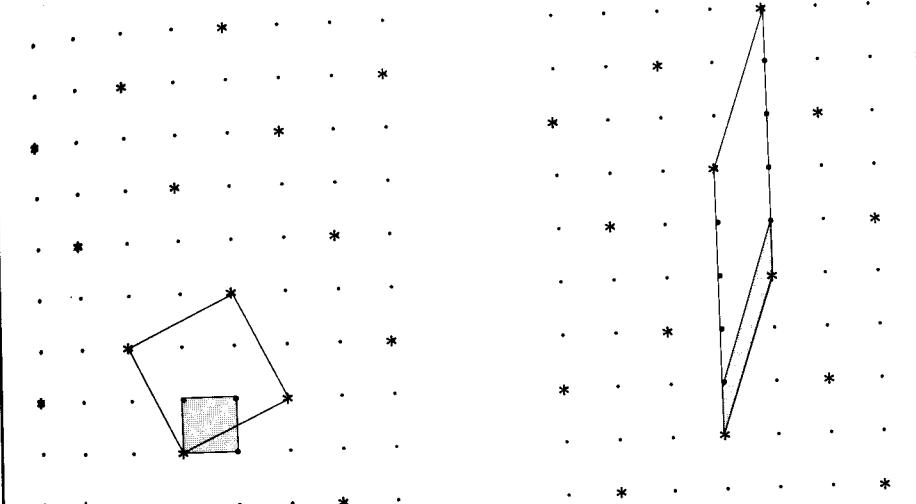
Il teorema (4.3) è davvero sorprendente quando viene usato per descrivere la posizione relativa di un sottoreticolo  $S$  in un reticolo  $L$ . Per illustrare ciò, basterà considerare reticoli piani. Il teorema afferma che esistono basi  $(v_1, v_2)$  e  $(w_1, w_2)$  di  $L$  e  $S$ , rispettivamente, tali che la matrice formata dai vettori delle coordinate di  $w_1, w_2$  rispetto alla base  $(v_1, v_2)$  sia diagonale. Rappresentiamo il reticolo  $L$  in  $\mathbb{Z}^2 \subset \mathbb{R}^2$  mediante la base  $(v_1, v_2)$ . Allora le equazioni  $w_i = d_i v_i$  provano che  $S$  somiglia alla figura seguente, in cui abbiamo preso  $d_1 = 2$  e  $d_2 = 4$ :



Indiamo [cap. 11 (10.13)], che l'indice  $[L : S]$  è il rapporto delle aree dei parallelogrammi generati dalle basi il che risulta evidente quando le basi sono in posizione.

Nella pratica, quando vengono assegnati due reticolati  $L$  e  $S$  in  $\mathbb{R}^2$ , il cambiamento di base richiesto per ottenere tali basi "commensurabili" di  $L$  e  $S$  porta a determinare parallelogrammi piuttosto lunghi e sottili, come viene illustrato qui sotto, con riferimento all'esempio (4.14):

(4.16)



Diagonalizzazione applicata a un sottoreticolo.

## 5 Generatori e relazioni per i moduli

In questo paragrafo rivolgeremo la nostra attenzione ai moduli che non sono liberi. Faremo vedere come sia possibile descrivere un'ampia classe di moduli per mezzo di matrici chiamate *matrici di presentazione*. A queste matrici applicheremo poi il procedimento di diagonalizzazione per lo studio dei gruppi abeliani.

Come esempio da tenere a mente, possiamo considerare un gruppo abeliano o  $\mathbb{Z}$ -modulo  $V$  generato da tre elementi  $(v_1, v_2, v_3)$  che soddisfano le relazioni:

$$(5.1) \quad \begin{aligned} 3v_1 + 2v_2 + v_3 &= 0 \\ 8v_1 + 4v_2 + 2v_3 &= 0 \\ 7v_1 + 6v_2 + 2v_3 &= 0 \\ 9v_1 + 6v_2 + v_3 &= 0. \end{aligned}$$

Le informazioni che descrivono questo modulo sono riassunte nella matrice:

$$(5.2) \quad A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix},$$

le cui colonne sono i coefficienti delle relazioni (5.1):

$$(v_1, v_2, v_3)A = (0, 0, 0, 0).$$

Come al solito, gli scalari compaiono a destra in questo prodotto di matrici. Ci proponiamo ora di formalizzare questo metodo per descrivere un modulo.

Se  $(v_1, \dots, v_m)$  sono elementi di un  $R$ -modulo  $V$ , equazioni della forma

$$(5.3) \quad a_1v_1 + \dots + a_mv_m = 0, \quad \text{con } a_i \in R,$$

vengono chiamate *relazioni* tra gli elementi. Naturalmente, quando diciamo che (5.3) è una relazione, intendiamo dire che l'espressione formale è una relazione, ossia che se la calcoliamo in  $V$  otteniamo  $0 = 0$ . Poiché la relazione è determinata dall' $R$ -vettore  $(a_1, \dots, a_m)^t$ , diremo che questo vettore è un *vettore di relazione*, nel senso che la relazione (5.3) è vera in  $V$ . Inoltre, si dice *insieme completo di relazioni* un insieme di vettori di relazione tali che ogni vettore di relazione è una combinazione lineare di essi. È chiaro che una matrice quale la (5.2) descrive completamente il modulo  $V$  solo se le sue colonne formano un insieme completo di relazioni.

Il concetto di insieme completo di relazioni può creare un po' di confusione. Diventa molto più chiaro quando lavoriamo con gli omomorfismi di moduli liberi anziché direttamente con le relazioni o con i vettori di relazione. Sia data una matrice  $A$  di tipo  $m \times n$  ad elementi in un anello  $R$ . Come sappiamo, la moltiplicazione a sinistra per questa matrice è un omomorfismo di  $R$ -moduli

$$(5.4) \quad \varphi : R^n \rightarrow R^m.$$

Oltre al nucleo e all'immagine, che abbiamo descritto nell'ultimo paragrafo quando  $R = \mathbb{Z}$ , vi è un altro importante modulo ausiliario associato a un omomorfismo  $\varphi : W \rightarrow W'$  di  $R$ -moduli, chiamato il suo *conucleo*. Il conucleo di  $\varphi$  è definito come il modulo quoziante

$$(5.5) \quad W' / (\text{im } \varphi).$$

Se indichiamo l'immagine della moltiplicazione a sinistra per  $A$  con  $AR^n$ , il conucleo di (5.4) è  $R^m/AR^n$ . Si dice allora che questo conucleo è *presentato* dalla matrice  $A$ . Più in generale, diremo che ogni isomorfismo del tipo

$$(5.6) \quad \sigma : R^m/AR^n \xrightarrow{\sim} V$$

presentazione di un modulo  $V$ , e che la matrice  $A$  è una *matrice di presentazione* per  $V$ , se un tale isomorfismo esiste.

Per esempio, il gruppo ciclico  $\mathbb{Z}/(5)$  è presentato, come  $\mathbb{Z}$ -modulo, dalla matrice

[5] di tipo  $1 \times 1$ . Consideriamo ancora, come esempio, lo  $\mathbb{Z}$ -modulo  $V$  presentato dalla matrice  $A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$ . Le colonne di questa matrice sono i

vettori di relazione, sicché  $V$  è generato da due elementi  $v_1, v_2$  con le relazioni

$2v_1 + v_2 = -v_1 + 2v_2 = 0$ . Possiamo risolvere la prima relazione, ottenendo  $v_2 = -2v_1$ .

Ciò permette di eliminare il secondo generatore. Infatti dalla seconda relazione,

per sostituzione, si ottiene  $-5v_1 = 0$ . Pertanto  $V$  può essere generato anche da un

solo generatore  $v_1$ , con l'unica relazione  $5v_1 = 0$ . Ciò prova che  $V$  è isomorfo a

$\mathbb{Z}/(5)$ , sicché anche la matrice  $A$  presenta il gruppo ciclico  $\mathbb{Z}/(5)$ .

Descriveremo ora un metodo teorico per trovare una presentazione di un dato modulo  $V$ . Per usare questo metodo nei casi pratici, il modulo dovrebbe essere assegnato in un modo molto esplicito. Il primo passo consiste nella scelta di un insieme di generatori  $(v_1, \dots, v_m)$ , sicché, per cominciare,  $V$  deve essere finitamente generato. Tali generatori forniscono un omomorfismo suriettivo

$$(5.7) \quad f : R^m \rightarrow V,$$

il quale manda il vettore colonna  $X = (x_1, \dots, x_m)$  in  $v_1x_1 + \dots + v_mx_m$ . Gli elementi del nucleo di  $f$  sono i vettori di relazione. Indichiamo questo nucleo con  $W$ ; in base al primo teorema di isomorfismo,  $V$  è isomorfo a  $R^m/W$ .

Ripetiamo il procedimento, scegliendo un insieme di generatori  $(w_1, \dots, w_n)$  per  $W$  mediante i quali definiamo un omomorfismo suriettivo

$$(5.8) \quad g : R^n \rightarrow W$$

come prima. Poiché  $W$  è un sottomodulo di  $R^m$ , la composizione dell'omomorfismo  $g$  con l'inclusione  $W \subset R^m$  ci dà un omomorfismo

$$(5.9) \quad \varphi : R^n \rightarrow R^m.$$

Questo omomorfismo è la moltiplicazione a sinistra per una matrice  $A$ . Per costruzione,  $W$  è l'immagine di  $\varphi$ , che è  $AR^n$ , sicché  $R^m/AR^n = R^m/W \approx V$ . Pertanto  $A$  è una matrice di presentazione per  $V$ .

Le colonne della matrice  $A$  sono i generatori scelti per il modulo  $W$ :

$$w_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \dots, w_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}.$$

Poiché generano  $W$ , che è il modulo dei vettori di relazione, queste colonne formano un insieme completo di relazioni tra i generatori  $(v_1, \dots, v_m)$  del modulo  $V$ . Essendo le colonne vettori di relazione, si ha

$$(5.10) \quad (v_1, \dots, v_m)A = 0.$$

Dunque la matrice di presentazione  $A$  per un modulo  $V$  è determinata da:

- (5.11) (i) un insieme di generatori per  $V$ , e  
(ii) un insieme completo di relazioni tra questi generatori.

Abbiamo sorvolato su un punto in questa descrizione. Affinché il modulo delle relazioni  $W$  abbia un insieme finito di generatori, deve essere finitamente generato. Questa non sembra un'ipotesi ragionevole, poiché la relazione tra il modulo  $V$  di partenza e  $W$  non è chiara: siamo disposti a supporre che  $V$  sia finitamente generato, ma non è una buona cosa imporre delle ipotesi su un modulo che viene fuori nel corso di qualche costruzione ausiliaria. Avremo bisogno di esaminare questo punto più da vicino [cfr. (5.17)], ma a parte questo, possiamo parlare ora di generatori e relazioni per un  $R$ -modulo  $V$  finitamente generato.

Poiché la matrice di presentazione dipende dalle scelte (5.11), molte matrici presentano lo stesso modulo, o moduli isomorfi. Ecco qui alcune regole per trasformare una matrice  $A$  senza cambiare la classe di isomorfismo del modulo che essa presenta:

(5.12) PROPOSIZIONE *Sia  $A$  una matrice di presentazione  $m \times n$  per un modulo  $V$ . Le seguenti matrici  $A'$  presentano lo stesso modulo  $V$ :*

- (i)  $A' = QAP^{-1}$ , dove  $Q \in GL_m(R)$  e  $P \in GL_n(R)$ ;
- (ii)  $A'$  è ottenuta cancellando in  $A$  una colonna di zeri;
- (iii) la  $j$ -esima colonna di  $A$  è  $e_i$ , e  $A'$  è ottenuta da  $A$  cancellando la  $i$ -esima riga e la  $j$ -esima colonna.

*Dimostrazione.*

- (i) Il modulo  $R^m/AR^n$  è isomorfo a  $V$ . Poiché il passaggio da  $A$  a  $QAP^{-1}$  corrisponde ad un cambiamento di base in  $R^m$  e  $R^n$ , la classe di isomorfismo del modulo quoziante non cambia.
- (ii) Una colonna di zeri corrisponde alla relazione banale, la quale può essere omessa.
- (iii) Supponiamo che la  $j$ -esima colonna della matrice  $A$  sia  $e_i$ . La relazione corrispondente è  $v_i = 0$ . Pertanto essa vale nel modulo  $V$ , e quindi  $v_i$  può essere eliminato nell'insieme dei generatori  $(v_1, \dots, v_m)$ . Così facendo, la matrice  $A$  viene cambiata cancellando la  $i$ -esima riga e la  $j$ -esima colonna. ■

In queste regole, talvolta è possibile semplificare di molto una matrice. Per esempio, la matrice intera (5.2) considerata all'inizio può essere ridotta nel modo seguente:

$$\begin{aligned} A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix} &\rightarrow \begin{bmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 2 & 4 \\ 1 & 2 & 2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 1 & 6 \\ 0 & 2 & 4 \end{bmatrix} \rightarrow \\ &\rightarrow \begin{bmatrix} 2 & 1 & 6 \\ -4 & 0 & -8 \end{bmatrix} \rightarrow [-4 \quad -8] \rightarrow [-4 \quad 0] \rightarrow [4]. \end{aligned}$$

Dunque  $A$  presenta il gruppo abeliano  $\mathbb{Z}/(4)$ .

Per definizione, una matrice  $m \times n$  presenta un modulo per mezzo di  $m$  generatori e  $n$  relazioni. Ma, come vediamo da questo esempio, il numero dei generatori e il numero delle relazioni non sono univocamente determinati dal modulo.

Consideriamo ancora due esempi. La matrice  $2 \times 1 \begin{bmatrix} 4 \\ 0 \end{bmatrix}$ , che non si può semplificare, presenta un gruppo abeliano  $V$  per mezzo di due generatori  $(v_1, v_2)$  e una relazione  $4v_1 = 0$ . Il gruppo che essa presenta è isomorfo al gruppo prodotto  $\mathbb{Z}/(4) \times \mathbb{Z}$ . D'altra parte, la matrice  $\begin{bmatrix} 4 & 0 \end{bmatrix}$  presenta un gruppo con un generatore  $v_1$  e due relazioni, la seconda delle quali è la relazione banale. Questo gruppo è  $\mathbb{Z}/(4)$ .

Esaminiamo ora la condizione che il modulo delle relazioni sia finitamente generato. Per i moduli su un anello dotato di una struttura complicata, il modulo delle relazioni non è necessariamente finitamente generato, anche se  $V$  è finitamente generato. Per fortuna, questo problema non si presenta per gli anelli da noi considerati, come ora dimostreremo.

(5.13) PROPOSIZIONE *Le seguenti condizioni su un  $R$ -modulo  $V$  sono equivalenti:*

- (i) *ogni sottomodulo  $W$  di  $V$  è finitamente generato;*
- (ii) *(condizione della catena ascendente) non esistono catene infinite strettamente crescenti  $W_1 < W_2 < \dots$  di sottomoduli di  $V$ .*

*Dimostrazione.* Supponiamo che  $V$  soddisfi alla condizione della catena ascendente, e sia  $W$  un sottomodulo di  $V$ . Scegliamo un insieme  $w_1, w_2, \dots, w_k$  di generatori di  $W$  nel modo seguente. Se  $W = 0$ , allora  $W$  è generato dall'insieme vuoto. Altrimenti, partiamo da un elemento non nullo  $w_1 \in W$ . Per continuare, supponiamo di aver scelto  $w_1, \dots, w_i$ , e sia  $W_i$  il sottomodulo generato da questi elementi. Se  $W_i$  è un sottomodulo proprio di  $W$ , sia  $w_{i+1}$  un elemento di  $W$  che non sia contenuto in  $W_i$ . Allora  $W_1 < W_2 < \dots$  Poiché  $V$  soddisfa alla condizione

della catena ascendente, tale catena di sottomoduli non può proseguire indefinitamente. Pertanto qualche sottomodulo  $W_k$  è uguale a  $W$ . Allora  $(w_1, \dots, w_k)$  genera  $W$ .

Il viceversa si ottiene seguendo la dimostrazione del teorema (2.12) del capitolo 11. Supponiamo che ogni sottomodulo di  $V$  sia finitamente generato, e sia  $W_1 \subset W_2 \subset \dots$  una catena ascendente infinita di sottomoduli di  $V$ . Si denoti con  $U$  l'unione di questi sottomoduli. Allora  $U$  è un sottomodulo [cfr. cap. 11 (2.11)], sicché è finitamente generato. Siano  $u_1, \dots, u_r$  generatori di  $U$ . Ciascun  $u_i$  appartiene ad uno dei moduli  $W_i$ , e poiché la catena è crescente, esiste un indice  $i$  tale che tutti i generatori appartengono a  $W_i$ . Allora il modulo  $U$  da essi generato è contenuto anch'esso in  $W_i$ , e si ha  $U \subset W_i \subset W_{i+1} \subset U$ . Ciò prova che  $U = W_i = W_{i+1}$  e che la catena non è strettamente crescente. ■

#### (5.14) LEMMA

- (a) *Sia  $\varphi : V \rightarrow W$  un omomorfismo di  $R$ -moduli. Se il nucleo e l'immagine di  $\varphi$  sono moduli finitamente generati, lo è anche  $V$ . Se  $V$  è finitamente generato e  $\varphi$  è suriettivo, allora  $W$  è finitamente generato. Più precisamente, supponiamo che  $(v_1, \dots, v_n)$  generi  $V$  e che  $\varphi$  sia suriettivo. Allora  $(\varphi(v_1), \dots, \varphi(v_n))$  genera  $W$ .*
- (b) *Sia  $W$  un sottomodulo di un  $R$ -modulo  $V$ . Se  $W$  e  $V/W$  sono entrambi finitamente generati, anche  $V$  è finitamente generato. Se  $V$  è finitamente generato, tale risulta  $V/W$ .*

*Dimostrazione.* Per la prima asserzione di (a), seguiamo la dimostrazione della formula della dimensione per le applicazioni lineari [cap. 4 (1.5)], scegliendo un insieme di generatori  $(u_1, \dots, u_k)$  per  $\ker \varphi$  e un insieme di generatori  $(w_1, \dots, w_m)$  per  $\text{im } \varphi$ . Inoltre scegliamo elementi  $v_i \in V$  tali che  $\varphi(v_i) = w_i$ . Allora affermiamo che l'insieme  $(u_1, \dots, u_k; v_1, \dots, v_m)$  genera  $V$ . Sia  $v \in V$  un elemento arbitrario. Allora  $\varphi(v)$  è una combinazione lineare di  $(w_1, \dots, w_m)$ , diciamo  $\varphi(v) = a_1 w_1 + \dots + a_m w_m$ . Poniamo  $v' = a_1 v_1 + \dots + a_m v_m$ . Allora  $\varphi(v') = \varphi(v)$ . Ne segue che  $v - v' \in \ker \varphi$ , sicché  $v - v'$  è una combinazione lineare di  $(u_1, \dots, u_k)$ , diciamo  $v - v' = b_1 u_1 + \dots + b_k u_k$ . Pertanto  $v = a_1 v_1 + \dots + a_m v_m + b_1 u_1 + \dots + b_k u_k$ . Ciò prova che l'insieme  $(u_1, \dots, u_k; v_1, \dots, v_m)$  genera  $V$ , come richiesto. La dimostrazione della seconda asserzione di (a) è facile e viene lasciata come esercizio. La parte (b) segue dalla parte (a), considerando l'omomorfismo canonico  $\pi : V \rightarrow V/W$ . ■

#### (5.15) DEFINIZIONE

*Un anello  $R$  si dice noetheriano se ogni ideale di  $R$  è finitamente generato.*

I domini a ideali principali sono ovviamente noetheriani, sicché gli anelli  $\mathbb{Z}[i]$  e  $F[x]$  (dove  $F$  è un campo) sono noetheriani.

#### (5.16) COROLLARIO

*Sia  $R$  un anello noetheriano. Allora ogni ideale proprio  $I$  di  $R$  è contenuto in un ideale massimale [cfr. cap. 10 (8.3)].*

*Dimostrazione.* Se  $I$  non è massimale, allora  $I$  è contenuto propriamente in un ideale proprio  $I_2$ , e se  $I_2$  non è massimale, esso è contenuto propriamente in un ideale proprio  $I_3$ , e così via. In virtù della condizione della catena ascendente (5.13), la catena  $I = I_1 \subset I_2 \subset I_3 \subset \dots$  è necessariamente finita. Pertanto  $I_k$  è massimale per qualche  $k$ . ■

L'importanza della nozione di anello noetheriano per il nostro problema è mostrata dalla seguente proposizione:

**(5.17) PROPOSIZIONE** *Sia  $V$  un modulo finitamente generato su un anello noetheriano  $R$ . Allora ogni sottomodulo di  $V$  è finitamente generato.*

*Dimostrazione.* Basta dimostrare la proposizione nel caso in cui  $V = R^m$ . Infatti, supponiamo di aver dimostrato che i sottomoduli di  $R^m$  sono finitamente generati, per ogni  $m$ . Sia  $V$  un  $R$ -modulo finitamente generato. Allora esiste un omomorfismo suriettivo  $\varphi : R^m \rightarrow V$ . Dato un sottomodulo  $S$  di  $V$ , poniamo:  $L = \varphi^{-1}(S)$ . Allora  $L$  è un sottomodulo del modulo  $R^m$  e pertanto  $L$  è finitamente generato. Inoltre, l'applicazione  $L \rightarrow S$  è suriettiva e quindi  $S$  è finitamente generato (5.14).

Per dimostrare la proposizione nel caso in cui  $V = R^m$ , procediamo per induzione su  $m$ . Un sottomodulo di  $R$  non è altro che un ideale di  $R$  (1.3). Pertanto l'ipotesi di noetherianità su  $R$  ci dice che la proposizione vale per  $V = R^m$ , quando  $m = 1$ . Supponiamo ora che  $m > 1$ . Consideriamo la proiezione

$$\pi : R^m \rightarrow R^{m-1}$$

ottenuta eliminando l'ultimo elemento:  $\pi(a_1, \dots, a_m) = (a_1, \dots, a_{m-1})$ . Il suo nucleo è  $\{(0, \dots, 0, a_m)\} \approx R$ . Sia  $W \subset R^m$  un sottomodulo e sia  $\varphi : W \rightarrow R^{m-1}$  la restrizione di  $\pi$  a  $W$ . L'immagine  $\varphi(W)$  è un sottomodulo finitamente generato di  $R^{m-1}$ , per l'ipotesi induttiva. Inoltre,  $\ker \varphi = (W \cap \ker \pi)$  è un sottomodulo di  $\ker \pi \approx R$ , sicché anch'esso è finitamente generato. In base al lemma (5.14),  $W$  è finitamente generato, come richiesto. ■

Questa proposizione completa la dimostrazione del teorema (4.11).

Poiché i domini a ideali principali sono noetheriani, i sottomoduli dei moduli finitamente generati su tali anelli sono finitamente generati. Ma in effetti, la maggior parte degli anelli incontrati finora sono noetheriani. Ciò segue da un altro famoso teorema di Hilbert:

**(5.18) TEOREMA DELLA BASE DI HILBERT** *Se un anello  $R$  è noetheriano, anche l'anello dei polinomi  $R[x]$  è noetheriano.*

Dal teorema della base di Hilbert si ottiene, procedendo per induzione, che l'anello dei polinomi in più variabili  $R[x_1, \dots, x_n]$  su un anello noetheriano  $R$  è

noetheriano, sicché gli anelli  $\mathbb{Z}[x_1, \dots, x_n]$  e  $F[x_1, \dots, x_n]$  (dove  $F$  è un campo) sono noetheriani. Inoltre, i quozienti di anelli noetheriani sono noetheriani:

(5.19) PROPOSIZIONE *Sia  $R$  un anello noetheriano e sia  $I$  un ideale di  $R$ . Allora l'anello quoziante  $\bar{R} = R/I$  è noetheriano.*

*Dimostrazione.* Sia  $\bar{J}$  un ideale di  $\bar{R}$ , e sia  $J = \pi^{-1}(\bar{J})$  l'ideale corrispondente di  $R$ , dove  $\pi : R \rightarrow \bar{R}$  è l'omomorfismo canonico. Allora  $J$  è finitamente generato, diciamo da  $(a_1, \dots, a_m)$ . Ne segue che l'insieme finito  $(\bar{a}_1, \dots, \bar{a}_m)$  genera  $\bar{J}$ , in virtù del lemma (5.14). ■

Mettendo insieme tale proposizione con il teorema della base di Hilbert, si ottiene il seguente risultato:

(5.20) COROLLARIO *Ogni anello quoziante di un anello di polinomi su  $\mathbb{Z}$  o su un campo è noetheriano.* ■

*Dimostrazione del teorema della base di Hilbert.* Sia  $R$  un anello noetheriano, e  $I$  un ideale dell'anello dei polinomi  $R[x]$ . Dobbiamo dimostrare che  $I$  è generato da un insieme finito di polinomi.

Rivediamo la dimostrazione nel caso in cui  $R$  è un campo, e cerchiamo di generalizzarla. In tal caso, possiamo scegliere un polinomio non nullo  $f \in I$  di grado minimo, diciamo

$$(5.21) \quad f(x) = a_n x^n + \dots + a_1 x + a_0, \quad \text{con } a_n \neq 0,$$

e dimostrare che esso genera l'ideale nel modo seguente. Sia

$$(5.22) \quad g(x) = b_m x^m + \dots + b_1 x + b_0, \quad \text{con } b_m \neq 0,$$

un elemento non nullo di  $I$ . Allora il grado  $m$  di  $g$  è  $\geq n$ . Procediamo per induzione su  $m$ . Il polinomio

$$(5.23) \quad g(x) - (b_m/a_n)x^{m-n}f(x) = g_1(x)$$

è un elemento di  $I$  di grado  $< m$ . In virtù dell'ipotesi induttiva,  $g_1$  è divisibile per  $f$ ; ne segue che  $g$  è divisibile per  $f$ .

La formula (5.23) è il primo passo nella divisione con resto di  $g$  per  $f$ . Questo metodo non si estende direttamente ad anelli arbitrari, poiché la divisione con resto richiede che il coefficiente direttore di  $f$  sia un'unità. Più precisamente, per poter scrivere l'espressione (5.23), abbiamo bisogno di sapere che  $a_n$  divide  $b_m$  nell'anello  $R$ , il che in generale non sarà vero. Avremo bisogno di più generatori.

Indichiamo con  $A$  l'insieme dei coefficienti direttori di tutti i polinomi in  $I$ , insieme con l'elemento nullo di  $R$ .

(5.24) LEMMA *L'insieme  $A$  dei coefficienti direttori dei polinomi in un ideale  $R[x]$ , insieme con l'elemento nullo di  $R$ , forma un ideale di  $R$ .*

*Dimostrazione.* Se  $\alpha = a_n$  è il coefficiente direttore di  $f$ , allora  $r\alpha$  è il coefficiente direttore di  $rf$ , a meno che non risulti  $r\alpha = 0$ . In ogni caso,  $r\alpha \in A$ . Inoltre, sia  $\alpha = a_n$  il coefficiente direttore di  $f$  e sia  $\beta = b_m$  il coefficiente direttore di  $g$ , e supponiamo  $m \geq n$ . Allora  $\alpha$  è anche il coefficiente direttore di  $x^{m-n}f$ . Pertanto il coefficiente di  $x^m$  nel polinomio  $h = x^{m-n}f + g$  è  $\alpha + \beta$ . Questo è il coefficiente direttore di  $h$ , a meno che non sia uguale a zero, e in ogni caso,  $\alpha + \beta \in A$ . ■

Ritorniamo ora alla dimostrazione del teorema della base di Hilbert. In base al lemma, l'insieme  $A$  è un ideale dell'anello noetheriano  $R$ , sicché esiste un insieme finito di generatori, diciamo  $(\alpha_1, \dots, \alpha_k)$ , per questo ideale. Per ciascun indice  $i$ , con  $1 \leq i \leq k$ , scegliamo un polinomio  $f_i \in I$  con coefficiente direttore  $\alpha_i$ , e moltiplichiamo questi polinomi per opportune potenze di  $x$ , in modo tale che i loro gradi risultino tutti uguali allo stesso intero  $n$ .

L'insieme di polinomi  $(f_1, \dots, f_k)$  ottenuto in questo modo ci permetterà di scrivere una relazione analoga alla (5.23), ma probabilmente non genererà  $I$ . Sarà difficile trovare un polinomio di grado  $< n$  nell'ideale  $(f_1, \dots, f_k)$ . Pertanto dobbiamo aggiungere alcuni polinomi di grado basso per ottenere generatori per il nostro ideale. Il lemma seguente è facile, e non verrà dimostrato.

(5.25) LEMMA *Sia  $P_n$  l'insieme dei polinomi in  $R[x]$  di grado  $< n$ , insieme con il polinomio nullo, e poniamo  $S_n = I \cap P_n$ . Allora  $S_n$  è un  $R$ -sottomodulo dell' $R$ -modulo  $P_n$ .* ■

L' $R$ -modulo  $P_n$  è generato dai monomi  $1, x, \dots, x^{n-1}$ , sicché è finitamente generato. Poiché  $R$  è noetheriano, possiamo usare il lemma (5.25) e la proposizione (5.17) per concludere che esiste un insieme finito di elementi  $(h_1, \dots, h_s)$  che genera  $S_n$  come  $R$ -modulo. Vogliamo dimostrare che  $(f_1, \dots, f_k; h_1, \dots, h_s)$  genera  $I$ .

Denotiamo con  $J$  l'ideale generato da tale insieme. Per costruzione,  $J \subset I$ . Dobbiamo dimostrare l'inclusione opposta, e a tale scopo procediamo per induzione sul grado di un elemento  $g \in I$ , diciamo  $m$ . Se  $m < n$ , allora  $g \in S_n$  e pertanto  $g$  è una combinazione lineare di  $(h_1, \dots, h_s)$  a coefficienti in  $R$ . In questo caso dunque  $g \in J$ . Supponiamo che  $m \geq n$ , e sia  $b = b_m$  il coefficiente direttore di  $g$ . Allora  $b$  appartiene all'ideale  $A$  dei coefficienti direttori, e quindi è una combinazione lineare dei generatori di  $A$ , diciamo  $b = r_1 \alpha_1 + \dots + r_k \alpha_k$ . Ricordando che  $\alpha_i$  è il coefficiente direttore di  $f_i$ , si vede che il polinomio

$$p = x^{m-n} \left( \sum_i r_i f_i \right)$$

ha lo stesso coefficiente direttore e lo stesso grado di  $g$ , e inoltre sta in  $J$ . Pertanto  $g_1 = g - p$  ha grado minore di  $m$ . In virtù dell'ipotesi induttiva,  $g_1 \in J$ , e quindi  $g \in J$ . ■

## 6 Il teorema di struttura per i gruppi abeliani

Il teorema di struttura per i gruppi abeliani afferma che un gruppo abeliano finitamente generato  $V$  è una somma diretta di gruppi ciclici. Il lavoro occorrente per la dimostrazione è stato già fatto. Sappiamo che esiste una matrice di presentazione diagonale per  $V$ , e ciò che ci resta da fare è interpretare il significato di questa matrice diagonale per il gruppo.

Innanzitutto, abbiamo bisogno di estendere il concetto di somma diretta dagli spazi vettoriali ai moduli. La definizione è la stessa: se  $W_1, \dots, W_k$  sono sottomoduli di un modulo  $V$ , la loro somma è il sottomodulo da essi generato. È costituito da tutte le somme, ossia

$$(6.1) \quad W_1 + \dots + W_k = \{v \in V \mid v = w_1 + \dots + w_k, \text{ con } w_i \in W_i\}.$$

La verifica che questo insieme è un sottomodulo è immediata ed è del tutto simile a quella relativa alle somme di sottospazi di uno spazio vettoriale. Si dice che  $V$  è la somma diretta dei sottomoduli  $W_i$ , se sono soddisfatte le seguenti condizioni:

- $$(6.2) \quad \begin{aligned} \text{(i)} & \quad \text{i } W_i \text{ generano } V, \text{ ossia } V = W_1 + \dots + W_k; \\ \text{(ii)} & \quad \text{i } W_i \text{ sono indipendenti, ossia, se } w_1 + \dots + w_k = 0, \text{ con } w_i \in W_i, \\ & \quad \text{allora } w_i = 0 \text{ per ogni } i. \end{aligned}$$

Dunque  $V$  è la somma diretta dei sottomoduli  $W_i$ , se ogni elemento  $v \in V$  può essere scritto in modo unico nella forma  $v = w_1 + \dots + w_k$ , con  $w_i \in W_i$ . Come abbiamo visto per gli spazi vettoriali, due sottomoduli  $W_1, W_2$  sono indipendenti se e solo se  $W_1 \cap W_2 = 0$  [cfr. cap. 3 (6.5)].

Come in precedenza, per denotare le somme dirette viene usato il simbolo  $\oplus$ . Pertanto la notazione

$$(6.3) \quad V = W_1 \oplus \dots \oplus W_k$$

significa che  $V$  è la somma diretta dei sottomoduli  $W_i$ .

(6.4) **TEOREMA DI STRUTTURA PER I GRUPPI ABELIANI** *Sia  $V$  un gruppo abeliano finitamente generato. Allora  $V$  è una somma diretta di sottogruppi ciclici finiti  $C_{d_1}, \dots, C_{d_k}$  e di un gruppo abeliano libero  $L$ :*

$$V = C_{d_1} \oplus \dots \oplus C_{d_k} \oplus L,$$

*dove l'ordine  $d_i$  di  $C_{d_i}$  è maggiore di 1, e  $d_1 \mid d_2 \mid d_3 \dots$*

Useremo qui la notazione additiva per la legge di composizione nei gruppi ciclici. Pertanto  $C_n$  è generato da un solo elemento  $v$ , con una sola relazione  $nv = 0$ . Dunque  $C_n$  è isomorfo a  $\mathbb{Z}/(n)$ . L'isomorfismo  $\mathbb{Z}/(n) \rightarrow C_n$  manda la classe resto di un intero  $r$  in  $rv$ .

**Dimostrazione.** Scegliamo una matrice di presentazione  $A$  per  $V$ , determinata da un insieme di generatori ed un insieme completo di relazioni. Possiamo farlo perché  $V$  è finitamente generato e perché  $\mathbb{Z}$  è un anello noetheriano (cfr. § 5). In virtù della proposizione (5.12) la matrice  $A$  può essere sostituita da  $QAP^{-1}$ , dove  $Q$  e  $P$  sono invertibili. Pertanto possiamo supporre che  $A$  sia diagonale, che gli elementi diagonali siano non nulli e che ciascun elemento diagonale divida il successivo. Inoltre, possiamo sopprimere qualsiasi colonna nulla e qualsiasi riga o colonna in cui l'elemento diagonale è 1 (5.12). Quindi possiamo supporre che gli elementi diagonali  $d_i$  siano diversi da 0 e da 1. La matrice  $A$  avrà allora la forma:

$$(6.5) \quad \left[ \begin{array}{cccc} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \\ \hline & & & \\ & & & 0 \end{array} \right].$$

Essa sarà pertanto una matrice  $m \times k$ , dove  $k \leq m$ . Il significato di ciò in termini di generatori e relazioni per il nostro modulo è che  $V$  è generato da  $m$  elementi  $v_1, \dots, v_m$ , e che

$$(6.6) \quad d_1 v_1 = 0, \quad d_2 v_2 = 0, \dots, \quad d_k v_k = 0$$

formano un insieme completo di relazioni tra questi generatori.

Per  $j = 1, \dots, k$ , denotiamo con  $C_j$  il sottogruppo ciclico generato da  $v_j$ . Sia  $L$  il sottogruppo generato dai rimanenti generatori  $v_{k+1}, \dots, v_m$ . Poiché le colonne di (6.5) sono un insieme completo di relazioni, non esiste nessuna relazione tra questi ultimi  $m - k$  generatori. Pertanto  $L$  è un gruppo abeliano libero di rango  $m - k$ . Verifichiamo ora che  $V = C_1 \oplus \dots \oplus C_k \oplus L$  e che  $C_j$  ha ordine  $d_j$ . Innanzitutto, poiché  $V$  è generato dai  $v_i$  e poiché ciascuno dei  $v_i$  è contenuto in uno degli addendi, è chiaro che  $V$  è la somma di questi sottogruppi. Inoltre, supponiamo che esista una relazione, diciamo

$$z_1 + \dots + z_k + w = 0,$$

dove  $z_j \in C_j$  e  $w \in L$ . Poiché  $C_j$  è il gruppo ciclico generato da  $v_j$ , possiamo scrivere  $z_j = r_j v_j$  per qualche intero  $r_j$ . Analogamente, possiamo scrivere  $w = r_{k+1}v_{k+1} + \dots + r_mv_m$ , essendo  $r_{k+1}, \dots, r_m$  interi opportuni. Allora la relazione ha la forma:

$$r_1v_1 + \dots + r_mv_m = 0.$$

Poiché le colonne di (6.5) formano un insieme completo di relazioni, il vettore  $(r_1, \dots, r_m)^t$  è una combinazione lineare di tali colonne. Pertanto  $r_j = 0$  se  $j > k$ , cioè  $w = 0$ . Inoltre,  $r_j$  deve essere divisibile per  $d_j$  se  $j \leq k$ , diciamo  $r_j = d_js_j$ . Allora  $z_j = s_jd_jv_j = 0$ . Dunque la relazione era banale, e ciò dimostra che i sottogruppi sono indipendenti, e inoltre che l'ordine del gruppo ciclico  $C_j$  è  $d_j$ . Pertanto risulta  $V = C_{d_1} \oplus \dots \oplus C_{d_k} \oplus L$ , come richiesto. ■

Un gruppo abeliano finito è finitamente generato, e quindi, in base al teorema di struttura (6.4), si decomponе in una somma diretta di gruppi ciclici finiti in cui l'ordine di ciascun addendo divide il successivo. In questo caso, l'addendo costituito dal gruppo abeliano libero è nullo. Talvolta conviene decomporre ulteriormente i gruppi ciclici in gruppi ciclici i cui ordini siano potenze di primi. Tale decomposizione è basata sulla proposizione (8.4) del capitolo 2, che qui rienunciamo:

(6.7) *Siano  $r, s$  interi primi tra loro. Il gruppo ciclico  $C_{rs}$  di ordine  $rs$  è la somma diretta dei sottogruppi ciclici di ordine  $r$  e  $s$ .* ■

Mettendo insieme questo lemma con il teorema di struttura, si ottiene il seguente corollario:

(6.8) COROLLARIO (Forma alternativa del teorema di struttura) *Ogni gruppo abeliano finitamente generato è una somma diretta di gruppi ciclici i cui ordini sono potenze di primi e di un gruppo abeliano libero.* ■

È naturale chiedersi se gli ordini dei sottogruppi ciclici in cui si decompone un gruppo abeliano finito siano univocamente determinati dal gruppo. Se l'ordine di  $V$  è un prodotto di primi distinti, non vi sono problemi. Per esempio, se l'ordine è 30, allora  $V$  deve essere isomorfo a  $C_2 \oplus C_3 \oplus C_5$ . Ma è possibile che uno stesso gruppo si scriva sia nella forma  $C_2 \oplus C_2 \oplus C_4$  che nella forma  $C_4 \oplus C_4$ ? La risposta è negativa, come è facile dimostrare contando gli elementi di ordine 1 o 2. Il gruppo  $C_4 \oplus C_4$  ne contiene quattro, mentre  $C_2 \oplus C_2 \oplus C_4$  ne contiene otto. Questo metodo di calcolo funziona sempre.

## (6.9) TEOREMA (Unicità per il teorema di struttura)

(a) *Supponiamo che un gruppo abeliano finito  $V$  sia una somma diretta di gruppi ciclici  $C_{d_1} \oplus \dots \oplus C_{d_k}$ , dove  $d_1|d_2|\dots$ . Allora gli interi  $d_j$  sono determinati dal gruppo  $V$ .*

(b) *Lo stesso risultato vale se ciascuno degli interi  $d_j$  è la potenza di un primo.*

La dimostrazione è lasciata come esercizio. ■

Il conto degli elementi si semplifica, dal punto di vista della notazione, rappresentando una somma diretta come un prodotto. Sia  $R$  un anello. Il *prodotto diretto* di  $R$ -moduli  $W_1, \dots, W_k$  è l'insieme prodotto  $W_1 \times \dots \times W_k$  delle  $k$ -uple, ossia:

$$(6.10) \quad W_1 \times \dots \times W_k = \{(w_1, \dots, w_k) \mid w_i \in W_i\}.$$

Esso risulta un modulo rispetto all'addizione tra "vettori" e alla moltiplicazione per uno "scalare", definite da:

$$(w_1, \dots, w_k) + (w'_1, \dots, w'_k) = (w_1 + w'_1, \dots, w_k + w'_k),$$

$$r(w_1, \dots, w_k) = (rw_1, \dots, rw_k).$$

La verifica degli assiomi di un modulo è immediata.

I prodotti diretti e le somme dirette sono isomorfi tra loro, come mostra la seguente proposizione:

(6.11) PROPOSIZIONE *Siano  $W_1, \dots, W_k$  sottomoduli di un  $R$ -modulo  $V$ .*

(a) *L'applicazione  $\sigma : W_1 \times \dots \times W_k \rightarrow V$  definita da*

$$\sigma(w_1, \dots, w_k) = w_1 + \dots + w_k$$

*è un omomorfismo di  $R$ -moduli, e la sua immagine è la somma  $W_1 + \dots + W_k$ .*

(b) *L'omomorfismo  $\sigma$  è un isomorfismo se e soltanto se  $V$  è la somma diretta dei sottomoduli  $W_i$ .*

Abbiamo visto enunciati simili parecchie volte prima d'ora, e pertanto la dimostrazione verrà omessa. Si noti che la seconda parte della proposizione è analoga all'enunciato che afferma che l'applicazione (2.5)  $R^k \rightarrow V$  definita da un insieme  $(v_1, \dots, v_k)$  è biettiva se e soltanto se tale insieme è una base. ■

Poiché un gruppo ciclico  $C_d$  di ordine  $d$  è isomorfo al gruppo ciclico  $\mathbb{Z}/(d)$ , possiamo utilizzare la proposizione (6.11) per rienunciare il teorema di struttura nella forma seguente:

(6.12) TEOREMA (Versione moltiplicativa del teorema di struttura) *Ogni gruppo abeliano finitamente generato  $V$  è isomorfo ad un prodotto diretto di gruppi ciclici:*

$$\mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k) \times \mathbb{Z}^r,$$

dove  $d_i, r$  sono interi. Esiste una decomposizione in cui ciascun  $d_i$  divide il successivo e una in cui ciascun  $d_i$  è una potenza di un primo. ■

Questa classificazione dei gruppi abeliani si estende senza variazioni essenziali ai domini euclidei. Poiché un dominio euclideo  $R$  è noetheriano, ogni  $R$ -modulo finitamente generato  $V$  ha una matrice di presentazione (5.6), e in base al teorema di diagonalizzazione (4.6), esiste una matrice di presentazione  $A$  che è diagonale.

Per mantenere l'analogia con i gruppi abeliani, diciamo che un  $R$ -modulo  $V$  è *ciclico* se è generato da un solo elemento  $v$ . Ciò equivale a dire che  $V$  è isomorfo ad un modulo quoziante  $R/I$ , dove  $I$  è l'ideale di  $R$  formato dagli elementi  $\alpha$  tali che  $\alpha v = 0$ . Precisamente, l'applicazione  $\varphi : R \rightarrow V$  che manda  $r$  in  $rv$  è un omomorfismo suriettivo di moduli, poiché  $v$  genera  $V$ , e il nucleo di  $\varphi$ , ossia il modulo delle relazioni, è un sottomodulo di  $R$ , dunque un ideale  $I$  (1.3). Pertanto  $V$  è isomorfo a  $R/I$ , in virtù del primo teorema di isomorfismo. Viceversa, se  $R/I \rightarrow V$  è un isomorfismo, l'immagine di 1 genererà  $V$ . Se  $R$  è un dominio euclideo l'ideale  $I$  sarà principale, e quindi  $V$  sarà isomorfo a  $R/(\alpha)$  per qualche  $\alpha \in R$ . In questo caso, anche il modulo delle relazioni sarà generato da un solo elemento.

Procedendo come nel caso dei gruppi abeliani, si dimostra il teorema seguente:

(6.13) TEOREMA DI STRUTTURA PER I MODULI SU UN DOMINIO EUCLIDEO  
Sia  $V$  un modulo finitamente generato su un dominio euclideo  $R$ . Allora  $V$  è una somma diretta di moduli ciclici  $C_j$  e di un modulo libero  $R$ . Più precisamente esiste un isomorfismo

$$\varphi : V \rightarrow R/(d_1) \times \cdots \times R/(d_k) \times R^r$$

dove  $r$  è un intero non negativo, gli elementi  $d_1, \dots, d_k$  sono diversi da zero e non invertibili. Esiste una decomposizione in cui

- (a)  $d_i$  divide  $d_{i+1}$  per  $i = 1, \dots, k-1$ ,  
e una in cui
- (b)  $d_i$  è la potenza di un elemento primo di  $R$ , cioè per  $i = 1, \dots, k$  esistono  $p_i$  primo in  $R$  ed  $e_i$  intero positivo tali che  $d_i = p_i^{e_i}$ . ■

Per esempio, consideriamo l' $F[t]$ -modulo  $V$  presentato dalla matrice  $A$  dell'esempio (4.7). In base a (5.12),  $V$  è presentato anche dalla matrice diagonale:

$$A' = \begin{bmatrix} 1 & & \\ & (t-1)^2(t-2) & \end{bmatrix},$$

possiamo sopprimere la prima riga e la prima colonna in questa matrice [r. (5.12)]. Pertanto  $V$  è presentato dalla matrice  $1 \times 1$  il cui unico elemento è  $f(t) = (t-1)^2(t-2)$ . Ciò significa che  $V$  è un modulo ciclico, isomorfo a  $F[t]/(g)$ . Poiché  $g$  ha due fattori primi tra loro,  $V$  può essere decomposto ulteriormente nel prodotto diretto di due moduli ciclici:

$$(6.14) \quad V \approx F[t]/(g) \approx [F[t]/(t-1)^2] \times [F[t]/(t-2)].$$

Con un po' più di lavoro, il teorema (6.13) può essere esteso ai moduli su un dominio a ideali principali. È ancora vero che le potenze di primi che compaiono in (b) sono uniche a meno di fattori invertibili. Per provare ciò, occorre trovare un'argomentazione che sostituisca quella basata sul conto degli elementi, utilizzata per il teorema (6.9), ma la dimostrazione non verrà data.

## 7 Applicazione agli operatori lineari

In questo paragrafo applicheremo in un modo inaspettato la teoria esposta nell'ultimo paragrafo agli operatori lineari sugli spazi vettoriali su un campo. Questa applicazione fornisce un buon esempio del modo in cui "l'analisi della dimostrazione" può condurre a nuovi risultati in matematica. Il metodo sviluppato all'inizio per i gruppi abeliani viene esteso formalmente ai moduli su un dominio euclideo, poi viene applicato a una nuova situazione concreta in cui l'anello è un anello di polinomi. Questo non è stato lo sviluppo storico: le teorie relative ai gruppi abeliani e agli operatori lineari sono state sviluppate indipendentemente e sono state legate insieme successivamente. Ma è davvero sorprendente che i due casi (i gruppi abeliani e gli operatori lineari) possano essere formalmente analoghi e tuttavia presentarsi alla fine tanto diversi tra loro, quando ad essi viene applicata la stessa teoria.

L'osservazione fondamentale che ci permette di procedere è che, se abbiamo un operatore lineare

$$(7.1) \quad T : V \rightarrow V$$

su uno spazio vettoriale su un campo  $F$ , lo possiamo usare per far diventare  $V$  un modulo sull'anello dei polinomi  $F[t]$ . Per fare ciò, dobbiamo definire la moltiplicazione di un vettore  $v$  per un polinomio  $f(t) = a_n t^n + \cdots + a_1 t + a_0$  a coefficienti in  $F$ . Poniamo per definizione:

$$(7.2) \quad f(t)v = a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v.$$

Il secondo membro può essere scritto come  $[f(T)](v)$ , dove  $f(T)$  denota l'operatore lineare  $a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0 I$ , ottenuto da  $f(t)$  sostituendo  $t$  con  $T$ .

(Abbiamo aggiunto le parentesi quadre soltanto per chiarezza.) Con tale notazione, otteniamo le formule:

$$(7.3) \quad tv = T(v) \quad \text{e} \quad f(t)v = [f(T)](v).$$

Si verifica facilmente che la definizione (7.2) dà a  $V$  una struttura di  $F[t]$ -modulo. Le formule (7.3) possono apparire tautologiche: ci si può chiedere perché abbiamo bisogno di un nuovo simbolo  $t$ , ma occorre ricordare che  $f(t)$  è un polinomio formale, mentre  $f(T)$  denota un certo operatore lineare.

Viceversa, sia  $V$  un  $F[t]$ -modulo. Allora la moltiplicazione scalare di un elemento di  $V$  per un polinomio  $f(t)$  è definita; in particolare, abbiamo una regola per la moltiplicazione per i polinomi costanti, ossia per gli elementi di  $F$ , la quale rende  $V$  uno spazio vettoriale su  $F$ , come mostrano gli assiomi (1.1). Inoltre, possiamo moltiplicare gli elementi di  $V$  per il polinomio  $t$ . Denotiamo con  $T$  l'operazione di moltiplicazione per  $t$  su  $V$ , cioè  $T$  è l'applicazione:

$$(7.4) \quad T : V \rightarrow V, \quad \text{definita da} \quad T(v) = tv.$$

Tale applicazione è un *operatore lineare* su  $V$ , considerato come spazio vettoriale su  $F$ . Infatti,  $t(v + v') = tv + tv'$  in base alla proprietà distributiva (1.1), e quindi  $T(v + v') = T(v) + T(v')$ . Inoltre, se  $c \in F$ , allora per la proprietà associativa (1.1) e la proprietà commutativa in  $F[t]$ ,  $tcv = ctv$ , sicché  $T(cv) = cT(v)$ . Pertanto un  $F[t]$ -modulo  $V$  fornisce un operatore lineare su uno spazio vettoriale.

Le operazioni che abbiamo descritto, ossia il passaggio dagli operatori lineari ai moduli e viceversa, sono l'una l'inversa dell'altra:

$$(7.5) \quad \begin{aligned} &\text{I concetti di operatore lineare su un } F\text{-spazio vettoriale} \\ &\text{e di } F[t]\text{-modulo sono equivalenti.} \end{aligned}$$

Applicheremo quest'osservazione agli spazi vettoriali di dimensione finita, tuttavia consideriamo, per inciso, l'operatore lineare che corrisponde all' $F[t]$ -modulo libero  $F[t]$  di rango 1. Sappiamo che  $F[t]$  ha dimensione infinita, come spazio vettoriale su  $F$ . I monomi  $(1, t, t^2, \dots)$  formano una base, e possiamo usare tale base per identificare  $F[t]$  con lo spazio  $Z$  degli  $F$ -vettori infiniti [cfr. cap. 10 (2.8)]:

$$Z = \{(a_0, a_1, a_2, \dots) \mid a_i \in F \text{ e gli } a_i \neq 0 \text{ sono in numero finito}\}.$$

La moltiplicazione per  $t$  su  $F[t]$  corrisponde all'*operatore di scorrimento*  $T$ :

$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0, a_1, a_2, \dots).$$

Dunque, a meno di isomorfismi, l' $F[t]$ -modulo libero di rango 1 corrisponde all'operatore spostamento sullo spazio  $Z$ .

Passiamo ora alla nostra applicazione agli operatori lineari. Dato un operatore lineare  $T$  su uno spazio vettoriale  $V$  su  $F$ , possiamo considerare  $V$  anche come

$F[t]$ -modulo. Supponiamo che  $V$  sia uno spazio vettoriale di dimensione finita, diciamo di dimensione  $n$ . Allora è certamente un modulo finitamente generato, e quindi ha una matrice di presentazione. Qui c'è qualche pericolo di confusione, poiché compaiono due matrici: la matrice di presentazione per il modulo  $V$  e la matrice dell'operatore lineare  $T$ . La matrice di presentazione è una matrice  $r \times s$  i cui elementi sono polinomi, dove  $r$  è il numero dei generatori scelti per il modulo e  $s$  è il numero delle relazioni. D'altra parte, la matrice dell'operatore lineare è una matrice  $n \times n$  i cui elementi sono scalari, dove  $n$  è la dimensione di  $V$  come spazio vettoriale. Entrambe le matrici contengono le informazioni necessarie per descrivere il modulo e l'operatore lineare.

Considerando  $V$  come un  $F[t]$ -modulo, possiamo applicare il teorema (6.13) per concludere che  $V$  è una somma diretta di sottomoduli ciclici, diciamo:

$$V = W_1 \oplus \cdots \oplus W_k,$$

dove  $W_i$  è isomorfo a  $F[t]/(p_i^{e_i})$ , essendo  $p_i(t)$  un polinomio irriducibile in  $F[t]$ . Non vi sono addendi liberi, poiché stiamo supponendo che  $V$  abbia dimensione finita.

Dobbiamo fare due cose: interpretare il significato di questa decomposizione in somma diretta per l'operatore lineare  $T$ , e descrivere l'operatore lineare nel caso in cui il modulo è ciclico. Non stupisce che la decomposizione in somma diretta fornisca una decomposizione in blocchi della matrice di  $T$ , purché si scelga una base opportuna. Infatti, ciascuno dei sottospazi  $W_i$  è  $T$ -invariante, essendo  $W_i$  un  $F[t]$ -sottomodulo. La moltiplicazione per  $t$  porta  $W_i$  in se stesso, e  $t$  agisce su  $V$  come l'operatore lineare  $T$ . Se sceglieremo delle basi  $\mathbf{B}_i$  per i sottospazi  $W_i$ , la matrice di  $T$  rispetto alla base  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_k)$  ha la forma a blocchi desiderata [cap. 4 (3.8)].

Inoltre, sia  $W$  un  $F[t]$ -modulo ciclico. Allora  $W$  è generato come modulo da un solo elemento  $w$ , ossia ogni elemento di  $W$  può essere scritto nella forma

$$g(t)w = b_rt^r w + \cdots + b_1t w + b_0w,$$

dove  $g(t) = b_rt^r + \cdots + b_1t + b_0 \in F[t]$ . Ne segue che gli elementi  $w, tw, t^2w, \dots$  generano  $W$  come spazio vettoriale. Utilizzando l'operatore lineare  $T$ ,  $W$  è generato dai vettori  $w, T(w), T^2(w), \dots$

Nella tabella seguente vengono riportate le proprietà di un  $F[t]$ -modulo e le proprietà dell'operatore lineare corrispondente:

### (7.6) DIZIONARIO

Moltiplicazione per $t$	Azione di $T$
Modulo libero di rango 1	Operatore spostamento
Modulo ciclico generato da $v$	Spazio vettoriale generato da $v, T(v), T^2(v), \dots$
Sottomodulo	Sottospazio $T$ -invariante
Somma diretta di sottomoduli	Somma diretta di sottospazi $T$ -invarianti
$F[t]$ -modulo	Operatore lineare $T$

Calcoliamo ora la matrice di un operatore lineare  $T$  su uno spazio vettoriale che corrisponde a un  $F[t]$ -modulo ciclico. Poiché ogni ideale di  $F[t]$  è principale, un modulo ciclico sarà isomorfo ad un modulo della forma:

$$(7.7) \quad W = F[t]/(f),$$

dove  $f = t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0$  è un polinomio in  $F[t]$ . Denotiamo con  $w_0$  la classe resto di 1 in  $W$ . Scegliamo  $w_0$  come generatore per il modulo. Allora vale la relazione  $fw_0 = 0$ , e  $f$  genera il modulo delle relazioni.

Gli elementi  $w_0, tw_0, \dots, t^{n-1}w_0$  formano una base per  $F[t]/(f)$  [cfr. cap. 10 (5.7)]. Denotiamo gli elementi di questa base con  $w_i = t^i w_0$ . Allora si ha

$$tw_0 = w_1, \quad tw_1 = w_2, \dots, \quad tw_{n-2} = w_{n-1},$$

e inoltre  $fw_0 = 0$ . Quest'ultima relazione può essere riscritta utilizzando le altre per determinare l'azione di  $t$  su  $w_{n-1}$ :

$$(t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0)w_0 =$$

$$tw_{n-1} + a_{n-1}w_{n-1} + \dots + a_1w_1 + a_0w_0 = 0.$$

Poiché  $T$  agisce come la moltiplicazione per  $t$ , si ottiene:

$$T(w_0) = w_1, \quad T(w_1) = w_2, \dots, \quad T(w_{n-2}) = w_{n-1},$$

e

$$T(w_{n-1}) = -a_{n-1}w_{n-1} - \dots - a_1w_1 - a_0w_0.$$

Ciò permette di determinare la matrice di  $T$ . Essa ha la forma seguente, in corrispondenza a vari valori di  $n$ :

$$(7.8) \quad [-a_0], \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix}, \dots, \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & 1 & 0 & \vdots \\ & & \ddots & \vdots \\ & & & 0 & \vdots \\ & & & & 1 & -a_{n-1} \end{bmatrix}.$$

(7.9) TEOREMA Sia  $T$  un operatore lineare su uno spazio vettoriale  $V$  di dimensione finita su un campo  $F$ . Allora esiste una base di  $V$  rispetto alla quale la matrice di  $T$  è costituita da blocchi del tipo (7.8). ■

Una forma siffatta per la matrice di un operatore lineare è chiamata una *forma canonica razionale*. Non è particolarmente espressiva, ma è la forma migliore che si possa ottenere per un campo qualsiasi.

Per esempio, il modulo (6.14) è una somma diretta di due moduli. La sua *forma canonica razionale* è

$$(7.10) \quad \left[ \begin{array}{c|c} -1 & \\ \hline 1 & 2 \\ \hline & 2 \end{array} \right].$$

Consideriamo ora più da vicino il caso in cui  $F$  è il campo dei numeri complessi. Ogni polinomio irriducibile in  $\mathbb{C}[t]$  è lineare, diciamo  $p(t) = t - \alpha$ , quindi in base al teorema (6.13), ogni  $\mathbb{C}[t]$ -modulo di dimensione finita come spazio vettoriale su  $\mathbb{C}$  è una somma diretta di sottomoduli isomorfi a moduli della forma

$$(7.11) \quad W = \mathbb{C}[t]/(t - \alpha)^n.$$

Come prima, denotiamo con  $w_0$  la classe resto di 1 in  $W$ , ma questa volta scegliamo un'altra base per  $W$ , ponendo  $w_i = (t - \alpha)^i w_0$ . Allora

$$(t - \alpha)w_0 = w_1, \quad (t - \alpha)w_1 = w_2, \dots, \quad (t - \alpha)w_{n-2} = w_{n-1}, \quad (t - \alpha)w_{n-1} = 0.$$

Sostituendo  $t$  con  $T$  e risolviamo, ottenendo:

$$Tw_i = w_{i+1} + \alpha w_i, \quad \text{per } i = 0, \dots, n-2,$$

e

$$Tw_{n-1} = \alpha w_{n-1}.$$

La matrice di  $T$  ha la forma:

$$(7.12) \quad [\alpha], \begin{bmatrix} \alpha & 0 \\ 1 & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & 0 & 0 \\ 1 & \alpha & 0 \\ 0 & 1 & \alpha \end{bmatrix}, \dots, \begin{bmatrix} \alpha & & & \\ \vdots & \ddots & \ddots & \\ & \ddots & \ddots & \\ & & & 1 & \alpha \end{bmatrix}.$$

Queste matrici sono chiamate *blocchi di Jordan*. Otteniamo così il teorema seguente:

(7.13) TEOREMA Sia  $T : V \rightarrow V$  un operatore lineare su uno spazio vettoriale complesso di dimensione finita. Allora esiste una base di  $V$  rispetto a cui la matrice di  $T$  è costituita da blocchi di Jordan. ■

Si dice che una matrice siffatta è in *forma di Jordan*, oppure è una *matrice di Jordan*. Si noti che è una matrice triangolare inferiore, sicché gli elementi diagonali sono i suoi autovalori. La forma di Jordan è molto più espressiva della forma canonica razionale.

Non è difficile dimostrare che ogni blocco di Jordan ha un solo autovettore, determinato a meno di una costante moltiplicativa.

Data una qualsiasi matrice quadrata complessa  $A$ , il teorema afferma che  $PAP^{-1}$  è in forma di Jordan per qualche matrice invertibile  $P$ . Spesso diremo che  $PAP^{-1}$  è “la forma di Jordan di  $A$ ”. Essa è unica a meno di permutazioni dei blocchi, poiché i termini nella decomposizione in somma diretta sono univocamente determinati, sebbene ciò non sia stato dimostrato.

La forma di Jordan del modulo (6.14) è costituita da due blocchi di Jordan:

$$(7.14) \quad \left[ \begin{array}{cc|c} 1 & & \\ & 1 & 1 \\ \hline & & 2 \end{array} \right].$$

Un'applicazione importante della forma di Jordan riguarda la soluzione esplicita di un sistema dato da un'equazione differenziale lineare del primo ordine:

$$(7.15) \quad \frac{dX}{dt} = AX.$$

Come abbiamo visto nel capitolo 4 (7.11), la soluzione di questa equazione è facilmente riconducibile a quella dell'equazione  $\frac{dX}{dt} = \tilde{A}X$ , dove  $\tilde{A} = PAP^{-1}$  è una matrice simile ad  $A$ . È sufficiente dunque, supposto che si riesca a determinare la forma di Jordan  $\tilde{A}$  della data matrice  $A$ , risolvere il sistema che ne risulta. Questo a sua volta si riduce al caso di un solo blocco di Jordan. Un esempio relativo ad un blocco di Jordan  $2 \times 2$  è stato calcolato nel capitolo 4 (8.18).

Le soluzioni per un blocco di Jordan  $k \times k$  arbitrario  $A$  si possono determinare calcolando la matrice esponenziale. Indichiamo con  $N$  la matrice  $k \times k$  ottenuta sostituendo  $\alpha = 0$  in (7.12). Allora  $N^k = 0$ . Ne segue che:

$$e^{Nt} = I + \frac{Nt}{1!} + \cdots + \frac{N^{k-1}t^{k-1}}{(k-1)!}.$$

Questa è una matrice triangolare inferiore che è costante sulle strisce diagonali e i cui elementi sulla  $i$ -esima striscia diagonale al disotto della diagonale principale sono  $t^i/i!$ . Poiché  $N$  e  $\alpha I$  commutano tra loro, si ha

$$e^{At} = e^{\alpha t} e^{Nt} = e^{\alpha t} \left( I + \frac{Nt}{1!} + \cdots + \frac{N^{k-1}t^{k-1}}{(k-1)!} \right).$$

Così, ad esempio, se  $A$  è la matrice:

$$A = \begin{bmatrix} 3 & & \\ & 1 & 3 \\ & & 1 & 3 \end{bmatrix},$$

Allora

$$e^{At} = \begin{bmatrix} e^{3t} & & \\ & e^{3t} & \\ & & e^{3t} \end{bmatrix} \begin{bmatrix} 1 & & \\ t & 1 & \\ \frac{1}{2}t^2 & t & 1 \end{bmatrix} = \begin{bmatrix} e^{3t} & & \\ & te^{3t} & e^{3t} \\ & \frac{1}{2}t^2e^{3t} & te^{3t} & e^{3t} \end{bmatrix}.$$

Il teorema (8.14) (cap. 4) ci dice che le colonne di questa matrice formano una base per lo spazio delle soluzioni dell'equazione differenziale (7.15).

Per calcolare la forma di Jordan di una data matrice, occorre trovare le radici del suo polinomio caratteristico  $p(t)$ . Se le radici  $\alpha_1, \dots, \alpha_n$  sono distinte, la forma di Jordan è diagonale:

$$\begin{bmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{bmatrix}.$$

Se invece  $p(t)$  ha una radice  $\alpha$  di molteplicità  $r$ , esistono varie possibilità per la parte della matrice di Jordan con gli elementi diagonali uguali a  $\alpha$ . Ecco i vari casi possibili per  $r = 1, 2, 3, 4$ :

$$r=1 : [\alpha]; \quad r=2 : \begin{bmatrix} \alpha & & \\ 1 & \alpha & \\ & & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & \\ & \alpha & \\ & & \alpha \end{bmatrix};$$

$$r=3 : \begin{bmatrix} \alpha & & & \\ 1 & \alpha & & \\ 1 & \alpha & \alpha & \\ & & & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & & \\ 1 & \alpha & & \\ & 1 & \alpha & \\ & & & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & & \\ & \alpha & & \\ & & \alpha & \\ & & & \alpha \end{bmatrix};$$

$$r=4 : \begin{bmatrix} \alpha & & & & \\ 1 & \alpha & & & \\ 1 & \alpha & \alpha & & \\ & 1 & \alpha & \alpha & \\ & & 1 & \alpha & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & & & \\ 1 & \alpha & & & \\ & 1 & \alpha & & \\ & & 1 & \alpha & \\ & & & 1 & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & & & \\ & \alpha & & & \\ & & \alpha & & \\ & & & \alpha & \\ & & & & \alpha \end{bmatrix},$$

$$\begin{bmatrix} \alpha & & & & \\ & 1 & \alpha & & \\ & & \alpha & & \\ & & & \alpha & \\ & & & & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & & & & \\ & \alpha & & & \\ & & \alpha & & \\ & & & \alpha & \\ & & & & \alpha \end{bmatrix}.$$

È possibile distinguere i vari casi calcolando gli autovettori di certi operatori collegati a  $T$ . Lo spazio delle soluzioni del sistema di equazioni:

$$(A - \alpha I)X = 0$$

è lo spazio degli autovettori di  $A$  con autovalore  $\alpha$  (incluso il vettore nullo). Dati  $A$  e  $\alpha$ , è possibile risolvere esplicitamente il sistema. Se  $r = 4$ , le dimensioni dello spazio delle soluzioni nei cinque casi sopra illustrati sono 1, 2, 2, 3, 4, rispettivamente, poiché a ciascun blocco è associato un solo autovettore (determinato a meno di una costante moltiplicativa). Pertanto tale dimensione contraddistingue i vari casi, ad eccezione del secondo e del terzo. È possibile distinguere questi due casi mediante la matrice  $(A - \alpha I)^2$ , che è la matrice nulla nel terzo caso ed è diversa dalla matrice nulla nel secondo caso.

Si può dimostrare che le dimensioni dei nuclei degli operatori  $(A - \alpha I)^\nu$ , con  $\nu = 1, 2, \dots, r - 1$ , permettono di distinguere le forme di Jordan in tutti i casi.

## 8 Moduli liberi su anelli di polinomi

Le strutture dei moduli su un anello diventano sempre più complicate col crescere della complessità dell'anello. È perfino difficile stabilire se un modulo presentato esplicitamente sia libero oppure no. In questo paragrafo descriveremo, senza dimostrazione, un teorema che caratterizza i moduli liberi sugli anelli di polinomi, dimostrato da Quillen e da Suslin nel 1976.

Sia  $R = \mathbb{C}[x_1, \dots, x_k]$  l'anello dei polinomi in  $k$  variabili, e sia  $V$  un  $R$ -modulo finitamente generato. Sceglimo una matrice di presentazione  $A$  per il modulo  $V$ . Gli elementi di  $A$  saranno polinomi  $a_{ij}(x)$ , e se  $A$  è una matrice  $m \times n$ , allora  $V$  è isomorfo al conucleo  $R^m / AR^n$  della moltiplicazione per  $A$  sugli  $R$ -vettori. Possiamo calcolare gli elementi  $a_{ij}(x)$  della matrice in ogni punto  $p = (p_1, \dots, p_k) \in \mathbb{C}^k$ , ottenendo una matrice complessa  $A(p)$ , il cui elemento di posto  $(i, j)$  è  $a_{ij}(p)$ .

(8.1) TEOREMA *Sia  $V$  un modulo finitamente generato sull'anello dei polinomi  $\mathbb{C}[x_1, \dots, x_k]$ , e sia  $A$  una matrice di presentazione  $m \times n$  per  $V$ . Denotiamo con  $A(p)$  la matrice ottenuta da  $A$  calcolando i suoi elementi in un punto  $p \in \mathbb{C}^k$ . Allora  $V$  è un modulo libero di rango  $r$  se e solo se la matrice  $A(p)$  ha rango  $m - r$  per ogni punto  $p$ . ■*

La dimostrazione di questo teorema richiede una preparazione che noi non abbiamo. Tuttavia, possiamo vedere facilmente come utilizzarlo per stabilire se un dato modulo è libero oppure no. Per esempio, consideriamo l'anello dei polinomi

in due variabili  $R = \mathbb{C}[x, y]$ , e sia  $V$  il modulo presentato dalla matrice  $4 \times 2$ :

$$(8.2) \quad A = \begin{bmatrix} 1 & x \\ y & x+3 \\ x & y \\ x^2 & y^2 \end{bmatrix}.$$

Pertanto  $V$  ha quattro generatori e due relazioni. Sia  $p$  un punto  $(a, b) \in \mathbb{C}^2$ . Le due colonne della matrice  $A(p)$  sono:

$$v_1 = (1, b, a, a^2)^t, \quad v_2 = (a, a+3, b, b^2)^t.$$

Non è difficile dimostrare che questi due vettori sono linearmente indipendenti per ogni scelta di  $a, b$ , da cui segue che il rango di  $A(p)$  è 2 per ogni punto  $(a, b)$ . Infatti, supponiamo che i vettori siano linearmente dipendenti, sicché  $v_2 = cv_1$  o viceversa. Allora, confrontando le prime coordinate, si ha che  $v_2 = av_1$ , da cui:

$$(8.3) \quad a + 3 = ab, \quad b = a^2, \quad b^2 = a^3$$

e queste equazioni non hanno soluzioni comuni. Allora, in base al teorema (8.1),  $V$  è un modulo libero di rango 2.

Possiamo capire intuitivamente questo teorema considerando lo spazio vettoriale  $V_p = \mathbb{C}^m / A(p)\mathbb{C}^n$  che è presentato dalla matrice complessa  $A(p)$ . Si può dimostrare che  $V_p$  è essenzialmente indipendente dalla scelta della matrice di presentazione. Pertanto possiamo utilizzare il modulo  $V$  per associare uno spazio vettoriale  $V_p$  ad ogni punto  $p \in \mathbb{C}^k$ . Se immaginiamo di far muovere il punto  $p$ , lo spazio vettoriale  $V_p$  varierà in modo continuo, purché la sua dimensione resti invariata. Ciò è vero poiché la matrice  $A(p)$  che presenta  $V_p$  dipende in modo continuo da  $p$ . Le famiglie di spazi vettoriali di dimensione costante, parametrizzate da uno spazio topologico, vengono chiamate *fibrati vettoriali*. Il modulo  $V$  è libero se e soltanto se la famiglia degli spazi vettoriali  $V_p$  forma un fibrato vettoriale.

Per una tipica deformazione professionale dei matematici, ho adottato un punto di vista troppo ristretto.  
Jean-Louis Verdier

### 1 Definizione di modulo

1. Sia  $R$  un anello, considerato come  $R$ -modulo. Determinare tutti gli omomorfismi di moduli  $\varphi : R \rightarrow R$ .
2. Sia  $W$  un sottomodulo di un  $R$ -modulo  $V$ . Dimostrare che l'opposto di un elemento di  $W$  sta in  $W$ .

3. Sia  $\varphi : V \rightarrow W$  un omomorfismo di moduli su un anello  $R$  e siano  $V', W'$  sottomoduli di  $V, W$  rispettivamente. Dimostrare che  $\varphi(V')$  è un sottomodulo di  $W$  e che  $\varphi^{-1}(W')$  è un sottomodulo di  $V$ .
4. (a) Sia  $V$  un gruppo abeliano. Dimostrare che se  $V$  ha una struttura di  $\mathbb{Q}$ -modulo, con l'addizione data dalla sua legge di composizione, allora tale struttura è univocamente determinata.  
 (b) Dimostrare che nessun gruppo abeliano finito ha una struttura di  $\mathbb{Q}$ -modulo.
5. Sia  $R = \mathbb{Z}[\alpha]$ , dove  $\alpha$  è un intero algebrico. Dimostrare che, per ogni intero  $m$ ,  $R/mR$  è finito, e determinare il suo ordine.
6. Un modulo si dice *semplice* se è diverso dal modulo nullo e se non contiene sottomoduli propri.  
 (a) Dimostrare che ogni modulo semplice è isomorfo a  $R/M$ , dove  $M$  è un ideale massimale.  
 (b) Dimostrare il *lemma di Schur*, il quale afferma che se  $\varphi : S \rightarrow S'$  è un omomorfismo di moduli semplici, allora o  $\varphi$  è l'omomorfismo nullo o è un isomorfismo.
7. L'annullatore di un  $R$ -modulo  $V$  è l'insieme  $I = \{r \in R \mid rV = 0\}$ .  
 (a) Dimostrare che  $I$  è un ideale di  $R$ .  
 (b) Determinare l'annullatore dei seguenti  $\mathbb{Z}$ -moduli:  

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4), \quad \mathbb{Z}.$$
8. Sia  $R$  un anello e sia  $V$  un  $R$ -modulo. Sia  $E$  l'insieme degli *endomorfismi* di  $V$ , ossia l'insieme degli omomorfismi da  $V$  a  $V$ . Dimostrare che  $E$  è un anello non commutativo, con l'addizione definita da  $[\varphi + \psi](m) = \varphi(m) + \psi(m)$ , e con la moltiplicazione data dalla composizione di funzioni.
9. Dimostrare che l'anello degli endomorfismi di un modulo semplice è un campo.
10. Determinare l'anello degli endomorfismi degli  $R$ -moduli:  
 (a)  $R$ ; (b)  $R/I$ , dove  $I$  è un ideale.
11. Siano  $W \subset V \subset U$  tre  $R$ -moduli.  
 (a) Descrivere degli omomorfismi naturali che collegano tra loro i tre moduli quoziante  $U/W$ ,  $U/V$  e  $V/W$ .  
 (b) Dimostrare il *terzo teorema di isomorfismo*:  

$$U/V \approx (U/W)/(V/W).$$
12. Siano  $V, W$  sottomoduli di un modulo  $U$ .  
 (a) Dimostrare che  $V \cap W$  e  $V + W$  sono sottomoduli di  $U$ .  
 (b) Dimostrare il *secondo teorema di isomorfismo*:  

$$(V + W)/W \approx V/(V \cap W).$$

13. Sia  $V$  un  $R$ -modulo, definito come in (1.1). Se l'anello  $R$  non è commutativo, non è una buona idea definire  $vr = rv$ . Spiegare perché.
- 2 Matrici, moduli liberi, basi
1. Sia  $R = \mathbb{C}[x, y]$  e sia  $M$  l'ideale di  $R$  generato dai due elementi  $x, y$ . È vero che  $M$  è un  $R$ -modulo libero?
2. Sia  $A$  una matrice  $n \times n$  a elementi in un anello  $R$ , sia  $\varphi : R^n \rightarrow R^n$  la moltiplicazione a sinistra per  $A$  e sia  $d = \det A$ . È vero che l'immagine di  $\varphi$  è uguale a  $dR^n$ ?
3. Sia  $I$  un ideale di un anello  $R$ . È vero che se  $R/I$  è un  $R$ -modulo libero allora  $I = 0$ ?
4. Sia  $R$  un anello e sia  $V$  un  $R$ -modulo libero di rango finito. Dimostrare o confutare ciascuna delle seguenti affermazioni:  
 (a) Ogni insieme di generatori contiene una base.  
 (b) Ogni insieme linearmente indipendente può essere esteso ad una base.
5. Sia  $I$  un ideale di un anello  $R$ . Dimostrare che  $I$  è un  $R$ -modulo libero se e soltanto se  $I$  è un ideale principale, generato da un elemento  $\alpha$  che non è un divisore dello zero in  $R$ .
6. Dimostrare che un anello  $R$  tale che ogni  $R$ -modulo finitamente generato sia libero o è un campo o è l'anello nullo.
7. Sia  $A$  la matrice di un omomorfismo  $\varphi : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$  tra moduli liberi.  
 (a) Dimostrare che  $\varphi$  è iniettivo se e solo se il rango di  $A$  è  $n$ .  
 (b) Dimostrare che  $\varphi$  è suriettivo se e solo se il massimo comune divisore dei determinanti dei minori  $m \times m$  di  $A$  è 1.
8. Conciliare la definizione di gruppo abeliano libero data nel paragrafo 2 con quella data nel cap. 6 (§ 8).
- 3 Il principio di permanenza delle identità
1. In ciascuno dei casi seguenti, stabilire se il principio di permanenza delle identità permette o no di estendere il risultato dal campo dei numeri complessi a un anello commutativo arbitrario:  
 (a) la proprietà associativa della moltiplicazione di matrici;  
 (b) il teorema di Cayley-Hamilton;  
 (c) la regola di Cramer;  
 (d) le regole per la derivazione del prodotto, del quoziante e della funzione composta per i polinomi;  
 (e) il fatto che un polinomio di grado  $n$  ha al più  $n$  radici;  
 (f) lo sviluppo di Taylor di un polinomio.

2. È vero che il principio di permanenza delle identità prova che  $\det AB = \det A \cdot \det B$ , nel caso in cui gli elementi delle matrici appartengono ad un anello  $R$  non commutativo?
3. In alcuni casi, può essere conveniente verificare un'identità soltanto per i numeri reali. È sufficiente?
4. Sia  $R$  un anello e sia  $A$  una matrice  $3 \times 3$  a elementi in  $R$  appartenente a  $SO(3)$ , ossia tale che  $A^t A = I$  e  $\det A = 1$ . È vero che il principio di permanenza delle identità prova che  $A$  ha un autovettore in  $R^3$  con autovalore 1?

#### 4 Diagonalizzazione delle matrici intere

1. Ridurre ciascuna delle matrici seguenti alla forma diagonale mediante operazioni intere sulle righe e sulle colonne:

$$(a) \begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}; \quad (b) \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}; \quad (c) \begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix}.$$

- (d) Nel primo caso, sia  $V = \mathbb{Z}^2$  e sia  $L = AV$ . Disegnare il sottoreticolo  $L$  e trovare basi di  $V$  e  $L$  che mostrano la diagonalizzazione.
2. Sia  $A$  una matrice i cui elementi appartengono all'anello dei polinomi  $F[t]$  e sia  $A'$  una matrice ottenuta da  $A$  mediante operazioni polinomiali sulle righe e sulle colonne. Mettere in relazione  $\det A$  con  $\det A'$ .
3. Determinare matrici intere  $P^{-1}, Q$  che diagonalizzano la matrice  $A = \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$ .

4. Siano  $d_1, d_2, \dots$  gli interi che compaiono nel teorema (4.3).
  - (a) Dimostrare che  $d_1$  è il massimo comune divisore degli elementi  $a_{ij}$  di  $A$ .
  - (b) Dimostrare che  $d_1 d_2$  è il massimo comune divisore dei determinanti dei minori  $2 \times 2$  di  $A$ .
  - (c) Enunciare e dimostrare un'estensione di (a) e (b) agli interi  $d_i$  per ogni  $i$ .

5. Determinare tutte le soluzioni intere del sistema di equazioni  $AX = 0$ , dove  $A = \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$ .

6. Trovare una base per i seguenti sottomoduli di  $\mathbb{Z}^3$ :
  - (a) il modulo generato da  $(1, 0, -1), (2, -3, 1), (0, 3, 1), (3, 1, 5)$ ;
  - (b) il modulo delle soluzioni del sistema di equazioni:  $x+2y+3z=0, x+4y+9z=0$ .
7. Dimostrare che le due matrici  $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$  e  $\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$  generano il gruppo  $SL_2(\mathbb{Z})$  delle matrici intere con determinante 1.
8. Dimostrare che il gruppo  $SL_n(\mathbb{Z})$  è generato dalle matrici elementari intere del primo tipo.

9. Siano  $\alpha, \beta, \gamma$  numeri complessi e sia  $A = \{\ell\alpha + m\beta + n\gamma \mid \ell, m, n \in \mathbb{Z}\}$  il sottogruppo di  $\mathbb{C}$  da essi generato. Sotto quali ipotesi  $A$  risulta un reticolo in  $\mathbb{C}$ ?
10. Sia  $\varphi : \mathbb{Z}^k \rightarrow \mathbb{Z}^k$  un omomorfismo dato dalla moltiplicazione per una matrice intera  $A$ . Dimostrare che l'immagine di  $\varphi$  è di indice finito se e soltanto se  $A$  è non singolare e che, in tal caso, l'indice è uguale a  $|\det A|$ .
11. (a) Sia  $A = (a_1, \dots, a_n)^t$  un vettore colonna a elementi interi. Utilizzare la riduzione per righe per dimostrare che esiste una matrice  $P \in GL_n(\mathbb{Z})$  tale che  $PA = (d, 0, \dots, 0)^t$ , dove  $d$  è il massimo comune divisore di  $a_1, \dots, a_n$ .
   
 (b) Dimostrare che, se  $d = 1$ , allora  $A$  è la prima colonna di una matrice  $M \in SL_n(\mathbb{Z})$ .

#### 5 Generatori e relazioni per i moduli

1. In ciascuno dei casi seguenti, determinare il gruppo abeliano avente la matrice di presentazione assegnata:

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 5 \end{bmatrix}, [2 \ 0 \ 0], \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 4 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 6 \\ 2 & 3 \end{bmatrix}.$$

2. Trovare un anello  $R$  e un ideale  $I$  di  $R$  che non sia finitamente generato.
3. Dimostrare che in un dominio di integrità noetheriano esiste una fattorizzazione in elementi irriducibili.
4. Sia  $V \subset \mathbb{C}^n$  il luogo degli zeri di un insieme infinito di polinomi  $f_1, f_2, f_3, \dots$ . Dimostrare che esiste un numero finito di questi polinomi, i cui zeri definiscono lo stesso luogo.
5. Sia  $S$  un sottoinsieme di  $\mathbb{C}^n$ . Dimostrare che esiste un insieme finito di polinomi  $(f_1, \dots, f_k)$  tale che ogni polinomio che si annulla identicamente su  $S$  è una combinazione lineare di tale insieme, con coefficienti polinomiali.
6. Determinare una matrice di presentazione per l'ideale  $(2, 1+\delta)$  di  $\mathbb{Z}[\delta]$ , dove  $\delta = \sqrt{-5}$ .
- \*7. Sia  $S$  un sottoanello dell'anello  $R = \mathbb{C}[t]$  contenente  $\mathbb{C}$  e diverso da  $\mathbb{C}$ . Dimostrare che  $R$  è un  $S$ -modulo finitamente generato.
8. Sia  $A$  la matrice di presentazione di un modulo  $V$  rispetto a un insieme di generatori  $(v_1, \dots, v_m)$ . Sia  $(w_1, \dots, w_r)$  un altro insieme di elementi di  $V$ , e scriviamo gli elementi per mezzo dei generatori, diciamo  $w_i = \sum p_{ij} v_j$ , con  $p_{ij} \in R$ . Poniamo  $P = (p_{ij})$ . Dimostrare che la matrice a blocchi

$$\left[ \begin{array}{c|c} A & -P \\ \hline 0 & I \end{array} \right]$$

è una matrice di presentazione per  $V$  rispetto all'insieme di generatori  $(v_1, \dots, v_m; w_1, \dots, w_r)$ .

- \*9. Con le notazioni del problema precedente, supponiamo che  $(w_1, \dots, w_r)$  sia anche un insieme di generatori di  $V$  e che  $B$  sia una matrice di presentazione per  $V$  rispetto a tale insieme di generatori. Inoltre, sia  $v_i = \sum q_{ij} w_j$  un'espressione dei generatori  $v_i$  per mezzo dei generatori  $w_j$ .

(a) Dimostrare che la matrice a blocchi

$$M = \left[ \begin{array}{c|c|c|c} A & -P & I & 0 \\ \hline 0 & I & -Q & B \end{array} \right]$$

presenta  $V$  rispetto ai generatori  $(v_1, \dots, v_m; w_1, \dots, w_r)$ .

(b) Dimostrare che  $M$  può essere ridotta ad  $A$  e a  $B$ , mediante una successione di operazioni della forma (5.12).

10. Utilizzando il problema 9, dimostrare che ogni matrice di presentazione di un modulo può essere trasformata in un'altra matrice di presentazione arbitraria mediante una successione di operazioni (5.12) e loro inverse.

## 6 Il teorema di struttura per i gruppi abeliani

1. Trovare una somma diretta di gruppi ciclici che sia isomorfa al gruppo abeliano

presentato dalla matrice  $\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}$ .

2. Scrivere il gruppo generato da  $x, y$ , con la relazione  $3x + 4y = 0$ , come una somma diretta di gruppi ciclici.

3. In ciascuno dei casi seguenti, trovare un prodotto diretto di gruppi ciclici isomorfo al gruppo abeliano  $V$  generato da  $x, y, z$ , con le relazioni assegnate:

- (a)  $3x + 2y + 8z = 0, 2x + 4z = 0$ ;
- (b)  $x + y = 0, 2x = 0, 4x + 2z = 0, 4x + 2y + 2z = 0$ ;
- (c)  $2x + y = 0, x - y + 3z = 0$ ;
- (d)  $2x - 4y = 0, 2x + 2y + z = 0$ ;
- (e)  $7x + 5y + 2z = 0, 3x + 3y = 0, 13x + 11y + 2z = 0$ .

4. Determinare il numero delle classi di isomorfismo dei gruppi abeliani di ordine 400.

5. Classificare i moduli finitamente generati su ciascuno dei seguenti anelli:

- (a)  $\mathbb{Z}/(4)$ ; (b)  $\mathbb{Z}/(6)$ ; (c)  $\mathbb{Z}/n\mathbb{Z}$ .

6. Sia  $R$  un anello e sia  $V$  un  $R$ -modulo presentato da una matrice diagonale  $A$  di dimensione  $m \times n$ :  $V \approx R^m / AR^n$ . Siano  $(v_1, \dots, v_m)$  i generatori corrispondenti di  $V$  e siano  $d_i$  gli elementi diagonali di  $A$ . Dimostrare che  $V$  è isomorfo a un prodotto diretto dei moduli  $R/(d_i)$ .

7. Sia  $V$  lo  $\mathbb{Z}[i]$ -modulo generato da due elementi  $v_1, v_2$ , con le relazioni  $(1+i)v_1 + (2-i)v_2 = 0, 3v_1 + 5iv_2 = 0$ . Scrivere questo modulo come somma diretta di moduli ciclici.

3. Siano  $W_1, \dots, W_k$  sottomoduli di un  $R$ -modulo  $V$  tali che  $V = \sum W_i$ . Supponiamo che  $W_1 \cap W_2 = 0, (W_1 + W_2) \cap W_3 = 0, \dots, (W_1 + W_2 + \dots + W_{k-1}) \cap W_k = 0$ . Dimostrare che  $V$  è la somma diretta dei moduli  $W_1, \dots, W_k$ .

9. Dimostrare i seguenti risultati:

- (a) Il numero degli elementi di  $\mathbb{Z}/(p^\nu)$  il cui ordine divide  $p^\nu$  è  $p^\nu$  se  $\nu \leq e$ , ed è  $p^e$  se  $\nu \geq e$ .

- (b) Siano  $W_1, \dots, W_k$  gruppi abeliani finiti, e sia  $u_j$  il numero degli elementi di  $W_j$ , il cui ordine divide un dato intero  $q$ . Allora il numero degli elementi del gruppo prodotto  $V = W_1 \times \dots \times W_k$  il cui ordine divide  $q$  è il prodotto  $u_1 \cdots u_k$ .

- (c) Con le notazioni precedenti, supponiamo che  $W_j$  sia un gruppo ciclico avente come ordine la potenza di un numero primo, diciamo  $d_j = p^{e_j}$ . Sia  $r_1$  il numero dei  $d_j$  uguali a un primo  $p$  assegnato, sia  $r_2$  il numero dei  $d_j$  uguali a  $p^2$ , e così via. Allora il numero degli elementi di  $V$  il cui ordine divide  $p^\nu$  è  $p^{s\nu}$ , dove  $s_1 = r_1 + \dots + r_k, s_2 = r_1 + 2r_2 + \dots + 2r_k, s_3 = r_1 + 2r_2 + 3r_3 + \dots + 3r_k$ , e così via.

- (d) Il teorema (6.9).

## 7 Applicazione agli operatori lineari

1. Sia  $T$  un operatore lineare la cui matrice è  $\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$ . È vero che il  $\mathbb{C}[t]$ -modulo corrispondente è ciclico?

2. Determinare la forma di Jordan della matrice  $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ .

3. Dimostrare che la matrice  $\begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{bmatrix}$  è idempotente, e trovare la sua forma di Jordan.

4. Sia  $V$  uno spazio vettoriale complesso di dimensione 5, e sia  $T$  un operatore lineare su  $V$  avente polinomio caratteristico  $(t - \alpha)^5$ . Supponiamo che il rango dell'operatore  $T - \alpha I$  sia 2. Quali sono le possibili forme di Jordan per  $T$ ?

5. Trovare tutte le possibili forme di Jordan per una matrice il cui polinomio caratteristico è  $(t+2)^2(t-5)^3$ .

6. Qual è la forma di Jordan di una matrice il cui polinomio caratteristico è  $(t-2)^2(t-5)^3$  e tale che lo spazio degli autovettori con autovalore 2 ha dimensione 1, mentre lo spazio degli autovettori con autovalore 5 ha dimensione 2?

7. (a) Dimostrare che un blocco di Jordan ha uno spazio di autovettori di dimensione 1.

- (b) Viceversa, dimostrare che se gli autovettori di una matrice complessa  $A$  sono multipli di uno stesso vettore la forma di Jordan di  $A$  è costituita da un solo blocco.

8. Determinare tutti i sottospazi invarianti di un operatore lineare la cui forma di Jordan è costituita da un solo blocco.
9. In ciascuno dei casi seguenti, risolvere l'equazione differenziale  $dX/dt = AX$ , dove  $A$  è un blocco di Jordan della forma:
- (a)  $\begin{bmatrix} 2 & \\ 1 & 2 \end{bmatrix}$ ; (b)  $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ ; (c)  $\begin{bmatrix} 1 & \\ 1 & 1 \\ & 1 \end{bmatrix}$ .
10. Risolvere l'equazione differenziale  $dX/dt = AX$ , quando  $A$  è
- (a) la matrice (7.14); (b) la matrice (7.10);  
 (c) la matrice dell'esercizio 2; (d) la matrice dell'esercizio 3.
11. È vero che due matrici  $n \times n$  complesse  $A, B$  sono simili se e solo se hanno la stessa forma di Jordan?
12. Dimostrare che ogni matrice  $n \times n$  complessa è simile a una matrice della forma  $D + N$ , dove  $D$  è diagonale,  $N$  è nilpotente, e  $DN = ND$ .
13. Sia  $R = F[x]$  l'anello dei polinomi in una variabile su un campo  $F$ , e sia  $V$  l' $R$ -modulo generato da un elemento  $v$  che soddisfa la relazione  $(x^3 + 3x + 2)v = 0$ . Scegliere una base di  $V$  come  $F$ -spazio vettoriale, e trovare rispetto a questa base la matrice dell'operatore dato dalla moltiplicazione per  $t$ .
14. Sia  $V$  un  $F[t]$ -modulo, sia  $\mathbf{B} = (v_1, \dots, v_n)$  una base di  $V$  come  $F$ -spazio vettoriale, e sia  $B$  la matrice di  $T$  rispetto a questa base. Dimostrare che  $A = tI - B$  è una matrice di presentazione per il modulo.
15. Sia  $p(t)$  un polinomio monico a coefficienti in un campo  $F$ . Dimostrare che esiste una matrice  $n \times n$  a elementi in  $F$  il cui polinomio caratteristico è  $p(t)$ .
16. È vero che una matrice complessa  $A$  tale che  $A^2 = A$  è diagonalizzabile?
17. Sia  $A$  una matrice  $n \times n$  complessa tale che  $A^k = I$  per qualche intero  $k$ . Dimostrare che la forma di Jordan di  $A$  è diagonale.
18. Dimostrare il teorema di Cayley-Hamilton: se  $p(t)$  è il polinomio caratteristico di una matrice  $A$  di tipo  $n \times n$ , allora  $p(A) = 0$ .
19. Il polinomio minimo  $m(t)$  di un operatore lineare  $T$  su uno spazio vettoriale complesso  $V$  è il polinomio monico di grado minimo tale che  $m(T) = 0$ .
- (a) Dimostrare che il polinomio minimo divide il polinomio caratteristico.  
 (b) Dimostrare che ogni radice del polinomio caratteristico  $p(t)$  è anche una radice del polinomio minimo  $m(t)$ .  
 (c) Dimostrare che  $T$  è diagonalizzabile se e soltanto se  $m(t)$  non ha radici multiple.
20. Trovare tutte le possibili forme di Jordan per le matrici  $8 \times 8$  il cui polinomio minimo è  $x^2(x-1)^3$ .
21. È vero che una matrice complessa  $A$  è simile alla propria trasposta?
22. Classificare gli operatori lineari su un  $F[t]$ -modulo finitamente generato, senza l'ipotesi che il modulo sia uno spazio vettoriale di dimensione finita.

23. Dimostrare che i ranghi delle matrici  $(A - \alpha I)^{\nu}$  permettono di distinguere tutte le forme di Jordan, e quindi che la forma di Jordan dipende soltanto dall'operatore e non dalla base.
24. Dimostrare che i seguenti concetti sono equivalenti tra loro:
- (i)  $R$ -modulo, con  $R = \mathbb{Z}[i]$ ;  
 (ii) gruppo abeliano  $V$  con un omomorfismo  $\varphi : V \rightarrow V$  tale che  $\varphi \circ \varphi = -\text{identità}$ .
25. Sia  $F = \mathbb{F}_p$ . Per quali primi  $p$  il gruppo additivo  $F^1$  ha una struttura di  $\mathbb{Z}[i]$ -modulo? Cosa si può dire per  $F^2$ ?
26. Classificare i moduli finitamente generati sull'anello  $\mathbb{C}[\epsilon]$ , dove  $\epsilon^2 = 0$ .
- ### 8 Moduli liberi su anelli di polinomi
1. Stabilire se i moduli su  $\mathbb{C}[x, y]$  presentati dalle seguenti matrici sono liberi oppure no:
- (a)  $\begin{bmatrix} x^2 + 1 & x \\ x^2y + x + y & xy + 1 \end{bmatrix}$ ; (b)  $\begin{bmatrix} xy - 1 \\ x^2 - y^2 \\ y \end{bmatrix}$ ; (c)  $\begin{bmatrix} x - 1 & x \\ y & y + 1 \\ x & y \\ x^2 & 2y \end{bmatrix}$ .
2. Dimostrare che il modulo presentato da (8.2) è libero descrivendo una sua base.
3. Seguendo il modello dell'anello dei polinomi in una variabile, descrivere i moduli sull'anello  $\mathbb{C}[x, y]$  per mezzo di spazi vettoriali reali con una struttura aggiuntiva.
4. Sia  $R$  un anello e sia  $V$  un  $R$ -modulo. Sia  $I$  un ideale di  $R$ , e sia  $IV$  l'insieme delle somme finite  $\sum s_i v_i$ , dove  $s_i \in I$  e  $v_i \in V$ .
- (a) Mostrare in che modo  $V/IV$  risulta un  $R/I$ -modulo.  
 (b) Sia  $A$  una matrice di presentazione per  $V$  e si denoti con  $\bar{A}$  la sua "classe resto" in  $R/I$ . Dimostrare che  $\bar{A}$  è una matrice di presentazione per  $V/IV$ .  
 (c) Spiegare perché il modulo  $V_p$  definito nel testo è essenzialmente indipendente dalla matrice di presentazione.
- \*5. Utilizzando l'esercizio 9 del paragrafo 5, dimostrare la parte facile del teorema di Quillen e Suslin, ossia che se  $V$  è libero il rango di  $A(p)$  è costante.
6. Sia  $R = \mathbb{Z}[\sqrt{-5}]$ , e sia  $V$  il modulo presentato dalla matrice  $A = \begin{bmatrix} 2 \\ 1 + \delta \end{bmatrix}$ .
- (a) Dimostrare che la classe resto di  $A$  ha rango 1, per ogni ideale primo  $P$  di  $R$ .  
 (b) Dimostrare che  $V$  non è libero.
- ### Esercizi vari
1. Sia  $G$  un gruppo cristallografico piano, e  $g$  una rotazione in  $G$ ; sia  $\bar{g}$  l'elemento associato del gruppo puntuale  $\bar{G}$ . Dimostrare che esiste una base di  $\mathbb{R}^2$ , non neces-

sariamente ortonormale, tale che la matrice di  $\bar{g}$  rispetto a questa base appartiene a  $GL_2(\mathbb{Z})$ .

- \*2. (a) Sia  $\alpha$  un numero complesso, e  $\mathbb{Z}[\alpha]$  il sottoanello di  $\mathbb{C}$  generato da  $\alpha$ . Dimostrare che  $\alpha$  è un intero algebrico se e solo se  $\mathbb{Z}[\alpha]$  è un gruppo abeliano finitamente generato.

(b) Dimostrare che, se  $\alpha, \beta$  sono interi algebrici, il sottoanello  $\mathbb{Z}[\alpha, \beta]$  di  $\mathbb{C}$  che essi generano è un gruppo abeliano finitamente generato.

(c) Dimostrare che gli interi algebrici formano un sottoanello di  $\mathbb{C}$ .

- \*3. (*Teorema di Pick*) Sia  $\Delta$  la regione del piano limitata da un poligono i cui vertici sono punti del reticolo intero. Sia  $I$  l'insieme dei punti del reticolo interni a  $\Delta$  e  $B$  l'insieme dei punti del reticolo sul bordo di  $\Delta$ . Se  $p$  è un punto del reticolo, denotiamo con  $r(p)$  la frazione di  $2\pi$  che corrisponde all'angolo sotteso da  $\Delta$  in  $p$ . Pertanto  $r(p)=0$  se  $p \notin \Delta$ ,  $r(p)=1$  se  $p$  è un punto interno a  $\Delta$ ,  $r(p)=\frac{1}{2}$  se  $p$  sta su un lato, e così via.

(a) Dimostrare che l'area di  $\Delta$  è  $\sum_p r(p)$ .

(b) Dimostrare che se il bordo di  $\Delta$  è costituito da una sola curva connessa l'area di  $\Delta$  è uguale a  $|I| + \frac{1}{2}(|B| - 2)$ .

4. Dimostrare che il gruppo ortogonale intero  $O_n(\mathbb{Z})$  è un gruppo finito.

- \*5. Consideriamo il prodotto scalare ordinario  $(v \cdot w) = v^t w$  sullo spazio  $V = \mathbb{R}^k$  dei vettori colonna. Sia  $L$  un reticolo in  $V$ , e definiamo  $L^* = \{w \mid (v \cdot w) \in \mathbb{Z} \text{ per ogni } v \in L\}$ .

(a) Dimostrare che  $L^*$  è un reticolo.

(b) Sia  $\mathbf{B} = (v_1, \dots, v_k)$  una base di reticolo per  $L$ , e sia  $P = [\mathbf{B}]^{-1}$  la matrice che collega questa base di  $V$  con la base canonica  $\mathbf{E}$ . Qual è la matrice  $A$  del prodotto scalare rispetto alla base  $\mathbf{B}$ ?

(c) Dimostrare che le colonne di  $P$  formano una base di reticolo per  $L^*$ .

(d) Dimostrare che se  $A$  è una matrice intera  $L \subset L^*$  e  $[L^* : L] = |\det A|$ .

6. Sia  $V$  uno spazio vettoriale reale avente una base infinita numerabile  $\{v_1, v_2, v_3, \dots\}$ , e sia  $E$  l'anello degli operatori lineari su  $V$ .

(a) Quali matrici infinite rappresentano gli operatori lineari su  $V$ ?

(b) Descrivere in che modo si può calcolare la matrice della composizione di due operatori lineari per mezzo delle matrici dei due operatori.

(c) Consideriamo gli operatori lineari  $T, T'$  definiti mediante le leggi:

$$T(v_{2n}) = v_n, \quad T(v_{2n-1}) = 0, \quad T'(v_{2n}) = 0, \quad T'(v_{2n-1}) = v_n,$$

per  $n = 1, 2, 3, \dots$ . Scrivere esplicitamente le loro matrici.

- (d) Possiamo considerare  $E^1 = E$  come un modulo sull'anello  $E$ , con la moltiplicazione per uno scalare a sinistra di un vettore. Dimostrare che  $\{T, T'\}$  è una base di  $E^1$  come  $E$ -modulo.

- (e) Dimostrare che gli  $E$ -moduli liberi  $E^k$ , con  $k = 1, 2, 3, \dots$ , sono tutti isomorfi tra loro.

7. Dimostrare che il gruppo  $\mathbb{Q}(+)/\mathbb{Z}(+)$  non è una somma diretta infinita di gruppi ciclici.

8. Dimostrare che il gruppo additivo  $\mathbb{Q}(+)$  dei numeri razionali non è una somma diretta di due sottogruppi propri.

9. Dimostrare che il gruppo moltiplicativo  $\mathbb{Q}^*(\cdot)$  dei numeri razionali è isomorfo alla somma diretta di un gruppo ciclico di ordine 2 e di un gruppo abeliano libero con un insieme numerabile di generatori.

10. Dimostrare che due matrici diagonalizzabili  $A, B$  sono simultaneamente diagonalizzabili, ossia esiste una matrice invertibile  $P$  tale che  $PAP^{-1}$  e  $PBP^{-1}$  sono entrambe diagonali, se e soltanto se  $AB = BA$ .

- \*11. Sia  $A$  un gruppo abeliano finito, e sia  $\varphi : A \rightarrow \mathbb{C}^*$  un omomorfismo diverso dall'omomorfismo banale ( $\varphi(x) = 1$  per ogni  $x$ ). Dimostrare che  $\sum_{a \in A} \varphi(a) = 0$ .

12. Sia  $A$  una matrice  $m \times n$  ad elementi in un anello  $R$ , e sia  $\varphi : R^n \rightarrow R^m$  la moltiplicazione a sinistra per  $A$ . Dimostrare che le seguenti condizioni sono equivalenti:

(i) l'applicazione  $\varphi$  è suriettiva;

(ii) i determinanti dei minori  $m \times m$  di  $A$  generano l'ideale unità;

(iii)  $A$  ha un'inversa destra, ossia una matrice  $B$  ad elementi in  $R$  tale che  $AB = I$ .

- \*13. Siano  $(v_1, \dots, v_m)$  generatori di un  $R$ -modulo  $V$ , e sia  $J$  un ideale di  $R$ . Definiamo  $JV$  come l'insieme di tutte le somme finite di prodotti  $av$ , con  $a \in J$  e  $v \in V$ .

- (a) Dimostrare che se  $JV = V$  esiste una matrice  $A$  di tipo  $m \times m$  a elementi in  $J$  tale che  $(v_1, \dots, v_m)(I - A) = 0$ .

- (b) Con le notazioni usate in (a), dimostrare che  $\det(I - A) = 1 + \alpha$ , dove  $\alpha \in J$ , e che  $\det(I - A)$  annulla  $V$ .

- (c) Un  $R$ -modulo  $V$  si dice *fedele* se  $rV = 0$  con  $r \in R$  implica  $r = 0$ . Dimostrare il *lemma di Nakayama*: Sia  $V$  un  $R$ -modulo fedele, finitamente generato e sia  $J$  un ideale di  $R$ . Se  $JV = V$ , allora  $J = R$ .

- (d) Sia  $V$  un  $R$ -modulo finitamente generato. Dimostrare che se  $MV = V$  per ogni ideale massimale  $M$ , allora  $V = 0$ .

- \*14. Possiamo usare una coppia  $x(t), y(t)$  di polinomi a coefficienti complessi in  $t$ , per definire un cammino complesso in  $\mathbb{C}^2$ , mandando  $t$  in  $(x(t), y(t))$ . Essi definiscono anche un omomorfismo  $\varphi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$ , dato da  $f(x, y) \mapsto f(x(t), y(t))$ . Questo esercizio analizza la relazione tra il cammino e l'omomorfismo. Escludiamo il caso banale che  $x(t)$  e  $y(t)$  siano entrambi costanti.

- (a) Denotiamo con  $S$  l'immagine di  $\varphi$ . Dimostrare che  $S$  è isomorfo al quoziente  $\mathbb{C}[x, y]/(f)$ , dove  $f(x, y)$  è un polinomio irriducibile.

- (b) Dimostrare che  $t$  è la radice di un polinomio monico a coefficienti in  $S$ .

- (c) Denotiamo con  $V$  la varietà degli zeri di  $f$  in  $\mathbb{C}^2$ . Dimostrare che per ogni punto  $(x_0, y_0) \in V$  esiste un elemento  $t_0 \in S$  tale che  $(x_0, y_0) = (x(t_0), y(t_0))$ .

## Capitolo 13

### Campi

La nostra difficoltà non è nelle dimostrazioni, ma nel capire che cosa dimostrare.

Emil Artin

### 1 Esempi di campi

La teoria dei campi, in gran parte, riguarda lo studio di coppie di campi contenuti l'uno nell'altro, diciamo  $F \subset K$ . A differenza della teoria dei gruppi, in cui l'attenzione è rivolta ai sottogruppi, cioè alla struttura interna del gruppo, nella teoria dei campi si studiano le estensioni di un dato campo, cioè, in qualche modo, la sua struttura "esterna". Un'estensione di campi di  $F$  è, per definizione, un campo che contiene  $F$  come sottocampo.

Vediamo subito le tre classi più importanti di campi.

(1.1) *Un campo di numeri è un sottocampo di  $\mathbb{C}$ .*

Ogni sottocampo di  $\mathbb{C}$  contiene 1, e quindi contiene il campo  $\mathbb{Q}$  dei numeri razionali. Pertanto un campo di numeri è un'estensione di  $\mathbb{Q}$ . I campi di numeri più comunemente studiati sono i campi di numeri *algebrici*, i cui elementi sono tutti numeri algebrici (cfr. cap. 10, §1). Abbiamo studiato i campi di numeri quadratici nel capitolo 11.

(1.2) *Un campo avente un numero finito di elementi è chiamato campo finito.*

Se  $K$  è un campo finito, il nucleo dell'unico omomorfismo  $\varphi : \mathbb{Z} \rightarrow K$  è un ideale primo [cap. 11 (8.6)], e poiché  $\mathbb{Z}$  è infinito mentre  $K$  è finito, il nucleo di  $\varphi$  è diverso da zero. Pertanto esso è generato da un numero primo  $p$ . L'immagine di  $\varphi$  è isomorfa al quoziante  $\mathbb{Z}/(p) = \mathbb{F}_p$ . Il campo  $K$  contiene dunque un sottocampo isomorfo al campo primo  $\mathbb{F}_p$ , e pertanto può essere considerato come una sua estensione. Descriveremo tutti i campi finiti nel paragrafo 6.

(1.3) *Talune estensioni del campo delle funzioni razionali  $F = \mathbb{C}(x)$  sono definite campi di funzioni.*

I campi di funzioni svolgono un ruolo importante nella teoria delle funzioni analitiche e in geometria algebrica. Non avendoli mai incontrati prima d'ora, li descriveremo brevemente. Un campo di funzioni può essere definito da un polinomio irriducibile in due variabili, diciamo  $f(x, y) \in \mathbb{C}[x, y]$ . Un buon esempio è il polinomio  $f(x, y) = y^2 - x^3 + x$ . Dato un polinomio di questo tipo, possiamo studiare l'equazione

$$(1.4) \quad f(x, y) = 0$$

analiticamente, utilizzando la (1.4) per definire  $y$  "implicitamente" come una funzione  $y(x)$  di  $x$ , come abbiamo imparato a fare in analisi. Nel nostro esempio, la funzione così definita è  $y = \sqrt{x^3 - x}$ . Essa non è univoca, essendo determinata soltanto a meno del segno (ma ciò non rappresenta una seria difficoltà). Non avremo, in generale, un'espressione esplicita per una funzione definita implicitamente; tuttavia, per definizione, essa soddisfa l'equazione (1.4), ossia:

$$(1.5) \quad f(x, y(x)) = 0.$$

D'altra parte, l'equazione può essere studiata anche algebricamente. Interpretiamo  $f(x, y)$  come un polinomio in  $y$  i cui coefficienti sono polinomi in  $x$ . Indichiamo con  $F$  il campo  $\mathbb{C}(x)$  delle funzioni razionali in  $x$ . Se  $f$  non è un polinomio nella sola  $x$ , allora, essendo irriducibile in  $\mathbb{C}[x, y]$ , sarà un elemento irriducibile di  $F[y]$  [cfr. cap. 11 (3.9)]. Pertanto l'ideale generato da  $f$  in  $F[y]$  è massimale [cap. 11 (1.6)], e il campo  $F[y]/(f) = K$  è un'estensione di  $F$ .

L'analisi e l'algebra sono collegate, poiché sia la funzione  $y(x)$  definita implicitamente che la classe resto  $\bar{y}$  di  $y$  in  $F[y]/(f)$  soddisfano l'equazione  $f(x, y) = 0$ . In tal modo la classe resto di  $y$ , e in realtà tutti gli elementi di  $K$ , possono essere interpretati come funzioni della variabile  $x$ . Per questo motivo, tali campi sono chiamati campi di funzioni. Studieremo i campi di funzioni nel paragrafo 7.

### 2 Elementi algebrici e trascendenti

Sia  $K$  un'estensione di un campo  $F$  e sia  $\alpha$  un elemento di  $K$ . In analogia con la definizione di numero algebrico (cap. 10, §1),  $\alpha$  si dice *algebrico su  $F$*  se è radice di un polinomio non nullo a coefficienti in  $F$ . Poiché i coefficienti appartengono a un campo, possiamo supporre che il polinomio sia monico, ad esempio della forma

$$(2.1) \quad x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad \text{con } a_i \in F.$$

Un elemento  $\alpha$  si dice *trascendente su  $F$*  se non è algebrico su  $F$ , ossia se non è radice di alcun polinomio di questo tipo.

Si noti che le due proprietà, di algebricità e di trascendenza, dipendono dal campo  $F$  assegnato. Per esempio, il numero complesso  $2\pi i$  è algebrico su  $\mathbb{R}$  ma

è trascendente su  $\mathbb{Q}$ . Inoltre ogni elemento  $\alpha$  di un campo  $K$  è algebrico su  $K$ , poiché è radice del polinomio  $x - \alpha$ , il quale ha i coefficienti in  $K$ .

Le due possibilità per  $\alpha$  possono essere descritte per mezzo dell'omomorfismo di sostituzione:

$$(2.2) \quad \varphi : F[x] \rightarrow K, \quad \text{che manda } f(x) \text{ in } f(\alpha).$$

L'elemento  $\alpha$  è trascendente su  $F$  se  $\varphi$  è iniettivo, ed è algebrico su  $F$  se  $\varphi$  non è iniettivo, ossia se il nucleo di  $\varphi$  è diverso da zero.

Supponiamo che  $\alpha$  sia algebrico su  $F$ . Poiché  $F[x]$  è un dominio a ideali principali,  $\ker \varphi$  è generato da un solo elemento  $f(x)$ , precisamente, il polinomio monico di grado minimo avente  $\alpha$  come radice. Poiché  $K$  è un campo, sappiamo che  $f(x)$  deve essere un polinomio irriducibile [cap. 11 (8.6)], e infatti esso sarà l'unico polinomio monico irriducibile nell'ideale. Ogni altro elemento dell'ideale è un multiplo di  $f(x)$ . Chiameremo questo polinomio  $f$  il *polinomio minimo di  $\alpha$  su  $F$* .

È importante osservare che questo polinomio irriducibile  $f$  dipende sia da  $F$  che da  $\alpha$ , poiché l'irriducibilità di un polinomio dipende dal campo. Per esempio, sia  $F = \mathbb{Q}[i]$  e sia  $\alpha$  il numero complesso  $\sqrt{i} = \frac{1}{2}\sqrt{2}(1+i)$ . Il polinomio minimo di  $\alpha$  su  $\mathbb{Q}$  è  $x^4 + 1$ , ma questo polinomio si fattorizza nel campo  $F$ :  $x^4 + 1 = (x^2 + i)(x^2 - i)$ . Il polinomio minimo di  $\alpha$  su  $F$  è  $x^2 - i$ . Quando vi sono diversi campi, dobbiamo stare attenti a specificare il campo al quale ci riferiamo. Dire che un polinomio è irriducibile è ambiguo. È meglio dire che  $f$  è *irriducibile su  $F$* , ovvero che è un *elemento irriducibile di  $F[x]$* .

Data un'estensione  $K$  di  $F$ , l'estensione di  $F$  generata da un elemento  $\alpha \in K$  sarà indicata con  $F(\alpha)$ :

$$(2.3) \quad F(\alpha) \text{ è il più piccolo campo che contiene sia } F \text{ che } \alpha.$$

Più in generale, se  $\alpha_1, \dots, \alpha_n$  sono elementi di un'estensione di campi  $K$  di  $F$ , denoteremo con  $F(\alpha_1, \dots, \alpha_n)$  il più piccolo sottocampo di  $K$  che contiene  $F$  e  $\alpha_1, \dots, \alpha_n$ .

Come nel capitolo 10, denotiamo l'*anello* generato da  $\alpha$  su  $F$  con  $F[\alpha]$ . Esso è costituito da tutti gli elementi di  $K$  che possono essere scritti come polinomi in  $\alpha$  a coefficienti in  $F$ :

$$(2.4) \quad F[\alpha] = \{a_n\alpha^n + \dots + a_1\alpha + a_0 \mid a_i \in F\}.$$

Il campo  $F(\alpha)$  è isomorfo al campo delle frazioni di  $F[\alpha]$ . I suoi elementi sono quozienti di elementi di  $F[\alpha]$  [cfr. cap. 10 (6.7)].

(2.5) PROPOSIZIONE *Se  $\alpha$  è trascendente su  $F$ , allora l'omomorfismo di sostituzione  $F[x] \rightarrow F[\alpha]$  è un isomorfismo, e quindi  $F(\alpha)$  è isomorfo al campo  $F(x)$  delle funzioni razionali.* ■

Da questo semplice fatto segue che le estensioni di campi  $F(\alpha)$  sono isomorfe tra loro per tutti gli elementi trascendenti  $\alpha$ , essendo isomorfe al campo delle funzioni razionali  $F(x)$ . Per esempio,  $\pi$  ed  $e$  sono entrambi trascendenti su  $\mathbb{Q}$  (sebbene non l'abbiamo dimostrato) e quindi  $\mathbb{Q}(\pi)$  e  $\mathbb{Q}(e)$  sono campi isomorfi, mediante l'isomorfismo che porta  $\pi$  in  $e$ . Ciò è abbastanza sorprendente, a prima vista. L'isomorfismo non è continuo, quando i campi in questione sono considerati come sottocampi del campo dei numeri reali.

La situazione è completamente diversa se  $\alpha$  è algebrico:

### (2.6) PROPOSIZIONE

- (a) *Supponiamo che  $\alpha$  sia algebrico su  $F$ , e sia  $f(x)$  il suo polinomio minimo. Allora l'omomorfismo  $F[x]/(f) \rightarrow F[\alpha]$  è un isomorfismo e  $F[\alpha]$  è un campo. Dunque  $F[\alpha] = F(\alpha)$ .*
- (b) *Più in generale, siano  $\alpha_1, \dots, \alpha_n$  elementi algebrici di un'estensione di campi  $K$  di  $F$ . Allora si ha:  $F[\alpha_1, \dots, \alpha_n] = F(\alpha_1, \dots, \alpha_n)$ .*

*Dimostrazione.* Sia  $\varphi$  l'omomorfismo (2.2), con  $K = F(\alpha)$ . Poiché  $f(x)$  genera  $\ker \varphi$ , sappiamo che  $F[x]/(f)$  è isomorfo all'immagine di  $\varphi$  [cap. 10 (3.1)], ossia a  $F[\alpha]$ . Poiché  $f$  è irriducibile, esso genera un ideale massimale [cap. 11 (1.6)], quindi  $F[\alpha]$  è un campo. Poiché  $F(\alpha)$  è isomorfo al campo delle frazioni di  $F[\alpha]$ , esso è uguale a  $F[\alpha]$ . La dimostrazione della parte (b) è lasciata come esercizio. ■

(2.7) PROPOSIZIONE *Sia  $\alpha$  un elemento algebrico su  $F$  e sia  $f(x)$  il suo polinomio minimo. Supponiamo che  $f(x)$  abbia grado  $n$ . Allora  $(1, \alpha, \dots, \alpha^{n-1})$  è una base per  $F[\alpha]$  come spazio vettoriale su  $F$ .*

*Dimostrazione.* Questo risultato è un caso speciale della proposizione (5.7) del capitolo 10. ■

In generale, non è facile stabilire se due elementi algebrici  $\alpha, \beta$  generano campi isomorfi, sebbene la proposizione (2.7) fornisca una condizione *necessaria*. Precisamente, i loro polinomi minimi su  $F$  devono avere lo stesso grado, poiché tale grado è la dimensione dell'estensione di campi, considerata come  $F$ -spazio vettoriale. Questa, ovviamente, non è una condizione sufficiente. Per esempio, tutti i campi quadratici immaginari studiati nel capitolo 11 si ottengono aggiungendo elementi  $\delta$  i cui polinomi minimi  $x^2 - d$  hanno grado 2, ma non sono tutti isomorfi tra loro. D'altra parte, se  $\alpha$  è una radice di  $x^3 - x + 1$ , allora  $\beta = \alpha^2$  è una radice di  $x^3 - 2x^2 + x - 1$ . I campi  $\mathbb{Q}(\alpha)$  e  $\mathbb{Q}(\beta)$  sono effettivamente uguali; tuttavia, se ci fossero stati mostrati soltanto i due polinomi, ci sarebbe voluto un po' di tempo per scoprire quale relazione intercorre tra essi.

Ciò che possiamo descrivere facilmente sono i casi in cui esiste un isomorfismo

$$(2.8) \quad F(\alpha) \xrightarrow{\sim} F(\beta)$$

che lascia fisso  $F$  e manda  $\alpha$  in  $\beta$ . La seguente proposizione è fondamentale per comprendere le estensioni di campi:

(2.9) PROPOSIZIONE *Siano  $K, L$  estensioni di un campo  $F$  e siano  $\alpha \in K$  e  $\beta \in L$  elementi algebrici su  $F$ . Allora esiste un isomorfismo di campi*

$$\sigma : F(\alpha) \xrightarrow{\sim} F(\beta)$$

*che è l'identità sul sottocampo  $F$  e manda  $\alpha$  in  $\beta$  se e soltanto se i polinomi minimi di  $\alpha$  e  $\beta$  su  $F$  sono uguali.*

*Dimostrazione.* Supponiamo che  $f(x)$  sia il polinomio minimo di  $\alpha$  e di  $\beta$  su  $F$ . Applicando la proposizione (2.6), otteniamo due isomorfismi:

$$F[x]/(f) \xrightarrow{\varphi} F[\alpha] \quad \text{e} \quad F[x]/(f) \xrightarrow{\psi} F[\beta].$$

L'applicazione composta  $\sigma = \psi\varphi^{-1}$  è l'isomorfismo richiesto. Viceversa, se esiste un isomorfismo  $\sigma$  che manda  $\alpha$  in  $\beta$ , e che coincide con l'identità su  $F$ , e se  $f(x) \in F[x]$  è un polinomio tale che  $f(\alpha) = 0$ , allora si ha anche  $f(\beta) = 0$  [cfr. proposizione (2.11)]. Pertanto i due elementi hanno lo stesso polinomio minimo. ■

(2.10) DEFINIZIONE *Siano  $K$  e  $K'$  due estensioni di un campo  $F$ . Si dice isomorfismo di estensioni di campi, o  $F$ -isomorfismo, un isomorfismo di campi  $\varphi : K \rightarrow K'$  che sia l'identità su  $F$ . In tal caso  $K$  e  $K'$  si dicono estensioni isomorfe.*

(2.11) PROPOSIZIONE *Sia  $\varphi : K \rightarrow K'$  un isomorfismo di estensioni di campi di  $F$ , e sia  $f(x)$  un polinomio a coefficienti in  $F$ . Sia  $\alpha$  una radice di  $f$  in  $K$  e sia  $\alpha' = \varphi(\alpha)$  la sua immagine in  $K'$ . Allora anche  $\alpha'$  è radice di  $f$ .*

*Dimostrazione.* Sia  $f(x) = a_n x^n + \dots + a_1 x + a_0$ . Allora  $\varphi(a_i) = a_i$  e  $\varphi(\alpha) = \alpha'$ . Poiché  $\varphi$  è un omomorfismo, si ha:

$$\begin{aligned} 0 &= \varphi(0) = \varphi(f(\alpha)) = \varphi(a_n \alpha^n + \dots + a_1 \alpha + a_0) \\ &= \varphi(a_n) \varphi(\alpha)^n + \dots + \varphi(a_1) \varphi(\alpha) + \varphi(a_0) \\ &= a_n \alpha'^n + \dots + a_1 \alpha' + a_0 = f(\alpha'). \end{aligned}$$

Quindi  $\alpha'$  è radice di  $f$ . ■

Per esempio, il polinomio  $x^3 - 2$  è irriducibile su  $\mathbb{Q}$ . Indichiamo con  $\alpha$  la radice cubica reale di 2, e sia  $\zeta = e^{2\pi i/3}$  una radice cubica complessa di 1. Le tre radici complesse di  $x^3 - 2$  sono  $\alpha$ ,  $\zeta\alpha$  e  $\zeta^2\alpha$ . Pertanto esiste un isomorfismo:

$$(2.12) \quad \mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}(\zeta\alpha).$$

che manda  $\alpha$  in  $\zeta\alpha$ . In questo caso, gli elementi di  $\mathbb{Q}(\alpha)$  sono tutti numeri reali, ma  $\mathbb{Q}(\zeta\alpha)$  non è un sottocampo di  $\mathbb{R}$ . Per comprendere l'isomorfismo (2.12), non dobbiamo più considerare questi campi come sottocampi di  $\mathbb{C}$ , ma considerare soltanto la loro struttura algebrica interna.

### 3 Grado di un'estensione di campi

Un'estensione  $K$  di un campo  $F$  ha una naturale struttura di  $F$ -spazio vettoriale data dalle operazioni di addizione e moltiplicazione in  $K$ . La dimensione di  $K$  come  $F$ -spazio vettoriale è chiamata il *grado* dell'estensione di campi  $K \supset F$ . Il grado è il più semplice invarianti di un'estensione; ma è comunque importante. Esso verrà denotato nel modo seguente:

$$(3.1) \quad [K : F] = \text{dimensione di } K, \text{ come } F\text{-spazio vettoriale.}$$

Per esempio,  $\mathbb{C}$  ha la  $\mathbb{R}$ -base  $(1, i)$ , sicché  $[\mathbb{C} : \mathbb{R}] = 2$ .

Un'estensione di campi  $K \supset F$  si dice *finita* se il suo grado  $[K : F]$  è finito. Le estensioni di grado 2 sono dette anche *quadratiche*, quelle di grado 3 *cubiche*, e così via. Il grado dell'estensione è 1 se e soltanto se  $F = K$ .

Il termine *grado* proviene dalle estensioni  $K = F(\alpha)$  generate da un solo elemento algebrico  $\alpha$ ; in tal caso,  $K$  ha la base  $(1, \alpha, \dots, \alpha^{n-1})$ , dove  $n$  è il grado del polinomio minimo di  $\alpha$  su  $F$  [proposizione (2.7)]. Otteniamo così la prima proprietà importante del grado:

(3.2) PROPOSIZIONE *Se  $\alpha$  è algebrico su  $F$ , allora  $[F(\alpha) : F]$  è il grado del polinomio minimo di  $\alpha$  su  $F$ .* ■

Questo grado è detto anche il *grado di  $\alpha$  su  $F$* . Si noti che un elemento  $\alpha$  ha grado 1 su  $F$  se e solo se è un elemento di  $F$ , e  $\alpha$  ha grado  $\infty$  se e solo se è trascendente su  $F$ .

Le estensioni di grado 2 si descrivono facilmente.

(3.3) PROPOSIZIONE *Supponiamo che il campo  $F$  non abbia caratteristica 2, ossia che in  $F$   $1 + 1 \neq 0$ . Allora ogni estensione quadratica  $K$  di  $F$  può essere ottenuta aggiungendo una radice quadrata:  $K = F(\delta)$ , dove  $\delta^2 = D$  è un elemento*

di  $F$ . Viceversa, se  $\delta$  è un elemento di un'estensione di  $F$ , e se  $\delta^2 \in F$  ma  $\delta \notin F$ , allora  $F(\delta)$  è un'estensione quadratica.

**Dimostrazione.** Dimostriamo innanzitutto che ogni estensione quadratica si ottiene aggiungendo una radice di un polinomio quadratico  $f(x) \in F[x]$ . A questo scopo, scegliamo un elemento arbitrario  $\alpha$  di  $K$  non appartenente a  $F$ . Allora  $(1, \alpha)$  è un insieme linearmente indipendente su  $F$ . Poiché  $K$ , come spazio vettoriale su  $F$ , ha dimensione 2,  $(1, \alpha)$  è una base di  $K$  su  $F$ , e  $K = F[\alpha]$ . Ne segue che  $\alpha^2$  è una combinazione lineare di  $(1, \alpha)$ , diciamo  $\alpha^2 = -b\alpha - c$ , con  $b, c \in F$ . Allora  $\alpha$  è una radice di  $f(x) = x^2 + bx + c$ .

Poiché  $2 \neq 0$  in  $F$ , possiamo utilizzare la formula  $\alpha = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$  per risolvere l'equazione  $x^2 + bx + c = 0$ . (Ciò si dimostra facendo il calcolo.) Vi sono due scelte per la radice quadrata, una delle quali dà la radice  $\alpha$  scelta all'inizio. Denotiamo con  $\delta$  l'elemento corrispondente a tale scelta:  $\delta = \sqrt{b^2 - 4c} = 2\alpha + b$ . Allora  $\delta$  è un elemento di  $K$  e genera  $K$  su  $F$ . Il suo quadrato è il discriminante  $b^2 - 4c$ , che sta in  $F$ .

L'ultima asserzione della proposizione (3.3) è evidente. ■

La seconda proprietà fondamentale del grado è la proprietà moltiplicativa relativa alle catene di campi:

(3.4) **TEOREMA** *Siano  $F \subset K \subset L$  campi. Allora  $[L : F] = [L : K][K : F]$ .*

**Dimostrazione.** Sia  $\mathbf{B} = (y_1, \dots, y_n)$  una base di  $L$  come  $K$ -spazio vettoriale, e sia  $\mathbf{C} = (x_1, \dots, x_m)$  una base di  $K$  come  $F$ -spazio vettoriale. Pertanto  $[L : K] = n$  e  $[K : F] = m$ . Faremo vedere che l'insieme degli  $mn$  prodotti  $\mathbf{P} = (\dots, x_i y_j, \dots)$  è una base di  $L$ , come  $F$ -spazio vettoriale, e ciò dimostrerà la proposizione. La stessa argomentazione continuerà a valere se  $\mathbf{B}$  o  $\mathbf{C}$  sono basi infinite.

Sia  $\alpha$  un elemento di  $L$ . Poiché  $\mathbf{B}$  è una base di  $L$  su  $K$ , possiamo scrivere  $\alpha = \beta_1 y_1 + \dots + \beta_n y_n$ , con  $\beta_j \in K$ , in modo unico. Poiché  $\mathbf{C}$  è una base di  $K$  su  $F$ , ciascun elemento  $\beta_j$  può essere espresso in modo unico nella forma  $\beta_j = a_{1j} x_1 + \dots + a_{mj} x_m$ , con  $a_{ij} \in F$ . Pertanto  $\alpha = \sum_{i,j} a_{ij} x_i y_j$ . Ciò prova che  $\mathbf{P}$  genera  $L$  come  $F$ -spazio vettoriale. Sappiamo che ciascun  $\beta_j$  è univocamente determinato da  $\alpha$ , e poiché  $\mathbf{B}$  è una base di  $K$  su  $F$ , gli elementi  $a_{ij}$  sono univocamente determinati da  $\beta_j$ . Di conseguenza essi sono univocamente determinati da  $\alpha$ . Ciò prova che  $\mathbf{P}$  è linearmente indipendente e quindi che  $\mathbf{P}$  è una base di  $L$  su  $F$ . ■

Un caso interessante è quello in cui, data un'estensione  $K$  di  $F$  e un elemento  $\alpha \in K$ , si considera il campo  $F(\alpha)$ , che risulta intermedio tra  $F$  e  $K$ :

(3.5)  $F \subset F(\alpha) \subset K$ .

(3.6) **COROLLARIO** *Sia  $K \supset F$  un'estensione di grado  $n$ , e sia  $\alpha$  un elemento di  $K$ . Allora  $\alpha$  è algebrico su  $F$  e il suo grado divide  $n$ .*

Per la dimostrazione applichiamo il teorema (3.4) ai campi  $F \subset F(\alpha) \subset K$  e usiamo il fatto che il grado di  $\alpha$  su  $F$  è  $[F(\alpha) : F]$  se  $\alpha$  è algebrico, mentre è  $\infty$  se  $\alpha$  è trascendente. ■

Vediamo ora alcune applicazioni significative:

(3.7) **COROLLARIO** *Sia  $K \supset F$  un'estensione di campi di  $F$  di grado  $p$  primo, e sia  $\alpha$  un elemento di  $K$  non appartenente a  $F$ . Allora  $\alpha$  ha grado  $p$  su  $F$ , e  $K = F(\alpha)$ .*

Infatti, si ha  $p = [K : F] = [K : F(\alpha)][F(\alpha) : F]$ . Uno dei termini del prodotto è uguale a 1. Poiché  $\alpha \notin F$ , risulta  $[K : F(\alpha)] = 1$  e  $[F(\alpha) : F] = p$ . Pertanto  $K = F(\alpha)$ . ■

(3.8) **COROLLARIO** *Ogni polinomio irriducibile in  $\mathbb{R}[x]$  ha grado 1 o 2.*

Questa proprietà è già stata dimostrata nel capitolo 11 (§1); qui ne daremo ora un'altra dimostrazione. Sia  $g$  un polinomio irriducibile in  $\mathbb{R}[x]$ . Allora  $g$  ha una radice  $\alpha$  in  $\mathbb{C}$ . Poiché  $|\mathbb{C} : \mathbb{R}| = 2$ , il grado di  $\alpha$  su  $\mathbb{R}$  divide 2, in virtù di (3.6). Pertanto il grado di  $g$  è 1 o 2. ■

(3.9) **Esempi**

(a) Sia  $\alpha = \sqrt[3]{2}$ ,  $\beta = \sqrt[4]{5}$ . Consideriamo il campo  $L = \mathbb{Q}(\alpha, \beta)$  ottenuto aggiungendo  $\alpha$  e  $\beta$  a  $\mathbb{Q}$ . Allora  $[L : \mathbb{Q}] = 12$ . Infatti  $L$  contiene il sottocampo  $\mathbb{Q}(\alpha)$ , il quale ha grado 3 su  $\mathbb{Q}$ , poiché il polinomio minimo di  $\alpha$  su  $\mathbb{Q}$  è  $x^3 - 2$ . Pertanto 3 divide  $[L : \mathbb{Q}]$ . Similmente,  $L$  contiene  $\mathbb{Q}(\beta)$  e  $\beta$  ha grado 4 su  $\mathbb{Q}$ , sicché 4 divide  $[L : \mathbb{Q}]$ . D'altra parte, il grado di  $\beta$  sul campo  $\mathbb{Q}(\alpha)$  è al più 4, poiché  $\beta$  è una radice di  $x^4 - 5$ , e questo polinomio ha i coefficienti in  $\mathbb{Q}(\alpha)$ . La catena di campi  $L = \mathbb{Q}(\alpha, \beta) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$  mostra che  $[L : \mathbb{Q}]$  è al più 12. Pertanto  $[L : \mathbb{Q}] = 12$ .

(b) Utilizzando la riduzione modulo 2, si ha che il polinomio  $f(x) = x^4 + 2x^3 + 6x^2 + x + 9$  è irriducibile su  $\mathbb{Q}$  [cap. 11 (4.3)]. Sia  $\gamma$  una radice di  $f(x)$ . Allora non è possibile esprimere  $\alpha = \sqrt[3]{2}$  razionalmente per mezzo di  $\gamma$ , ossia,  $\alpha \notin \mathbb{Q}(\gamma)$ . Infatti  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ ,  $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$ , e 3 non divide 4. È impossibile dunque che si abbia  $\mathbb{Q}(\gamma) > \mathbb{Q}(\alpha)$ . D'altra parte, poiché  $i$  ha grado 2 su  $\mathbb{Q}$ , non è così facile stabilire se  $i$  sta in  $\mathbb{Q}(\gamma)$ . (In realtà,  $i \notin \mathbb{Q}(\gamma)$ ). ■

I due teoremi seguenti stabiliscono le conseguenze più importanti della proprietà moltiplicativa dei gradi.

(3.10) TEOREMA Sia  $K$  un'estensione di  $F$ . Gli elementi di  $K$  algebrici su  $F$  formano un sottocampo di  $K$ .

*Dimostrazione.* Siano  $\alpha, \beta$  elementi algebrici di  $K$ . Dobbiamo far vedere che  $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$  (se  $\alpha \neq 0$ ) sono anch'essi algebrici. Innanzitutto, poiché  $\alpha$  è algebrico, si ha  $[F(\alpha) : F] < \infty$ . Inoltre, essendo  $\beta$  algebrico su  $F$ , è algebrico anche sul campo più grande  $F(\alpha)$ . Di conseguenza il campo  $F(\alpha, \beta)$  generato su  $F(\alpha)$  da  $\beta$  è un'estensione finita di  $F(\alpha)$ , ossia  $[F(\alpha, \beta) : F(\alpha)] < \infty$ . In base al teorema (3.4), anche il grado  $[F(\alpha, \beta) : F]$  è finito, e quindi ogni elemento di  $F(\alpha, \beta)$  è algebrico su  $F$  (3.6). Gli elementi  $\alpha + \beta, \alpha\beta, \dots$  stanno tutti in  $F(\alpha, \beta)$ , e quindi sono algebrici. Ciò prova che gli elementi di  $K$  algebrici su  $F$  formano un campo. ■

Supponiamo, per esempio, che  $\alpha = \sqrt{a}, \beta = \sqrt{b}$ , con  $a, b \in F$ . Vogliamo determinare un polinomio avente  $\gamma = \alpha + \beta$  come radice. A tale scopo, calcoliamo le potenze di  $\gamma$  e utilizziamo le relazioni  $\alpha^2 = a, \beta^2 = b$  per semplificare le espressioni ottenute. Cerchiamo poi una relazione lineare tra le potenze di  $\gamma$ :

$$\gamma^2 = \alpha^2 + 2\alpha\beta + \beta^2 = (a + b) + 2\alpha\beta$$

$$\gamma^4 = (a + b)^2 + 4(a + b)\alpha\beta + 4\alpha^2\beta^2 = (a^2 + 6ab + b^2) + 4(a + b)\alpha\beta.$$

Non avremo bisogno di altre potenze, poiché possiamo eliminare  $\alpha\beta$  da queste due equazioni per ottenere l'equazione  $\gamma^4 - 2(a + b)\gamma^2 + (a - b)^2 = 0$ . Pertanto  $\gamma$  è una radice del polinomio

$$g(x) = x^4 - 2(a + b)x^2 + (a - b)^2,$$

che ha coefficienti in  $F$ , come richiesto.

Questo metodo dei coefficienti indeterminati darà sempre luogo a un polinomio avente come radice un elemento della forma  $\alpha + \beta$ , se sono noti i polinomi minimi di  $\alpha$  e  $\beta$ . Indicati con  $d_1$  e  $d_2$  i gradi di  $\alpha$  e  $\beta$  poniamo  $n = d_1d_2$ , allora ogni elemento di  $F(\alpha, \beta)$  è una combinazione lineare a coefficienti in  $F$  degli  $n$  monomi  $\alpha^i\beta^j$ , con  $0 \leq i < d_1, 0 \leq j < d_2$ . Infatti  $F(\alpha, \beta) = F[\alpha, \beta]$  [cfr. (2.6)], e questi monomi generano  $F[\alpha, \beta]$ . Dato un elemento  $\gamma \in F(\alpha, \beta)$ , scriviamo le potenze  $1, \gamma, \gamma^2, \dots, \gamma^n$  come combinazioni lineari a coefficienti in  $F$  di questi monomi, e poiché vi sono soltanto  $n$  monomi  $\alpha^i\beta^j$ , le  $n+1$  potenze  $\gamma^i$  sono linearmente dipendenti. Una relazione di dipendenza lineare individua un polinomio a coefficienti in  $F$  avente  $\gamma$  come radice.

Tuttavia vi è un punto che può creare delle complicazioni: il polinomio  $g(x)$  avente  $\gamma$  come radice ottenuto in tal modo potrebbe essere riducibile. Per esempio, può accadere che  $\gamma$  appartenga al campo  $F$ , anche se  $\alpha$  e  $\beta$  non stanno in  $F$ . In tal caso, è poco probabile che il procedimento descritto fornisca il suo polinomio

minimo  $x - \gamma$ . In generale, è più difficile determinare il polinomio minimo di  $\gamma$  su  $F$ . ■

Un'estensione  $K$  di un campo  $F$  è chiamata *estensione algebrica*, e si dice che  $K$  è *algebrico su  $F$* , se tutti i suoi elementi sono algebrici su  $F$ .

(3.11) TEOREMA Siano  $F \subset K \subset L$  campi. Se  $L$  è algebrico su  $K$  e  $K$  è algebrico su  $F$ , allora  $L$  è algebrico su  $F$ .

*Dimostrazione.* Dobbiamo far vedere che ogni elemento  $\alpha \in L$  è algebrico su  $F$ . Poiché, per ipotesi,  $\alpha$  è algebrico su  $K$ , esiste una relazione della forma

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

con  $a_0, \dots, a_{n-1} \in K$ . Pertanto  $\alpha$  è algebrico sul campo  $F(a_0, \dots, a_{n-1})$  generato da  $a_0, \dots, a_{n-1}$  su  $F$ . Si noti che ciascun coefficiente  $a_i$  è algebrico su  $F$ , poiché  $a_i \in K$ . Consideriamo la catena di campi:

$$F \subset F(a_0) \subset F(a_0, a_1) \subset \cdots \subset F(a_0, a_1, \dots, a_{n-1}) \subset F(a_0, a_1, \dots, a_{n-1}, \alpha)$$

ottenuti aggiungendo, uno dopo l'altro, gli elementi  $a_0, \dots, a_{n-1}, \alpha$ . Per ogni  $i$ , l'elemento  $a_{i+1}$  è algebrico su  $F(a_0, \dots, a_i)$ , poiché è algebrico su  $F$ . Inoltre,  $\alpha$  è algebrico su  $F(a_0, a_1, \dots, a_{n-1})$ . Pertanto ogni estensione nella catena è finita. In base al teorema (3.4), il grado di  $F(a_1, a_2, \dots, a_{n-1}, \alpha)$  su  $F$  è finito. Ne segue, in virtù del corollario (3.6), che  $\alpha$  è algebrico su  $F$ . ■

#### 4 Costruzioni con riga e compasso

Esistono famosi teoremi che affermano l'impossibilità di effettuare con riga e compasso determinate costruzioni geometriche, come la trisezione di un angolo. Useremo ora la nozione di grado di un'estensione di campi per dimostrare qualcuno di questi teoremi.

Enunciamo innanzitutto le regole per le costruzioni fondamentali con riga e compasso:

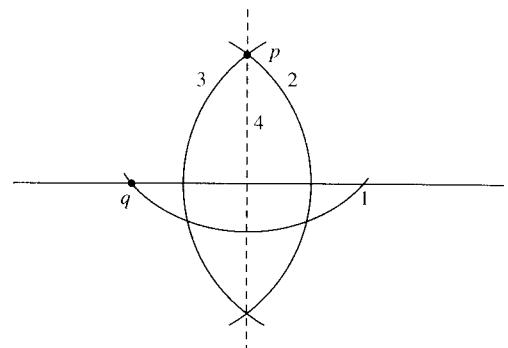
- (4.1) (a) Per cominciare, sono dati due punti nel piano che possiamo supporre siano stati *costruiti* (con riga e compasso).
- (b) Costruita una coppia di punti, possiamo *costruire* con riga e compasso la retta passante per essi e la circonferenza col centro in uno dei punti e passante per l'altro.
- (c) Possiamo *costruire* i punti di intersezione di rette e circonferenze così costruite.

Con la riga di cui disponiamo possiamo soltanto tracciare rette passanti per punti già costruiti; non possiamo effettuare misure.

Desriveremo tutte le possibili costruzioni, cominciando da alcune ben note. In ciascuna delle figure seguenti, le rette e le circonferenze vanno disegnate nell'ordine indicato.

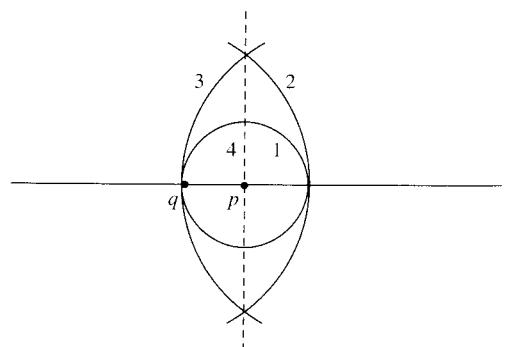
- (4.2) *Disegnare una retta passante per un punto costruito  $p$  e perpendicolare a una retta costruita  $\ell$ .*

*Caso 1:  $p \notin \ell$*

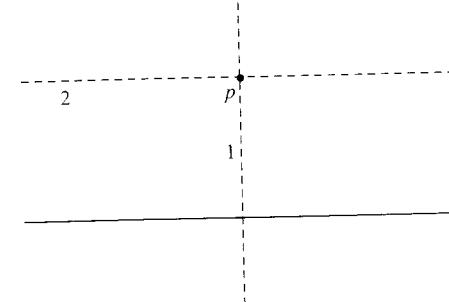


Questa costruzione può essere effettuata con un punto  $q \in \ell$  qualsiasi, purché non appartenente alla perpendicolare. Tuttavia, faremmo bene a non scegliere i punti arbitrariamente, poiché così facendo avremmo difficoltà a distinguere i punti che abbiamo costruito da quelli finti che compaiono in conseguenza di una scelta arbitraria. Ogniqualvolta avremo bisogno di un punto arbitrario, ne costruiremo uno *ad hoc*.

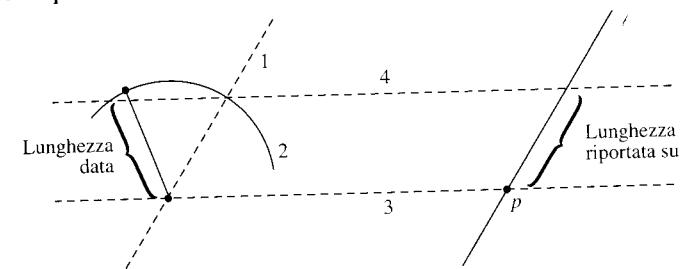
*Caso 2:  $p \in \ell$*



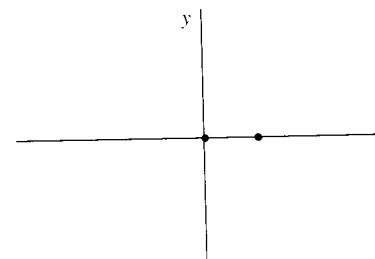
- (3) *Tracciare una retta parallela a  $\ell$  e passante per  $p$ . (Basta applicare i casi 1 e 2 precedenti).*



- (4.4) *Ripartire una lunghezza definita da due punti su una retta costruita  $\ell$ , partendo da un punto costruito  $p \in \ell$ . (Basta utilizzare la costruzione di rette parallele).*



Queste costruzioni permettono di introdurre coordinate cartesiane nel piano sicché possiamo supporre che i due punti assegnati all'inizio abbiano coordinate  $(0,0)$  e  $(0,1)$ . Potremmo scegliere altri sistemi di coordinate che comunque condurrebbero a teorie equivalenti.



Diremo che un numero reale è *costruibile* (con righi e compasso) se il suo valore assoluto  $|a|$  è la distanza tra due punti costruibili con righi e compasso, l'unità di lunghezza essendo la distanza tra i punti assegnati all'inizio.

- (4.5) PROPOSIZIONE *Un punto  $p = (a, b)$  è costruibile se e solo se le sue coordinate cartesiane  $a$  e  $b$  sono numeri costruibili.*

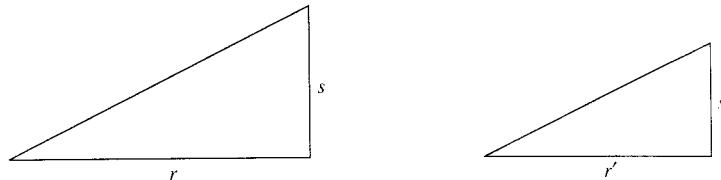
*Dimostrazione.* Ciò segue dalle costruzioni precedenti. Dato un punto costruito  $p$ , possiamo costruire le sue coordinate conducendo le perpendicolari agli assi. Viceversa, siano  $a$  e  $b$  numeri costruibili. Allora possiamo costruire il punto  $p$  riportando  $a, b$  sui due assi, come specificato in (4.4), e conducendo perpendicolari. ■

(4.6) PROPOSIZIONE *I numeri costruibili formano un sottocampo di  $\mathbb{R}$ .*

*Dimostrazione.* Faremo vedere che se  $a$  e  $b$  sono numeri costruibili positivi, allora  $a+b$ ,  $ab$ ,  $a-b$  (se  $a > b$ ) e  $a^{-1}$  (se  $a \neq 0$ ) sono anch'essi costruibili. Da ciò si ottiene facilmente la chiusura nel caso in cui  $a$  o  $b$  sia negativo.

Per l'addizione e la sottrazione, basta riportare le lunghezze su una retta, utilizzando la costruzione (4.4).

Per la moltiplicazione, utilizziamo triangoli rettangoli simili:



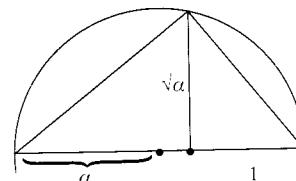
Dati un triangolo e un segmento parallelo ad uno dei suoi lati, tracciando le parallele agli altri due lati passanti per gli estremi del segmento si costruisce su di esso un triangolo simile a quello dato.

Per costruire il prodotto  $ab$ , poniamo  $r = 1$ ,  $s = a$  e  $r' = b$ . Allora poiché  $r/s = r'/s'$ , si ha  $s' = ab$ . Per costruire  $a^{-1}$ , poniamo  $r = a$ ,  $s = 1$  e  $r' = 1$ . Allora risulta  $s' = a^{-1}$ . ■

(4.7) PROPOSIZIONE *Se  $a$  è un numero costruibile positivo, tale risulta  $\sqrt{a}$ .*

*Dimostrazione.* Usiamo di nuovo i triangoli simili. Dobbiamo costruirli in modo che  $r = a$ ,  $r' = s$  e  $s' = 1$ . Allora risulta:  $s = r' = \sqrt{a}$ .

Questa volta la costruzione è meno ovvia, ma possiamo utilizzare i triangoli inscritti in una circonferenza. Come sappiamo dalle scuole superiori, un triangolo inscritto in una circonferenza avente un diametro come lato è un triangolo rettangolo. Questo teorema si può dimostrare usando l'equazione di una circonferenza e il teorema di Pitagora. Tracciamo dunque una circonferenza di diametro  $1+a$  e procediamo nel modo illustrato nella figura qui sotto. Si noti che il triangolo grande si compone di due triangoli simili. ■



(4.8) PROPOSIZIONE *Supponiamo assegnati quattro punti, le cui coordinate appartengono a un sottocampo  $F$  di  $\mathbb{R}$ . Siano  $A, B$  rette o circonferenze costruite utilizzando tali punti. Allora i punti di intersezione di  $A$  e  $B$  hanno coordinate in  $F$  o in un campo della forma  $F(\sqrt{r})$ , dove  $r$  è un numero positivo in  $F$ .*

*Dimostrazione.* La retta passante per  $(a_0, b_0)$ ,  $(a_1, b_1)$  ha equazione:

$$(a_1 - a_0)(y - b_0) = (b_1 - b_0)(x - a_0).$$

La circonferenza di centro  $(a_0, b_0)$  e passante per  $(a_1, b_1)$  ha equazione:

$$(x - a_0)^2 + (y - b_0)^2 = (a_1 - a_0)^2 + (b_1 - b_0)^2.$$

L'intersezione di due rette può essere determinata risolvendo un sistema di due equazioni lineari a coefficienti in  $F$ , quindi le sue coordinate stanno anch'esse in  $F$ . Per trovare le intersezioni di una retta e di una circonferenza usiamo l'equazione della retta per eliminare una variabile dall'equazione della circonferenza, ottenendo un'equazione di secondo grado in una sola incognita. Tale equazione ha soluzioni nel campo  $F(\sqrt{D})$ , dove  $D$  è il discriminante, il quale è un elemento di  $F$ . Se  $D < 0$ , la retta e la circonferenza non si intersecano.

Consideriamo ora le intersezioni di due circonferenze, aventi ad esempio, equazioni

$$(x - a_1)^2 + (y - b_1)^2 = r_1^2 \quad \text{e} \quad (x - a_2)^2 + (y - b_2)^2 = r_2^2,$$

con  $a_i, b_i, r_i \in F$ . In generale, le soluzioni di un sistema di due equazioni di secondo grado in due incognite si ottengono risolvendo un'equazione di quarto grado. In questo caso siamo fortunati, poiché la differenza delle due equazioni di secondo grado è un'equazione lineare che può essere usata, come prima, per eliminare una variabile. ■

(4.9) TEOREMA *Siano  $a_1, \dots, a_m$  numeri reali costruibili. Allora esiste una catena di sottocampi  $Q = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_n = K$  tali che*

- (i)  $K$  è un sottocampo di  $\mathbb{R}$ ;
- (ii)  $a_1, \dots, a_m \in K$ ;
- (iii) per ogni  $i = 0, \dots, n-1$ , il campo  $F_{i+1}$  si ottiene a partire da  $F_i$  aggiungendo la radice quadrata di un numero positivo  $r_i \in F_i$  che non è un quadrato in  $F_i$ .

Viceversa, sia  $Q = F_0 \subset F_1 \subset \dots \subset F_n = K$  una catena di sottocampi di  $\mathbb{R}$  che soddisfi alla condizione (iii). Allora ogni elemento di  $K$  è costruibile.

*Dimostrazione.* Abbiamo introdotto un sistema di coordinate tale che i punti da cui siamo partiti abbiano coordinate in  $Q$ . Il procedimento per costruire i numeri  $a_i$  consiste essenzialmente nel tracciare rette e circonferenze e prendere le

loro intersezioni. Pertanto la prima parte del teorema segue, per induzione, dalla proposizione (4.8). Viceversa, data una catena di campi che soddisfa la condizione (iii), i suoi elementi sono costruibili, in base alle proposizioni (4.6) e (4.7). ■

(4.10) COROLLARIO *Se  $a$  è un numero reale costruibile, allora  $a$  è algebrico e il suo grado su  $\mathbb{Q}$  è una potenza di 2.*

*Dimostrazione.* Nella catena di campi (4.9), il grado di  $F_{i+1}$  su  $F_i$  è 2, e quindi  $[K : \mathbb{Q}] = 2^n$ . Il corollario (3.6) ci dice che il grado di  $a$  divide  $2^n$ , e quindi è una potenza di 2. ■

L'enunciato inverso del corollario (4.10) è falso: per esempio esistono numeri reali  $\alpha$  che hanno grado 4 su  $\mathbb{Q}$ , ma non sono costruibili. Lo dimostreremo più avanti, utilizzando la teoria di Galois.

Siamo ora in grado di dimostrare l'impossibilità di talune costruzioni geometriche. Il nostro metodo consistrà nel far vedere che se fosse possibile una certa costruzione, sarebbe anche possibile costruire un numero algebrico il cui grado su  $\mathbb{Q}$  non è una potenza di 2, in contraddizione col corollario (4.10).

Come primo esempio, trattiamo il problema della trisezione dell'angolo. Dobbiamo fare attenzione a porre correttamente il problema, poiché è possibile trisecare molti angoli particolari, ad esempio un angolo di  $45^\circ$ . Di solito, il problema si enuncia richiedendo un unico metodo di costruzione che valga per *un angolo assegnato qualsiasi*.

Per essere precisi il più possibile, diciamo che un angolo  $\theta$  è *costruibile* se il suo coseno  $\cos \theta$  è costruibile. È possibile dare altre definizioni equivalenti. Per esempio,  $\theta$  è costruibile se e solo se la retta che passa per l'origine e forma un angolo  $\theta$  con l'asse  $x$  è costruibile. Oppure,  $\theta$  è costruibile se e solo se è possibile costruire due rette qualsiasi formanti tra loro un angolo  $\theta$ .

Ora, basta assegnare un angolo  $\theta$  (ad esempio riportando il suo coseno sull'asse  $x$ ) per disporre di una nuova informazione utilizzabile in un'eventuale trisezione. Per analizzare le implicazioni di questa nuova informazione, dovremmo cominciare a determinare tutte le costruzioni che potrebbero essere effettuate quando, oltre a due punti, venisse assegnata all'inizio un'altra lunghezza ( $= \cos \theta$ ). Preferiremmo non perdere troppo tempo, e per fortuna c'è una via di uscita. Esibiremo un angolo  $\theta$  particolare, con le seguenti proprietà:

- (4.11) (i)  $\theta$  è costruibile,
- (ii)  $\frac{1}{3}\theta$  non è costruibile.

La prima condizione ci dice che l'assegnazione dell'angolo  $\theta$  non ci dà alcuna nuova informazione, nel senso che, se l'angolo  $\theta$ , una volta assegnato, può essere trisecato, esso può essere trisecato anche senza esser stato assegnato. La seconda condizione ci dice che non esiste un metodo generale di trisezione, poiché non è possibile trisecare  $\theta$ .

L'angolo  $\theta = 60^\circ$  risolve il problema. Un angolo di  $60^\circ$  è costruibile, poiché  $\cos 60^\circ = \frac{1}{2}$ . D'altra parte, è impossibile costruire un angolo di  $20^\circ$ . Per dimostrarlo faremo vedere che  $\cos 20^\circ$  è un numero algebrico di grado 3 su  $\mathbb{Q}$ . Ne seguirà, in virtù del corollario (4.10), che  $\cos 20^\circ$  non è costruibile e quindi che l'angolo di  $60^\circ$  non può essere trisecato.

Le formule di addizione per il seno e il coseno possono essere usate per dimostrare l'identità:

$$(4.12) \quad \cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta.$$

Ponendo  $\theta = 20^\circ$  e  $\alpha = \cos 20^\circ$ , si ottiene la relazione:  $\frac{1}{2} = 4\alpha^3 - 3\alpha$ , ossia,  $8\alpha^3 - 6\alpha - 1 = 0$ .

(4.13) LEMMA *Il polinomio  $f(x) = 8x^3 - 6x - 1$  è irriducibile su  $\mathbb{Q}$ .*

*Dimostrazione.* È sufficiente cercare fattori lineari  $ax+b$ , con  $a, b$  interi tali che  $a$  divida 8, e  $b$  sia uguale a  $\pm 1$ . Un altro modo per dimostrare l'irriducibilità è quello di verificare che  $f$  non ha radici modulo 5. ■

Questo lemma ci dice che  $\alpha$  ha grado 3 su  $\mathbb{Q}$ , e quindi non può essere costruito.

Come secondo esempio, dimostriamo che è impossibile costruire con riga e compasso il poligono regolare di 7 lati. (Questo problema è simile al precedente, poiché la costruzione dell'angolo di  $20^\circ$  è equivalente alla costruzione del poligono regolare di 18 lati.) Denotiamo con  $\theta$  l'angolo  $2\pi/7$  e poniamo  $\zeta = \cos \theta + i \sin \theta$ . Allora  $\zeta$  è una radice del polinomio  $x^6 + x^5 + \dots + 1$ , che è irriducibile [cap. 11 (4.6)]. Pertanto  $\zeta$  ha grado 6 su  $\mathbb{Q}$ . Se l'ettagono regolare fosse costruibile, allora  $\cos \theta$  e  $\sin \theta$  sarebbero numeri costruibili, e quindi apparirebbero a un'estensione reale di grado  $2^n$  su  $\mathbb{Q}$ , in virtù del teorema (4.9). Chiamiamo  $K$  tale campo e consideriamo l'estensione  $K(i)$ . Essa ha grado 2, e pertanto  $[K(i) : \mathbb{Q}] = 2^{n+1}$ . Ma  $\zeta = \cos \theta + i \sin \theta \in K(i)$ . Ciò contraddice il fatto che il grado di  $\zeta$  è 6 [cfr. (3.6)].

Conviene notare che la precedente argomentazione non vale soltanto per il numero 7: essa è applicabile a un numero primo  $p$  qualsiasi, con l'unica condizione che  $p-1$ , ossia il grado del polinomio irriducibile  $x^{p-1} + x^{p-2} + \dots + x + 1$ , non sia una potenza di 2.

(4.14) COROLLARIO *Sia  $p$  un numero primo. Se il poligono regolare di  $p$  lati può essere costruito con riga e compasso, allora  $p = 2^r + 1$ , essendo  $r$  un intero opportuno. ■*

Gauss ha dimostrato il viceversa, ossia che, se un numero primo  $p$  ha la forma  $2^r + 1$ , è possibile costruire il poligono regolare di  $p$  lati. Per esempio, il poligono regolare di 17 lati può essere costruito con riga e compasso. Nel prossimo capitolo vedremo come si dimostra.

## 5 Aggiunzione simbolica di radici

Finora abbiamo usato come esempi sottocampi del campo dei numeri complessi. Per ottenere questi campi, non c'è bisogno di ricorrere a costruzioni astratte (ad eccezione della costruzione di  $\mathbb{C}$  a partire da  $\mathbb{R}$ ). Semplicemente di volta in volta, noi aggiungiamo numeri complessi al campo dei numeri razionali e lavoriamo con il sottocampo che essi generano. Ma i campi finiti e i campi di funzioni non sono sottocampi di un campo ben noto, analogo a  $\mathbb{C}$ , che li racchiuda tutti, pertanto devono essere costruiti. Lo strumento fondamentale per la loro costruzione è l'aggiunzione di elementi a un anello (cfr. cap. 10, § 5). Nel caso in esame l'anello di partenza è un campo  $F$ .

Richiamiamo tale costruzione. Dato un polinomio  $f(x)$  a coefficienti in  $F$ , possiamo aggiungere a  $F$  un elemento  $\alpha$  che soddisfa l'equazione  $f(\alpha) = 0$ . Il procedimento astratto consiste nel costruire l'anello dei polinomi  $F[x]$  e prendere l'anello quoziante

$$(5.1) \quad R' = F[x]/(f).$$

Questa costruzione fornisce sempre un anello  $R'$  e un omomorfismo  $F \rightarrow R'$  tale che la classe resto  $\bar{x}$  di  $x$  soddisfi la relazione  $f(\bar{x}) = 0$ .

Tuttavia, noi vogliamo costruire non soltanto un anello, ma un campo, e qui entra in gioco la teoria dei polinomi a coefficienti in un campo, la quale ci dice che l'ideale principale  $(f)$  è un ideale massimale se e solo se  $f$  è irriducibile [cap. 11 (1.6)]. Pertanto l'anello  $R'$  sarà un campo se e solo se  $f$  è un polinomio irriducibile.

**(5.2) LEMMA** *Sia  $F$  un campo e sia  $f$  un polinomio irriducibile in  $F[x]$ . Allora l'anello  $K = F[x]/(f)$  è un campo, che risulta un'estensione di  $F$ , e la classe resto  $\bar{x}$  di  $x$  è una radice di  $f(x)$  in  $K$ .*

*Dimostrazione.* L'anello  $K$  è un campo, poiché  $(f)$  è un ideale massimale. Inoltre, l'omomorfismo  $F \rightarrow K$  che manda gli elementi di  $F$  nelle classi resto dei polinomi costanti, è iniettivo perché  $F$  è un campo. Possiamo identificare  $F$  con la sua immagine, che è un sottocampo di  $K$ , e con tale identificazione il campo  $K$  diventa un'estensione di  $F$ . Infine,  $\bar{x}$  soddisfa l'equazione  $f(x) = 0$ , ossia  $\bar{x}$  è una radice di  $f$ . ■

**(5.3) PROPOSIZIONE** *Sia  $F$  un campo e sia  $f(x)$  un polinomio monico in  $F[x]$  di grado positivo. Allora esiste un'estensione di campi  $K$  di  $F$  tale che  $f(x)$  si scomponga in fattori lineari su  $K$ .*

*Dimostrazione.* Procediamo per induzione sul grado di  $f$ . Il primo caso è quello in cui  $f$  ha una radice  $\alpha$  in  $F$ , sicché  $f(x) = (x - \alpha)g(x)$  con  $g(x) \in F[x]$ ,

e  $\deg g < \deg f$ . In tal caso possiamo concludere in virtù dell'ipotesi induttiva. Altrimenti, scegliamo un fattore irriducibile  $g(x)$  di  $f(x)$ . In base al lemma (5.2) esiste un'estensione di campi di  $F$ , diciamo  $F_1$ , in cui  $g(x)$  ha una radice  $\alpha$ . A questo punto sostituiamo  $F$  con  $F_1$  e ci riduciamo così al primo caso. ■

Come abbiamo visto, l'anello dei polinomi  $F[x]$  è uno strumento importante per studiare le estensioni di un campo  $F$ , per cui, lavorando contemporaneamente con due campi, occorre tener conto delle relazioni che intercorrono tra i loro anelli di polinomi. Lo studio di tali relazioni non presenta serie difficoltà, e anziché disperdere nel testo i punti che devono essere menzionati, li abbiamo raccolti qui tutti insieme.

Osserviamo che se  $K$  è un'estensione di campi di  $F$  l'anello dei polinomi  $K[x]$  contiene  $F[x]$  come sottoanello. Pertanto i calcoli effettuati nell'anello  $F[x]$  sono validi anche in  $K[x]$ .

**(5.4) PROPOSIZIONE** *Siano  $f$  e  $g$  polinomi a coefficienti in un campo  $F$  e sia  $K$  un'estensione di campi di  $F$ .*

- (a) *La divisione con resto di  $g$  per  $f$  dà lo stesso risultato, sia che venga effettuata in  $F[x]$  o in  $K[x]$ .*
- (b)  *$f$  divide  $g$  in  $K[x]$  se e solo se  $f$  divide  $g$  in  $F[x]$ .*
- (c) *Il massimo comune divisore monico  $d$  di  $f$  e  $g$  è lo stesso, sia in  $F[x]$  che in  $K[x]$ .*
- (d) *Se  $f$  e  $g$  hanno una radice comune in  $K$ , allora non sono primi tra loro in  $F[x]$ . Viceversa, se  $f$  e  $g$  non sono primi tra loro in  $F[x]$ , allora esiste un'estensione di campi di  $F$  in cui essi hanno una radice comune.*
- (e) *Se  $f$  è irriducibile in  $F[x]$  e se  $f$  e  $g$  hanno una radice comune in  $K$ , allora  $f$  divide  $g$  in  $F[x]$ .*

*Dimostrazione.* (a) Effettuando la divisione con resto in  $F[x]$ , si ha  $g = fq + r$ . Tale relazione vale anche nell'anello più grande  $K[x]$ , e non è possibile dividere ulteriormente il resto  $r$  per  $f$ , poiché il grado di  $r$  è minore del grado di  $f$ , oppure  $r = 0$ .

(b) Questo è il caso in cui il resto è zero in (a).

(c) Denotiamo con  $d, d'$  i massimi comuni divisori monici di  $f$  e  $g$  in  $F[x]$  e in  $K[x]$ . Allora  $d$  è anche un divisore comune in  $K[x]$ , e dunque divide  $d'$  in  $K[x]$ , in base alla definizione di  $d'$ . Inoltre, sappiamo che  $d$  ha la forma  $d = pf + qg$ , con  $p, q \in F[x]$ . Poiché  $d'$  divide  $f$  e  $g$ , esso divide anche  $pf + qg = d$ . Ne segue che  $d$  e  $d'$  sono associati in  $K[x]$ , e quindi, essendo monici, sono uguali.

(d) Sia  $\alpha$  una radice comune di  $f$  e  $g$  in  $K$ . Allora  $x - \alpha$  è un divisore comune di  $f$  e  $g$  in  $K[x]$ . Pertanto il loro massimo comune divisore in  $K[x]$  è diverso

da 1. In base a (c), esso è diverso da 1 anche in  $F[x]$ . Viceversa, se  $f$  e  $g$  hanno un divisore comune  $d$  di grado  $> 0$ , allora, in virtù di (5.3),  $d$  ha una radice in qualche estensione di campi di  $F$ . Questa radice sarà una radice comune di  $f$  e  $g$ .

(e) Se  $f$  è irriducibile, allora i suoi unici divisori in  $F[x]$  sono 1,  $f$ , e i loro associati. Il punto (d) precedente ci dice che il massimo comune divisore di  $f$  e  $g$  in  $F[x]$  è diverso da 1; di conseguenza, esso è uguale a  $f$ . ■

L'ultimo argomento di questo paragrafo riguarda la derivata  $f'(x)$  di un polinomio  $f(x)$ . In algebra, essa si calcola utilizzando le stesse regole introdotte in analisi per derivare le funzioni polinomiali. In altre parole, definiamo la derivata di  $x^n$  come il polinomio  $nx^{n-1}$  e inoltre, se  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , allora:

$$(5.5) \quad f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1.$$

I coefficienti interi in questa formula vanno interpretati come elementi di  $F$  in virtù dell'omomorfismo  $\mathbb{Z} \rightarrow F$  [cap. 10 (3.18)]. Pertanto la derivata è un polinomio a coefficienti nello stesso campo. Si può dimostrare che valgono varie regole, come, ad esempio, la regola per la derivata del prodotto.

Sebbene la derivazione sia un'operazione algebrica, non c'è motivo, a priori, per supporre che essa abbia un forte significato algebrico; tuttavia, ciò è vero. Per noi, la proprietà più importante della derivata è il fatto che si può usare per riconoscere le radici multiple di un polinomio.

(5.6) LEMMA *Sia  $F$  un campo, sia  $f(x) \in F[x]$  un polinomio, e sia  $\alpha \in F$  una radice di  $f(x)$ . Allora  $\alpha$  è una radice multipla, ossia  $(x - \alpha)^2$  divide  $f(x)$ , se e soltanto se  $\alpha$  è anche radice di  $f'(x)$ .*

*Dimostrazione.* Se  $\alpha$  è una radice di  $f$ , allora  $x - \alpha$  divide  $f$ , ossia  $f(x) = (x - \alpha)g(x)$ ; quindi  $\alpha$  è una radice di  $g$  se e solo se è una radice multipla di  $f$ . In virtù della regola per la derivata del prodotto, si ottiene:

$$f'(x) = (x - \alpha)g'(x) + g(x).$$

Sostituendo  $x$  con  $\alpha$ , si ha che  $f'(\alpha) = 0$  se e solo se  $g(\alpha) = 0$ . ■

(5.7) PROPOSIZIONE *Sia  $f(x) \in F[x]$  un polinomio. Allora esiste un'estensione di campi  $K$  di  $F$  in cui  $f$  ha una radice multipla se e soltanto se  $f$  e  $f'$  non sono primi tra loro.*

*Dimostrazione.* Se  $f$  ha una radice multipla in  $K$ , allora  $f$  e  $f'$  hanno una radice comune in  $K$ , in virtù del lemma (5.6), e pertanto non sono primi tra loro in  $K[x]$ . Ne segue che essi non sono primi tra loro neppure in  $F[x]$ . Viceversa,

se  $f$  e  $f'$  non sono primi tra loro, allora hanno una radice comune in qualche estensione di campi  $K$ , e quindi  $f$  ha una radice multipla in  $K$ . ■

Stabiliamo ora una delle applicazioni più importanti della derivata alla teoria dei campi:

(5.8) PROPOSIZIONE *Sia  $f$  un polinomio irriducibile in  $F[x]$ . Allora  $f$  non ha radici multiple in alcuna estensione di  $F$ , a meno che la derivata  $f'$  non sia il polinomio nullo. In particolare, se  $F$  è un campo di caratteristica zero, allora  $f$  non ha radici multiple.*

*Dimostrazione.* In base alla proposizione precedente, dobbiamo dimostrare che  $f$  e  $f'$  sono primi tra loro, a meno che  $f'$  non sia il polinomio nullo. Poiché  $f$  è irriducibile, l'unico caso in cui  $f$  ha un fattore non costante in comune con un altro polinomio  $g$  è quello in cui  $f$  divide  $g$  (5.4e). Inoltre, se  $f$  divide  $g$ , allora  $\deg g \geq \deg f$ , oppure  $g = 0$ . Ora il grado della derivata  $f'$  è minore del grado di  $f$ , quindi  $f$  e  $f'$  non hanno fattori non costanti in comune, a meno che non risulti  $f' = 0$ , come richiesto. In particolare, in un campo di caratteristica zero, la derivata di un polinomio non costante è diversa dal polinomio nullo. ■

La derivata di un polinomio non costante  $f(x)$  può essere identicamente nulla se la caratteristica del campo  $F$  è un numero primo  $p$ . Ciò accade quando l'esponente di ogni monomio che compare in  $f$  è divisibile per  $p$ . Un tipico polinomio la cui derivata è identicamente nulla, nel caso di un campo  $F$  di caratteristica 5, è:

$$f(x) = x^{15} + ax^{10} + bx^5 + c,$$

dove  $a, b, c$  sono elementi di  $F$ . Poiché la derivata di questo polinomio è identicamente nulla, le sue radici in un'estensione arbitraria di  $F$  sono tutte multiple. L'irriducibilità di questo polinomio dipende da  $F$  e da  $a, b, c$ .

## 6 Campi finiti

In questo paragrafo descriveremo tutti i campi aventi un numero finito di elementi. Abbiamo osservato nel paragrafo 1 che un campo finito  $K$  contiene uno dei campi primi  $\mathbb{F}_p$ , e naturalmente, poiché  $K$  è finito, esso risulterà uno spazio vettoriale di dimensione finita su tale campo. Denotiamo  $\mathbb{F}_p$  con  $F$  e il grado  $[K : F]$  con  $r$ . Come  $F$ -spazio vettoriale,  $K$  è isomorfo allo spazio  $F^r$ , e questo spazio contiene  $p^r$  elementi. Pertanto l'ordine di un campo finito è sempre una potenza di un numero primo. Tale numero viene denotato di solito con  $q$ :

$$(6.1) \quad q = p^r = |K|.$$

Quando parleremo di campi finiti,  $p$  denoterà sempre un numero primo e  $q$ , dato da una potenza di  $p$ , denoterà il numero degli elementi, ossia l'*ordine*, del campo.

I campi con  $q$  elementi si denotano spesso con  $\mathbb{F}_q$ . Faremo vedere che tutti i campi con uno stesso numero di elementi sono isomorfi tra loro, sicché questa notazione non è troppo ambigua. Tuttavia, l'isomorfismo non sarà unico quando  $r > 1$ .

L'esempio più semplice di un campo finito diverso da un campo primo  $\mathbb{F}_p$  è il campo  $K = \mathbb{F}_4$  di ordine 4. Esiste un unico polinomio irriducibile  $f(x)$  di grado 2 in  $\mathbb{F}_2[x]$ , precisamente:

$$(6.2) \quad f(x) = x^2 + x + 1$$

[cfr. cap. 11 (4.3)], e il campo  $K$  si ottiene aggiungendo a  $F = \mathbb{F}_2$  una radice  $\alpha$  di  $f(x)$ :

$$K \approx F[x]/(x^2 + x + 1).$$

L'ordine di questo campo è 4, poiché  $\alpha$  ha grado 2; ne consegue che  $K$ , come spazio vettoriale su  $F$ , ha dimensione 2.

L'insieme  $(1, \alpha)$  forma una base di  $K$  su  $F$ , e pertanto gli elementi di  $K$  sono le quattro combinazioni lineari di questi due elementi, con coefficienti 0, 1 modulo 2. Essi sono:

$$(6.3) \quad \{0, 1, \alpha, 1 + \alpha\} = \mathbb{F}_4.$$

L'elemento  $1 + \alpha$  è la seconda radice del polinomio  $f(x)$  in  $K$ . I calcoli in  $K$  si effettuano utilizzando le relazioni:  $1 + 1 = 0$  e  $\alpha^2 + \alpha + 1 = 0$ . Il campo  $\mathbb{F}_4$  non va confuso con l'anello  $\mathbb{Z}/(4)$ !

Enunciamo ora le principali proprietà dei campi finiti:

(6.4) TEOREMA Sia  $p$  un numero primo e sia  $q = p^r$  una potenza di  $p$ , con  $r \geq 1$ .

- (a) Esiste un campo di ordine  $q$ .
- (b) Due campi di ordine  $q$  sono isomorfi.
- (c) Sia  $K$  un campo di ordine  $q$ . Il gruppo moltiplicativo  $K^*$  degli elementi non nulli di  $K$  è un gruppo ciclico di ordine  $q - 1$ .
- (d) Gli elementi di  $K$  sono radici del polinomio  $x^q - x$ , che ha radici distinte e si scomponete in fattori lineari in  $K[x]$ .
- (e) Ogni polinomio irriducibile di grado  $r$  in  $\mathbb{F}_p[x]$  è un fattore di  $x^q - x$ . I fattori irriducibili di  $x^q - x$  in  $\mathbb{F}_p[x]$  sono esattamente i polinomi irriducibili in  $\mathbb{F}_p[x]$  il cui grado divide  $r$ .

(f) Un campo  $K$  di ordine  $q$  contiene un sottocampo di ordine  $q' = p^k$  se e soltanto se  $k$  divide  $r$ .

La dimostrazione non è particolarmente difficile, ma comprendendo parecchie parti, richiederà un po' di tempo. Perché se ne capisca meglio l'utilità, vediamo innanzitutto alcune conseguenze del teorema.

Il fatto sorprendente espresso da (c) è che tutti gli elementi non nulli di  $K$  possono essere elencati come potenze di un solo elemento, opportunamente scelto. Ciò non è ovvio nemmeno per il campo primo  $\mathbb{F}_p$ . Per esempio, la classe resto di 3 è un generatore di  $\mathbb{F}_7^*$ ; le sue potenze,  $3^0, 3^1, 3^2, \dots$ , forniscono l'elenco degli elementi non nulli di  $\mathbb{F}_7$  nel seguente ordine:

$$(6.5) \quad \mathbb{F}_7^* = \{1, 3, 2, 6, 4, 5\}.$$

Come altro esempio, 2 è un generatore di  $\mathbb{F}_{11}^*$ , e le sue potenze descrivono l'intero gruppo nell'ordine:

$$(6.6) \quad \mathbb{F}_{11}^* = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}.$$

Un generatore del gruppo ciclico  $\mathbb{F}_p^*$  è detto *elemento primitivo modulo  $p$* . Si noti che il teorema ci dice soltanto che un elemento primitivo esiste, ma non come trovarlo. Non è ben chiaro quali siano le classi resto modulo  $p$  che risultano elementi primitivi; tuttavia, dato un numero primo  $p$  piccolo, possiamo trovare un elemento primitivo per tentativi.

Possiamo ora elencare gli elementi non nulli di  $\mathbb{F}_p$  in due modi, mediante l'addizione e mediante la moltiplicazione:

$$(6.7) \quad \mathbb{F}_p^* = \{1, 2, 3, \dots, p-1\} = \{1, \nu, \nu^2, \dots, \nu^{p-2}\},$$

dove  $\nu$  è un elemento primitivo modulo  $p$ . A seconda dei casi l'una o l'altra forma sarà preferibile per i calcoli.

Naturalmente, il gruppo additivo  $\mathbb{F}_p(+)$  del campo primo è sempre un gruppo ciclico di ordine  $p$ . Entrambe le strutture del campo primo, quella additiva e quella moltiplicativa, sono molto semplici: sono cicliche. Ma la struttura di campo di  $\mathbb{F}_p$ , governata dalla proprietà distributiva, le combina tra loro in modo misterioso.

La parte (e) del teorema è anch'essa sorprendente. È il punto di partenza per molti metodi di fattorizzazione dei polinomi modulo  $p$ . Vediamo ad esempio alcuni casi in cui  $q$  è una potenza di 2:

### (6.8) Esempi

(a) Gli elementi del campo  $\mathbb{F}_4$  sono le radici del polinomio:

$$(6.9) \quad x^4 - x = x(x-1)(x^2 + x + 1).$$

In questo caso, i fattori irriducibili di  $x^4 - x$  in  $\mathbb{Z}[x]$  rimangono irriducibili in  $\mathbb{F}_2[x]$ . Si noti che qui compaiono i fattori di  $x^2 - x$  poiché  $\mathbb{F}_4$  contiene  $\mathbb{F}_2$ . Poiché stiamo lavorando in caratteristica 2, i segni non hanno importanza, sicché ad esempio  $x - 1 = x + 1$ .

(b) Il campo  $\mathbb{F}_8$  di ordine 8 ha grado 3 sul campo primo  $\mathbb{F}_2$ . I suoi elementi sono le otto radici del polinomio:

$$(6.10) \quad x^8 - x = x(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1), \quad \text{in } \mathbb{F}_2[x].$$

Pertanto i sei elementi di  $\mathbb{F}_8$  che non appartengono a  $\mathbb{F}_2$  si dividono in due classi: le tre radici di  $x^3 + x + 1$  e le tre radici di  $x^3 + x^2 + 1$ .

I fattori cubici di (6.10) sono i due polinomi irriducibili di grado 3 in  $\mathbb{F}_2[x]$  [cfr. cap. 11 (4.3)]. La scomposizione in fattori irriducibili di questo polinomio nell'anello  $\mathbb{Z}[x]$  è la seguente:

$$(6.11) \quad x^8 - x = x(x - 1)(x^6 + x^5 + \dots + x + 1).$$

Il terzo fattore è riducibile modulo 2.

Per fare i calcoli nel campo  $\mathbb{F}_8$ , scegliamo una radice  $\beta$  di uno dei fattori cubici, ad esempio, di  $x^3 + x + 1$ . Allora  $(1, \beta, \beta^2)$  è una base di  $\mathbb{F}_8$  come spazio vettoriale su  $\mathbb{F}_2$ . Gli elementi di  $\mathbb{F}_8$  sono le otto combinazioni lineari con coefficienti 0, 1:

$$(6.12) \quad \mathbb{F}_8 = \{0, 1, \beta, 1 + \beta, \beta^2, 1 + \beta^2, \beta + \beta^2, 1 + \beta + \beta^2\}.$$

I calcoli in  $\mathbb{F}_8$  si effettuano utilizzando la relazione  $\beta^3 + \beta + 1 = 0$ .

Conviene notare che  $\mathbb{F}_4$  non è contenuto in  $\mathbb{F}_8$ , infatti  $[\mathbb{F}_8 : \mathbb{F}_2] = 3$ ,  $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ , e 2 non divide 3.

(c) Il campo  $\mathbb{F}_{16}$  si costruisce a partire dal polinomio  $x^{16} - x = x(x^{15} - 1)$ , il quale è divisibile in  $\mathbb{Z}[x]$  per  $x^3 - 1$  e per  $x^5 - 1$ . Effettuando la divisione in  $\mathbb{Z}[x]$ , si ottiene la seguente fattorizzazione:

$$(6.13) \quad \begin{aligned} x^{16} - x &= \\ &= x(x - 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1). \end{aligned}$$

Questa è la scomposizione in fattori irriducibili in  $\mathbb{Z}[x]$ . Ma in  $\mathbb{F}_2[x]$ , il fattore di grado 8 non è irriducibile, e risulta:

$$(6.14) \quad \begin{aligned} x^{16} - x &= \\ &= x(x - 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1). \end{aligned}$$

In questa fattorizzazione compaiono i tre polinomi irriducibili di grado 4 in  $\mathbb{F}_2[x]$ . Inoltre, compaiono i fattori di  $x^4 - x$ , in accordo col fatto che  $\mathbb{F}_{16}$  contiene  $\mathbb{F}_4$ . ■

Cominceremo ora la dimostrazione del teorema (6.4), dimostrando i vari enunciati nel seguente ordine: (d), (c), (a), (b), (e), (f).

*Dimostrazione di (6.4d).* Sia  $K$  un campo di ordine  $q$ . Il gruppo moltiplicativo  $K^*$  ha ordine  $q - 1$ . Pertanto l'ordine di qualsiasi elemento  $\alpha \in K^*$  divide  $q - 1$ , sicché  $\alpha^{q-1} = 1$ . Ciò significa che  $\alpha$  è una radice del polinomio  $x^{q-1} - 1$ . L'elemento restante in  $K$ , ossia lo zero, è la radice del polinomio  $x$ . Pertanto ogni elemento di  $K$  è una radice di  $x(x^{q-1} - 1) = x^q - x$ . Questo polinomio, avendo  $q$  radici distinte in  $K$ , si scomponete in fattori lineari in  $K[x]$ :

$$(6.15) \quad x^q - x = \prod_{\alpha \in K} (x - \alpha).$$

Ciò dimostra la parte (d) del teorema. ■

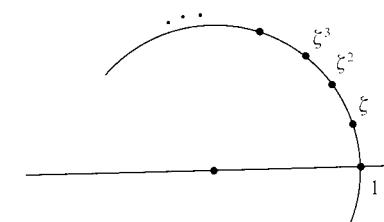
*Dimostrazione di (6.4c).* Per radice  $n$ -esima dell'unità in un campo  $F$ , si intende un elemento  $\alpha$  tale che  $\alpha^n = 1$ . Pertanto  $\alpha$  è una radice  $n$ -esima dell'unità se e soltanto se  $\alpha$  è una radice del polinomio:

$$(6.16) \quad x^n - 1,$$

ossia se e soltanto se il suo ordine, come elemento del gruppo moltiplicativo  $F^*$ , divide  $n$ . Gli elementi non nulli di un campo finito con  $q$  elementi sono le  $(q - 1)$ -esime radici dell'unità.

Nel campo dei numeri complessi, le radici  $n$ -esime dell'unità formano un gruppo ciclico di ordine  $n$  generato da

$$(6.17) \quad \zeta_n = e^{2\pi i/n} :$$



Un campo non ha necessariamente molte radici dell'unità. Per esempio, le uniche radici reali dell'unità sono  $\pm 1$ . C'è tuttavia una proprietà dei numeri complessi che vale per un campo qualsiasi: in un campo le radici  $n$ -esime dell'unità formano

un gruppo ciclico. Per esempio, nel campo  $K = \mathbb{F}_4$ , di ordine 4, il gruppo  $K^*$  è un gruppo ciclico di ordine 3, generato da  $\alpha$  [cfr. (6.3)].

(6.18) PROPOSIZIONE *Sia  $F$  un campo e sia  $H$  un sottogruppo finito di ordine  $n$  del gruppo moltiplicativo  $F^*$ . Allora  $H$  è un gruppo ciclico, ed è costituito da tutte le radici  $n$ -esime dell'unità in  $F$ .*

*Dimostrazione.* Se  $H$  ha ordine  $n$  l'ordine di un elemento  $\alpha$  di  $H$  divide  $n$ , sicché  $\alpha$  è una radice  $n$ -esima dell'unità, ossia una radice del polinomio  $x^n - 1$ . Tale polinomio ha al più  $n$  radici, e pertanto non vi sono altre radici in  $F$  [cap. 11 (1.18)]. Ne segue che  $H$  è l'insieme di tutte le radici  $n$ -esime dell'unità in  $F$ .

È più difficile dimostrare che  $H$  è ciclico. A questo scopo, utilizziamo il teorema di struttura per i gruppi abeliani, il quale ci dice che  $H$  è isomorfo a un prodotto diretto di gruppi ciclici:

$$H \approx \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k),$$

dove  $d_1|d_2 \cdots |d_k$  e  $n = d_1 \cdots d_k$ . L'ordine di qualunque elemento di questo prodotto divide  $d_k$ , poiché  $d_k$  è un multiplo comune di tutti gli interi  $d_i$ . Pertanto ogni elemento di  $H$  è una radice del polinomio  $x^{d_k} - 1$  che ha al più  $d_k$  radici in  $F$ . Ma  $H$  contiene  $n$  elementi e inoltre  $n = d_1 \cdots d_k$ . Allora l'unica possibilità è che  $n = d_k$ , con  $k = 1$ , e quindi  $H$  è ciclico. ■

*Dimostrazione di (6.4a).* Dobbiamo dimostrare che esiste un campo con  $q$  elementi. Poiché abbiamo già dimostrato la parte (d) del teorema, sappiamo che gli elementi di un campo di ordine  $q$  sono radici del polinomio  $x^q - x$ . Inoltre, esiste un campo  $L$  contenente  $\mathbb{F}_p$  in cui questo polinomio (o qualunque polinomio assegnato) si scomponga in fattori lineari (5.3). Allora la cosa più naturale è prendere le radici di  $x^q - x$  in  $L$  e sperare che formino il campo  $K$  che stiamo cercando. Ciò è quanto afferma la seguente proposizione:

(6.19) PROPOSIZIONE *Sia  $p$  un numero primo, e sia  $q = p^r$ .*

- (a) *Il polinomio  $x^q - x$  non ha radici multiple in nessun campo  $L$  di caratteristica  $p$ .*
- (b) *Sia  $L$  un campo di caratteristica  $p$ , e sia  $K$  l'insieme delle radici di  $x^q - x$  in  $L$ . Allora  $K$  è un sottocampo di  $L$ .*

Unitamente alla proposizione (5.3), la (6.19) dimostra che esiste un campo con  $q$  elementi.

*Dimostrazione della proposizione (6.19).* (a) La derivata di  $x^q - x$  è  $qx^{q-1} - 1$ . In caratteristica  $p$ , il coefficiente  $q$  è uguale a 0, sicché la derivata è uguale a  $-1$ .

Poiché il polinomio costante  $-1$  non ha radici, il polinomio  $x^q - x$  e la sua derivata non hanno radici comuni! Allora, in virtù della proposizione (5.7),  $x^q - x$  non ha radici multiple.

(b) Siano  $\alpha, \beta \in L$  radici del polinomio  $x^q - x$ . Dobbiamo far vedere che  $\alpha \pm \beta$ ,  $\alpha\beta$  e  $\alpha^{-1}$  (se  $\alpha \neq 0$ ) sono radici dello stesso polinomio. Ciò è chiaro per il prodotto e per il quoziente, ossia, se  $\alpha^q = \alpha$  e  $\beta^q = \beta$ , allora  $(\alpha\beta)^q = \alpha\beta$  e  $(\alpha^{-1})^q = \alpha^{-1}$ . Per la somma è meno ovvio, e si otterrà come conseguenza della seguente proposizione:

(6.20) PROPOSIZIONE *Sia  $L$  un campo di caratteristica  $p$ , e sia  $q = p^r$ . Allora, nell'anello dei polinomi  $L[x, y]$ , si ha:  $(x+y)^q = x^q + y^q$ .*

*Dimostrazione.* Dimostriamo innanzitutto la proposizione nel caso in cui  $q = p$ . Sviluppiamo la potenza  $(x+y)^p$  in  $\mathbb{Z}[x, y]$ , ottenendo:

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p,$$

in virtù del teorema del binomio. Il coefficiente binomiale  $\binom{p}{r}$  è un intero, e se  $0 < r < p$ , esso è divisibile per  $p$  [cfr. cap. 11, dimostrazione di (4.6)]. Ne segue che l'omomorfismo  $\mathbb{Z}[x, y] \rightarrow L[x, y]$  manda questi coefficienti nello zero e che  $(x+y)^p = x^p + y^p$  in  $L[x, y]$ .

Passiamo ora al caso generale in cui  $q = p^r$ , procedendo per induzione su  $r$ . Supponiamo che la proposizione sia stata dimostrata per gli interi minori di  $r$  e che si abbia  $r > 1$ . Poniamo  $q' = p^{r-1}$ . Allora, in virtù dell'ipotesi induttiva, si ha  $(x+y)^q = ((x+y)^{q'})^p = (x^{q'} + y^{q'})^p = (x^{q'})^p + (y^{q'})^p = x^q + y^q$ . ■

Per completare la dimostrazione della proposizione (6.19), sostituiamo  $x, y$  con  $\alpha, \beta$  e otteniamo:  $(\alpha+\beta)^q = \alpha^q + \beta^q$ . Allora, se  $\alpha^q = \alpha$  e  $\beta^q = \beta$ , risulta:  $(\alpha+\beta)^q = \alpha+\beta$ , come richiesto. La verifica relativa ad  $\alpha-\beta$  si ottiene sostituendo  $\beta$  con  $-\beta$ . ■

*Dimostrazione del teorema (6.4b).* Siano  $K$  e  $K'$  campi di ordine  $q$ , e sia  $\alpha$  un generatore del gruppo ciclico  $K^*$ . Allora  $K$  è certamente generato, come estensione di campi di  $F = \mathbb{F}_p$ , dall'elemento  $\alpha$ , ossia  $K = F(\alpha)$ . Sia  $f(x)$  il polinomio minimo di  $\alpha$  su  $F$ , sicché  $K \approx F[x]/(f)$ , in virtù di (2.6). Allora  $\alpha$  è radice di due polinomi,  $f(x)$  e  $x^q - x$ . Poiché  $f$  è irriducibile, esso divide  $x^q - x$ , in base a (5.4e). Passiamo ora al campo  $K'$ . Poiché  $x^q - x$  si scomponga in fattori lineari in  $K'$ ,  $f$  ha una radice  $\alpha'$  in  $K'$ . Allora si ha:  $K \approx F[x]/(f) \approx F(\alpha')$ . Poiché  $K$  e  $K'$  hanno lo stesso ordine, risulta  $F(\alpha') = K'$ ; pertanto  $K$  e  $K'$  sono isomorfi. ■

*Dimostrazione del teorema (6.4e).* Sia  $f(x)$  un polinomio irriducibile di grado  $r$  in  $F[x]$ , dove  $F = \mathbb{F}_p$  come prima. Esso ha una radice  $\alpha$  in qualche estensione di campi  $L$  di  $F$ , e il sottocampo  $K = F(\alpha)$  di  $L$  ha grado  $r$  su  $F$  (3.2). Pertanto  $K$  ha ordine  $q = p^r$ , e in base alla parte (d) del teorema,  $\alpha$  è anche radice di  $x^q - x$ . Poiché  $f$  è irriducibile,  $f$  divide  $x^q - x$ , come richiesto.

Per dimostrare la stessa proprietà per i polinomi irriducibili il cui grado  $k$  divide  $r$ , basta dimostrare il lemma seguente:

(6.21) LEMMA *Sia  $k$  un divisore intero di  $r$ , ad esempio  $r = ks$ , e poniamo  $q = p^r$ ,  $q' = p^k$ . Allora  $x^{q'} - x$  divide  $x^q - x$ .*

Infatti, se  $f$  è un polinomio irriducibile di grado  $k$ , allora, come prima,  $f$  divide  $x^{q'} - x$ , che a sua volta divide  $x^q - x$  in  $F[x]$ , per ogni campo  $F$ .

*Dimostrazione.* La dimostrazione è ingegnosa, poiché useremo due volte l'identità:

$$(6.22) \quad y^d - 1 = (y - 1)(y^{d-1} + \cdots + y + 1).$$

Ponendo  $y = q'$  e  $d = s$ , otteniamo che  $q' - 1$  divide  $q - 1 = q'^s - 1$ . Allora, ponendo  $y = x^{q'-1}$  e  $d = (q-1)/(q'-1)$  possiamo concludere che  $x^{q'-1} - 1$  divide  $x^q - 1$ . Pertanto  $x^{q'} - x$  divide  $x^q - x$ . ■

Abbiamo dunque dimostrato che ogni polinomio irriducibile il cui grado divide  $r$  è un fattore di  $x^q - x$ . D'altra parte, se  $f$  è irriducibile e il suo grado  $k$  non divide  $r$ , allora, dato che  $[K : F] = r$ ,  $f$  non ha radici in  $K$  e pertanto non divide  $x^q - x$ . ■

*Dimostrazione del teorema (6.4f).* Se  $k$  non divide  $r$ , allora  $q = p^r$  non è una potenza di  $q' = p^k$ , e pertanto un campo di ordine  $q$  non può essere un'estensione di un campo di ordine  $q'$ . D'altra parte, se  $k$  divide  $r$ , il lemma (6.21) e la parte (d) del teorema mostrano che il polinomio  $x^{q'} - x$  ha tutte le sue radici in un campo  $K$  di ordine  $q$ . Ne segue, in virtù della proposizione (6.19), che  $K$  contiene un campo con  $q'$  elementi. ■

Ciò completa la dimostrazione del teorema (6.4).

## 7 Campi di funzioni

In questo paragrafo daremo uno sguardo ai *campi di funzioni*, che costituiscono la terza classe di estensioni di campi menzionata nel paragrafo 1. Il campo  $\mathbb{C}(x)$  delle funzioni razionali in una variabile  $x$  sarà denotato con  $F$  in tutto il paragrafo. I suoi elementi sono quozienti  $g(x) = p(x)/q(x)$  di polinomi  $p, q \in \mathbb{C}[x]$ , con  $q \neq 0$ .

Di solito cancelleremo i fattori comuni in  $p$  e  $q$ , sicché essi non avranno radici comuni.

Useremo il simbolo  $P$  per denotare il piano complesso, con la coordinata complessa  $x$ . Una funzione razionale  $g = p/q$  individua una funzione di  $x$  a valori complessi, la quale è definita per ogni  $x \in P$  tale che  $q(x) \neq 0$ , ossia, tranne che nelle radici del polinomio  $q$ . In prossimità di una radice di  $q$ , la funzione definita da  $g$  tende all'infinito. Tali radici sono chiamate *poli* di  $g$ . (Di solito, usiamo l'espressione "funzione razionale" per indicare un elemento del campo delle frazioni dell'anello dei polinomi. Purtroppo, in tale espressione è già presente il termine *funzione*. Ciò ci impedisce di modificare l'espressione in modo naturale, quando vogliamo riferirci proprio alla funzione definita da un quoziente di polinomi. La terminologia è ambigua, ma ciò è inevitabile).

Qui si presenta una complicazione minore, poiché in certi punti, precisamente nei loro poli, le funzioni razionali formali non definiscono funzioni. Quando lavoriamo con l'intero campo  $F$ , dobbiamo accettare il fatto che ogni valore  $\alpha$  di  $x$  può essere un polo di una funzione razionale, per esempio, della funzione  $(x - \alpha)^{-1}$ . È impossibile scegliere un dominio in cui tutte le funzioni razionali siano definite, nello stesso tempo. Per fortuna, il problema può essere aggirato. È possibile ad esempio introdurre un nuovo valore,  $\infty$ , e porre per definizione  $g(\infty) = \infty$  se  $\alpha$  è un polo di  $g$ . In molti casi, questa è in effetti la soluzione migliore, ma ce n'è una più comoda, che consiste semplicemente nell'ignorare il cattivo comportamento della funzione in un numero finito di punti.

Tutti i calcoli particolari che dovremo effettuare riguarderanno un numero finito di funzioni, sicché essi saranno validi tranne che in un insieme finito di punti del piano  $P$ , cioè i poli di queste funzioni. Una funzione razionale è determinata dai suoi valori in un qualunque insieme infinito di punti (la dimostrazione è data qui sotto, nel lemma (7.2)), possiamo dunque escludere degli insiemi finiti di punti dal dominio di definizione, se necessario, senza perdere il controllo della funzione. Poiché una funzione razionale è continua in ogni punto in cui è definita, possiamo riottenere il suo valore in un punto  $x_0$  che fosse stato escluso per sbaglio, mediante la relazione

$$(7.1) \quad g(x_0) = \lim_{x \rightarrow x_0} g(x).$$

(7.2) LEMMA *Se due funzioni razionali  $f_1, f_2$  assumono gli stessi valori in infiniti punti del piano, allora, considerate come elementi di  $F$ , coincidono.*

*Dimostrazione.* Scriviamo  $f_i = p_i/q_i$ , con  $p_i, q_i \in \mathbb{C}[t]$ . Poniamo  $h(x) = p_1q_2 - p_2q_1$ . Se  $h(x)$  è il polinomio nullo, allora  $f_1 = f_2$ . Se  $h(x)$  non è nullo, allora ha un numero finito di radici, sicché esiste soltanto un numero finito di punti in cui  $f_1 = f_2$ . ■

Per formalizzare il procedimento intuitivo di ignorare le difficoltà relative ad insiemi finiti di punti, conviene avere una notazione per l'insieme ottenuto ad eliminando un insieme finito. Dato un insieme infinito  $U$ , denoteremo con  $U'$  un insieme ottenuto da  $U$  eliminando un generico sottoinsieme finito, variabile a seconda delle necessità:

$$(7.3) \quad U' = U - (\text{sottoinsieme finito non precisato}).$$

Chiameremo *funzione* su  $U'$  una classe di equivalenza di funzioni a valori complessi definite tranne che in un sottoinsieme finito di  $U$ . Due funzioni siffatte  $f, g$  si dicono *uguali* su  $U'$  se esiste un sottoinsieme finito  $\Delta$  di  $U$  tale che  $f$  e  $g$  siano definite e uguali su  $U - \Delta$ . (Potremmo anche enunciare questa proprietà dicendo che  $f = g$  quasi ovunque su  $U$ ). Tuttavia, in altri contesti matematici, "quasi ovunque" spesso significa "tranne che in un insieme di misura nulla", piuttosto che "tranne che in un insieme finito"). Una funzione  $f$  su  $U'$  sarà detta *continua* se è rappresentata da una funzione continua su qualche insieme  $U - \Delta$ .

L'insieme delle funzioni continue su  $U'$  sarà denotato con  $\mathcal{F}(U)$ :

$$(7.4) \quad \mathcal{F}(U) = \{\text{funzioni continue su } U'\}.$$

Questo insieme forma un anello, rispetto alle operazioni usuali di addizione e moltiplicazione di funzioni:

$$(7.5) \quad [f+g](x) = f(x) + g(x) \quad \text{e} \quad [fg](x) = f(x)g(x).$$

Il lemma (7.2) ha il seguente corollario:

(7.6) PROPOSIZIONE *Il campo  $F = \mathbb{C}(x)$  è isomorfo a un sottoanello dell'anello  $\mathcal{F}(P)$ , dove  $P$  è il piano complesso.* ■

Esaminiamo ora in dettaglio uno dei più semplici campi di funzioni. Avremo bisogno di polinomi a coefficienti nel campo  $F$ . Poiché il simbolo  $x$  è stato già assegnato, useremo  $y$  per denotare la nuova variabile. Studieremo l'estensione quadratica ottenuta a partire dal campo  $F$  aggiungendo una radice di  $f(y)$ , dove  $f = y^2 - x$ . Poiché  $f$  dipende sia dalla variabile  $x$  che dalla variabile  $y$ , scriveremo anche

$$(7.7) \quad f = f(x, y) = y^2 - x.$$

Il polinomio  $y^2 - x$  è un elemento irriducibile di  $F[y]$ , sicché  $K$  può essere costruito come il campo astratto  $F[y]/(f)$ . La classe resto della variabile  $y$  è una radice di  $f$  in  $K$ .

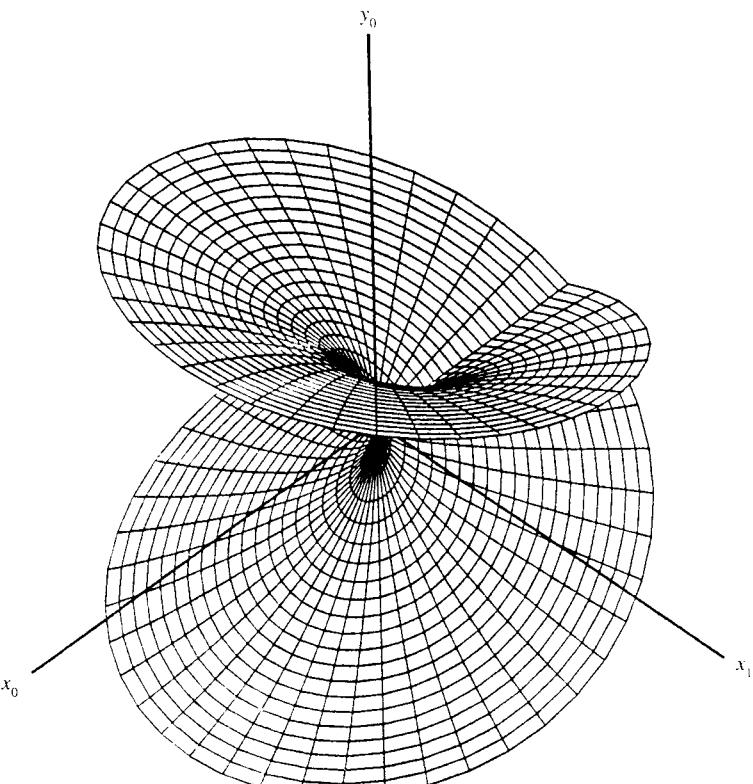
L'importanza dei campi di funzioni proviene dal fatto che i loro elementi possono essere interpretati come vere funzioni. Nel nostro caso, possiamo definire una *funzione* radice quadrata  $h$ , scegliendo, per ogni numero complesso  $x$ , uno

dei due valori della radice:  $h(x) = \sqrt{x}$ . Allora  $h$  può essere interpretata come una funzione su  $P'$ . Tuttavia, poiché vi sono due valori della radice quadrata per ogni  $x \neq 0$ , dobbiamo fare delle scelte arbitrarie per definire questa funzione. Ciò non è molto soddisfacente. Se  $x$  è reale positivo, è naturale scegliere la radice quadrata positiva, ma nessuna scelta darà una funzione continua sull'intero piano complesso.

Il luogo  $S$  delle soluzioni dell'equazione  $y^2 - x = 0$  in  $\mathbb{C}^2$  è detto *superficie di Riemann* del polinomio  $y^2 - x$  [cfr. cap. 10, § 8]. Esso è rappresentato nella figura (7.9), ove tuttavia, per ottenere una superficie nello spazio reale di dimensione 3, abbiamo eliminato una coordinata. Lo spazio complesso  $\mathbb{C}^2$  viene identificato con  $\mathbb{R}^4$  nel solito modo:  $(x, y) = (x_0 + x_1 i, y_0 + y_1 i) \leftrightarrow (x_0, x_1, y_0, y_1)$ . La figura rappresenta il luogo

$$(7.8) \quad \{(x_0, x_1, y_0) \mid y_0 = \text{parte reale di } (x_0 + x_1 i)^{1/2}\}.$$

Esso è una proiezione di  $S$  da  $\mathbb{R}^4$  a  $\mathbb{R}^3$ .



La superficie di Riemann  $y^2 = x$ .

La superficie di Riemann  $S$  non interseca se stessa lungo il semiasse negativo dell'asse  $x_0$ , come la superficie proiezione. Ogni numero reale negativo  $x$  ha due radici quadrate date da numeri immaginari puri, cioè numeri complessi aventi la parte reale uguale a zero. Ciò produce l'apparente autointersezione nella superficie proiezione. In effetti in base alla definizione data nel capitolo 10 (8.13),  $S$  è un rivestimento ramificato a due fogli di  $P$ , e l'unico punto di ramificazione è  $x=0$ .

La figura (7.9) mostra il problema che si presenta quando cerchiamo di definire la radice quadrata come funzione univoca. Quando  $x$  è reale e positivo, la radice quadrata positiva è la scelta naturale. Vorremmo poter estendere questa scelta in modo continuo sul piano complesso, ma ci imbattiamo in una difficoltà: facendo un giro intorno all'origine nel piano complesso della variabile  $x$ , ritorniamo alla radice quadrata negativa. È preferibile accettare che la radice quadrata, come soluzione dell'equazione  $y^2 - x = 0$ , sia una funzione a più valori su  $P'$ .

Ora, esiste un artificio sorprendente che ci permetterà di risolvere qualunque equazione polinomiale  $f(x, y) = 0$  con una funzione *univoca*, senza fare scelte arbitrarie. L'artificio consiste nel sostituire il piano complesso  $P$  con la superficie di Riemann  $S$ , ossia il luogo  $f(x, y) = 0$ . Abbiamo due funzioni su  $S$ , precisamente le restrizioni delle funzioni coordinate su  $\mathbb{C}^2$ . Per ragioni di chiarezza, le indichiamo con nuovi simboli, ad esempio  $X, Y$ :

$$(7.10) \quad X(x, y) = x \quad \text{e} \quad Y(x, y) = y, \quad \text{per } (x, y) \in S.$$

Queste restrizioni delle funzioni coordinate a  $S$  sono legate dall'equazione  $f(X, Y) = 0$ , in quanto in base alla definizione di  $S$ , si ha  $f(x, y) = 0$  in ogni punto di  $S$ .

(7.11) PROPOSIZIONE *Sia  $f(x, y)$  un polinomio irriducibile in  $\mathbb{C}[x, y]$  che non sia un polinomio nella sola  $x$ , e sia  $S = \{(x, y) | f(x, y) = 0\}$  la sua superficie di Riemann. Sia  $K = F[y]/(f)$  l'estensione di campi definita da  $f$ . Allora  $K$  è isomorfo a un sottoanello dell'anello  $\mathcal{F}(S)$  delle funzioni continue su  $S'$ .*

*Dimostrazione.* Sia  $g(x)$  una funzione razionale. Poiché  $X$  è la restrizione di una funzione coordinata su  $\mathbb{C}^2$ , la funzione composta  $g(X)$  è continua su  $S$ , tranne che nei punti che giacciono sopra i poli di  $g$ . Vi è un numero finito di questi punti [cap. 10 (8.11)], e pertanto  $g(X)$  è una funzione continua su  $S'$ . Definiamo un omomorfismo  $F \rightarrow \mathcal{F}(S)$  mandando  $g(x)$  in  $g(X)$ . Il principio di sostituzione estende questa applicazione a un omomorfismo

$$(7.12) \quad \varphi : F[y] \rightarrow \mathcal{F}(S),$$

mandando  $y$  in  $Y$ . Poiché  $f(X, Y) = 0$ , il polinomio  $f(x, y)$  appartiene al nucleo di  $\varphi$ . Poiché  $K = F[y]/(f)$ , la proprietà di rappresentazione dei quozienti [cap. 10 (4.2)] ci dà un omomorfismo  $\bar{\varphi} : K \rightarrow \mathcal{F}(S)$  che manda la classe resto di  $y$  in  $Y$ . Poiché  $K$  è un campo,  $\bar{\varphi}$  è iniettivo. ■

(7.13) DEFINIZIONE *Un isomorfismo di rivestimenti ramificati  $S_1, S_2$  del piano  $P$  è un omeomorfismo  $\varphi' : S'_1 \rightarrow S'_2$  compatibile con le applicazioni  $\pi_i : S_i \rightarrow P$ , ossia tale che  $\pi'_2 \circ \varphi' = \pi'_1$ :*

$$\begin{array}{ccc} S'_1 & \xrightarrow{\varphi'} & S'_2 \\ \pi'_1 \searrow & & \swarrow \pi'_2 \\ & P & \end{array}$$

Ciò significa che  $\varphi'$  è definito tranne che su un sottoinsieme finito di  $S'_1$  e che, eliminando sottoinsiemi finiti opportuni in  $S'_1$  e  $S'_2$ ,  $\varphi'$  è un omeomorfismo.

Un rivestimento ramificato  $S$  si dice *connesso* se il sottoinsieme complementare  $S'$  di un sottoinsieme finito arbitrario di  $S$  è connesso per archi.

Enunciamo ora un bel teorema che descrive le estensioni finite del campo delle funzioni razionali. Denotiamo con  $\mathcal{E}_n$  l'insieme delle classi di isomorfismo delle estensioni  $K$  di  $F$  di grado  $n$  e con  $\mathcal{C}_n$  l'insieme delle classi di isomorfismo dei rivestimenti ramificati a  $n$  fogli, connessi  $\pi : S \rightarrow P$  del piano.

(7.14) TEOREMA DI ESISTENZA DI RIEMANN *Esiste un'applicazione biettiva  $\Phi_n : \mathcal{E}_n \rightarrow \mathcal{C}_n$ . Se  $K$  è l'estensione ottenuta aggiungendo una radice di un polinomio irriducibile  $f(x, y) \in \mathbb{C}[x, y]$ , allora la classe dei rivestimenti ramificati corrispondente a  $K$  è rappresentata dalla superficie di Riemann di  $f$ .*

La dimostrazione è un argomento più consono a un corso di analisi complessa, e pertanto la tralasciamo. Tuttavia questo teorema è importante perché consente di associare un rivestimento ramificato del piano, definito a meno di isomorfismi, ad ogni estensione finita  $K$  di  $F$ . Tale rivestimento è denominato la *superficie di Riemann dell'estensione  $K$* . La superficie di Riemann di  $F$  è il piano complesso  $P$  stesso.

Vediamo ora due notevoli conseguenze del teorema:

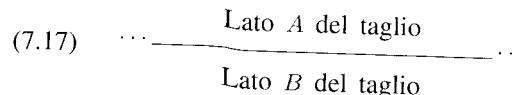
(7.15) COROLLARIO *Sia  $S$  un rivestimento ramificato a  $n$  fogli connesso del piano. Allora esiste un polinomio  $f(x, y)$  di grado  $n$  in  $y$ , la cui superficie di Riemann è isomorfa a  $S$ .*

Ciò segue dalla suriettività dell'applicazione  $\Phi_n$  e dal fatto [cfr. cap. 14 (4.1)], che ogni estensione finita  $K$  di  $F$  può essere ottenuta aggiungendo un solo elemento. ■

(7.16) COROLLARIO *Siano  $f, g$  polinomi irriducibili in  $\mathbb{C}[x, y]$ , con superfici di Riemann  $S, T$ . Sia  $\alpha$  una radice di  $f(y)$  in un'estensione di  $F$ . Se  $S$  e  $T$  sono rivestimenti ramificati isomorfi, allora  $g(y)$  ha una radice in  $F(\alpha)$ .*

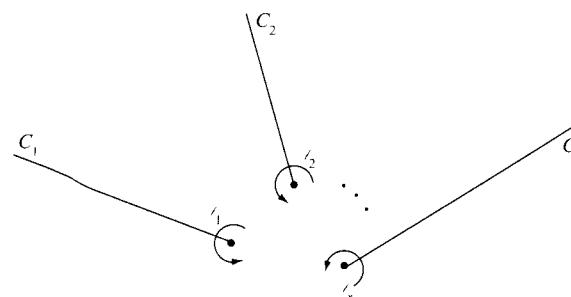
Ciò segue dall'iniettività dell'applicazione  $\Phi_n$ . ■

La visualizzazione delle superfici di Riemann è complicata dal fatto che esse sono immerse in  $\mathbb{C}^2$ , che è uno spazio reale di dimensione 4. Un aiuto per costruire e visualizzare tali superfici è fornito dal cosiddetto metodo *taglia e incolla*. Se tagliamo la superficie  $y^2 - x$  lungo il semiasse negativo dell'asse reale, ossia il luogo doppio nella (7.9), essa si decomponne nelle due parti  $\operatorname{re} Y < 0$  e  $\operatorname{re} Y > 0$ . Ciascuna di queste parti si proietta sul piano  $P$  della variabile  $x$  in modo biunivoco tranne che lungo il taglio. Con questo procedimento possiamo costruire una superficie omeomorfa a  $S$  nel modo che ora illustreremo. Sovrapponiamo a  $P$  due copie  $P_1, P_2$  di  $P$  e tagliamole lungo il semiasse negativo dell'asse reale a  $(-\infty, 0]$ . Tali copie di  $P$  vengono chiamate *fogli*. Incolliamo poi il lato  $A$  di  $P_1$  al lato  $B$  di  $P_2$  e viceversa [cfr. fig. (7.17)]. Per immergere  $S$  senza che vi siano intersezioni, sono necessarie quattro dimensioni.



Per costruire, in generale, un rivestimento ramificato  $S$  del piano col procedimento "taglia e incolla", partiamo da  $n$  fogli  $P_1, \dots, P_n$  e sovrapponiamoli a  $P$ . Inoltre scegliamo un insieme finito di punti  $\alpha_1, \dots, \alpha_r$  di  $P$  come punti di ramificazione. Per ciascun punto  $\alpha_\nu$  scegliamo una curva  $C_\nu$  che parte da  $\alpha_\nu$  e va all'infinito in una direzione arbitraria. Le curve  $C_\nu$  non devono intersecarsi. I fogli  $P_i$  vengono tagliati lungo di esse, e più fogli vengono incollati assieme lungo i lati opposti dei tagli.

Per descrivere il rivestimento  $S$  che così si ottiene, dobbiamo soltanto descrivere le permutazioni  $\sigma_\nu$  secondo cui i fogli sono incollati lungo i tagli. Per essere precisi, disegniamo in senso antiorario un piccolo cappio  $\ell_\nu$  intorno al punto  $\alpha_\nu$ . Se la permutazione  $\sigma_\nu$  manda l'indice 1 in 3, incolliamo il foglio  $P_1$  al foglio  $P_3$  mentre attraversiamo  $C_\nu$ . Ciò significa che, se partiamo su  $P_1$  e facciamo un giro lungo il cappio  $\ell_\nu$ , ritorniamo su  $P_3$ . La permutazione  $\sigma_\nu$  può essere qualunque.



I punti  $\alpha_\nu$  sono detti *punti di ramificazione* di  $S$ : la superficie infatti si decomponе in  $n$  fogli disgiunti sopra ogni altro punto di  $P$ , ma non avrà  $n$  fogli

disgiunti sopra il punto  $\alpha_\nu$ , a meno che la permutazione  $\sigma_\nu$  non sia l'identità. Se  $\sigma_\nu = 1$ , ciascun foglio viene incollato a se stesso lungo il taglio  $C_\nu$ , che pertanto non era necessario. Tuttavia conviene considerare anche questa possibilità. Diremo che  $\alpha_\nu$  è un vero punto di ramificazione se  $\sigma_\nu \neq 1$ . Alcuni  $\alpha_\nu$  possono non essere veri punti di ramificazione, ma certamente tutti i veri punti di ramificazione si trovano tra gli  $\alpha_\nu$ .

È importante osservare che la numerazione dei fogli è arbitraria e, in particolare, che il concetto di "foglio superiore" non ha alcun significato intrinseco per la superficie di Riemann di un polinomio. Se ci fosse un foglio superiore (rispetto a tutti gli altri), potremmo definire  $y$  come funzione univoca scegliendo il valore su quel foglio. Ma ciò si può fare soltanto quando la superficie di Riemann sia stata "aperta". Questo è il punto fondamentale: muovendoci sulla superficie, finiremo col passare da un foglio a un altro.

Non è difficile stabilire quando due rivestimenti ramificati così costruiti sono isomorfi.

(7.18) PROPOSIZIONE Siano  $S, T$  rivestimenti ramificati costruiti come sopra, aventi gli stessi punti di ramificazione  $\alpha_\nu$  e le stesse curve  $C_\nu$ , ma con insiemi diversi di permutazioni  $(\sigma_1, \dots, \sigma_r)$  e  $(\tau_1, \dots, \tau_r)$ . Allora  $S$  e  $T$  sono rivestimenti isomorfi se e solo se i due insiemi di permutazioni sono coniugati, ossia se e solo se esiste una permutazione  $\rho$  tale che  $\tau_\nu = \rho^{-1} \sigma_\nu \rho$  per ogni  $\nu$ .

*Dimostrazione.* Denotiamo  $\sigma_\nu, C_\nu$  semplicemente con  $\sigma, C$ . La regola è che  $P_i$  viene incollato a  $P_{i\rho}$  lungo  $C$ . Supponiamo di rinumerare i fogli  $P_1, \dots, P_n$ , cambiando gli indici mediante una permutazione  $\rho$ . Per non fare confusione tra i vecchi e i nuovi indici, indichiamo i fogli rinumerati con  $Q_j$ . Per ogni  $i$ ,  $P_i$  verrà ribattezzato  $Q_{i\rho}$ . In base alla regola, dobbiamo incollare  $P_i = Q_{i\rho}$  con  $Q_{i\rho} = P_{i\rho}$ . Utilizzando la sostituzione  $i = j\rho^{-1}$ , risulta che  $Q_j$  va incollato a  $Q_{j\rho^{-1}\sigma\rho}$ . Pertanto la permutazione che descrive questa regola di incollamento è la coniugata  $\rho^{-1}\sigma\rho$  della vecchia permutazione  $\sigma_\nu$ . Poiché il rivestimento non cambia per effetto della rinumerazione, ciò mostra che un insieme coniugato di permutazioni definisce un rivestimento isomorfo.

Viceversa, sia  $\varphi : S \rightarrow T$  un isomorfismo di rivestimenti. Siano  $P_1, \dots, P_n$  i fogli usati per costruire  $S$  e  $Q_1, \dots, Q_n$  i fogli usati per costruire  $T$ . Allora, poiché  $P_i$  è connesso e poiché  $T$ , dopo i tagli, è un'unione disgiunta degli insiemi aperti  $Q_j$ , l'immagine di  $P_i$  deve essere contenuta in un solo foglio  $Q_j$ . Poiché  $\varphi$  è compatibile con le proiezioni su  $P$ , le quali sono degli omeomorfismi tranne che sui tagli, la restrizione di  $\varphi$  a  $P_i$  deve essere una biiezione sul foglio  $Q_j$ . Possiamo dunque rinumerare i fogli  $Q_j$  in modo tale che  $P_i$  venga mandato in  $Q_i$ . Ciò muta le permutazioni  $\tau_\nu$  in permutazioni coniugate, come sopra. Dunque possiamo supporre che  $\varphi$  porti  $P_i$  in  $Q_i$ . Inoltre, l'applicazione  $\varphi$  è continua attraverso i tagli. Ne segue che, se l'attraversamento del taglio  $C_\nu$  sul foglio  $P_i$  conduce a  $P_j$ , allora l'attraversamento sul foglio  $Q_i$  deve condurre a  $Q_j$ . Pertanto  $\sigma_\nu = \tau_\nu$ . ■

Possiamo anche partire da un rivestimento ramificato arbitrario  $S$  e ricostruirlo nel modo seguente. Supponiamo che  $S$  sia ramificato nei punti  $\alpha_1, \dots, \alpha_r \in P$ . Come prima, scegliamo curve  $C_i$  non intersecantisi che hanno origine in  $\alpha_i$  e vanno all'infinito. Allora, se  $S$  viene tagliato lungo le curve  $C_i$ , si decompone in  $n$  fogli. Questo è un teorema di topologia, poiché il sottoinsieme complementare delle curve  $C_i$  in  $P$  è semplicemente connesso.\* Pertanto un rivestimento omeomorfo a  $S$  può essere ricostruito a partire da  $n$  fogli  $P_1, \dots, P_n$ , aprendo tali fogli lungo le curve e poi incollandoli insieme per mescolarli.

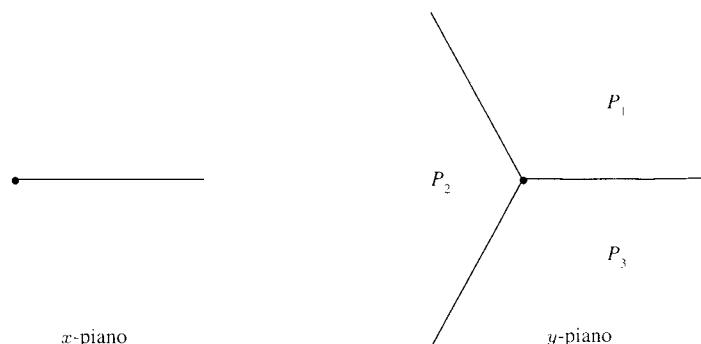
Descriptoremo ora le superfici di Riemann di alcuni semplici polinomi (se il polinomio è complicato la cosa non è così facile!).

#### (7.19) Esempio

Consideriamo la superficie di Riemann di  $y^3 - x$ . In questo caso,  $y$  è una radice cubica di  $x$  e  $S$  è un rivestimento a tre fogli di  $P$ . L'unico punto di ramificazione è  $x = 0$ . Tagliamo  $S$  lungo il semiasse positivo dell'asse reale  $C = [0, \infty)$ . In tal modo  $S$  si decompone in tre fogli  $P_1, P_2, P_3$ , ed è ragionevole supporre che l'incollamento lungo il taglio sia fatto mediante una permutazione ciclica.

Questo caso è abbastanza facile da analizzare, poiché  $x$  è una funzione univoca di  $y$ . Possiamo allora interpretare  $S$  come il grafico di una funzione dal piano della variabile  $y$  (o  $y$ -piano) al piano della variabile  $x$  (o  $x$ -piano), il che implica che la proiezione di  $S$  sul piano della variabile complessa  $y$  è biiettiva. Identifichiamo pertanto  $S$  con il piano della variabile  $y$  e tagliamo il piano lungo  $C$ . In tal modo il piano si decomporrà in tre parti, corrispondenti ai fogli  $P_i$ . Le regole per l'incollamento saranno evidenti quando tale decomposizione sarà resa esplicita.

I valori di  $y$  situati sopra il taglio  $C$  sono quelli per i quali  $y^3 = x$  è reale e positivo. Essi sono dati da  $y = re^{i\theta}$ , dove  $\theta = 0, 2\pi/3, 4\pi/3$ . Pertanto i fogli sono dei settori.



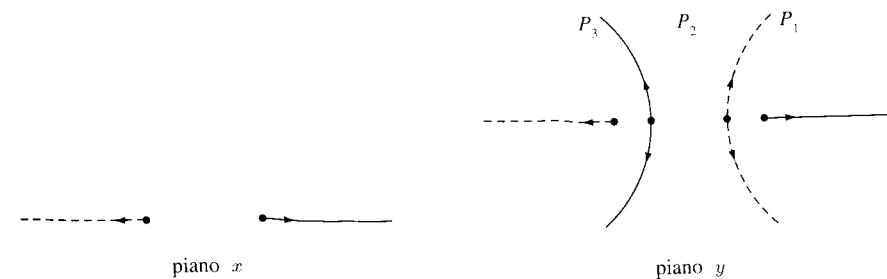
\* J.R. Munkres, *Topology: A First Course*, Prentice Hall, Englewood Cliffs (NJ) 1975, p. 342, esercizio 8.

Nella figura, i settori sono stati numerati in modo arbitrario. Mediante l'applicazione  $y \mapsto y^3 = x$ , ciascun settore viene dilatato in senso radiale e, tranne che sul taglio, mandato biunivocamente sull'intero piano. Quando, muovendoci lungo  $S$ , attraversiamo il taglio nell' $x$ -piano, attraversiamo anche uno dei tre tagli nell' $y$ -piano. Come previsto, ciò permette i fogli con la permutazione ciclica (123). ■

#### (7.20) Esempio

Consideriamo la superficie di Riemann di  $f(x, y) = y^3 - 3y - x$ . I punti  $x$  in cui questo polinomio ha meno di tre radici si trovano risolvendo il sistema formato dalle equazioni  $f = 0$ ,  $\partial f / \partial y = 0$  [cfr. cap. 10 (8.12)]. Nel nostro caso,  $\partial f / \partial y = 3(y^2 - 1)$ . Pertanto le soluzioni sono  $y = \pm 1$ , e quindi  $x = \pm 2$ . Possiamo tagliare  $S$  lungo le curve  $C_1 = (-\infty, -2]$  e  $C_2 = [2, \infty)$ , per decomporlo in tre fogli.

Di nuovo,  $x$  è una funzione univoca di  $y$ , e possiamo analizzare l'incollamento dei fogli tagliando il piano della variabile  $y$  in modo opportuno. Per fare ciò, cerchiamo i valori di  $y$  tali che  $x$  appartenga a una delle curve  $C_i$ . Poiché tali curve sono situate sull'asse reale del piano della variabile  $x$ , cominciamo a risolvere l'equazione  $\text{im } x = 0$ . Ponendo  $y = u + vi$ , otteniamo  $\text{im } x = \text{im}(y^3 - 3y) = v(3u^2 - v^2 - 3)$ . Le soluzioni sono l'asse  $u$  di equazione  $v = 0$  e i due rami dell'iperbole di equazione  $3u^2 - v^2 = 3$ . I punti sull'asse  $u$  nell'intervallo  $(-2, 2)$  corrispondono ai punti  $x \in (-2, 2)$ , e dunque non giacciono sopra i tagli.



Di nuovo, ciascuna delle tre regioni in cui si decompone il piano della variabile  $y$  viene mandato biiettivamente (ignorando come sempre il taglio), sul piano della variabile  $x$ , mediante la funzione  $y^3 - 3y$ . Nella figura, le curve tratteggiate sono quelle che giacciono sopra  $C_1$ . La figura mostra che, se ci muoviamo su  $S$  per attraversare la curva  $(-\infty, -2]$ , i fogli  $P_1, P_2$  si scambiano tra loro, mentre  $P_3$  resta invariato, e analogamente, che l'attraversamento sopra la curva  $[2, \infty)$  scambia tra loro  $P_2, P_3$ . Pertanto la ramificazione è descritta dalla trasposizione (23) nel punto di ramificazione  $x = -2$  e dalla trasposizione (12) in  $x = 2$ . ■

#### (7.21) Esempio

Consideriamo la superficie di Riemann di  $y^2 - x^3 + x^2$ . Vi sono due punti  $x = 0, 1$  al di sopra dei quali  $S$  ha meno di due punti. Tuttavia, in  $x = 0$  i

fogli si attraversano senza mescolarsi, sicché l'unico vero punto di ramificazione è  $x = 1$ . Per verificarlo, effettuiamo il cambiamento di variabili  $x = x$ ,  $z = y/x$ , il quale è ben definito e invertibile tranne che in  $x = 0$ . Allora  $z^2 - x + 1 = 0$ . La superficie assegnata  $S$  diventa omeomorfa alla superficie di Riemann di  $z^2 - x + 1$ , quando vengono eliminati i punti al di sopra dell'origine, e può essere ridotta alla superficie descritta in (7.9) mediante una traslazione nel piano della variabile  $x$ . ■

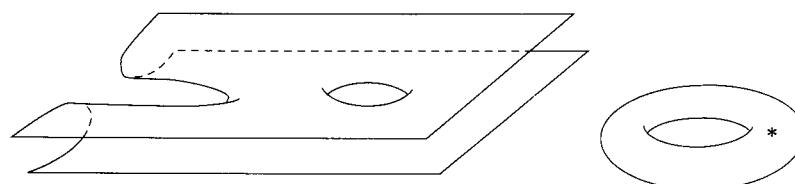
Quando  $x$  non è esprimibile come funzione univoca di  $y$  è più difficile descrivere gli incollamenti.

### (7.22) Esempio

Consideriamo la superficie di Riemann di  $y^2 - (x^3 - x)$ . Vi sono tre punti in cui  $x^3 - x = 0$ , precisamente  $x = 0, \pm 1$ , e la superficie ha tre punti di ramificazione in cui si comporta come la superficie di Riemann di  $y^2 - x$  nell'origine. Il nostro metodo usuale è di fare dei tagli che dai punti di ramificazione vanno all'infinito, ma in questo caso è più facile operare diversamente. I valori di  $x$  per i quali  $y$  è un numero immaginario puro sono i numeri reali  $x$  tali che  $x^3 - x \leq 0$ , appartengono cioè agli intervalli  $(-\infty, -1]$  e  $[0, 1]$ . Se tagliamo  $S$  lungo questi intervalli,  $S$  si decomporrà nelle parti  $\text{re } y > 0$  e  $\text{re } y < 0$ . Possiamo allora ricostruire la superficie  $S$  sovrapponendo due copie di  $P$ , tagliandole lungo gli intervalli e incollando così da mescolare i fogli come prima.

$$(7.23) \quad \text{---} \quad -1 \quad 0 \quad 1 \quad \text{---}$$

Il fatto che una superficie costruita col metodo "taglia e incolla" attraversi se stessa lungo i tagli rende difficile una visualizzazione diretta. Ma poiché qui i tagli sono disposti lungo l'asse reale, possiamo evitare gli attraversamenti, rivoltando uno dei fogli. Ciò distrugge la rappresentazione di  $S$  come rivestimento doppio di  $P$ , ma ha il vantaggio che ora i fogli sono incollati lungo lo stesso lato del taglio. Nella figura (7.23) vi sono due tagli di questo tipo. Rivoltando un foglio e tirando per allargare le fessure, prima di effettuare gli incollamenti, si ottiene la figura rappresentata qui sotto, la quale mostra che la superficie di Riemann in esame è omeomorfa a un toro privato di un punto. ■



### 8 Estensioni trascendenti

In questo paragrafo daremo un breve sguardo ad alcune estensioni trascendenti di campi. Abbiamo visto nella proposizione (2.5) che la struttura dell'estensione  $F(\alpha)$  generata da un solo elemento trascendente  $\alpha$  su un campo  $F$  non dipende da  $\alpha$ . Ma se a  $F$  vengono aggiunti simultaneamente due elementi trascendenti  $\alpha$  e  $\beta$ , la struttura del campo  $F(\alpha, \beta)$  così ottenuto dipenderà dall'esistenza o meno di una relazione algebrica tra  $\alpha$  e  $\beta$  e, in caso affermativo, dalla natura di questa relazione. Per esempio,  $\alpha = \sqrt{\pi}$  e  $\beta = \sqrt[4]{\pi} \sqrt{\pi - 1}$  sono numeri trascendenti su  $\mathbb{Q}$ , collegati dall'equazione

$$\beta^2 - \alpha^3 + \alpha = 0.$$

In generale, si dice che un insieme di elementi  $\{\alpha_1, \dots, \alpha_n\}$  di un'estensione di campi  $K \supset F$  è *algebricamente dipendente su  $F$*  se esiste un polinomio non nullo in  $n$  variabili  $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$  tale che

$$f(\alpha_1, \dots, \alpha_n) = 0;$$

se invece non esiste alcun polinomio di questo tipo, l'insieme viene detto *algebricamente indipendente su  $F$* . Dunque  $\sqrt{\pi}$  e  $\sqrt[4]{\pi} \sqrt{\pi - 1}$  sono algebricamente indipendenti su  $\mathbb{Q}$ . Si pensa che  $\pi$  ed  $e$  siano algebricamente indipendenti, ma ciò non è stato dimostrato.

Possiamo interpretare l'indipendenza algebrica per mezzo dell'omomorfismo di sostituzione  $\varphi : F[x_1, \dots, x_n] \rightarrow K$ , il quale manda  $f(x_1, \dots, x_n)$  in  $f(\alpha_1, \dots, \alpha_n)$ . Gli elementi  $\alpha_1, \dots, \alpha_n$  sono algebricamente indipendenti se  $\ker \varphi = 0$ , ossia se  $\varphi$  è iniettivo, e algebricamente dipendenti se  $\ker \varphi \neq 0$ . Passando ai campi delle frazioni, si ottiene la seguente proposizione:

(8.1) PROPOSIZIONE *Se  $\alpha_1, \dots, \alpha_n$  sono algebricamente indipendenti, allora  $F(\alpha_1, \dots, \alpha_n)$  è isomorfo al campo  $F(x_1, \dots, x_n)$  delle funzioni razionali nelle variabili  $x_1, \dots, x_n$ , ossia al campo delle frazioni di  $F[x_1, \dots, x_n]$ .* ■

Un'estensione della forma  $F(\alpha_1, \dots, \alpha_n)$ , dove gli elementi  $\alpha_i$  sono algebricamente indipendenti, è detta *trascendente pura*.

(8.2) DEFINIZIONE *Una base di trascendenza di un'estensione di campi  $K$  di  $F$  è un insieme di elementi  $(\alpha_1, \dots, \alpha_n)$  algebricamente indipendenti e tali che  $K$  è un'estensione algebrica di  $F(\alpha_1, \dots, \alpha_n)$ .*

(8.3) TEOREMA *Siano  $(\alpha_1, \dots, \alpha_m)$  e  $(\beta_1, \dots, \beta_n)$  elementi in un'estensione  $K$  di un campo  $F$ . Supponiamo che  $K$  sia algebrica su  $F(\beta_1, \dots, \beta_n)$  e che  $\alpha_1, \dots, \alpha_m$  siano algebricamente indipendenti su  $F$ . Allora  $m \leq n$  e l'insieme*

$(\alpha_1, \dots, \alpha_m)$  può essere completato in modo da ottenere una base di trascendenza di  $K$  aggiungendo  $n - m$  elementi scelti tra i  $\beta_j$ .

La dimostrazione è lasciata come esercizio. ■

(8.4) COROLLARIO Due basi di trascendenza di un'estensione  $K \supset F$  hanno lo stesso numero di elementi. ■

(8.5) DEFINIZIONE Il grado di trascendenza di  $K$  è il numero degli elementi di una base di trascendenza, oppure è infinito se non esiste una base di trascendenza finita.

#### (8.6) Esempi

- (a) I campi  $F(x_1, \dots, x_n)$  delle funzioni razionali in  $n$  variabili non sono estensioni isomorfe di  $F$  per valori diversi di  $n$ , poiché  $(x_1, \dots, x_n)$  è una base di trascendenza.
- (b) Siano  $\alpha, \beta$  i numeri scelti all'inizio del paragrafo. Il solo elemento  $\pi$  forma una base di trascendenza per  $K = \mathbb{Q}(\alpha, \beta)$  su  $\mathbb{Q}$ . Pertanto dal teorema (8.3) segue, come asserito in precedenza, che due elementi qualunque di  $K$  sono algebricamente dipendenti. L'elemento  $\beta$  forma un'altra base di trascendenza.
- (c) Siano dati due polinomi oppure due funzioni razionali in una variabile  $f, g \in F(x)$ . Esiste un polinomio non nullo  $\varphi(y, z) \in F[y, z]$  tale che  $\varphi(f, g) = 0$ . Infatti, il grado di trascendenza di  $F(x)$  è 1, e quindi  $f, g$  sono algebricamente dipendenti.

La maggior parte delle estensioni di campi non sono trascendenti pure, sebbene ciò possa essere difficile da stabilire per un'estensione particolare. Ecco qui due esempi:

#### (8.7) PROPOSIZIONE

- (a) Il campo di funzioni  $L = \mathbb{C}(x)[y]/(y^2 - x^3)$  è un'estensione trascendente pura di  $\mathbb{C}$ : è il campo delle funzioni razionali in  $t = y/x$ .
- (b) Il campo di funzioni  $K = \mathbb{C}(x)[y]/(y^2 - x^3 + x)$  non è un'estensione trascendente pura di  $\mathbb{C}$ : non esiste alcun elemento  $t \in K$  tale che  $K = \mathbb{C}(t)$ .

*Dimostrazione.* In entrambi i casi, il grado di trascendenza di  $K$  su  $\mathbb{C}$  è 1, poiché  $x$  è una base di trascendenza.

- (a) Poniamo  $t = y/x$ . Allora  $\mathbb{C}(t) \subset L$  poiché  $t \in L$ . Ora  $L$  è generato da  $x$  e  $y$ , per definizione. D'altra parte,  $x = t^2$  e  $y = t^3$ , quindi  $L = \mathbb{C}(t)$ . Poiché  $K$  ha grado di trascendenza 1, ne segue, in virtù del corollario (8.4), che  $t$  è trascendente.

(b) (*Schema di dimostrazione*) Per dimostrare che  $K$  non è un campo di funzioni razionali, ricorriamo alle proprietà geometriche della sua superficie di Riemann. Abbiamo visto (§ 7) che questa superficie è un toro privato di un punto. D'altra parte, la superficie di Riemann del campo delle funzioni razionali  $\mathbb{C}(t)$  è il piano complesso stesso. Ora, esiste un teorema di topologia, il quale afferma che il toro e il piano non sono omeomorfi e che non possono essere resi tali eliminando insiemi finiti di punti. Se ammettiamo questo teorema, la proposizione seguente completerà la dimostrazione.

(8.8) PROPOSIZIONE Siano  $K = \mathbb{C}(x)[y]/(f)$  e  $L = \mathbb{C}(t)[u]/(g)$  campi di funzioni con superfici di Riemann  $S$  e  $T$  rispettivamente. Un omomorfismo  $\varphi : L \rightarrow K$ , che sia l'identità sul sottocampo  $\mathbb{C}$ , induce tra le loro superfici di Riemann un'applicazione  $\varphi^* : S' \rightarrow T$  definita e continua tranne che su un insieme finito di punti di  $S'$ . Se  $\varphi$  è un isomorfismo,  $\varphi^*$  diventa un omeomorfismo eliminando da  $S$  e  $T$  insiemi finiti opportuni.

Si noti che l'applicazione  $\varphi^*$  va dalla superficie di Riemann di  $K$  a quella di  $L$ , nella direzione opposta a  $\varphi$ .

*Dimostrazione.* La superficie di Riemann  $T$  è il luogo  $g(t, u) = 0$  in  $\mathbb{C}^2$ . In base alla proposizione (7.11), ogni elemento  $\alpha \in K$  definisce una funzione continua su  $S'$ , sicché la coppia di funzioni  $(\varphi(t), \varphi(u))$  definisce un'applicazione continua  $S' \rightarrow \mathbb{C}^2$ . Poiché  $g(t, u) = 0$  in  $L$  e poiché  $\varphi$  è un omomorfismo che lascia fissi i coefficienti di  $g$ , si ha anche  $g(\varphi(t), \varphi(u)) = 0$ . Dunque  $S'$  viene mandata in  $T$ , e questa è l'applicazione  $\varphi^*$  richiesta. Se  $\varphi$  è un isomorfismo, il suo inverso  $\varphi^{-1}$  definisce un'applicazione  $T' \rightarrow S'$ , che è una funzione inversa di  $\varphi^*$  sul complementare di un insieme finito. ■

## 9 Campi algebricamente chiusi

Un campo  $F$  si dice *algebricamente chiuso* se ogni polinomio  $f(x) \in F[x]$  di grado positivo ha una radice in  $F$ . Il fatto che il campo  $\mathbb{C}$  dei numeri complessi è algebricamente chiuso è noto come teorema fondamentale dell'algebra.

(9.1) TEOREMA FONDAMENTALE DELL'ALGEBRA Ogni polinomio non costante a coefficienti complessi ha una radice complessa.

Abbiamo già usato spesso questo teorema. Una dimostrazione si trova alla fine del paragrafo (p. 621).

Se un campo  $F$  è algebricamente chiuso, ogni polinomio non costante  $f(x) \in F[x]$  ha un fattore lineare  $x - \alpha$ , sicché gli unici polinomi irriducibili sono i polinomi di grado 1. Ne segue che ogni polinomio è un prodotto di fattori

lineari. Inoltre, non esistono estensioni algebriche di  $F$  diverse da  $F$  stesso (da cui l'espressione "algebricamente chiuso"). Infatti ogni elemento algebrico su  $F$  è una radice di un polinomio irriducibile monico  $f(x) \in F[x]$ . Tale polinomio deve essere della forma  $x - \alpha$ , sicché  $\alpha \in F$ .

Può essere conveniente considerare il campo  $F$  che si sta studiando come un sottocampo di un campo algebricamente chiuso. Per esempio, conviene considerare i campi di numeri come sottocampi di  $\mathbb{C}$ . Si dice che un'estensione  $K$  di  $F$  è una *chiusura algebrica* di  $F$  se soddisfa alle seguenti condizioni:

- (9.2) (a)  $K$  è algebrico su  $F$ ,  
(b)  $K$  è un campo algebricamente chiuso.

(9.3) COROLLARIO Sia  $F$  un sottocampo di  $\mathbb{C}$ . Allora il sottoinsieme  $\overline{F}$  di  $\mathbb{C}$  costituito da tutti i numeri che sono algebrici su  $F$  è una chiusura algebrica di  $F$ .

*Dimostrazione.* È già stato dimostrato (3.10) che  $\overline{F}$  è un campo. Facciamo vedere che  $\overline{F}$  è algebricamente chiuso. Sia  $f(x) \in \overline{F}[x]$  un polinomio non costante. Allora  $f(x)$  ha una radice  $\alpha$  in  $\mathbb{C}$ , e  $\overline{F}(\alpha)$  è algebrico su  $\overline{F}$ . Poiché  $\overline{F}$  è algebrico su  $F$ ,  $\alpha$  è algebrico su  $F$ , in base a (3.11). Pertanto  $\alpha \in \overline{F}$ . ■

Non è difficile costruire una chiusura algebrica di un campo finito  $\mathbb{F}_p$  come un'unione dei campi  $\mathbb{F}_q$ , dove  $q = p^r$  è una potenza di  $p$ . Per fare ciò, scegliamo una successione di interi  $r_1, r_2, \dots$  con le seguenti proprietà: (i)  $r_i$  divide  $r_{i+1}$ , e (ii) ogni intero  $n$  divide qualche  $r_i$ . Possiamo prendere  $r_i = i!$ , per esempio. Poniamo  $q_i = p^{r_i}$  e  $F_i = \mathbb{F}_{q_i}$ . Ora, da (i) segue che  $F_{i+1}$  contiene un sottocampo isomorfo a  $F_i$  (6.4), sicché possiamo costruire una catena di campi  $F_1 \subset F_2 \subset \dots$ . Sia  $\overline{F}$  l'unione insiemistica di questa catena di campi. Allora, (ii) ci dice che ogni campo finito  $\mathbb{F}_q$ , con  $q = p^r$ , è isomorfo a un sottocampo di qualche campo  $F_i$ , e quindi ad un sottocampo  $\overline{F}$ , che è una chiusura algebrica di  $\mathbb{F}_p$ .

Il teorema seguente può essere dimostrato usando il lemma di Zorn.

(9.4) TEOREMA Ogni campo  $F$  ha una chiusura algebrica, e se  $K_1, K_2$  sono due chiusure algebriche di  $F$ , esiste un isomorfismo  $\varphi : K_1 \rightarrow K_2$ , che è l'identità sul sottocampo  $F$ . ■

Dunque la chiusura algebrica di un campo è essenzialmente unica.

(9.5) COROLLARIO Sia  $\overline{F}$  una chiusura algebrica di  $F$  e sia  $K$  un'estensione algebrica arbitraria di  $F$ . Allora esiste una sottoestensione  $K' \subset \overline{F}$  isomorfa a  $K$ . ■

*Dimostrazione del teorema fondamentale dell'algebra.* Per dimostrare che  $f(x_0) = 0$ , basta dimostrare che il valore assoluto  $|f(x_0)|$  è zero. L'esistenza di un tale  $x_0 \in \mathbb{C}$  è dimostrata dai due lemmi seguenti:

(9.6) LEMMA Sia  $f(x)$  un polinomio non costante e sia  $x_0 \in \mathbb{C}$  un punto in cui  $f(x_0) \neq 0$ . Allora  $|f(x_0)|$  non è il minimo di  $|f(x)|$ .

(9.7) LEMMA. Sia  $f(x)$  un polinomio a coefficienti complessi. Allora  $|f(x)|$  ha un minimo in qualche punto  $x_0 \in \mathbb{C}$ .

*Dimostrazione del lemma (9.6).* Osserviamo innanzitutto che il polinomio  $x^k - c$  ha una radice, per ogni  $c \in \mathbb{C}$ . Un numero reale non negativo  $r$  ha una radice  $k$ -esima reale, poiché la funzione continua  $x^k$ , la quale vale zero per  $x = 0$  e tende a  $+\infty$  per  $x$  che tende a  $+\infty$ , assume tutti i valori reali  $\geq 0$ , in virtù del teorema del valor medio. Scriviamo il numero complesso  $c$  nella forma  $c = re^{i\theta}$ , dove  $r = |c|$  e  $\theta = \arg c$ . Sia  $s$  una radice  $k$ -esima reale di  $r$ . Allora la radice  $k$ -esima richiesta di  $c$  è

$$(9.8) \quad \alpha = se^{i\theta/k}.$$

Sia ora  $f(x)$  un polinomio non costante e sia  $x_0 \in \mathbb{C}$  un punto in cui  $f(x_0) \neq 0$ . È conveniente normalizzare  $f$ . Effettuiamo un cambiamento di variabile, sostituendo  $x$  con  $x + x_0$ , per spostare il punto in questione nell'origine, sicché  $x_0 = 0$ . Inoltre moltiplichiamo  $f(x)$  per  $f(0)^{-1}$ . Allora  $f(0) = 1$ , e dobbiamo dimostrare che 1 non è il valore minimo di  $|f(x)|$ .

Denotiamo con  $k$  il minimo esponente non nullo di  $x$  che compare in  $f$ , sicché

$$f(x) = 1 + ax^k + (\text{termini di grado } > k).$$

Sia  $\alpha$  una radice  $k$ -esima di  $-a^{-1}$ . Effettuiamo un ulteriore cambiamento di variabile, sostituendo  $x$  con  $\alpha x$ . Allora  $f$  assume la forma seguente:

$$f(x) = 1 - x^k + (\text{termini di grado più alto}) = 1 - x^k + x^{k+1}g(x),$$

per qualche polinomio  $g(x)$ . Se  $x$  è un numero reale positivo piccolo, per la diseguaglianza triangolare si ha:

$$|f(x)| \leq |1 - x^k| + |x^{k+1}g(x)| = 1 - x^k + x^{k+1}|g(x)| = 1 - x^k(1 - x|g(x)|).$$

Poiché  $x|g(x)|$  è piccolo per piccoli valori di  $x$ , il termine  $x^k(1 - x|g(x)|)$  è positivo se  $x$  è un numero reale positivo sufficientemente piccolo. Per un tale  $x$  si ha:  $|f(x)| < |f(0)|$ . ■

*Dimostrazione del lemma (9.7).* Possiamo supporre che il polinomio  $f$  non sia una costante. Per valori grandi di  $x$ , anche  $f(x)$  assume valori grandi; si ha cioè

$$(9.9) \quad |f(x)| \rightarrow \infty \text{ per } |x| \rightarrow \infty.$$

Per dimostrare ciò, il termine noto di  $f$  è irrilevante, sicché possiamo supporre che esso sia nullo. Allora  $f(x)$  è divisibile per  $x$ , ossia:  $f(x) = xg(x)$ . Procedendo per induzione sul grado, l'asserzione è vera per  $g(x)$ , oppure  $g(x)$  è costante, e di conseguenza essa risulta vera anche per  $f(x)$ .

Ora, poiché  $f(x)$  assume valori grandi per valori grandi di  $x$ , l'estremo inferiore  $m$  di  $|f(x)|$  nell'intero piano complesso è anche l'estremo inferiore in un disco sufficientemente grande  $|x| \leq r$ . Poiché il disco è compatto e  $|f(x)|$  è una funzione continua, essa ha un minimo nel disco. ■

Oltre a quella appena sviluppata, vi sono varie altre dimostrazioni del teorema fondamentale dell'algebra. Una è particolarmente interessante, sebbene non sia così facile renderla precisa come quella appena vista. A grandi linee, la dimostrazione è la seguente. Come prima, dobbiamo dimostrare che un polinomio non costante

$$(9.10) \quad f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0$$

ha una radice. Se  $a_0 = 0$ , allora 0 è una radice, sicché possiamo supporre che  $a_0 \neq 0$ . Consideriamo la funzione  $f : \mathbb{C} \rightarrow \mathbb{C}$  definita dal polinomio (9.10).

Denotiamo con  $C_r$  una circonferenza di raggio  $r$  col centro nell'origine. Studiamo le immagini  $f(C_r)$  delle circonferenze  $C_r$ . In coordinate polari, scriviamo  $z = re^{i\theta}$ . Allora  $z^n = r^n e^{in\theta}$ . Mentre  $\theta$  varia da 0 a  $2\pi$ , il punto  $z$  percorre un giro lungo la circonferenza di raggio  $r$ . Nello stesso tempo,  $n\theta$  varia da 0 a  $2\pi n$ , sicché il punto  $z^n$  percorre  $n$  giri lungo la circonferenza di raggio  $r^n$ .

Per valori sufficientemente grandi di  $r$ , il termine  $z^n$  è dominante nell'espressione (9.10), e otterremo

$$|f(z) - z^n| \leq \frac{1}{2}r^n.$$

La dimostrazione di questo fatto è simile alla dimostrazione del lemma (9.6). Per i nostri scopi, il fattore  $\frac{1}{2}$  potrebbe essere sostituito da un qualunque numero reale positivo minore di 1. La precedente diseguaglianza mostra che, mentre  $z^n$  percorre  $n$  volte la circonferenza di raggio  $r^n$ , anche  $f(z)$  percorre  $n$  giri intorno all'origine. Un buon modo per visualizzare questo fatto è dato dal modello del "cane al guinzaglio". Se si porta a spasso un cane girando  $n$  volte intorno a un isolato, anche il cane gira  $n$  volte, sia pure seguendo un percorso diverso. Ciò sarà vero purché il guinzaglio sia più corto del raggio dell'isolato. Qui  $z^n$  rappresenta la posizione della persona al tempo  $\theta$ , e  $f(z)$  rappresenta la posizione del cane. La lunghezza del guinzaglio è  $\frac{1}{2}r^n$ .

Facciamo variare ora il raggio  $r$ . Poiché  $f$  è una funzione continua, l'immagine  $f(C_r)$  varierà con  $r$  in modo continuo. Quando  $r$  è molto piccolo,  $f(C_r)$  descrive un piccolo cappio intorno al termine noto  $a_0$  di  $f$ . Questo piccolo cappio non si

avvolgerà affatto intorno all'origine. Ma come abbiamo appena visto, l'immagine  $f(C_r)$  si avvolge  $n$  volte intorno all'origine, se  $r$  è abbastanza grande. L'unica spiegazione per questo fatto è che, per qualche raggio intermedio  $r'$ ,  $f(C_{r'})$  passi per l'origine. Ciò significa che per qualche punto  $\alpha$  sulla circonferenza  $C_{r'}$  risulta  $f(\alpha) = 0$ . Questo numero  $\alpha$  è una radice di  $f$ .

Si noti che tutti gli  $n$  cappi devono passare per l'origine, il che è in accordo col fatto che un polinomio di grado  $n$  ha  $n$  radici.

Per me questa non è algebra, ma ciò non significa che gli algebristi non possano farla.  
Garrett Birkhoff

### Esercizi

#### 1 Esempi di campi

- Sia  $F$  un campo. Trovare tutti gli elementi  $a \in F$  tali che  $a = a^{-1}$ .
- Sia  $K$  un sottocampo di  $\mathbb{C}$  non contenuto in  $\mathbb{R}$ . Dimostrare che  $K$  è un sottoinsieme denso di  $\mathbb{C}$ .
- Sia  $R$  un dominio di integrità contenente un campo  $F$  come sottoanello e avente dimensione finita come spazio vettoriale su  $F$ . Dimostrare che  $R$  è un campo.
- Sia  $F$  un campo contenente esattamente otto elementi. È vero che la caratteristica di  $F$  è 2?

#### 2 Elementi algebrici e trascendenti

- Sia  $\alpha$  la radice cubica reale di 2. Calcolare il polinomio minimo di  $1 + \alpha^2$  su  $\mathbb{Q}$ .
- Dimostrare il lemma (2.7), secondo cui l'insieme  $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$  è una base di  $F[\alpha]$ .
- Determinare il polinomio minimo di  $\alpha = \sqrt[3]{3} + \sqrt[3]{5}$  su ciascuno dei campi seguenti:
  - $\mathbb{Q}$ ;
  - $\mathbb{Q}(\sqrt{5})$ ;
  - $\mathbb{Q}(\sqrt{10})$ ;
  - $\mathbb{Q}(\sqrt{15})$ .
- Sia  $\alpha$  una radice complessa del polinomio irriducibile  $x^3 - 3x + 4$ . Scrivere esplicitamente l'inverso di  $\alpha^2 + \alpha + 1$  in  $F(\alpha)$ , nella forma  $a + b\alpha + c\alpha^2$ , con  $a, b, c \in \mathbb{Q}$ .
- Sia  $K = F(\alpha)$ , dove  $\alpha$  è una radice del polinomio irriducibile  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ . Determinare esplicitamente l'elemento  $\alpha^{-1}$  per mezzo di  $\alpha$  e dei coefficienti  $a_i$ .
- Sia  $\beta = \zeta\sqrt[3]{2}$ , dove  $\zeta = e^{2\pi i/3}$  e poniamo  $K = \mathbb{Q}(\beta)$ . Dimostrare che  $-1$  non può essere scritto come una somma di quadrati in  $K$ .

#### 3 Il grado di un'estensione di campi

- Sia  $F$  un campo e sia  $\alpha$  un elemento che genera un'estensione di campi di  $F$  di grado 5. Dimostrare che  $\alpha^2$  genera la stessa estensione.
- Poniamo  $\zeta = e^{2\pi i/7}$  e  $\eta = e^{2\pi i/5}$ . Dimostrare che  $\eta \notin \mathbb{Q}(\zeta)$ .

3. Definiamo  $\zeta_n = e^{2\pi i/n}$ . Trovare il polinomio minimo su  $\mathbb{Q}$  di ciascuno dei seguenti elementi:  
**(a)**  $\zeta_4$ ; **(b)**  $\zeta_6$ ; **(c)**  $\zeta_8$ ; **(d)**  $\zeta_9$ ; **(e)**  $\zeta_{10}$ ; **(f)**  $\zeta_{12}$ .
4. Poniamo  $\zeta_n = e^{2\pi i/n}$ . Determinare il polinomio minimo su  $\mathbb{Q}(\zeta_3)$  di ciascuno dei seguenti elementi:  
**(a)**  $\zeta_6$ ; **(b)**  $\zeta_9$ ; **(c)**  $\zeta_{12}$ .
5. Dimostrare che un'estensione  $K$  di  $F$  di grado 1 è uguale a  $F$ .
6. Sia  $a \in \mathbb{Q}$  un elemento che non sia un quadrato in  $\mathbb{Q}$ . Dimostrare che  $\sqrt[4]{a}$  ha grado 4 su  $\mathbb{Q}$ .
7. In ciascuno dei casi seguenti, stabilire se  $i$  appartiene o non appartiene al campo:  
**(a)**  $\mathbb{Q}(\sqrt{-2})$ ; **(b)**  $\mathbb{Q}(\sqrt[4]{-2})$ ; **(c)**  $\mathbb{Q}(\alpha)$ , dove  $\alpha^3 + \alpha + 1 = 0$ .
8. Sia  $K$  un campo generato su  $F$  da due elementi  $\alpha, \beta$  di gradi  $m, n$  rispettivamente, primi tra loro. Dimostrare che  $[K : F] = mn$ .
9. Siano  $\alpha, \beta$  numeri complessi di grado 3 su  $\mathbb{Q}$ , e poniamo  $K = \mathbb{Q}(\alpha, \beta)$ . Determinare i valori possibili per  $[K : \mathbb{Q}]$ .
10. Siano  $\alpha, \beta$  numeri complessi. Dimostrare che, se  $\alpha + \beta$  e  $\alpha\beta$  sono numeri algebrici, anche  $\alpha$  e  $\beta$  sono algebrici.
11. Siano  $\alpha, \beta$  radici complesse di polinomi irriducibili  $f(x), g(x) \in \mathbb{Q}[x]$ . Poniamo  $F = \mathbb{Q}[\alpha]$  e  $K = \mathbb{Q}[\beta]$ . Dimostrare che  $f(x)$  è irriducibile in  $K[x]$  se, e soltanto se,  $g(x)$  è irriducibile in  $F[x]$ .
12. **(a)** Siano  $F \subset F' \subset K$  estensioni di campi. Dimostrare che, se  $[K : F] = [K : F']$ , allora  $F = F'$ .  
**(b)** Dare un esempio che mostri che ciò non è necessariamente vero, se  $F$  non è contenuto in  $F'$ .
13. Siano  $\alpha_1, \dots, \alpha_k$  elementi di un'estensione di campi  $K$  di  $F$  e supponiamo che essi siano tutti algebrici su  $F$ . Dimostrare che  $F(\alpha_1, \dots, \alpha_k) = F[\alpha_1, \dots, \alpha_k]$ .
14. È vero che, se  $\alpha, \beta$  sono elementi algebrici su un campo  $F$ , di gradi  $d, e$  rispettivamente, i monomi  $\alpha^i \beta^j$ , con  $i = 0, \dots, d-1$ ,  $j = 0, \dots, e-1$ , formano una base di  $F(\alpha, \beta)$  su  $F$ ?
15. È vero che ogni estensione algebrica è un'estensione finita?

#### 4 Costruzioni con riga e compasso

1. Esprimere  $\cos 15^\circ$  per mezzo di radici quadrate.
2. Dimostrare che il pentagono regolare può essere costruito con riga e compasso **(a)** per mezzo della teoria dei campi e **(b)** trovando una costruzione esplicita.
3. Dimostrare la formula (4.12).
4. È vero che il poligono regolare di 9 lati può essere costruito con riga e compasso?
5. È possibile costruire un quadrato di area uguale a quella di un triangolo assegnato?

6. Sia  $\alpha$  una radice reale del polinomio  $x^3 + 3x + 1$ . Dimostrare che  $\alpha$  non può essere costruito con riga e compasso.
7. Sapendo che  $\pi$  è un numero trascendente, dimostrare l'impossibilità di quadrare il cerchio con riga e compasso (vale a dire, di costruire un quadrato di area uguale a quella di un cerchio di raggio unitario).
8. Dimostrare l'impossibilità di "duplicare il cubo", ossia, di costruire il lato di un cubo il cui volume sia 2.
9. **(a)** Con riferimento alla dimostrazione della proposizione (4.8), dimostrare che il discriminante  $D$  è negativo se, e soltanto se, le circonferenze non si intersecano.  
**(b)** Determinare geometricamente la retta che compare alla fine della dimostrazione della proposizione (4.8), nel caso  $D \geq 0$  come pure nel caso  $D < 0$ .
10. Dimostrare che, se un numero primo  $p$  ha la forma  $2^r + 1$ , esso ha in realtà la forma  $2^{2^k} + 1$ .
11. Denotiamo con  $C$  il campo dei numeri reali costruibili. Dimostrare che  $C$  è il più piccolo sottocampo di  $\mathbb{R}$  tale che, se  $a \in C$  e  $a > 0$ , allora  $\sqrt{a} \in C$ .
12. I punti del piano possono essere considerati come numeri complessi. Descrivere esplicitamente l'insieme dei punti costruibili come sottoinsieme di  $\mathbb{C}$ .
13. Caratterizzare i numeri reali costruibili nel caso in cui siano assegnati all'inizio tre punti nel piano.
- \*14. Supponiamo che le regole per le costruzioni nello spazio a tre dimensioni siano le seguenti:  
**(i)** Sono assegnati tre punti non allineati che consideriamo costruiti.  
**(ii)** È possibile costruire un piano passante per tre punti costruiti non allineati.  
**(iii)** È possibile costruire una sfera col centro in un punto costruito e passante per un altro punto costruito.  
**(iv)** I punti di intersezione di piani e sfere costruiti sono considerati come punti costruiti se sono punti isolati, ossia se non appartengono ad una curva intersezione.
- Dimostrare che è possibile introdurre un sistema di coordinate, e caratterizzare le coordinate dei punti costruibili.

#### 5 Aggiunzione simbolica di radici

1. Sia  $F$  un campo di caratteristica zero. Denotiamo con  $f'$  la derivata di un polinomio  $f \in F[x]$  e sia  $g$  un polinomio irriducibile che divida  $f$  e  $f'$ . Dimostrare che  $g^2$  divide  $f$ .
2. Per quali campi  $F$  e per quali numeri primi  $p$ , il polinomio  $x^p - x$  ha una radice multipla?
3. Sia  $F$  un campo di caratteristica  $p$ .  
**(a)** Applicare la proposizione (5.7) al polinomio  $x^p + 1$ .  
**(b)** Decomporre quest'ultimo in fattori irriducibili in  $F[x]$ .

4. Siano  $\alpha_1, \dots, \alpha_n$  le radici di un polinomio  $f \in F[x]$  di grado  $n$  in un'estensione di campi  $K$ . Trovare la migliore stima possibile di un maggiorante per  $|F(\alpha_1, \dots, \alpha_n) : F|$ .

### 6 Campi finiti

1. Descrivere il gruppo  $F_4(+)$ .
2. Scrivere le tabelle relative all'addizione e alla moltiplicazione per  $F_4$  e per  $\mathbb{Z}/(4)$ , e confrontarle tra loro.
3. Trovare una radice tredicesima di 3 nel campo  $F_{13}$ .
4. Determinare il polinomio minimo su  $F_2$  di ciascuno degli elementi (6.12) di  $F_8$ .
5. Determinare il numero dei polinomi irriducibili di grado 3 sul campo  $F_3$ .
6. (a) Verificare che (6.9, 6.10, 6.13) sono fattorizzazioni irriducibili su  $F_2$ .  
 (b) Verificare che (6.11, 6.13) sono fattorizzazioni irriducibili su  $\mathbb{Z}$ .
7. Fattorizzare i polinomi  $x^9 - x$  e  $x^{27} - x$  in  $F_3[x]$ .
8. Fattorizzare il polinomio  $x^{16} - x$ , rispettivamente, in  $F_4[x]$  e in  $F_8[x]$ .
9. Determinare tutti i polinomi  $f(x)$  in  $F_q[x]$  tali che  $f(\alpha) = 0$  per ogni  $\alpha \in F_q$ .
10. Sia  $K$  un campo finito. Dimostrare che il prodotto degli elementi non nulli di  $K$  è uguale a  $-1$ .
11. Dimostrare che ogni elemento di  $F_p$  ha una e una sola radice  $p$ -esima.
12. Completare la dimostrazione della proposizione (6.19), dimostrando che la differenza  $\alpha - \beta$  di due radici di  $x^q - x$  è anch'essa una radice del polinomio.
13. Sia  $p$  un numero primo. Descrivere gli interi  $n$  tali che esistono un campo finito  $K$  di ordine  $n$  e un elemento  $\alpha \in K^*$  il cui ordine in  $K^*$  è  $p$ .
14. Risolvere questo problema senza ricorrere al teorema (6.4).
  - (a) Sia  $F = F_p$ . Determinare il numero dei polinomi irriducibili monici di grado 2 in  $F[x]$ .
  - (b) Sia  $f(x)$  uno dei polinomi descritti in (a). Dimostrare che  $K = F[x]/(f)$  è un campo contenente  $p^2$  elementi e che gli elementi di  $K$  hanno la forma  $a + b\alpha$ , dove  $a, b \in F$  e  $\alpha$  è una radice di  $f$  in  $K$ . Dimostrare che ogni elemento  $a + b\alpha$ , con  $b \neq 0$ , è la radice di un polinomio irriducibile di secondo grado in  $F[x]$ .
  - (c) Dimostrare che ogni polinomio di secondo grado in  $F[x]$  ha una radice in  $K$ .
  - (d) Dimostrare che, per un dato numero primo  $p$ , tutti i campi  $K$  costruiti come sopra sono isomorfi.
15. I polinomi  $f(x) = x^3 + x + 1$ ,  $g(x) = x^3 + x^2 + 1$  sono irriducibili su  $F_2$ . Sia  $K$  l'estensione di campi ottenuta aggiungendo una radice di  $f$  e sia  $L$  l'estensione ottenuta aggiungendo una radice di  $g$ . Descrivere esplicitamente un isomorfismo tra  $K$  e  $L$ .
16. (a) Dimostrare il lemma (6.21) nel caso in cui  $F = \mathbb{C}$ , considerando le radici dei due polinomi.

- (b) Utilizzare il principio di permanenza delle identità per dedurre il risultato precedente nel caso in cui  $F$  è un anello arbitrario.

### 7 Campi di funzioni

1. Determinare un polinomio in tre variabili a coefficienti reali, il cui luogo degli zeri sia la superficie di Riemann proiettata (7.9).
2. Dimostrare che l'insieme  $\mathcal{F}(U)$  delle funzioni continue su  $U'$  forma un anello.
3. Sia  $f(x)$  un polinomio in  $F[x]$ , dove  $F$  è un campo. Dimostrare che, se esiste una funzione razionale  $r(x)$  tale che  $r^2 = f$ , allora  $r$  è un polinomio.
4. Con riferimento alla dimostrazione della proposizione (7.11) spiegare perché l'applicazione  $F \rightarrow \mathcal{F}(S)$  definita da  $g(x) \mapsto g(X)$  è un omomorfismo.
5. Determinare i punti di ramificazione e gli incollamenti relativi alle superfici di Riemann dei seguenti polinomi:
  - (a)  $y^2 - x^2 + 1$ ; (b)  $y^5 - x$ ; (c)  $y^4 - x - 1$ ; (d)  $y^3 - xy - x$ ; (e)  $y^3 - y^2 - x$ ;
  - (f)  $y^3 - x(x-1)$ ; (g)  $y^3 - x(x-1)^2$ ; (h)  $y^3 + xy^2 + x$ ; (i)  $x^2y^2 - xy - x$ .
6. (a) Determinare il numero delle classi di isomorfismo dei campi di funzioni  $K$  di grado 3 su  $F = \mathbb{C}(x)$ , le cui superfici di Riemann sono ramificate soltanto nei punti  $\pm 1$ .  
 (b) Descrivere gli incollamenti relativi alla superficie di Riemann corrispondente a ciascuna classe di isomorfismo di campi come una coppia di permutazioni.  
 (c) Per ciascuna classe di isomorfismo, determinare un polinomio  $f(x, y)$  tale che  $K = F[y]/(f)$  rappresenti la classe di isomorfismo.
- \*7. Dimostrare il teorema di esistenza di Riemann per le estensioni quadratiche.
- \*8. Sia  $S$  un rivestimento ramificato costruito con punti di ramificazione  $\alpha_1, \dots, \alpha_r$ , curve  $C_1, \dots, C_r$ , e permutazioni  $\sigma_1, \dots, \sigma_r$ . Dimostrare che  $S$  è connesso, se e soltanto se, il sottogruppo  $\Sigma$  del gruppo simmetrico  $S_n$ , che è generato dalle permutazioni  $\sigma_\nu$ , agisce transitivamente sugli indici  $1, \dots, n$ .
- \*9. Si può dimostrare che la superficie di Riemann  $S$  di un campo di funzioni è omeomorfa al complementare di un insieme finito di punti in una varietà di dimensione 2 orientata, compatta  $\bar{S}$ . Il genere di una tale superficie è definito come il numero dei buchi nella varietà corrispondente  $\bar{S}$ . Pertanto, se  $\bar{S}$  è una sfera, il genere di  $S$  è 0, mentre se  $\bar{S}$  è un toro, il genere di  $S$  è 1. Il genere di un campo di funzioni è definito come il genere della sua superficie di Riemann.  
 Determinare il genere del campo di funzioni definito da ciascuno dei seguenti polinomi:
  - (a)  $y^2 - (x^2 - 1)(x^2 - 4)$ ; (b)  $y^2 - x(x^2 - 1)(x^2 - 4)$ ; (c)  $y^3 + y + x$ ;
  - (d)  $y^3 - x(x-1)$ ; (e)  $y^3 - x(x-1)^2$ .
8. Estensioni trascendenti
1. Sia  $K = F(\alpha)$  un'estensione di campi generata da un elemento  $\alpha$ , e sia  $\beta \in K, \beta \notin F$ . Dimostrare che  $\alpha$  è algebrico sul campo  $F(\beta)$ .

## Capitolo 14

### Teoria di Galois

In una parola, i calcoli sono impossibili.  
Evariste Galois

#### 1 Il teorema fondamentale della teoria di Galois

Nell'ultimo capitolo abbiamo studiato le estensioni algebriche di campi, utilizzando principalmente le estensioni generate da un solo elemento. Ciò equivale a studiare le proprietà di una radice di un polinomio irriducibile

$$(1.1) \quad f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

La teoria di Galois, che costituisce l'argomento di questo capitolo, considera *tutte* le radici di un tale polinomio e ne studia le simmetrie.

Ci limiteremo a considerare qui campi di *caratteristica zero*: tutti i campi che incontreremo saranno di questo tipo, e d'ora in poi non ribadiamo esplicitamente questo fatto.

La notazione  $K/F$  indicherà che  $K$  è un'estensione di campi di  $F$ . Si tratta di una notazione standard, sebbene vi sia qualche pericolo di confusione con quella,  $R/I$ , del quoziente di un anello  $R$  rispetto a un ideale  $I$ .

Come abbiamo visto, i calcoli in un campo  $F(\alpha)$  generato da una radice di  $f$  possono essere effettuati facilmente identificando  $F(\alpha)$  con il campo  $F[x]/(f)$  costruito in modo formale. Ma supponiamo ora che in un'estensione di campi  $K$  un polinomio irriducibile  $f(x)$  si spezzi in fattori lineari, e che le sue radici in  $K$  siano  $\alpha_1, \dots, \alpha_n$ . Non è chiaro come svolgere i calcoli con tutte queste radici nello stesso tempo. Per questo dovremmo sapere quali relazioni intercorrono tra le radici, e ciò dipende dal caso particolare. In teoria, tali relazioni si possono ricavare sviluppando il polinomio nella forma  $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ . Si trova allora che la somma delle radici è  $-a_{n-1}$ , il loro prodotto è  $(-1)^n a_0$ , e così via. Ma non sempre è facile interpretare direttamente queste relazioni.

Il risultato fondamentale emerso dai lavori di vari matematici, soprattutto di Lagrange e Galois, è che le relazioni tra le radici sono esprimibili in termini di simmetria. Il primo modello di questa simmetria è il coniugio in  $\mathbb{C}$ , che scambia

tra loro le due radici  $\pm i$  del polinomio reale irriducibile  $x^2 + 1$  in  $\mathbb{R}[x]$ , lasciando fissi i numeri reali. Cominceremo con l'osservare che una simmetria di questo tipo esiste per ogni estensione quadratica di campi.

Un'estensione  $K/F$  di grado 2 è generata da ogni elemento  $\alpha$  di  $K$  non appartenente a  $F$ . Inoltre,  $\alpha$  è radice di un polinomio di secondo grado irriducibile:

$$(1.2) \quad f(x) = x^2 + bx + c,$$

a coefficienti in  $F$ . Allora anche  $\alpha' = -b - \alpha$  è una radice di  $f$ , e pertanto questo polinomio si spezza in fattori lineari in  $K[x]$ :  $f(x) = (x - \alpha)(x - \alpha')$ .

Il fatto che  $\alpha$  e  $\alpha'$  siano radici di uno stesso polinomio irriducibile ci fornisce la simmetria in questione. In base alla proposizione (2.9) del capitolo 13, esiste un isomorfismo

$$(1.3) \quad \sigma : F(\alpha) \rightarrow F(\alpha'),$$

che è l'identità su  $F$  e manda  $\alpha$  in  $\alpha'$ . D'altra parte, ciascuna delle due radici genera l'estensione, ossia:  $F(\alpha) = K = F(\alpha')$ . Pertanto  $\sigma$  è un automorfismo di  $K$ .

Tale automorfismo scambia tra loro  $\alpha$  e  $\alpha'$ . Infatti, essendo  $\sigma$  l'identità su  $F$ , lascia fisso  $b$ , e d'altra parte  $\alpha + \alpha' = b$ . Pertanto, se  $\sigma(\alpha) = \alpha'$ , si deve avere  $\sigma(\alpha') = \alpha$ . Ne segue che  $\sigma^2$  manda  $\alpha$  in  $\alpha$  e quindi, essendo  $K$  generato da  $\alpha$  su  $F$ , che  $\sigma^2$  è l'identità.

Conviene notare inoltre che  $\sigma$  non è l'automorfismo banale, poiché le due radici  $\alpha$  e  $\alpha'$  sono distinte. Se  $\alpha$  fosse una radice doppia del polinomio di secondo grado (1.2), la formula risolutiva dell'equazione  $f(x) = 0$  darebbe  $\alpha = -\frac{1}{2}b$ . Ne seguirebbe che  $\alpha \in F$ , contro l'ipotesi che  $f$  è irriducibile.

Poiché per ipotesi il nostro campo  $F$  ha caratteristica zero, l'estensione quadratica  $K$  può essere ottenuta aggiungendo una radice quadrata  $\delta$  del discriminante  $D = b^2 - 4c$ , ossia una radice del polinomio irriducibile  $x^2 - D$ . L'altra sua radice è  $-\delta$ , e  $\sigma$  scambia tra loro le due radici quadrate.

Ogni volta che  $K$  è ottenuto aggiungendo una radice quadrata  $\delta$ , esiste un automorfismo che manda  $\delta$  in  $-\delta$ . Per esempio, sia  $\alpha = 1 + \sqrt{2}$ , e poniamo  $K = \mathbb{Q}(\alpha)$ . Il polinomio minimo di  $\alpha$  su  $\mathbb{Q}$  è  $x^2 - 2x - 1$ , e l'altra radice di questo polinomio è  $\alpha' = 1 - \sqrt{2}$ . Esiste un automorfismo  $\sigma$  di  $K$  che manda  $\sqrt{2}$  in  $-\sqrt{2}$  e  $\alpha$  in  $\alpha'$ . È importante osservare immediatamente che un tale automorfismo non sarà continuo se si considera  $K$  come un sottocampo di  $\mathbb{R}$ . Esso è una simmetria della struttura algebrica di  $K$ , ma non rispetta la struttura geometrica data dall'immersione di  $K$  nella retta reale.

Per definizione, si dice *F-automorfismo* di un'estensione di campi  $K$  un automorfismo che sia l'identità sul sottocampo  $F$  [cfr. cap. 13 (2.10)]. In altre parole, un automorfismo  $\sigma$  di  $K$  è un *F-automorfismo* se  $\sigma(c) = c$ , per ogni  $c \in F$ . Pertanto il coniugio in  $\mathbb{C}$  è un  $\mathbb{R}$ -automorfismo di  $\mathbb{C}$ , e la simmetria  $\sigma$  che abbiamo appena trovato è un *F-automorfismo* dell'estensione quadratica  $K$ . Non è

2. Dimostrare che l'isomorfismo  $\mathbb{Q}(\pi) \rightarrow \mathbb{Q}(e)$  che manda  $\pi$  in  $e$  è discontinuo.

3. Siano  $F \subset K \subset L$  campi. Dimostrare che

$$\text{tr deg}_F L = \text{tr deg}_F K + \text{tr deg}_K L.$$

4. Sia  $(\alpha_1, \dots, \alpha_n) \subset K$  un insieme algebricamente indipendente su  $F$ . Dimostrare che un elemento  $\beta \in K$  è trascendente su  $F(\alpha_1, \dots, \alpha_n)$  se e soltanto se l'insieme  $(\alpha_1, \dots, \alpha_n; \beta)$  è algebricamente indipendente.

5. Dimostrare il teorema (8.3).

### 9 Campi algebricamente chiusi

1. Dedurre il corollario (9.5) dal teorema (9.4).

2. Dimostrare che il campo  $\bar{F}$  da noi costruito come unione di campi finiti è algebricamente chiuso.

\*3. Con le notazioni introdotte alla fine del paragrafo 9, un confronto delle immagini  $f(C_r)$  al variare del raggio mostra un altro aspetto geometrico interessante: per valori grandi di  $r$ , la curva  $f(C_r)$  ha  $n$  cappi. Ciò può essere espresso formalmente dicendo che la sua curvatura totale è  $2\pi n$ . Per piccoli valori di  $r$ , il termine lineare  $a_1 z + a_0$  domina  $f(z)$ . Allora  $f(C_r)$  descrive un solo cappio intorno ad  $a_0$  e la sua curvatura totale è semplicemente  $2\pi$ . Qualcosa accade per i cappi e per la curvatura, al variare di  $r$ . Spiegare questo fatto.

\*4. Se si dispone di un computer con un buon sistema grafico, usarlo per illustrare l'andamento di  $f(C_r)$  al variare di  $r$ . Utilizzare le coordinate  $(\log r, \theta)$ .

### Esercizi vari

1. Sia  $f(x)$  un polinomio irriducibile di grado 6 su un campo  $F$ , e sia  $K$  un'estensione quadratica di  $F$ . Dimostrare o confutare quanto segue:  $f$  è irriducibile su  $K$ , o è il prodotto di due polinomi irriducibili di terzo grado su  $K$ .

2. (a) Sia  $p$  un numero primo dispari. Dimostrare che esattamente metà degli elementi di  $\mathbb{F}_p^*$  sono quadrati e che, se  $\alpha, \beta$  non sono quadrati,  $\alpha\beta$  è un quadrato.

(b) Dimostrare la stessa proprietà enunciata in (a) per qualunque campo finito di ordine dispari.

(c) Dimostrare che in un campo finito di ordine pari, ogni elemento è un quadrato.

3. Scrivere esplicitamente il polinomio minimo su  $\mathbb{Q}$  di  $\alpha = \sqrt{2} + \sqrt{3}$  e dimostrare che esso è riducibile modulo  $p$  per ogni primo  $p$ .

\*4. (a) Dimostrare che ogni elemento di  $GL_2(\mathbb{Z})$  di ordine finito ha ordine 1, 2, 3, 4 o 6.

(b) Estendere tale risultato a  $GL_3(\mathbb{Z})$  e dimostrare che esso non vale in  $GL_4(\mathbb{Z})$ .

5. Sia  $c$  un numero reale diverso da 2, -2. La curva piana  $C$  di equazione  $x^2 + cxy + y^2 = 1$  possiede una rappresentazione parametrica razionale. Per ottenere tale rappresentazione, basta scegliere il punto  $(0, 1)$  su  $C$  e parametrizzare le rette, diciamo,  $L_t$  passanti

per questo punto mediante il loro coefficiente angolare:  $y = tx + 1$ . Il punto in cui la retta  $L_t$  interseca  $C$  può essere trovato algebricamente.

(a) Trovare esplicitamente le coordinate di questo punto.

(b) Usare tale procedimento per trovare tutte le soluzioni dell'equazione  $x^2 + cxy + y^2 = 1$  nel campo  $F = \mathbb{F}_p$ , con  $c \in F$  e  $c \neq \pm 2$ .

(c) Dimostrare che il numero delle soluzioni è  $p - 1$ ,  $p$  oppure  $p + 1$ , e descrivere in quale modo tale numero dipende dalle radici del polinomio  $t^2 + ct + 1$ .

6. Il *grado* di una funzione razionale  $f(x) = p(x)/q(x) \in \mathbb{C}(x)$  è definito come il massimo dei gradi di  $p$  e  $q$ , quando  $p, q$  sono scelti in modo da risultare primi tra loro. Ogni funzione razionale  $f$  definisce un'applicazione  $P' \rightarrow P'$ , data da  $x \mapsto f(x)$ . Denoteremo tale applicazione ancora con  $f$ .

(a) Supponiamo che  $f$  abbia grado  $d$ . Dimostrare che per ogni punto  $y_0$  nel piano, la fibra  $f^{-1}(y_0)$  contiene al più  $d$  punti.

(b) Dimostrare che, tranne che per un numero finito di punti  $y_0$ ,  $f^{-1}(y_0)$  consiste precisamente di  $d$  punti. Specificare per mezzo di  $f$  e  $df/dx$  i valori  $y_0$  per cui vi sono meno di  $d$  punti.

\*7. (a) Dimostrare che una funzione razionale  $f(x)$  genera il campo delle funzioni razionali  $\mathbb{C}(x)$  se, e soltanto se, è della forma  $(ax + b)/(cx + d)$ , con  $ad - bc \neq 0$ .

(b) Determinare il gruppo degli automorfismi di  $\mathbb{C}(x)$  che coincidono con l'identità su  $\mathbb{C}$ .

\*8. Sia  $K/F$  un'estensione quadratica di campi di funzioni razionali, diciamo  $K = \mathbb{C}(t)$  e  $F = \mathbb{C}(x)$ . Dimostrare che esistono generatori  $x', t'$  per i due campi, tali che  $t = (\alpha t' + \beta)/(\gamma t' + \delta)$  e  $x = (ax' + b)/(cx' + d)$ , con  $\alpha, \beta, \gamma, \delta, a, b, c, d \in \mathbb{C}$ , tali che  $t'^2 = x'$ .

\*9. Utilizzare i suggerimenti qui sotto riportati per dare una dimostrazione algebrica del fatto che  $K = \mathbb{C}(x)[y]/(y^2 - x^3 + x)$  non è un'estensione trascendente pura di  $\mathbb{C}$ . Supponiamo che  $K = \mathbb{C}(t)$  per qualche  $t$ . Allora  $x$  e  $y$  sono funzioni razionali di  $t$ .

(a) Usando il risultato del problema precedente e sostituendo  $t$  con  $t'$ , se necessario, ridursi al caso in cui  $x = (at^2 + b)/(ct^2 + d)$ .

(b) Scriviamo  $y = p(t)/q(t)$ . Allora l'equazione  $y^2 = x(x+1)(x-1)$  diventa:

$$\frac{p(t)^2}{q(t)^2} = \frac{(at^2 + b)((a+c)t^2 + b+d)((a-c)t^2 + b-d)}{(ct^2 + d)^3}.$$

Ora, o i numeratori e i denominatori nei due membri coincidono, oppure vi sono termini da cancellare nel secondo membro.

(c) Completare la dimostrazione, analizzando le due possibilità date in (b).

\*10. (a) Dimostrare che l'omomorfismo  $SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{F}_p)$  ottenuto riducendo gli elementi delle matrici modulo  $p$  è suriettivo.

(b) Dimostrare la proprietà analogica per  $SL_n$ .

\*11. Determinare le classi di coniugio degli elementi di ordine 2 in  $GL_n(\mathbb{Z})$ .

difficile dimostrare che  $\sigma$  è l'unico  $F$ -automorfismo di questa estensione diverso dall'identità.

Il gruppo di tutti gli  $F$ -automorfismi di un'estensione  $K$  di  $F$  è detto *gruppo di Galois* dell'estensione di campi. Tale gruppo si denota spesso con  $G(K/F)$ . Se  $K/F$  è un'estensione quadratica,  $G(K/F)$  è un gruppo di ordine 2.

Consideriamo ora il caso più semplice dopo quello dell'estensione quadratica, ossia un'estensione biquadratica. Diremo che un'estensione di campi  $K/F$  è un'estensione *biquadratica* se  $[K : F] = 4$  e  $K$  è generato dalle radici di *due* polinomi irriducibili di secondo grado. Ogni estensione biquadratica ha la forma:

$$(1.4) \quad K = F(\alpha, \beta),$$

dove  $\alpha^2 = a$  e  $\beta^2 = b$ , con  $a, b \in F$ . L'elemento  $\beta$  genera un campo intermedio, cioè un campo  $F(\beta)$  tale che  $F \subset F(\beta) \subset K$ . Poiché  $K = F(\alpha, \beta)$ , la condizione  $[K : F] = 4$  implica che  $F(\beta)$  ha grado 2 su  $F$  e che  $\alpha$  non appartiene al campo  $F(\beta)$ . Il polinomio  $x^2 - a$  è dunque irriducibile su  $F(\beta)$ , e analogamente, il polinomio  $x^2 - b$  è irriducibile sul campo intermedio  $F(\alpha)$ .

Si noti che il campo  $K$  è un'estensione di  $F(\beta)$  di grado 2 generata da  $\alpha$ . Applichiamo dunque ad esso quanto abbiamo appena appreso sulle estensioni quadratiche. Sostituendo  $F$  con  $F(\beta)$ , troviamo che esiste un  $F(\beta)$ -automorfismo di  $K$  che scambia tra loro le due radici  $\pm\alpha$  di  $x^2 - a$ . Chiamiamo  $\sigma$  tale automorfismo. Poiché  $\sigma$  è l'identità su  $F(\beta)$ ,  $\sigma$  è anche l'identità su  $F$ , sicché risulta anche un  $F$ -automorfismo. Analogamente, esiste un  $F(\alpha)$ -automorfismo  $\tau$  di  $K$  che scambia tra loro le radici  $\pm\beta$  di  $x^2 - b$ , e  $\tau$  è anche un  $F$ -automorfismo.

I due automorfismi che abbiamo trovato agiscono sulle radici  $\alpha, \beta$  nel modo seguente:

$$(1.5) \quad \begin{array}{l} \alpha \xrightarrow{\sigma} -\alpha \quad \alpha \xrightarrow{\tau} \alpha \\ \beta \xrightarrow{\sigma} \beta \quad \beta \xrightarrow{\tau} -\beta. \end{array}$$

Componendo questi automorfismi, troviamo che  $\sigma\tau$  cambia i segni di entrambe le radici  $\alpha, \beta$  e che gli automorfismi  $\sigma^2, \tau^2$  e  $\sigma\tau\sigma\tau$  lasciano fisse  $\alpha$  e  $\beta$ . Poiché  $K$  è generato su  $F$  dalle radici  $\alpha, \beta$ , questi ultimi tre automorfismi sono tutti uguali all'identità. Pertanto i quattro automorfismi  $\{1, \sigma, \tau, \sigma\tau\}$  formano un gruppo di ordine 4, con le relazioni

$$\sigma^2 = 1, \quad \tau^2 = 1, \quad \sigma\tau = \tau\sigma.$$

Abbiamo dimostrato che il gruppo di Galois  $G(K/F)$  contiene il gruppo quadrinomio di Klein. Di fatto è uguale al gruppo di Klein, come vedremo subito.

Per esempio, sia  $F = \mathbb{Q}$ ,  $\alpha = i$  e  $\beta = \sqrt{2}$ , sicché  $K = \mathbb{Q}(i, \sqrt{2})$ . In questo caso, l'automorfismo  $\sigma$  è il coniugio relativo ai numeri complessi, mentre  $\tau$  manda  $\sqrt{2}$  in  $-\sqrt{2}$ , lasciando fisso  $i$ .

Per le estensioni quadratiche o biquadratiche, il grado  $[K : F]$  è uguale all'ordine del gruppo di Galois  $G(K/F)$ . Enunceremo ora i teoremi (1.6) e (1.11), i quali descrivono le circostanze generali in cui ciò accade. Le dimostrazioni verranno date più avanti (p. 650).

(1.6) TEOREMA *Per ogni estensione finita  $K/F$ , l'ordine  $|G(K/F)|$  del gruppo di Galois divide il grado  $[K : F]$  dell'estensione.*

Un'estensione finita di campi  $K/F$  è detta *estensione di Galois* se l'ordine del gruppo di Galois è uguale al grado:

$$(1.7) \quad |G(K/F)| = [K : F].$$

Il teorema (1.6) prova che il gruppo di Galois di un'estensione biquadratica ha al più ordine 4. Poiché abbiamo già quattro automorfismi, non ve ne sono altri, e il gruppo di Galois è il gruppo quadrinomio di Klein, come asserito. Tutte le estensioni quadratiche e biquadratiche sono estensioni di Galois.

Se  $G$  è un gruppo di automorfismi di un campo  $K$ , l'insieme degli elementi di  $K$  che sono lasciati fissi da tutti gli automorfismi di  $G$  forma un sottocampo detto il *campo fisso* di  $G$ . Esso si denota spesso con  $K^G$ :

$$(1.8) \quad K^G = \{\alpha \in K \mid \varphi(\alpha) = \alpha \text{ per ogni } \varphi \in G\}.$$

Dal teorema 1.6 segue in particolare che, se  $K/F$  è un'estensione di Galois, gli unici elementi di  $K$  che sono lasciati fissi dall'intero gruppo di Galois sono gli elementi di  $F$ :

(1.9) COROLLARIO *Sia  $K/F$  un'estensione di Galois, con gruppo di Galois  $G = G(K/F)$ . Allora il campo fisso di  $G$  è  $F$ .*

Infatti, denotiamo il campo fisso con  $L$ . Allora  $F \subset L$ , e ciò mostra che ogni  $L$ -automorfismo di  $K$  è anche un  $F$ -automorfismo, ossia che  $G(K/L) \subset G$ . D'altra parte, essendo  $L$  il campo fisso di  $G$ , ogni elemento di  $G$  è un  $L$ -automorfismo. Pertanto  $G(K/L) = G$ . Ora  $|G| = [K : F]$ , poiché  $K/F$  è un'estensione di Galois, e, in base al teorema (1.6),  $|G|$  divide  $[K : L]$ . Poiché  $F \subset L \subset K$ , ciò mostra che  $[K : F] = [K : L]$ , e quindi che  $F = L$ . ■

Questo corollario è importante poiché fornisce un metodo per verificare che un elemento di un'estensione di Galois  $K/F$  appartiene effettivamente al campo  $F$ . Noi lo useremo spesso.

La condizione perché un'estensione di campi sia un'estensione di Galois è formalmente restrittiva; tuttavia, vi sono molte estensioni di Galois. Questo è il fatto fondamentale che ha condotto alla teoria di Galois. Per poter enunciare il teorema che descrive le estensioni di Galois, abbiamo ancora bisogno di una definizione.

- (1.10) DEFINIZIONE Sia  $f(x) \in F[x]$  un polinomio monico non costante. Un campo di spezzamento di  $f(x)$  su  $F$  è un'estensione di campi  $K$  di  $F$  tale che
- $f(x)$  si scomponga in fattori lineari in  $K[x]$ , ossia  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ , con  $\alpha_i \in K$ ;
  - $K$  è generato dalle radici di  $f(x)$ :  $K = F(\alpha_1, \dots, \alpha_n)$ .

La seconda condizione dice esattamente che  $K$  è la più piccola estensione di  $F$  che contiene tutte le radici. L'estensione biquadratica (1.4) è un campo di spezzamento di  $f(x) = (x^2 - a)(x^2 - b)$ .

Ogni polinomio  $f(x) \in F[x]$  ha un campo di spezzamento. Per trovarne uno, scegliamo un campo  $L \supset F$  in cui  $f$  si scomponga in fattori lineari [cap. 13 (5.3)] e prendiamo poi per  $K$  il sottocampo  $F(\alpha_1, \dots, \alpha_n)$  di  $L$  generato dalle radici.

- (1.11) TEOREMA Se  $K$  è un campo di spezzamento di un polinomio  $f(x)$  su  $F$ , allora  $K$  è un'estensione di Galois di  $F$ . Viceversa, ogni estensione di Galois di  $F$  è un campo di spezzamento di qualche polinomio  $f(x) \in F[x]$ .

- (1.12) COROLLARIO Ogni estensione finita è contenuta in un'estensione di Galois.

Per dimostrare questo corollario a partire dal teorema, sia  $K/F$  un'estensione finita, siano  $\alpha_1, \dots, \alpha_n$  generatori di  $K$  su  $F$ , e siano  $f_i(x)$  i polinomi minimi di  $\alpha_i$  su  $F$ . Estendiamo  $K$  a un campo di spezzamento  $L$  del prodotto  $f = f_1 \cdots f_n$  su  $K$ . Allora  $L$  sarà anche un campo di spezzamento di  $f$  su  $F$ . Pertanto  $L$  è l'estensione di Galois richiesta. ■

- (1.13) COROLLARIO Sia  $K/F$  un'estensione di Galois, e sia  $L$  un campo intermedio:  $F \subset L \subset K$ . Allora anche  $K/L$  è un'estensione di Galois.

Infatti, se  $K$  è il campo di spezzamento di un polinomio  $f(x)$  su  $F$ , esso è anche il campo di spezzamento dello stesso polinomio sul campo più grande  $L$ , e pertanto è un'estensione di Galois di  $L$ . ■

Ritorniamo ora alle estensioni biquadratiche. Possiamo dimostrare che il gruppo di Galois di un'estensione biquadratica ha ordine 4 senza ricorrere al teorema (1.6). Tutto ciò di cui abbiamo bisogno è la seguente proposizione elementare:

#### (1.14) PROPOSIZIONE

- Sia  $K$  un'estensione di un campo  $F$ , sia  $f(x)$  un polinomio a coefficienti in  $F$ , e sia  $\sigma$  un  $F$ -automorfismo di  $K$ . Se  $\alpha$  è una radice di  $f(x)$  in  $K$  allora anche  $\sigma(\alpha)$  è una radice.

- Sia  $K$  un'estensione di campi generata su  $F$  da elementi  $\alpha_1, \dots, \alpha_n$ , e sia  $\sigma$  un  $F$ -automorfismo di  $K$ . Se  $\sigma$  lascia fissi tutti i generatori  $\alpha_i$ , è l'automorfismo banale.
- Sia  $K$  un campo di spezzamento di un polinomio  $f(x)$  su  $F$ . Allora il gruppo di Galois  $G(K/F)$  agisce fedelmente sull'insieme  $\{\alpha_1, \dots, \alpha_n\}$ .

*Dimostrazione.* La parte (a) è stata dimostrata nell'ultimo capitolo [cap. 13 (2.10)]. Avendo supposto in (b) che il campo  $K$  sia generato da  $\alpha_1, \dots, \alpha_n$ , ogni elemento di  $K$  può essere espresso come un polinomio in  $\alpha_1, \dots, \alpha_n$  a coefficienti in  $F$  [cap. 13 (2.6b)]. Se  $\sigma$  è un automorfismo di  $K$  che è l'identità su  $F$  e lascia fisso ciascun  $\alpha_i$ , allora  $\sigma$  lascia fisso ogni polinomio in  $\alpha_1, \dots, \alpha_n$  a coefficienti in  $F$ , e pertanto è l'identità. L'asserzione (c) è conseguenza delle prime due. Infatti, la prima dice che ogni automorfismo  $\sigma \in G(K/F)$  permuta l'insieme  $\{\alpha_1, \dots, \alpha_n\}$ , e la seconda ci dice che l'azione su questo insieme è fedele. ■

La proposizione (1.14) non tocca la questione più interessante, che è il problema centrale della teoria di Galois: *quali permutazioni delle radici di un polinomio si estendono ad automorfismi del campo di spezzamento?*

Applichiamo la (1.14) all'estensione biquadratica (1.4). La parte (a), applicata al polinomio  $x^2 - a$ , mostra che ogni  $F$ -automorfismo  $\varphi$  di  $K$  permuta le radici  $\pm\sqrt{a}$ . Similmente,  $\varphi$  permuta  $\pm\sqrt{b}$ . Soltanto quattro permutazioni dell'insieme  $\{\pm\sqrt{a}, \pm\sqrt{b}\}$  agiscono in tal modo. Poiché gli elementi  $\alpha, \beta$  generano  $K$ , l'enunciato (1.14b) ci dice che un  $F$ -automorfismo che lascia fissi  $\alpha$  e  $\beta$  è l'identità. Pertanto i quattro automorfismi già trovati sono gli unici, e ciò dimostra che  $G(K/F)$  è il gruppo quadrinomio di Klein.

Una delle parti più importanti della teoria di Galois è la determinazione dei campi intermedi  $L$ , compresi tra  $F$  e  $K$ :  $F \subset L \subset K$ . Il teorema fondamentale della teoria di Galois afferma che, se  $K/F$  è un'estensione di Galois, i campi intermedi sono in corrispondenza biunivoca con i sottogruppi del gruppo di Galois. L'importanza di questa corrispondenza biunivoca non è chiara immediatamente. Dovremo vederla applicata per comprenderla.

Il campo intermedio corrispondente a un sottogruppo  $H$  di  $G(K/F)$  è il campo fisso  $K^H$  di  $H$  definito in precedenza. Nell'altra direzione, se  $L$  è un campo intermedio, il gruppo di Galois  $G(K/L)$  è un sottogruppo di  $G(K/F)$ . È questo il sottogruppo corrispondente a  $L$ .

- (1.15) TEOREMA FONDAMENTALE Sia  $K$  un'estensione di Galois di un campo  $F$ , e sia  $G = G(K/F)$  il suo gruppo di Galois. La funzione

$$H \mapsto K^H$$

è un'applicazione biiettiva dall'insieme dei sottogruppi di  $G$  all'insieme dei campi intermedi  $F \subset L \subset K$ . La sua funzione inversa è

$$L \mapsto G(K/L).$$

Tale corrispondenza ha la proprietà che, se  $H = G(K/L)$ , allora si ha

$$(1.16) \quad [K : L] = |H|, \quad \text{e quindi } [L : F] = |G : H|.$$

Dimostreremo questo teorema nel paragrafo 5.

I campi  $F$  e  $K$  sono inclusi tra i campi intermedi. Il sottogruppo corrispondente a  $F$  è l'intero gruppo  $G$  [cfr. (1.9)], e quello corrispondente a  $K$  è il sottogruppo banale  $\{1\}$ .

Ritorniamo ora all'esempio precedente dell'estensione biquadratica  $K = \mathbb{Q}(i, \sqrt{2})$ , per la quale  $\sigma$  è il coniugio relativo ai numeri complessi, mentre  $\tau$  scambia  $\sqrt{2}$  e  $-\sqrt{2}$ . Il suo gruppo di Galois, che è il gruppo quadrinomio di Klein, ha tre sottogruppi propri:

$$H_1 = \{1, \sigma\}, \quad H_2 = \{1, \tau\}, \quad H_3 = \{1, \sigma\tau\}.$$

Per il teorema fondamentale, vi sono tre campi intermedi propri, precisamente i campi  $L_i$  lasciati fissi da questi sottogruppi. Essi si determinano facilmente:

$$L_1 = \mathbb{Q}(\sqrt{2}), \quad L_2 = \mathbb{Q}(i), \quad L_3 = \mathbb{Q}(i\sqrt{2}).$$

Un gruppo di Galois è finito, e pertanto ha un numero finito di sottogruppi. Ma, senza il teorema fondamentale, non è ovvio che esista soltanto un numero finito di campi intermedi. Ci si potrebbe aspettare che due elementi scelti a caso di un'estensione di Galois  $K/F$  generino sottocampi distinti. In genere ciò non accade, e infatti la maggior parte degli elementi genereranno l'intera estensione  $K$ . Il caso dell'estensione biquadratica  $K = \mathbb{Q}(i, \sqrt{2})$  servirà a illustrare questo punto. Sia  $\gamma$  un elemento arbitrario di  $K$ . Il campo  $\mathbb{Q}(\gamma)$  generato da  $\gamma$  deve essere uno dei campi intermedi trovati. Se dunque  $\gamma$  non è contenuto in  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt{2})$  o  $\mathbb{Q}(i\sqrt{2})$ , allora  $\mathbb{Q}(\gamma) = K$ . Ora, l'insieme  $(1, i, \sqrt{2}, i\sqrt{2})$  è una base di  $K$  su  $\mathbb{Q}$ , sicché possiamo scrivere un elemento arbitrario  $\gamma$  nella forma

$$\gamma = c_1 + c_2 i + c_3 \sqrt{2} + c_4 i\sqrt{2}, \quad \text{con } c_i \in \mathbb{Q}.$$

Questo elemento non appartiene a nessuno dei tre campi intermedi propri, a meno che due dei coefficienti  $c_2, c_3, c_4$  non siano nulli. Per esempio, l'elemento  $i + \sqrt{2}$  genera l'intera estensione  $K$ . Ritneremo su questo punto nel paragrafo 4.

## 2 Equazioni di terzo grado

Dopo le equazioni biquadratiche, la successiva classe generale di esempi di cui ci occuperemo, è data dai campi di spezzamento dei polinomi di terzo grado. Le equazioni di terzo grado:

$$(2.1) \quad f(x) = x^3 + a_2 x^2 + a_1 x + a_0 = 0,$$

furono risolte esplicitamente per mezzo di radici quadrate e radici cubiche nel sedicesimo secolo dai matematici Tartaglia e Cardano. Cominceremo col riprendere in esame la soluzione "ad hoc" da essi trovata, davvero notevole.

I calcoli sono più semplici quando il coefficiente del termine di grado 2 in  $f(x)$  è uguale a zero. Il termine di secondo grado nell'equazione generale (2.1) può essere eliminato mediante la sostituzione

$$(2.2) \quad x = x_1 - a_2/3.$$

Scriviamo un polinomio di terzo grado, con il termine di grado 2 uguale a zero, nella forma

$$(2.3) \quad f(x) = x^3 + px + q,$$

dove i coefficienti  $p, q$  sono elementi del campo  $F$ . La soluzione di Cardano dell'equazione  $f = 0$  inizia con la sostituzione  $x = u - v$ . Raccogliendo i termini in  $f(u - v)$ , troviamo

$$f(u - v) = (u^3 - v^3) - (3uv - p)(u - v) + q.$$

Il vantaggio della sostituzione della variabile  $x$  con una somma di variabili è dato dalla possibilità di spezzare l'equazione. Chiaramente, se le due equazioni

$$3uv - p = 0, \quad u^3 - v^3 + q = 0$$

sono soddisfatte, allora  $f(u - v) = 0$ . Inoltre, poiché abbiamo due variabili, possiamo sperare di ottenere soluzioni per tale coppia di equazioni, anche se non è chiaro a priori se ciò sarà utile. Risolvendo la prima equazione rispetto a  $v$ , otteniamo  $v = p/3u$ , e sostituiamo tale espressione nella seconda. Eliminando i denominatori, si ha:

$$3^3 u^6 - p^3 + 3^3 u^3 q = 0.$$

Miracolosamente, questa equazione è di secondo grado in  $u^3$ . Ponendo  $y = u^3$ , essa si riduce a

$$(2.4) \quad 3^3 y^2 + 3^3 qy - p^3 = 0,$$

che può essere risolta mediante la formula ben nota

$$(2.5) \quad y = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Otteniamo in tal modo la *formula di Cardano*:  $x = u - v$ , dove

$$(2.6) \quad u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad v = \sqrt[3]{u^3 + q} = \sqrt[3]{+\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Saremo in grado di dimostrare l'esistenza di una soluzione generale di questo tipo più avanti, senza calcoli esplicativi [cfr. (7.6)].

Esaminiamo ora la teoria di Galois di un polinomio di terzo grado irriducibile  $f(x)$ . Possiamo supporre che  $f(x)$  abbia la forma (2.3). Sia  $K$  un campo di spezzamento di  $f(x)$  su  $F$ , e siano  $\alpha_1, \alpha_2, \alpha_3$  le tre radici di  $f(x)$  in  $K$ , ordinate in modo arbitrario, sicché:

$$(2.7) \quad f(x) = x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Sviluppando il secondo membro, otteniamo le relazioni

$$(2.8) \quad \begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 &= p \\ \alpha_1\alpha_2\alpha_3 &= -q. \end{aligned}$$

La prima di queste relazioni mostra che la terza radice  $\alpha_3$  appartiene al campo generato dalle prime due. Abbiamo così una catena di campi

$$F \subset F(\alpha_1) \subset K,$$

con  $K = F(\alpha_1, \alpha_2) = F(\alpha_1, \alpha_2, \alpha_3)$ . Denotiamo  $F(\alpha_1)$  con  $L$ . Allora possono presentarsi due casi fondamentalmente diversi, precisamente

$$(2.9) \quad L = K \quad \text{oppure} \quad L < K.$$

In termini di radici, il primo caso si presenta quando le ultime due radici  $\alpha_2$  e  $\alpha_3$  possono essere espresse per mezzo di  $\alpha_1$  e di elementi di  $F$ , ossia, se esse possono essere scritte come polinomi in  $\alpha_1$  a coefficienti in  $F$  [cfr. cap. 13 (2.6)]. Il secondo caso si presenta quando questo non succede.

Per esempio, sia  $f(x) = x^3 - 2$ . Le tre radici di questo polinomio sono  $\alpha_1 = \sqrt[3]{2}$ ,  $\alpha_2 = \zeta \sqrt[3]{2}$ ,  $\alpha_3 = \zeta^2 \sqrt[3]{2}$ , dove  $\sqrt[3]{2}$  denota la radice cubica reale di 2, e  $\zeta = e^{2\pi i/3}$ . Poiché  $\alpha_1$  è reale, il campo  $\mathbb{Q}(\alpha_1)$  è contenuto in  $\mathbb{R}$ . Esso non contiene le altre radici, che sono complesse. Pertanto, se  $F = \mathbb{Q}$  e  $L = \mathbb{Q}(\alpha_1)$ , siamo nel secondo caso. D'altra parte, se poniamo  $F = \mathbb{Q}(\zeta)$ , allora  $F(\alpha_1)$  contiene  $\alpha_2$ , sicché siamo nel primo caso.

Per analizzare la dicotomia (2.9), consideriamo il modo in cui il polinomio irriducibile  $f(x)$  si fattorizza in  $L[x]$ . Per ipotesi,  $f(x)$  è irriducibile in  $F[x]$  e si decomponete in fattori lineari in  $K[x]$ . Nell'anello  $L[x]$ ,  $f(x)$  ha il fattore  $(x - \alpha_1)$ :

$$(2.10) \quad f(x) = (x - \alpha_1)h(x).$$

dove  $h(x)$  è un polinomio di secondo grado a coefficienti in  $L$ . La divisione per  $x - \alpha_1$  dà lo stesso risultato se viene effettuata nel campo più grande  $K$ . Se

consideriamo (2.7), vediamo che  $h(x) = (x - \alpha_2)(x - \alpha_3)$  in  $K[x]$ . Pertanto  $L < K$  se e soltanto se  $h(x)$  è irriducibile in  $L[x]$ . In tal caso, il grado di  $L(\alpha_2) = K$  su  $L$  è 2. Inoltre, poiché supponiamo che  $f(x)$  sia irriducibile su  $F$ , si ha:  $[L : F] = 3$ , in entrambi i casi. Pertanto risulta

$$(2.11) \quad [K : F] = \begin{cases} 3, & \text{se } L = K \\ 6, & \text{se } L < K. \end{cases}$$

### (2.12) Esempio

Il polinomio  $f(x) = x^3 + 3x + 1$  è irriducibile su  $\mathbb{Q}$  e ha una sola radice reale. Per vedere che esiste una sola radice reale, basta osservare che la derivata di  $f$  non si annulla sulla retta reale. Pertanto  $f(x)$  definisce una funzione crescente della variabile reale  $x$ . Essa assume il valore 0 una sola volta. La radice reale non genera il campo di spezzamento  $K$ , il quale contiene anche due radici complesse. Quindi, in questo caso,  $[K : \mathbb{Q}] = 6$ .

D'altra parte, il campo di spezzamento del polinomio  $f(x) = x^3 - 3x + 1$  su  $\mathbb{Q}$  ha grado 3. Una delle sue radici è  $\eta_1 = 2 \cos 2\pi/9 = \zeta + \zeta^8$ , dove  $\zeta = e^{2\pi i/9}$ . Ciò si può verificare direttamente. Ma in realtà, abbiamo fatto questo esempio calcolando il polinomio minimo di  $\eta_1$  su  $\mathbb{Q}$ . Il modo per calcolare questo polinomio è quello di provare a indovinare le altre sue radici. Osserviamo che  $\eta_1$  è la somma di una radice nona di 1 e della sua inversa. Vi sono altre due somme di questo tipo:  $\eta_2 = \zeta^2 + \zeta^7$  e  $\eta_3 = \zeta^4 + \zeta^5$ . Ora supponiamo che queste siano le altre radici e sviluppiamo il prodotto  $(x - \eta_1)(x - \eta_2)(x - \eta_3)$ , ottenendo  $f$ . In questo esempio, si ha che  $\eta_2$  è uguale a  $\eta_1^2 - 2$ , e  $\eta_3 = -\eta_1 - \eta_2$ .

Pertanto  $K = \mathbb{Q}(\eta_1)$ . ■

Ritorniamo allo studio di un'equazione generica di terzo grado. In base al teorema (1.11), l'ordine del gruppo di Galois  $G = G(K/F)$  è il grado dell'estensione  $[K : F]$ . Per le equazioni di terzo grado tale grado determina completamente il gruppo  $G$ . Precisamente, la proposizione (1.14) ci dice che  $G$  agisce fedelmente sull'insieme delle radici  $\{\alpha_1, \alpha_2, \alpha_3\}$ . Queste radici sono distinte [cap. 13 (5.8)], e pertanto  $G$  è un sottogruppo del gruppo simmetrico  $S_3$ , il quale ha ordine 6. Se  $[K : F] = 6$ ,  $G$  è l'intero gruppo simmetrico. In questo caso, ogni permutazione delle radici è indotta da un  $F$ -automorfismo di  $K$ . D'altra parte, l'unico sottogruppo di  $S_3$  di ordine 3 è il gruppo alterno  $A_3$ , che è un gruppo ciclico. Quindi, se  $[K : F] = 3$ , si ha  $G = A_3$ . In tal caso, le permutazioni cicliche e l'identità sono le uniche permutazioni che si estendono ad  $F$ -automorfismi. Dunque le radici di un polinomio di terzo grado irriducibile possono avere o simmetria diedrale o simmetria ciclica. Tuttavia queste simmetrie sono algebriche; esse non saranno simmetrie di  $K$  se questo campo viene considerato come un insieme di punti nel piano complesso.

Determiniamo i campi intermedi nel caso in cui il grado  $[K : F]$  è 6. (Quando  $[K : F] = 3$  non vi sono campi intermedi tra  $F$  e  $K$ , in senso stretto). Il gruppo simmetrico  $S_3$  ha tre sottogruppi coniugati di ordine 2 e un sottogruppo,  $A_3$ , di ordine 3. Vi sono ovviamente i tre campi intermedi:  $F(\alpha_1)$ ,  $F(\alpha_2)$ ,  $F(\alpha_3)$ . Essi sono sottocampi di  $K$  isomorfi, ma non uguali, e corrispondono ai tre sottogruppi di ordine 2. Ma il campo intermedio che corrisponde al sottogruppo  $A_3$  non è ovvio. Denotiamo questo campo misterioso con  $L$ . In base al teorema fondamentale,  $G(K/L) = A_3$ . Ne segue che  $[K : L] = 3$  e  $[L : F] = 2$ . Pertanto  $L$  è un'estensione quadratica di  $F$ , che può essere ottenuta aggiungendo una radice quadrata. Il teorema fondamentale ci assicura che vale una proprietà interessante, precisamente che  $K$  contiene la radice quadrata  $\delta$  di un elemento di  $F$ . Inoltre, poiché vi è una sola estensione intermedia di grado 2, tale radice quadrata è essenzialmente unica. Il teorema fondamentale ci dice anche che  $L$  è il campo fisso del sottogruppo  $A_3$ . Pertanto una permutazione pari delle radici lascia fisso  $\delta$ , mentre una permutazione dispari non fa altrettanto. L'elemento richiesto è

$$(2.13) \quad \delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

Una permutazione delle radici moltiplica  $\delta$  per il segno della permutazione. Ne segue che  $\delta$  non è lasciato fisso da tutti gli elementi di  $G(K/F) = S_3$ , sicché  $\delta \notin F$ . Ma l'elemento  $\delta^2$  è lasciato fisso da ogni permutazione. Il corollario (1.9) ci dice allora che  $\delta^2 \in F$ .

Dato un qualunque polinomio di terzo grado  $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ , l'elemento

$$(2.14) \quad D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

è detto *discriminante* del polinomio. Esso è un elemento di  $F$ , ed è uguale a zero se e soltanto se due radici di  $f(x)$  sono uguali. È dunque analogo al discriminante del polinomio di secondo grado  $x^2 + bx + c = (x - \alpha_1)(x - \alpha_2)$ , che è  $b^2 - 4c = (\alpha_1 - \alpha_2)^2$ . Se il polinomio di terzo grado  $f$  è irriducibile, le sue radici sono distinte, e quindi  $D \neq 0$ .

Il fatto che il discriminante del polinomio di terzo grado sia un elemento di  $F$  segue dal corollario (1.9), ma non è banale. Dimostreremo tale fatto in un contesto astratto nel prossimo paragrafo, ma esso può anche essere verificato mediante un calcolo diretto. Utilizzando le formule (2.8), possiamo calcolare il discriminante per mezzo dei coefficienti  $p, q$ . Si ha allora:

$$(2.15) \quad D = -4p^3 - 27q^2.$$

(2.16) PROPOSIZIONE *Il discriminante di un polinomio di terzo grado irriducibile  $f(x) \in F[x]$  è un quadrato in  $F$  se e soltanto se il grado del campo di spezzamento è 3.*

Se sceglioamo a caso un polinomio a coefficienti interi, vi sono buone probabilità che il suo discriminante non sia un quadrato in  $\mathbb{Q}$ . Per esempio, il discriminante di  $x^3 + 3x + 1$  è  $-135$ . D'altra parte, il discriminante di  $x^3 - 3x + 1$  è  $81$ , dunque un quadrato. Ciò è in accordo col fatto che  $[K : F] = 3$  [cfr. (2.12)].

*Dimostrazione.* Se  $D$  non è un quadrato, allora  $\delta \notin F$ , e pertanto  $[F(\delta) : F] = 2$ . Poiché  $\delta \in K$ ,  $[K : F]$  è divisibile per 2, e quindi [cfr. (2.11)] si ha  $[K : F] = 6$ . D'altra parte, se  $\delta \in F$ , allora ogni elemento del gruppo di Galois  $G = G(K/F)$  lascia fisso  $\delta$ . Poiché le permutazioni dispari cambiano il segno di  $\delta$ , esse non appartengono a  $G$ , e quindi  $G \neq S_3$ . Pertanto  $[K : F] = 3$ . ■

Come potrebbe essere vera tale proposizione? Ci deve essere una formula che esprime la seconda radice  $\alpha_2$  per mezzo degli elementi  $\alpha_1, \delta$ , e dei coefficienti  $p, q$ . Questa formula esiste, ed è istruttivo calcolarla esplicitamente.

### 3 Funzioni simmetriche

La teoria di Galois si occupa del problema di determinare le permutazioni delle radici di un polinomio che si estendono ad automorfismi di campi. In questo paragrafo esamineremo una situazione semplice in cui ogni permutazione si estende, precisamente quando le radici sono variabili indipendenti.

Sia  $R$  un anello arbitrario, e consideriamo l'anello dei polinomi  $R[u_1, \dots, u_n]$  nelle  $n$  variabili  $u_i$ . Si può fare in modo che una permutazione  $\sigma$  di  $\{1, \dots, n\}$  agisca sui polinomi, permutando le variabili. Dobbiamo decidere qui come vogliamo fare agire le permutazioni. Supponiamo di voler conservare gli automorfismi a sinistra. In tal caso  $\sigma$  agisce mediante la permutazione inversa sugli indici:

$$(3.1) \quad f = f(u_1, \dots, u_n) \xrightarrow{\sigma} f(u_{1\sigma^{-1}}, \dots, u_{n\sigma^{-1}}) = \sigma f.$$

Questo è chiaramente un automorfismo di  $R[u]$ . Poiché agisce come l'identità su  $R$ ,  $\sigma$  è detto *R-automorfismo*. Pertanto il gruppo simmetrico  $S_n$  agisce mediante *R-automorfismi* sull'anello dei polinomi  $R[u]$ . Un polinomio si dice *simmetrico* se è lasciato fisso da tutte le permutazioni.

È facile descrivere i polinomi simmetrici. Affinché un polinomio  $g$  sia simmetrico, due monomi in  $u_1, \dots, u_n$  che differiscono per una permutazione degli indici, ad esempio  $u_1^2 u_2$  e  $u_2^2 u_3$ , devono avere gli stessi coefficienti in  $g$ . Un polinomio simmetrico che contiene un certo monomio deve contenere l'intera orbita. Ad esempio

$$g(u) = (u_1^3 + u_2^3 + u_3^3) + 5(u_1^2 u_2 + u_1^2 u_3 + u_2^2 u_3 + u_2^2 u_1 + u_3^2 u_2 + u_3^2 u_1) - u_1 u_2 u_3$$

è un polinomio simmetrico di grado 3 in tre variabili.

Vi sono  $n$  polinomi simmetrici speciali a coefficienti interi che prendono il nome di *funzioni simmetriche elementari*  $s_i$ :

$$(3.2) \quad s_1 = u_1 + u_2 + \cdots + u_n$$

$$s_2 = u_1 u_2 + u_1 u_3 + \cdots + u_{n-1} u_n = \sum_{i < j} u_i u_j$$

$$s_3 = \sum_{i < j < k} u_i u_j u_k$$

 $\vdots$ 

$$s_n = u_1 u_2 \cdots u_n.$$

Essi sono i coefficienti del polinomio  $(x - u_1)(x - u_2) \cdots (x - u_n)$ , sviluppato come polinomio in  $x$ :

$$(3.3) \quad p(x) = (x - u_1)(x - u_2) \cdots (x - u_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots \pm s_n.$$

Abbiamo qui invertito l'ordine degli indici e messo i segni alternati. I coefficienti  $s_i$  sono simmetrici, poiché  $p(x)$  è simmetrico rispetto alle permutazioni degli indici.

Il teorema fondamentale sulle funzioni simmetriche afferma che le funzioni simmetriche elementari generano l'anello di tutti i polinomi simmetrici:

(3.4) TEOREMA *Ogni polinomio simmetrico  $g(u_1, \dots, u_n) \in R[u]$  può essere scritto in modo unico come polinomio nelle funzioni simmetriche elementari  $s_1, \dots, s_n$ . In altre parole, siano  $z_1, \dots, z_n$  delle variabili. Per ciascun polinomio simmetrico  $g(u)$  esiste uno e un solo polinomio  $\varphi(z_1, \dots, z_n) \in R[z_1, \dots, z_n]$  tale che:*

$$g(u_1, \dots, u_n) = \varphi(s_1, \dots, s_n).$$

La dimostrazione si trova alla fine del paragrafo.

Per esempio,

$$(3.5) \quad u_1^2 + \cdots + u_n^2 = s_1^2 - 2s_2.$$

Il *discriminante* del polinomio  $p(x)$  (3.3), definito nel modo seguente:

$$D = (u_1 - u_2)^2 (u_1 - u_3)^2 \cdots (u_{n-1} - u_n)^2 =$$

$$(3.6) \quad = \prod_{i < j} (u_i - u_j)^2 = \pm \prod_{i \neq j} (u_i - u_j),$$

è forse il polinomio simmetrico più importante. Le ultime due espressioni del discriminante possono essere entrambe convenienti, ma sfortunatamente possono

differire per il segno. Per passare dalla seconda all'ultima occorrono  $\frac{1}{2} n(n-1)$  cambiamenti di segno, sicché il segno corretto da sostituire al simbolo  $\pm$  è:

$$(3.7) \quad (-1)^{n(n-1)/2}.$$

È chiaro che  $D$  è un polinomio simmetrico a coefficienti interi. Il teorema (3.4) ci dice allora che esso può essere scritto come un polinomio a coefficienti interi nelle funzioni simmetriche elementari. In altre parole, esiste un polinomio

$$(3.8) \quad \Delta(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$$

tale che  $D = \Delta(s_1, \dots, s_n)$ . Purtroppo, tale espressione di  $D$  è molto complicata. Io non saprei dire che forma ha per  $n > 3$ .

Per  $n = 2$ , possiamo calcolare facilmente il discriminante:

$$(3.9) \quad (u_1 - u_2)^2 = s_1^2 - 4s_2.$$

Questa è la formula ben nota per il discriminante del polinomio di secondo grado  $p(x) = x^2 - s_1 x + s_2$ . Per  $n = 3$ , la formula è già troppo complicata da ricordare:

$$(3.10) \quad (u_1 - u_2)^2 (u_1 - u_3)^2 (u_2 - u_3)^2 = s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 - 27s_3^2 + 18s_1 s_2 s_3.$$

È importante osservare che questa espressione è un'*identità* in  $\mathbb{Z}[u_1, \dots, u_n]$ , cioè è verificata per qualunque valore delle variabili  $u_i$ . Se ci vengono assegnati ad esempio  $n$  elementi  $\alpha_1, \dots, \alpha_n$  in un anello  $R$ , possiamo sviluppare il polinomio ottenuto sostituendo gli  $\alpha_i$  alle  $u_i$  in  $p(x)$ :

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n - b_1 x^{n-1} + b_2 x^{n-2} - \cdots \pm b_n.$$

Indici e segni sono stati adattati in modo da essere concordi con la (3.3). Allora risulta

$$b_i = s_i(\alpha_1, \dots, \alpha_n),$$

e

$$\prod_{i < j} (\alpha_i - \alpha_j)^2 = \Delta(b_1, \dots, b_n).$$

Ciò si ottiene sostituendo le  $u_i$  con gli  $\alpha_i$ .

Inoltre è importante che l'espressione di un polinomio simmetrico per mezzo delle funzioni simmetriche elementari sia unica:

(3.11) COROLLARIO *Non esiste nessuna relazione polinomiale tra le funzioni simmetriche elementari  $s_1, \dots, s_n$ . Equivalentemente, il sottoanello  $R[s_1, \dots, s_n]$*

di  $R[u]$  generato da  $s_1, \dots, s_n$  è isomorfo all'anello dei polinomi in  $n$  variabili  $R[z_1, \dots, z_n]$ .

Si tratta di una riformulazione della proprietà di unicità data nel teorema (3.4). ■

Il corollario può essere usato nel modo seguente, che ora illustriamo. Sia

$$(3.12) \quad f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \dots \pm a_n$$

un polinomio a coefficienti in un anello  $R$ . Definiamo il *discriminante* di  $f(x)$  come l'elemento  $\Delta(a_1, \dots, a_n)$  di  $R$ , dove  $\Delta(z_1, \dots, z_n)$  è il polinomio (3.8). Poiché questo polinomio è unico, il discriminante è ben definito in ogni caso, anche se il polinomio  $f(x)$  non si spezza in un prodotto di fattori lineari in  $R[x]$ .

Per esempio, sia  $n = 3$ . Allora la formula (3.10) mostra che:

$$(3.13) \quad \Delta(0, p, -q) = -4p^3 - 27q^2,$$

che concorda con l'espressione (2.15) del discriminante del polinomio  $x^3 + px + q$ .

Per calcolare l'espressione di un polinomio simmetrico per mezzo delle funzioni simmetriche elementari possiamo usare il metodo dei coefficienti indeterminati. Per applicare tale metodo, osserviamo che la funzione simmetrica elementare  $s_i$  ha grado  $i$  nelle variabili  $u_1, \dots, u_n$ . Ecco perché abbiamo scelto per essa l'indice  $i$ . Assegnamo il *peso*  $i$  alla variabile  $z_i$  e definiamo il *grado ponderato* di un monomio  $z_1^{e_1} z_2^{e_2} \cdots z_n^{e_n}$  come l'intero

$$(3.14) \quad e_1 + 2e_2 + \dots + ne_n.$$

Sostituendo  $z_i$  con  $s_i$  in un polinomio di grado ponderato  $d$  nelle variabili  $z_1, \dots, z_n$ , otteniamo un polinomio di grado (ordinario)  $d$  in  $u_1, \dots, u_n$ .

Per esempio, per calcolare il discriminante di un polinomio di terzo grado per mezzo delle funzioni simmetriche elementari, osserviamo che il suo grado nelle variabili  $u_i$  è 6. Vi sono sette monomi in  $z_1, z_2, z_3$  di grado ponderato 6:

$$(3.15) \quad z_1^6, z_1^4 z_2, z_1^3 z_3, z_1^2 z_2^2, z_1 z_2 z_3, z_2^3, z_3^2,$$

e dunque  $D$  è una loro combinazione lineare. Per determinare i suoi coefficienti, calcoliamo  $D$  su alcuni polinomi speciali. Prendendo ad esempio  $f(x) = x^2(x-1)$ , otteniamo  $D = 0$ ,  $s_1 = 1$  e  $s_2 = s_3 = 0$ . Poiché tra i monomi (3.15) l'unico che non contiene né  $z_2$  né  $z_3$  è  $z_1^6$ , il coefficiente di  $z_1^6$  nel discriminante è zero. I coefficienti di  $z_2^3$  e  $z_3^2$  possono essere calcolati usando, ad esempio, i polinomi speciali  $x^3 - x$  e  $x^3 - 1$ .

*Dimostrazione del teorema (3.4).* Cominciamo ad esaminare, come esempio, il caso del polinomio simmetrico

$$f(u) = u_1^2 u_2 + u_1^2 u_3 + u_2^2 u_1 + u_2^2 u_3 + u_3^2 u_1 + u_3^2 u_2.$$

Il primo passo consiste nel porre  $u_3 = 0$ . Otteniamo così un polinomio simmetrico  $f^0 = u_1^2 u_2 + u_2^2 u_1$  nelle variabili rimanenti  $u_1, u_2$ . Denotiamo le funzioni simmetriche elementari in  $u_1, u_2$  con  $s_1^0 = u_1 + u_2$  e  $s_2^0 = u_1 u_2$ . Osserviamo che  $f^0 = s_1^0 s_2^0$ .

Il secondo passo consiste nel confrontare  $f$  con il polinomio in tre variabili  $s_1 s_2$ . Calcolando il polinomio  $f - s_1 s_2$ , dove  $s_1 = u_1 + u_2 + u_3$  e  $s_2 = u_1 u_2 + u_1 u_3 + u_2 u_3$ , troviamo che

$$f - s_1 s_2 = -3u_1 u_2 u_3.$$

Ci accorgiamo che tale polinomio è il polinomio  $-3s_3$ . Pertanto risulta:  $f = s_1 s_2 - 3s_3$ .

Il caso generale si tratta in modo simile. Se  $n = 1$ , non vi è nulla da dimostrare, poiché in tal caso  $u_1 = s_1$ . Procedendo per induzione su  $n$ , supponiamo che il teorema sia stato dimostrato per  $n - 1$  variabili ( $n > 1$ ). Dato un polinomio simmetrico  $f$  in  $u_1, \dots, u_n$ , consideriamo il polinomio  $f^0$  ottenuto ponendo  $u_n = 0$ , ossia  $f^0(u_1, \dots, u_{n-1}) = f(u_1, \dots, u_{n-1}, 0)$ . Osserviamo che  $f^0$  è un polinomio simmetrico in  $u_1, \dots, u_{n-1}$ . In virtù dell'ipotesi induttiva,  $f^0$  può essere espresso come un polinomio nelle funzioni simmetriche elementari in  $u_1, \dots, u_{n-1}$ , che denotiamo con

$$s_1^0 = u_1 + \dots + u_{n-1}, \dots, s_{n-1}^0 = u_1 \cdots u_{n-1}.$$

Pertanto possiamo scrivere  $f^0 = g(s_1^0, \dots, s_{n-1}^0)$ . Inoltre dalla definizione dei polinomi  $s_i$  segue che

$$s_i^0 = s_i(u_1, \dots, u_{n-1}, 0), \quad \text{per } i = 1, \dots, n-1.$$

Consideriamo il polinomio in  $u_1, \dots, u_n$

$$p(u_1, \dots, u_n) = f(u_1, \dots, u_n) - g(s_1, \dots, s_{n-1}).$$

Essendo una differenza di polinomi simmetrici, esso è simmetrico. Inoltre, ha la proprietà che  $p(u_1, \dots, u_{n-1}, 0) = 0$ . Pertanto ogni monomio che compare in  $p$  è divisibile per  $u_n$ . Per ragioni di simmetria,  $p$  è divisibile per  $u_i$  per ogni  $i$ , e quindi è divisibile per  $s_n$ . Dunque si ha

$$(3.16) \quad f(u_1, \dots, u_n) = g(s_1, \dots, s_{n-1}) + s_n h(u_1, \dots, u_n).$$

per qualche polinomio simmetrico  $h$ . Operiamo ora su  $h(u_1, \dots, u_n)$ . Procedendo per induzione sul grado, si ha che  $h$  è un polinomio nelle funzioni simmetriche, e quindi anche  $f$  è tale.

Resta da dimostrare l'unicità di  $\varphi(s_1, \dots, s_n)$ , ossia che esiste uno e un solo polinomio  $\varphi(z_1, \dots, z_n)$  nelle variabili  $z_i$  tale che  $\varphi(s_1, \dots, s_n) = f(u_1, \dots, u_n)$  sono

uguali come polinomi in  $u_1, \dots, u_n$ . In altre parole, il nucleo dell'omomorfismo di sostituzione

$$\sigma : R[z] \rightarrow R[u],$$

che manda  $z_i$  in  $s_i$  è zero. Per dimostrarlo, supponiamo che  $\varphi(s_1, \dots, s_n) = 0$  per qualche  $\varphi \in R[z]$ . Ponendo  $u_n = 0$  in questa espressione, otteniamo ancora zero, ossia  $\varphi(s_1^0, \dots, s_{n-1}^0, 0) = 0$ . Procedendo per induzione su  $n$ , ciò implica che  $\varphi(z_1, \dots, z_{n-1}, 0) = 0$ . Pertanto  $z_n$  divide  $\varphi(z)$ , e quindi possiamo scrivere:  $\varphi(z) = z_n \psi(z)$ . Allora  $0 = \varphi(s) = s_n \psi(s) = u_1 \dots u_n \psi(s)$ . Poiché il prodotto  $u_1 \dots u_n$  non è un divisore dello zero nell'anello dei polinomi  $R[u]$ , si ha  $\psi(s) = 0$ . Il polinomio  $\psi(z)$  ha grado totale nelle  $z$  minore del grado di  $\varphi(z)$ , sicché possiamo applicare l'induzione sul grado per concludere che  $\psi = 0$ . Ne segue allora che  $\varphi = 0$ . ■

Ora, supponiamo che  $R = F$  sia un campo. Allora possiamo considerare anche il campo delle funzioni razionali nelle variabili  $u_i$ , ossia, il campo dei quozienti di  $F[u_1, \dots, u_n]$ . Il gruppo simmetrico agisce anche su questo campo, e l'enunciato corrispondente è vero:

(3.17) TEOREMA *Ogni funzione razionale simmetrica è una funzione razionale in  $s_1, \dots, s_n$ .*

*Dimostrazione.* Sia  $r(u) = f(u)/g(u)$  una funzione razionale simmetrica, dove  $f, g \in F[u]$ . Possiamo costruire una funzione simmetrica a partire da  $g$  moltiplicando tutti insieme i  $\sigma g$ , sicché

$$G = \prod_{\sigma \in S_n} \sigma g$$

è un polinomio simmetrico. Allora  $G(u)r(u)$  è una funzione razionale simmetrica ed è anche un polinomio in  $u_1, \dots, u_n$ ; dunque è un polinomio simmetrico. In base al teorema (3.4),  $G(u)$  e  $G(u)r(u)$  sono polinomi nelle funzioni simmetriche elementari  $s_1, \dots, s_n$ . Pertanto  $r(u)$  è una funzione razionale in  $s_1, \dots, s_n$ . ■

La coppia di campi:

$$(3.18) \quad F(s) = F(s_1, \dots, s_n) \subset F(u_1, \dots, u_n) = F(u)$$

è un esempio di un'estensione di Galois. Ciò segue dal teorema (1.11), poiché  $F(u)$  è un campo di spezzamento del polinomio  $p(x)$  (3.3), e poiché le radici  $u_1, \dots, u_n$  sono distinte. In base alla proposizione (1.14), il gruppo di Galois  $G = G(F(u)/F(s))$  agisce fedelmente sulle radici. D'altra parte,  $G$  contiene l'intero gruppo simmetrico, per costruzione. Pertanto  $G = S_n$ . Come corollario, si ha che  $[F(u) : F(s)] = n!$

#### 4 Elementi primitivi

Alla fine del paragrafo 1, abbiamo visto che elementi di un'estensione biquadratica  $K/F$  scelti a caso generano  $K$ . È possibile ottenere un risultato generale di questo tipo come corollario del teorema fondamentale della teoria di Galois. Qui tuttavia lo dimostreremo direttamente per utilizzarlo nella dimostrazione del teorema fondamentale.

(4.1) TEOREMA (Esistenza di un elemento primitivo) *Sia  $K$  un'estensione finita di un campo  $F$  di caratteristica zero. Allora esiste un elemento  $\gamma \in K$  tale che  $K = F(\gamma)$ .*

Un elemento  $\gamma$  che genera un'estensione di campi  $K/F$  è detto *elemento primitivo* di  $K$  su  $F$ . Pertanto il teorema può essere riformulato dicendo che ogni estensione finita  $K$  di un campo  $F$  contiene un elemento primitivo. Abbiamo ribadito l'ipotesi generale (fatta all'inizio del capitolo), che  $F$  abbia caratteristica zero, poiché il teorema non vale per i campi di caratteristica  $p$ .

*Dimostrazione.* Procediamo per induzione sul numero dei generatori di  $K$ , che scriviamo nella forma  $K = F(\alpha_1, \dots, \alpha_n)$ . Se  $n = 1$ , non vi è nulla da dimostrare. Sia ora  $n > 1$  e supponiamo, in virtù dell'ipotesi induttiva, che il teorema sia vero per il campo intermedio  $K_1 = F(\alpha_1, \dots, \alpha_{n-1})$ . Possiamo quindi supporre che  $K_1$  sia generato da un solo elemento  $\beta$ . Allora si ha  $K = K_1(\alpha_n) = F(\beta, \alpha_n)$ . Dobbiamo far vedere che questo campo contiene un elemento primitivo. Siamo così ridotti al caso  $n = 2$ , cioè  $K$  è generato da due elementi  $\alpha, \beta$ .

Siano  $f(x), g(x)$  i polinomi minimi di  $\alpha, \beta$  su  $F$ , e sia  $K'$  un'estensione di  $K$  in cui  $f$  e  $g$  si spezzano in fattori lineari [cap. 13 (5.3)]. Denotiamo le loro radici con  $\alpha = \alpha_1, \dots, \alpha_m$  e  $\beta = \beta_1, \dots, \beta_n$ . Come si ricorderà [cfr. cap. 13 (5.8)] le  $\alpha_i$  sono distinte.

Ci proponiamo di far vedere che per la maggior parte delle scelte di  $c \in F$ , la combinazione lineare  $\gamma = \beta + c\alpha$  genera  $K$ . Indicato con  $L$  il campo  $F(\gamma)$  basterà dimostrare che  $\alpha \in L$ , poiché in tal caso, anche  $\beta = \gamma - c\alpha$  apparirà a  $L$ , e ciò implicherà che  $L = K$ . Procederemo in modo indiretto: precisamente, determineremo il polinomio minimo di  $\alpha$  su  $L$ . Come sappiamo, questo è il polinomio monico di grado minimo in  $L[x]$  che ha  $\alpha$  come radice.

Per cominciare,  $\alpha$  è una radice di  $f(x)$ . L'idea ingegnosa è quella di utilizzare il polinomio  $g(x)$  per costruire un secondo polinomio avente  $\alpha$  come radice, precisamente  $h(x) = g(\gamma - cx)$ . Si noti che  $h(x)$  ha i coefficienti in  $L$  e che  $h(\alpha) = 0$ . Se dimostriamo che il massimo comune divisore di  $f$  e  $h$  in  $L[x]$  è  $x - \alpha$ , ne seguirà che  $-\alpha$ , essendo uno dei coefficienti di  $x - \alpha$ , appartiene a  $L$ . Ora, il massimo comune divisore monico di  $f$  e  $h$  è lo stesso, sia che venga calcolato in  $L[x]$  o in  $K'[x]$  [cap. 13 (5.4)]. Pertanto possiamo svolgere i calcoli

in  $K'[x]$ . In tale anello,  $f$  è il prodotto dei fattori lineari  $x - \alpha_i$ , sicché basta dimostrare che nessun fattore  $x - \alpha_i$ , con  $i > 1$ , divide  $h$ , ossia che nessuno degli elementi  $\alpha_i$ , ad eccezione di  $\alpha_1 = \alpha$ , è una radice di  $h(x)$ . Giunti a questo punto, resterà soltanto da calcolare le radici di  $h$ .

Poiché le radici di  $g$  sono  $\beta_1, \dots, \beta_n$ , le radici di  $h(x) = g(\gamma - cx)$  si ottengono risolvendo le equazioni in  $x$ :

$$\gamma - cx = \beta_j \quad (j = 1, \dots, n).$$

Dato che  $\gamma = \beta + c\alpha$ , le radici sono  $(\gamma - \beta_j)/c = (\beta - \beta_j)/c + \alpha$ . Vogliamo che queste radici siano diverse da  $\alpha_i$ , con  $i \neq 1$ . Ciò accadrà, purché  $c$  non assuma uno dei valori seguenti, che sono un numero finito:

$$(4.2) \quad -\frac{\beta_j - \beta}{\alpha_i - \alpha},$$

con  $i \neq 1$ ,  $j \neq 1$ . ■

### (4.3) Esempio

Consideriamo il campo  $K = \mathbb{Q}[i, \sqrt[3]{2}]$ , che ha grado 6 su  $\mathbb{Q}$  [cfr. cap. 13 (3.5d)]. Con le notazioni introdotte nella dimostrazione precedente, si ha:  $\beta_1 = i$ ,  $\beta_2 = -i$ , e inoltre  $\alpha_1 = \sqrt[3]{2}$ ,  $\alpha_2 = \zeta \sqrt[3]{2}$ ,  $\alpha_3 = \zeta^2 \sqrt[3]{2}$ , dove  $\zeta = e^{2\pi i/3}$ . La condizione (4.2) diventa

$$\sqrt[3]{2}c \neq -\frac{\pm i - i}{\zeta^\nu - \zeta}, \quad \nu = 1, 2.$$

Tale condizione è verificata per ogni  $c \in \mathbb{Q}$ , tranne che per  $c = 0$ . Pertanto  $\gamma = i + c\sqrt[3]{2}$  genera  $K$  su  $\mathbb{Q}$ , per ogni numero razionale  $c \neq 0$ . Naturalmente, molte altre combinazioni dei due elementi  $\beta, \alpha$  genereranno  $F(\beta, \alpha)$ . In questo esempio, anche il prodotto  $i\sqrt[3]{2}$  genera  $K$ . ■

Il teorema (4.1) è importante per due motivi. In primo luogo, il calcolo esplicito in un'estensione della forma  $F(\gamma)$  è facile se si conosce il polinomio minimo di  $\gamma$  su  $F$ . In secondo luogo, poiché le estensioni finite hanno la forma  $F(\gamma)$ , possiamo dedurre le loro proprietà da alcuni risultati relativi agli elementi algebrici. Ed è questo aspetto che è il più importante per noi.

L'applicazione del teorema (4.1) allo studio degli automorfismi di campi mostra la potenza di tale risultato. Consideriamo un gruppo finito  $G$  di automorfismi del campo  $K$  e denotiamo con  $F$  il suo campo fisso  $K^G$ .

**(4.4) PROPOSIZIONE** *Sia  $G$  un gruppo finito di automorfismi di un campo  $K$  e sia  $F$  il suo campo fisso. Sia  $\{\beta_1, \dots, \beta_r\}$  l'orbita di un elemento  $\beta = \beta_1 \in K$  rispetto all'azione di  $G$ . Allora  $\beta$  è algebrico su  $F$ , il suo grado su  $F$  è  $r$ , e inoltre il suo polinomio minimo su  $F$  è  $g(x) = (x - \beta_1) \cdots (x - \beta_r)$ .*

Si noti che il grado di  $\beta$ , essendo l'ordine di un'orbita, divide l'ordine del gruppo.

**Dimostrazione.** Sia  $f(x)$  il polinomio minimo di  $\beta$  su  $F$ . Poiché  $f(x)$  è lasciato fisso da  $G$ , ciascuno degli elementi  $\beta_i$  è radice di  $f$  (1.14), e pertanto  $g$  divide  $f$ . Inoltre,  $g$  è lasciato fisso da tutte le permutazioni di  $\{\beta_1, \dots, \beta_r\}$ , e quindi dall'azione di  $G$ , che permuta l'orbita. Pertanto  $g(x) \in F[x]$ . Poiché  $f$  è irriducibile, si ha:  $g = f$ . ■

Questa proposizione fornisce un metodo per determinare il polinomio minimo di un elemento  $\beta$  di un'estensione di Galois  $K$  su  $F$ . Per esempio, sia  $K$  l'estensione biquadratica  $\mathbb{Q}(i, \sqrt{2})$ , e poniamo  $\beta = i + \sqrt{2}$ . Il gruppo di Galois di  $K/\mathbb{Q}$  è il gruppo quadrinomio di Klein, e l'orbita di  $\beta$  è costituita dai quattro elementi  $\pm i \pm \sqrt{2}$ . Pertanto il polinomio minimo di  $\beta$  su  $\mathbb{Q}$  è

$$\begin{aligned} (x - i - \sqrt{2})(x - i + \sqrt{2})(x + i - \sqrt{2})(x + i + \sqrt{2}) &= \\ &= (x^2 - 2ix - 3)(x^2 + 2ix - 3) = x^4 - 2x^2 + 9. \end{aligned}$$

Per determinare questo polinomio potremmo anche calcolare le potenze di  $\beta$  e cercare la relazione lineare di grado minimo tra esse (cfr. cap. 13, § 3). Tuttavia, il metodo qui illustrato è preferibile, poiché produce sempre un polinomio irriducibile.

**(4.5) COROLLARIO** *Sia  $K/F$  un'estensione di Galois e sia  $g(x)$  un polinomio irriducibile in  $F[x]$ . Se  $g$  ha una radice in  $K$ , allora si spezza in fattori lineari in  $K[x]$ .*

**Dimostrazione.** In base al corollario (1.9),  $F$  è il campo fisso del gruppo di Galois  $G = G(K/F)$ . Sia  $\beta$  una radice di  $g(x)$  in  $K$ . In base alla proposizione (4.4), il polinomio minimo di  $\beta$  su  $F$  è  $(x - \beta_1) \cdots (x - \beta_r)$ , dove  $\{\beta_1, \dots, \beta_r\}$  è la  $G$ -orbita di  $\beta$ . Poiché  $g(x)$  è il polinomio minimo di  $\beta$ , esso è uguale a questo prodotto, sicché si spezza in fattori lineari in  $K[x]$ , come asserito. ■

Il corollario ci dice in particolare che ogni estensione di Galois è un campo di spezzamento, come stabilito dal teorema (1.11). Infatti, prendiamo generatori arbitrari  $\alpha, \beta, \dots$  di  $K$  su  $F$ , e sia  $f(x)$  il prodotto dei loro polinomi minimi. Allora  $f$  si spezza completamente in  $K[x]$ , e quindi  $K$  è un campo di spezzamento di  $f$ .

**(4.6) TEOREMA** *Sia  $G$  un gruppo di ordine  $n$  di automorfismi di un campo  $K$  e sia  $F$  il suo campo fisso. Allora si ha:  $[K : F] = n$ .*

**Dimostrazione.** La proposizione (4.4) mostra che ogni elemento  $\beta$  di  $K$  è algebrico su  $F$  e che il suo grado divide  $n = |G|$ . Il teorema dell'elemento primitivo implica che il grado dell'intera estensione di campi  $K/F$  è maggiorato ancora da  $n$ . Per vedere ciò, formiamo una catena di estensioni di campi, nel modo che ora illustreremo. Per cominciare, scegliamo un elemento  $\alpha_1 \in K$  non

appartenente a  $F$ , e poniamo  $F_1 = F(\alpha_1)$ . Allora  $[F_1 : F] \leq n$ . Se  $F_1 \neq K$ , sceglieremo un elemento  $\alpha_2 \in K$  non appartenente a  $F_1$ , e poniamo  $F_2 = F(\alpha_1, \alpha_2)$ . In virtù del teorema dell'elemento primitivo,  $F_2$  è generato da un solo elemento  $\gamma$ , e in base al corollario (3.6) (cap. 13), il grado di  $\gamma$  su  $F$  è maggiorato da  $n$ . Pertanto  $[F_2 : F] \leq n$ . Proseguendo in questo modo, otteniamo una catena  $F < F_1 < F_2 \dots$  in cui  $[F_i : F] \leq n$  per ogni  $i$ . Questa catena deve essere finita. Pertanto  $F_i = K$  per qualche  $i$ , e quindi  $[K : F] \leq n$ .

Applicando nuovamente il teorema (4.1), concludiamo che  $K$  contiene un elemento primitivo  $K = F(\beta)$ . Ogni elemento di  $G$  che lascia fisso  $\beta$  agisce come l'identità su  $K = F(\beta)$ . Poiché stiamo supponendo che  $G$  sia un gruppo di automorfismi di  $K$ , l'identità è l'unico elemento di questo tipo. Pertanto lo stabilizzatore di  $\beta$  è  $\{1\}$ , e l'orbita ha ordine  $n$ . In base alla proposizione (4.4),  $\beta$  ha grado  $n$  su  $F$ , e quindi  $[K : F] = n$ . ■

Utilizzando il teorema che abbiamo appena dimostrato, possiamo ricavare il teorema (1.6), il quale afferma che l'ordine del gruppo di Galois di ogni estensione finita  $K/F$  divide il suo grado. Per dimostrare ciò, poniamo  $G = G(K/F)$ . Allora  $G$  agisce su  $K$  e pertanto, in base al teorema (4.6),  $|G| = [K : K^G]$ . Inoltre, poiché  $F \subset K^G \subset K$ ,  $[K : K^G]$  divide  $[K : F]$ . ■

Il teorema (4.6) fornisce anche un risultato che è l'inverso del corollario (1.9):

(4.7) COROLLARIO *Sia  $G$  un gruppo finito di automorfismi di un campo  $K$  e sia  $F$  il suo campo fisso. Allora  $K$  è un'estensione di Galois di  $F$ , e il suo gruppo di Galois è  $G$ .*

*Dimostrazione.* Essendo  $F$  il sottocampo di  $K$  lasciato fisso da  $G$ , gli elementi di  $G$  sono  $F$ -automorfismi di  $K$ . Pertanto  $G \subset G(K/F)$ . Poiché  $|G(K/F)| \leq [K : F]$  e  $[K : F] = |G|$ , ne consegue che  $|G(K/F)| = [K : F]$  e che  $G = G(K/F)$ . ■

Possiamo ottenere alcuni esempi interessanti per illustrare la proposizione (4.4) e il teorema (4.6) considerando gli automorfismi del campo  $\mathbb{C}(y) = K$  delle funzioni razionali in  $y$ . Per esempio, sia  $\sigma$  l'automorfismo definito da  $y \mapsto iy^{-1}$ , e si denoti con  $G$  il gruppo ciclico di ordine 4 generato da  $\sigma$ . Vale allora la seguente proposizione:

(4.8) PROPOSIZIONE *Siano  $K$  e  $G$  come sopra. Il campo  $F = K^G$  è il campo  $\mathbb{C}(w)$  delle funzioni razionali in  $w = y^2 - y^{-2}$ .*

In altre parole, ogni funzione razionale  $f(y)$  che è lasciata fissa da  $\sigma$  può essere espressa come una funzione razionale in  $w$ .

*Dimostrazione.* Innanzitutto,  $\sigma$  lascia fisso  $w = y^2 - y^{-2}$ , sicché  $w \in K^G$ . Pertanto il campo fisso  $F = K^G$  contiene il campo  $\mathbb{C}(w)$ . Calcoliamo ora il polinomio minimo di  $y$  su  $F$ . L'orbita di  $y$  è  $\{y, iy^{-1}, -y, -iy^{-1}\}$ , e pertanto dalla proposizione (4.4) segue che il polinomio minimo di  $y$  è  $(x - y)(x - iy^{-1})(x + y)(x + iy^{-1}) = x^4 - w^2 - 1$ . Questo polinomio ha i coefficienti in  $\mathbb{C}(w)$ , sicché  $y$  ha grado 4 su tale campo. Ne segue che  $[K : \mathbb{C}(w)] = 4$ . D'altra parte,  $\mathbb{C}(w) \subset F \subset K$ , e poiché  $|G| = 4$ , il teorema (4.6) ci dice che  $[K : F] = 4$ . A questo punto, contando i gradi, si vede che  $\mathbb{C}(w) = F$ . ■

Un famoso teorema, chiamato *teorema di Liuroth*, afferma che ogni sottocampo di  $\mathbb{C}(y)$  contenente propriamente  $\mathbb{C}$  è il campo delle funzioni razionali in qualche funzione razionale  $w$  di  $y$ .

## 5 Dimostrazione del teorema fondamentale

Sia  $f(x)$  un polinomio monico di grado  $n$  a coefficienti in un campo  $F$ . Ricordiamo che un campo di spezzamento di  $f(x) \in F[x]$  è un campo della forma  $K = F(\alpha_1, \dots, \alpha_n)$ , tale che  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$  in  $K[x]$ . L'esistenza di un campo di spezzamento è stata dimostrata nel capitolo 13 (5.3). Ora vogliamo dimostrare che due campi di spezzamento qualsiasi di un dato polinomio sono isomorfi. Ciò segue dal fatto che un'estensione di campi della forma  $F(\alpha)$  è determinata dal polinomio minimo di  $\alpha$  su  $F$ , e da un po' di calcoli. I calcoli richiesti per la dimostrazione possono creare un po' di confusione, per via delle notazioni, ma non sono difficili.

Ogni isomorfismo di campi  $\varphi : F \rightarrow \tilde{F}$  si estende in modo naturale a un isomorfismo  $F[x] \rightarrow \tilde{F}[x]$  tra gli anelli dei polinomi, che manda  $a_n x^n + \dots + a_0$  in  $\tilde{a}_n x^n + \dots + \tilde{a}_0$ , dove  $\tilde{a}_i = \varphi(a_i)$ . Denotiamo l'immagine di  $f(x)$  con  $\tilde{f}(x)$ . Poiché  $\varphi$  è un isomorfismo,  $\tilde{f}(x)$  sarà un polinomio irriducibile se e solo se  $f(x)$  è irriducibile.

Il lemma seguente generalizza la proposizione (2.9) del capitolo 13.

(5.1) LEMMA *Con le notazioni sopra introdotte, sia  $f(x)$  un polinomio irriducibile in  $F[x]$ . Sia  $\alpha$  una radice di  $f(x)$  in un'estensione di campi  $K$  di  $F$ , e sia  $\tilde{\alpha}$  una radice di  $\tilde{f}(x)$  in un'estensione  $\tilde{K}$  di  $\tilde{F}$ . Allora esiste uno e un solo isomorfismo*

$$\varphi_1 : F(\alpha) \rightarrow \tilde{F}(\tilde{\alpha}),$$

*che si restringe a  $\varphi$  sul sottocampo  $F$  e che manda  $\alpha$  in  $\tilde{\alpha}$ .*

*Dimostrazione.* Sappiamo che  $F(\alpha)$  è isomorfo al quoziente  $F[x]/(f)$ , e analogamente  $\tilde{F}(\tilde{\alpha})$  è isomorfo a  $\tilde{F}[x]/(\tilde{f})$ . Gli anelli  $F[x]$  e  $\tilde{F}[x]$  sono isomorfi, come abbiamo appena visto, e poiché  $f$  e  $\tilde{f}$  si corrispondono in questo isomorfismo, altrettanto fanno gli ideali  $(f)$  e  $(\tilde{f})$  da essi generati. Di conseguenza gli anelli

quoziente  $F[x]/(f)$  e  $\tilde{F}[x]/(\tilde{f})$  sono anch'essi isomorfi. Combinando questi isomorfismi otteniamo l'isomorfismo richiesto  $\varphi_1$ . Questa estensione di  $\varphi$  è unica, poiché  $\alpha$  genera  $F(\alpha)$  su  $F$ . ■

(5.2) PROPOSIZIONE *Sia  $\varphi : F \rightarrow \tilde{F}$  un isomorfismo di campi. Sia  $f(x)$  un polinomio non costante in  $F[x]$  e sia  $\tilde{f}(x)$  il polinomio corrispondente in  $\tilde{F}[x]$ . Siano  $K$  e  $\tilde{K}$  campi di spezzamento di  $f(x)$  e  $\tilde{f}(x)$ . Allora esiste un isomorfismo  $\psi : K \rightarrow \tilde{K}$  che si restringe a  $\varphi$  sul sottocampo  $F$  di  $K$ .*

Se poniamo  $F = \tilde{F}$  e  $\varphi =$  identità, otteniamo il seguente corollario:

(5.3) COROLLARIO *Due campi di spezzamento qualsiasi di  $f(x) \in F[x]$  su  $F$  sono isomorfi.* ■

È questo il risultato che ci interessa davvero. L'isomorfismo ausiliario  $\varphi$  viene introdotto nella proposizione per poter effettuare il passo induttivo della dimostrazione.

*Dimostrazione della proposizione (5.2).* Se  $f(x)$  si spezza in fattori lineari su  $F$ , anche  $\tilde{f}(x)$  si spezza in fattori lineari. In tal caso  $K = F$  e  $\tilde{K} = \tilde{F}$ , sicché  $\varphi = \psi$ . Supponiamo che  $f$  non si spezzi in fattori lineari. Scegliamo un fattore irriducibile  $g(x)$  di  $f(x)$  di grado  $> 1$ . Il polinomio corrispondente  $\tilde{g}(x)$  sarà un fattore irriducibile di  $\tilde{f}(x)$ . Sia  $\alpha$  una radice di  $g$  in  $K$  e scriviamo  $F_1 = F(\alpha)$ . Facciamo una scelta simile per  $\tilde{\alpha}$  in  $\tilde{K}$  e scriviamo  $\tilde{F}_1 = \tilde{F}(\tilde{\alpha})$ . Allora, in base al lemma (5.1), possiamo estendere  $\varphi$  ad un isomorfismo  $\varphi_1 : F_1 \rightarrow \tilde{F}_1$  che manda  $\alpha$  in  $\tilde{\alpha}$ . Essendo un campo di spezzamento di  $f$  su  $F$ ,  $K$  è anche un campo di spezzamento di  $f$  sul campo più grande  $F_1$ , e analogamente  $\tilde{K}$  è un campo di spezzamento di  $\tilde{f}$  su  $\tilde{F}_1$ . Pertanto possiamo sostituire  $F, \tilde{F}, \varphi$  con  $F_1, \tilde{F}_1, \varphi_1$  e procedere per induzione sul grado di  $K$  su  $F$ . ■

Siamo ora in grado di dimostrare il secondo dei teoremi enunciati nel paragrafo 1, ossia il teorema (1.11). Una parte di questo teorema è stata dimostrata nell'ultimo paragrafo, utilizzando il corollario (4.5). Per comodità, rienunciamo qui l'altra parte del teorema.

TEOREMA *Sia  $K$  il campo di spezzamento di un polinomio  $f(x) \in F[x]$ . Allora  $K$  è un'estensione di Galois di  $F$ , ossia  $|G(K/F)| = [K : F]$ .*

Dimostreremo il teorema tornando indietro a riprendere la dimostrazione della proposizione (5.2), tenendo ben presente il numero delle scelte.

(5.4) LEMMA *Con le notazioni della proposizione (5.2), il numero degli isomorfismi  $\psi : K \rightarrow \tilde{K}$  che estendono  $\varphi$  è uguale al grado  $[K : F]$ .*

Il teorema discende dal lemma, se poniamo  $\tilde{F} = F$ ,  $\tilde{K} = K$ , e  $\varphi =$  identità. ■

*Dimostrazione del lemma (5.4).* Procediamo come nella dimostrazione della proposizione (5.2), scegliendo un fattore irriducibile  $g(x)$  di  $f(x)$  e una delle radici  $\alpha$  di  $g(x)$  in  $K$ . Poniamo  $F_1 = F(\alpha)$ . Ogni isomorfismo  $\psi : K \rightarrow \tilde{K}$  che estende  $\varphi$  manderà  $F_1$  in qualche sottocampo  $\tilde{F}_1$  di  $\tilde{K}$ . Tale campo  $\tilde{K}$  avrà la forma  $\tilde{F}(\tilde{\alpha})$ , dove  $\tilde{\alpha} = \psi(\alpha)$  è una radice di  $\tilde{g}(x)$  in  $\tilde{K}$ .

Viceversa, per estendere  $\varphi$  a  $\psi$ , possiamo cominciare scegliendo una radice arbitraria  $\tilde{\alpha}$  di  $\tilde{g}(x)$  in  $\tilde{K}$ . Estendiamo poi  $\varphi$  a un'applicazione  $\varphi_1 : F_1 \rightarrow \tilde{F}_1 = \tilde{F}(\tilde{\alpha})$ , ponendo  $\varphi_1(\alpha) = \tilde{\alpha}$ . Procediamo per induzione sul grado  $[K : F]$ . Poiché  $[K : F_1] < [K : F]$ , l'ipotesi induttiva ci dice che, per questa scelta particolare di  $\varphi_1$ , vi sono  $[K : F_1]$  estensioni di  $\varphi_1$  a un isomorfismo  $\psi : K \rightarrow \tilde{K}$ . D'altra parte,  $\tilde{g}$  ha radici distinte in  $\tilde{K}$ , poiché  $g$  e  $\tilde{g}$  sono irriducibili [cap. 13 (5.8)]. Pertanto il numero delle scelte di  $\tilde{\alpha}$  è il grado di  $\tilde{g}$ , che è  $[F_1 : F]$ . Vi sono  $[F_1 : F]$  scelte per l'isomorfismo  $\varphi_1$ . Otteniamo così un numero totale di  $[K : F_1][F_1 : F] = [K : F]$  estensioni di  $\varphi$  a  $\psi : K \rightarrow \tilde{K}$ . ■

Poiché due campi di spezzamento  $K$  di un polinomio  $f(x) \in F[x]$  sono isomorfi, il gruppo di Galois  $G(K/F)$  dipende, a meno di isomorfismi, soltanto da  $f$ . Spesso si dice che esso è il *gruppo di Galois del polinomio  $f$  su  $F$* .

Il corollario seguente raccoglie insieme vari criteri affinché un'estensione di campi sia un'estensione di Galois. La maggior parte di essi sono stati già dimostrati, e le dimostrazioni rimanenti sono lasciate come esercizi.

(5.5) COROLLARIO *Sia  $K/F$  un'estensione finita di campi. Le seguenti condizioni sono equivalenti tra loro:*

- (i)  $K$  è un'estensione di Galois di  $F$ ;
- (ii)  $K$  è il campo di spezzamento di un polinomio irriducibile  $f(x) \in F[x]$ ;
- (ii)'  $K$  è il campo di spezzamento di un polinomio  $f(x) \in F[x]$ ;
- (iii)  $F$  è il sottocampo di  $K$  che resta fisso rispetto all'azione del gruppo di Galois  $G(K/F)$  su  $K$ ;
- (iii)'  $F$  è il sottocampo di  $K$  che resta fisso rispetto all'azione di un gruppo finito di automorfismi di  $K$ .

Abbiamo ora abbastanza informazioni per dimostrare il teorema fondamentale della teoria di Galois, il quale mette in relazione i campi intermedi con i sottogruppi del gruppo di Galois.

*Dimostrazione del teorema (1.15).* Sia  $K/F$  un'estensione di Galois. Dobbiamo dimostrare che le applicazioni

$$L \mapsto G(K/L) \quad \text{e} \quad H \mapsto K^H$$

sono l'una l'inversa dell'altra tra l'insieme dei campi intermedi e l'insieme dei sottogruppi di  $G = G(K/F)$ . Per fare ciò, verifichiamo che la composizione di queste due applicazioni in entrambe le direzioni è l'identità.

Sia  $L$  un campo intermedio. Il sottogruppo di  $G$  corrispondente è  $H = G(K/L)$ . Per definizione,  $H$  agisce in modo banale su  $L$ , sicché  $L \subset K^H$ . D'altra parte,  $K$  è un'estensione di Galois di  $L$ , in virtù di (1.13); pertanto  $[K : L] = |H|$ . In base al teorema (4.6),  $|H| = [K : K^H]$ , e quindi  $L = K^H$ .

Nell'altra direzione, supponiamo di partire con un sottogruppo  $H \subset G$ , e poniamo  $L = K^H$ . Allora  $H \subset G(K/L)$ . Ma  $|H| = [K : K^H] = [K : L] = |G(K/L)|$ . Pertanto  $H = G(K/L)$ . Ciò prova che le due applicazioni sono l'una l'inversa dell'altra, come richiesto. Poiché  $K$  è un'estensione di Galois di  $L = K^H$ , si ha  $[K : L] = |H|$  e  $[L : F] = [G : H]$ . ■

La corrispondenza biunivoca data dal teorema fondamentale ha ancora altre proprietà, che ora studieremo. Innanzitutto, la corrispondenza tra i campi e i sottogruppi *inverte l'ordinamento*, ossia, se  $L, L'$  sono campi intermedi e se  $H = G(K/L)$ ,  $H' = G(K/L')$  sono i sottogruppi corrispondenti, allora  $L \subset L'$  se e soltanto se  $H \supset H'$ . Ciò segue chiaramente dalle definizioni delle applicazioni ed è coerente con le relazioni (1.16).

Per completare il quadro generale, dimostreremo che i campi intermedi  $L$  che sono *estensioni di Galois* di  $F$  corrispondono ai *sottogruppi normali* di  $G$ . Sia  $L$  un campo intermedio. Un  $F$ -automorfismo  $\sigma$  di  $K$  porterà  $L$  in un campo intermedio  $\sigma L$ , il quale non è necessariamente uguale a  $L$ . Diremo allora che  $\sigma L$  è un *sottocampo coniugato*.

**(5.6) TEOREMA** *Sia  $K/F$  un'estensione di Galois e sia  $L$  un campo intermedio. Sia  $H = G(K/L)$  il sottogruppo corrispondente di  $G = G(K/F)$ .*

- (a) *Sia  $\sigma$  un elemento di  $G$ . Il sottogruppo di  $G$  che corrisponde al sottocampo coniugato  $\sigma L$  è il sottogruppo coniugato  $\sigma H \sigma^{-1}$ . In altre parole,  $G(K/\sigma L) = \sigma H \sigma^{-1}$ .*
- (b)  *$L$  è un'estensione di Galois di  $F$  se e soltanto se  $H$  è un sottogruppo normale di  $G$ . Se ciò accade, allora  $G(L/F)$  è isomorfo al gruppo quoziante  $G/H$ :*

### (5.7) SCHEMA

$G = G(K/F)$ agisce su $K$ lasciando fisso $F$	$\left\{ \begin{array}{l} K \\ L \\ F \end{array} \right\}$	$H = G(K/L)$ agisce su $K$ lasciando fisso $L$
		$\text{Se } H \text{ è normale,}$ $\text{allora } G/H = G(L/F)$ agisce qui

### (5.8) Esempio

Nel caso dell'equazione di terzo grado (2.1), il cui campo di spezzamento ha grado 6, l'unico campo intermedio che sia un'estensione di Galois, diverso da  $F$  e  $K$ , è  $F(\delta)$ , che corrisponde al gruppo alterno  $H = A_3 \subset S_3$ . Il gruppo di Galois  $G(F(\delta)/F)$  è ciclico di ordine 2, e tale risulta anche il gruppo quoziante  $S_3/A_3$ . I tre campi  $F(\alpha_i)$  sono coniugati. Ciò concorda col fatto che i tre sottogruppi di  $S_3$  di ordine 2 sono coniugati.

*Dimostrazione del teorema (5.6).* (a) Poniamo  $\sigma L = L'$ . Se  $\tau$  è un elemento di  $H = G(K/L)$ , allora  $\sigma \tau \sigma^{-1}$  appartiene a  $H' = G(K/L')$ . Per verificare ciò, dobbiamo dimostrare che  $\sigma \tau \sigma^{-1}$  lascia fisso ogni elemento  $\alpha' \in L'$ . In base alla definizione di  $\sigma L$ , si ha che  $\alpha' = \sigma(\alpha)$  per qualche  $\alpha \in L$ . Allora  $\sigma \tau \sigma^{-1}(\alpha') = \sigma \tau(\alpha) = \sigma(\alpha) = \alpha'$ , come richiesto. Ne segue che  $H' \supset \sigma H \sigma^{-1}$  e, per ragioni di simmetria, o contando gli elementi, che  $H' = \sigma H \sigma^{-1}$ . Il fatto che abbiamo appena verificato è in realtà una proprietà generale dell'azione di un gruppo su un insieme [cap. 5 (6.4)].

(b) Supponiamo ora che  $H$  sia normale. Allora  $H = \sigma H \sigma^{-1}$  per ogni  $\sigma \in G$ ; pertanto  $G(K/L) = G(K/\sigma L)$ . Ciò implica che  $L = \sigma L$  per ogni  $\sigma$  [cfr. (1.9)]. Dunque ogni  $F$ -automorfismo di  $K$  porta  $L$  in se stesso e quindi induce un  $F$ -automorfismo di  $L$ , per restrizione. Tale restrizione definisce un omomorfismo:

$$(5.9) \quad \pi : G \rightarrow G(L/F).$$

Il suo nucleo è l'insieme degli elementi  $\sigma \in G$  che inducono l'identità su  $L$ , ossia  $H$ . Pertanto  $G/H$  è isomorfo a un sottogruppo di  $G(L/F)$ . Contando i gradi e gli ordini, otteniamo:

$$[L : F] = |G/H| \leq |G(L/F)|.$$

Ne segue che  $L$  è un'estensione di Galois e  $G/H \approx G(L/F)$ .

Viceversa, supponiamo che  $L/F$  sia un'estensione di Galois. Allora  $L$  è un campo di spezzamento di qualche polinomio  $g(x) \in F[x]$ , ossia,  $L = F(\beta_1, \dots, \beta_k)$ , dove gli elementi  $\beta_i$  sono le radici di  $g(x)$  in  $K$ . Un  $F$ -automorfismo  $\sigma$  di  $K$  permuta queste radici e pertanto manda  $L$  in sé, sicché  $L = \sigma L$ . In virtù di (a),  $H = \sigma H \sigma^{-1}$ ; dunque  $H$  è un sottogruppo normale. ■

## 6 Equazioni di quarto grado

Sia  $K/F$  un'estensione di Galois. Abbiamo visto che, se  $\beta$  è un elemento di  $K$  il cui polinomio minimo su  $F$  è  $g(x)$ , allora  $g$  si spezza in fattori lineari in  $K[x]$  e la  $G$ -orbita di  $\beta$  è l'insieme delle radici di  $g$  (4.4). Dunque  $G$  agisce *transitivamente* sulle radici di un polinomio irriducibile  $g \in F[x]$ , purché tale

polinomio abbia almeno una radice in  $K$ . Combinando questa osservazione con la proposizione (1.14), otteniamo il risultato seguente:

(6.1) PROPOSIZIONE *Sia  $K/F$  un campo di spezzamento di un polinomio  $f(x) \in F[x]$ . Allora il gruppo di Galois  $G$  di  $K/F$  agisce fedelmente sull'insieme  $\{\alpha_1, \dots, \alpha_n\}$  delle radici di  $f$ . Pertanto tale azione rappresenta  $G$  come un sottogruppo del gruppo simmetrico  $S_n$ . Le radici formano una sola orbita se e solo se  $f$  è irriducibile su  $F$ .* ■

Quando l'estensione di Galois  $K$  viene assegnata come il campo di spezzamento di un polinomio di grado  $n$ , di solito il gruppo di Galois  $G$  viene considerato come sottogruppo del gruppo simmetrico  $S_n$ . Se il polinomio  $f$  è irriducibile,  $G$  è un sottogruppo transitivo, cioè agisce transitivamente sugli indici  $\{1, \dots, n\}$ . Tuttavia, la stessa estensione di Galois  $K/F$  può essere ottenuta come campo di spezzamento di molti polinomi, quindi tale rappresentazione di  $G$  come un sottogruppo di  $S_n$  non è unica.

Per esempio, sia  $K/F$  il campo di spezzamento di un polinomio di terzo grado irriducibile tale che  $[K : F] = 6$ . Allora il gruppo di Galois è rappresentato come l'intero gruppo simmetrico  $S_3$ . Tuttavia, il teorema dell'elemento primitivo ci dice che  $K$  può essere generato anche da un solo elemento  $\gamma$ , e poiché  $[K : F] = 6$ ,  $\gamma$  ha grado 6 su  $F$ . Ciò significa che la sua orbita ha ordine 6 e che il suo polinomio minimo ha grado 6. Pertanto, se consideriamo  $K$  come il campo di spezzamento di questo polinomio di sesto grado, il gruppo di Galois è rappresentato come un sottogruppo di  $S_6$ . Questo non è un modo molto efficiente per rappresentare  $S_3$ .

Supponiamo che l'estensione di Galois  $K$  in esame sia il campo di spezzamento di un polinomio  $f(x)$  e che le sue radici in  $K$  siano  $\alpha_1, \dots, \alpha_n$ . Allora, considerando  $G$  come un sottogruppo di  $S_n$ , possiamo porre i due problemi seguenti:

- (6.2) (i) Dato un sottogruppo  $\mathcal{H}$  di  $S_n$ , stabilire se  $G \subset \mathcal{H}$ .  
(ii) Determinare  $G$ .

Se sapessimo risolvere il problema (i) per ogni sottogruppo  $\mathcal{H}$ , anche il problema (ii) sarebbe risolto.

L'approccio di Lagrange allo studio di questi problemi consiste nel cercare funzioni delle radici che siano *parzialmente simmetriche*. Un polinomio parzialmente simmetrico è un polinomio  $p(u_1, \dots, u_n)$  nelle variabili  $u_1, \dots, u_n$  che è lasciato fisso dalle permutazioni appartenenti a un dato sottogruppo  $\mathcal{H}$  di  $S_n$  e da nessun'altra permutazione. Per esempio, abbiamo visto in (2.13) che

$$(u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$$

è una funzione parzialmente simmetrica rispetto al gruppo alterno, per  $n = 3$ . Non vi è nessuna difficoltà a generalizzare questa costruzione per un intero  $n$  qualsiasi, definendo la funzione:

$$(6.3) \quad \delta(u) = (u_1 - u_2)(u_1 - u_3) \cdots (u_{n-1} - u_n) = \prod_{i < j} (u_i - u_j).$$

Essa è una radice quadrata del discriminante (3.6). L'effetto di una permutazione degli indici è quello di moltiplicare  $\delta$  per il segno della permutazione. Avendo a disposizione questa funzione parzialmente simmetrica, sostituiamo in essa le radici  $\alpha_1, \dots, \alpha_n$  del nostro polinomio, per ottenere un elemento  $\delta(\alpha) = \delta$  di  $K$  che è lasciato fisso dalle permutazioni pari delle radici. Possiamo stabilire se  $\delta$  appartiene o no a  $F$  verificando se il discriminante  $D$  è o non è un quadrato. Ciò fornirà informazioni sul gruppo di Galois.

(6.4) PROPOSIZIONE *Sia  $K/F$  un'estensione di Galois che sia il campo di spezzamento di un polinomio irriducibile  $f(x) \in F[x]$  di grado  $n$ . Siano  $\alpha_1, \dots, \alpha_n$  le radici di  $f(x)$  in  $K$ , e poniamo  $\delta = \delta(\alpha)$ . Allora  $\delta \neq 0$ . Inoltre:*

- (a)  $\delta \in F$  se e soltanto se il gruppo di Galois  $G$  è un sottogruppo del gruppo alterno  $A_n$ .  
(b) In ogni caso, il sottogruppo  $G(K/F(\delta))$  di  $G$  è contenuto nel gruppo alterno.

*Dimostrazione.* Il caso  $\delta = 0$  si presenta soltanto se due radici sono uguali, e ciò non può accadere se  $f$  è irriducibile [cap. 13 (5.8)]. Ora, supponiamo che  $\delta$  stia in  $F$ . Poiché le permutazioni dispari mandano  $\delta$  in  $-\delta$  e poiché  $\delta \neq 0$ , le permutazioni dispari non lasciano fisso  $\delta$ . D'altra parte, gli elementi di  $F$  sono lasciati fissi da ogni automorfismo in  $G$ ; ne segue che  $G$  non contiene permutazioni dispari, e quindi che  $G \subset A_n$ . Viceversa, se  $\delta \notin F$ , utilizziamo il fatto che  $K^G = F$ . Allora deve esistere un elemento di  $G$  che non lascia fisso  $\delta$ . Tale elemento sarà una permutazione dispari, sicché  $G \not\subset A_n$ . Ciò dimostra (a). La parte (b) si ottiene da (a) sostituendo  $F$  con  $F(\delta)$ . ■

Studieremo ora le equazioni di quarto grado, cominciando da un caso speciale di notevole interesse, che è controllato dal discriminante. Consideriamo un numero complesso espresso mediante un radicale doppio, diciamo  $\alpha = \sqrt{r + s\sqrt{t}}$ , dove  $r, s, t$  appartengono a un campo  $F$ . Prendiamo, ad esempio, i numeri:

$$(6.5) \quad \sqrt{3 + 2\sqrt{2}}, \quad \sqrt{5 + \sqrt{21}}, \quad \sqrt{7 + 2\sqrt{5}}, \quad \sqrt{5 + 2\sqrt{5}}.$$

Poniamo allora il seguente problema: È possibile esprimere  $\alpha$  per mezzo di due radici quadrate che non stiano una dentro l'altra?

Poiché  $\alpha^2 = r + s\sqrt{t}$ , è facile scrivere esplicitamente un polinomio di quarto grado che ha  $\alpha$  come radice, precisamente

$$(6.6) \quad f(x) = (x^2 - (r + s\sqrt{t}))(x^2 - (r - s\sqrt{t})) = x^4 + bx^2 + c,$$

dove  $b = -2r$  e  $c = r^2 - s^2t$ . Se  $\alpha'$  denota una delle due radici quadrate di  $r - s\sqrt{t}$ , allora le radici di questo polinomio di quarto grado sono:

$$(6.7) \quad \alpha, \alpha', -\alpha, -\alpha'.$$

Il campo di spezzamento  $K = F(\alpha, \alpha')$  di  $f$  può essere ottenuto aggiungendo, nell'ordine, le tre radici quadrate  $\sqrt{t}, \alpha, \alpha'$ , sicché il grado  $[K : F]$  divide 8. Il grado sarà minore di 8 se non è necessario aggiungere una delle radici quadrate.

Dobbiamo stabilire se  $f$  è o non è irriducibile. Per fare ciò, verifichiamo innanzitutto l'irriducibilità del polinomio di secondo grado  $q(y) = y^2 + by + c$ , le cui radici sono  $\alpha^2, \alpha'^2$ . Se  $q$  è irriducibile  $f$  non ha radici in  $F$ . In tal caso  $f$ , se è riducibile, sarà il prodotto di due polinomi di secondo grado. Usando il metodo dei coefficienti indeterminati, troviamo che il prodotto deve avere la forma

$$(6.8) \quad x^4 + bx^2 + c = (x^2 + ux + v)(x^2 - ux + v).$$

Saremo in grado di stabilire se una fattorizzazione di questo tipo esiste oppure no, almeno quando  $F = \mathbb{Q}$ .

Se  $f(x)$  è riducibile  $\alpha$  è radice di un polinomio di secondo grado, sicché può essere scritto usando soltanto una radice quadrata. Ciò accade, ad esempio, con  $\sqrt{3+2\sqrt{2}}$ , che è uguale a  $1+\sqrt{2}$ , come si verifica elevando al quadrato entrambe le espressioni. I polinomi di quarto grado ottenuti a partire dagli altri esempi (6.5) sono irriducibili su  $\mathbb{Q}$ .

Ritorniamo ora al problema in esame. Supponiamo che  $f$  sia irriducibile. Osserviamo che scrivere  $\alpha$  per mezzo di radici quadrate  $\sqrt{p}, \sqrt{q}$  non contenute l'una nell'altra equivale a trovare un'estensione biquadratica  $K = F(\sqrt{p}, \sqrt{q})$  di  $F$  che contiene  $\alpha$ . Supponiamo che si possa trovare un'estensione biquadratica  $K$  contenente  $\alpha$ ; allora  $K$  è un'estensione di Galois di  $F$ , e  $f(x)$  si spezza in fattori lineari in  $K[x]$ . Ciò significa che  $K$  contiene un campo di spezzamento di  $f$ . In effetti,  $K$  stesso è il campo di spezzamento, poiché  $f$  è irriducibile e di grado 4. Pertanto il gruppo di Galois  $G$  di  $f$  sarà il gruppo quadrinomio di Klein. Se  $G$  non fosse il gruppo quadrinomio di Klein,  $\alpha$  non potrebbe essere scritto per mezzo di radici quadrate non contenute l'una nell'altra.

Viceversa, se  $K/F$  è un'estensione di Galois il cui gruppo di Galois è il gruppo quadrinomio di Klein,  $K$  contiene tre campi intermedi di grado 2 su  $F$ . Due qualsiasi di questi campi, presi insieme, generano  $K$ ; quindi  $K$  è un'estensione biquadratica di  $F$  e ogni suo elemento può essere scritto per mezzo di due radici quadrate non contenute l'una nell'altra.

Calcoliamo il discriminante di  $f(x)$ , utilizzando l'elenco (6.7) delle radici. Otteniamo:

$$D = \prod_{i < j} (\alpha_i - \alpha_j)^2 = (4\alpha\alpha')^2(\alpha - \alpha')^4(\alpha + \alpha')^4$$

$$= 2^4(b^2 - 4c)^2c = 2^8s^3t^2(r^2 - s^2t).$$

Se  $D$  è un quadrato in  $F$ , allora  $G$  è un sottogruppo transitivo del gruppo alterno  $A_4$ , il cui ordine divide 8. Il gruppo quadrinomio di Klein è l'unico gruppo di questo tipo. Esso è costituito dalle permutazioni pari di ordine 2:

$$(6.9) \quad V = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

Non esistendo altre azioni transitive di  $V$  su  $\{1, 2, 3, 4\}$  si ha il risultato seguente:

(6.10) PROPOSIZIONE Poniamo  $\alpha = \sqrt{r+s\sqrt{t}}$ , con  $r, s, t \in F$ , e supponiamo che il polinomio  $f(x) = x^4 - 2rx^2 + (r^2 - s^2t)$  sia irriducibile su  $F$ . Allora  $\alpha$  può essere scritto per mezzo di due radici quadrate non contenute l'una nell'altra se e soltanto se  $r^2 - s^2t$  è un quadrato in  $F$ . ■

Se  $\alpha = \sqrt{5+\sqrt{21}}$ , allora  $r^2 - s^2t = 25 - 21 = 4$ , che è un quadrato. Negli ultimi due esempi (6.5),  $r^2 - s^2t$  non è un quadrato in  $\mathbb{Q}$ .

Determiniamo esplicitamente l'espressione "semplificata" di  $\alpha = \sqrt{5+\sqrt{21}}$ . La teoria di Galois fornisce la traccia suggerendoci di determinare i campi intermedi. Essendo estensioni quadratiche di  $\mathbb{Q}$ , tali campi sono generati da radici quadrate, e queste sono quelle di cui abbiamo bisogno per esprimere  $\alpha$ . Vi è un'estensione quadratica intermedia ovvia:  $\mathbb{Q}(\sqrt{21})$ , ma non è quella di cui abbiamo bisogno. Per trovarne un'altra determiniamo il campo fisso del sottogruppo  $H$  di ordine 2 che è generato da  $\sigma = (12)(34)$ . Se le radici di  $f$  sono elencate nell'ordine (6.7), l' $H$ -orbita di  $\alpha$  è  $\{\alpha, \alpha'\}$ , dove  $\alpha' = \sqrt{5-\sqrt{21}}$ , e il polinomio minimo di  $\alpha$  su  $K^H$  è  $(x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha'$ . Pertanto  $K$  ha grado 2 sul campo  $L = F(\alpha + \alpha', \alpha\alpha')$ , e questo è contenuto in  $K^H$ . Considerando i gradi, si ha che  $L = K^H$ . Utilizzando questa traccia, effettuiamo i calcoli e ricaviamo:  $\alpha\alpha' = 2$ ,  $(\alpha + \alpha')^2 = 14$  e  $\alpha + \alpha' = \sqrt{14}$ . Analogamente,  $\alpha - \alpha' = \sqrt{6}$ . Risolvendo per  $\alpha$ , otteniamo:  $\alpha = \frac{1}{2}(\sqrt{6} + \sqrt{14})$ . ■

È più difficile analizzare un'equazione generica di quarto grado, le cui radici di solito non possono essere scritte esplicitamente in una forma utile. Tuttavia, esiste un'altra funzione parzialmente simmetrica che è di aiuto per la determinazione del gruppo di Galois. Sia  $f(x)$  un polinomio di quarto grado irriducibile, con radici  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  in un campo di spezzamento  $K$ . Allora, per la (6.1), il suo gruppo di Galois è un sottogruppo di  $S_4$  e le radici formano una sola orbita. I sottogruppi transitivi di  $S_4$  sono:

$$(6.11) \quad S_4, \quad A_4, \quad D_4, \quad C_4, \quad V,$$

dove  $V$  è il gruppo (6.9). Di fatto, vi sono tre sottogruppi coniugati isomorfi a  $D_4$  e tre sottogruppi coniugati isomorfi a  $C_4$ . Gli altri sono univocamente determinati. Vi sono ancora alcuni sottogruppi di  $S_4$  che sono isomorfi al gruppo quadrinomio di Klein, ma non sono transitivi.

Per distinguere questi gruppi cerchiamo funzioni parzialmente simmetriche delle radici. Come abbiamo visto, l'elemento  $\delta$  permette di stabilire se  $G \subset A_4$  oppure no. I sottogruppi di  $A_4$  nel nostro elenco sono  $A_4$  e  $V$ , quindi  $\delta \in F$  se e soltanto se  $G$  è uno di questi due gruppi.

Consideriamo ora il polinomio parzialmente simmetrico

$$(6.12) \quad \beta_1(u) = u_1u_3 + u_2u_4.$$

Una permutazione degli indici manda  $\beta_1(u)$  in uno dei tre polinomi  $\beta_i(u)$ , con  $i = 1, 2, 3$ , dove

$$\beta_2(u) = u_1u_2 + u_3u_4 \quad \text{e} \quad \beta_3(u) = u_1u_4 + u_2u_3.$$

Poiché  $S_4$  ha ordine 24, lo stabilizzatore di  $\beta_1(u)$  ha ordine 8: è uno dei tre gruppi diedrali  $D_4$ . Il polinomio  $(x - \beta_1(u))(x - \beta_2(u))(x - \beta_3(u))$  è lasciato fisso da tutte le permutazioni delle variabili  $u_i$ , sicché i suoi coefficienti sono funzioni simmetriche. Essi possono essere calcolati esplicitamente per mezzo delle funzioni simmetriche elementari.

Ritornando al nostro polinomio di quarto grado, sostituiamo le radici  $\alpha_i$  in  $\beta_j(u)$ , per ottenere tre elementi  $\beta_j(\alpha) = \beta_j \in K$ , i quali formano una sola orbita rispetto all'azione del gruppo simmetrico sulle radici. Se sono elementi distinti di  $K$ , lo stabilizzatore di  $\beta_1$  in  $S_4$  avrà ordine 8, e pertanto sarà il gruppo diedrale  $D_4$ . Siamo fortunati poiché gli elementi  $\beta_j$  sono distinti. Per esempio, si ha:

$$\beta_1 - \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2).$$

Avendo supposto  $f$  irriducibile, le sue radici  $\alpha_i$  sono distinte, e di conseguenza  $\beta_1 - \beta_2 \neq 0$ .

Poiché il gruppo di Galois  $G$  permuta gli elementi  $\beta_i$ , il polinomio  $g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$  ha i coefficienti in  $F$ . Esso è detto polinomio *cubico risolvente* del polinomio di quarto grado  $f(x)$ .

Sebbene il gruppo simmetrico agisca transitivamente su  $\{\beta_1, \beta_2, \beta_3\}$ , il gruppo di Galois  $G$ , che è un sottogruppo di  $S_4$ , può non agire transitivamente. Il fatto che ciò accada o meno fornisce informazioni su  $G$ . Se, per esempio,  $G$  lascia fisso  $\beta_1$ ,  $G$  è contenuto nello stabilizzatore  $D_4$  di  $\beta_1$ . In tal caso,  $\beta_1$  apparirà al campo  $F$  (1.9), e il polinomio cubico risolvente avrà una radice in  $F$ . Procedendo come nella dimostrazione della proposizione (6.4), otteniamo il risultato seguente:

(6.13) PROPOSIZIONE *Sia  $g(x)$  il polinomio cubico risolvente di un polinomio di quarto grado irriducibile  $f(x)$ , e sia  $K$  un campo di spezzamento di  $f$ . Allora  $g(x)$  ha una radice in  $F$  se e solo se il gruppo di Galois  $G = G(K/F)$  è un sottogruppo di uno dei gruppi diedrali  $D_4$ . In ogni caso, se  $\beta$  è una radice di  $g(x)$  in  $K$ , il gruppo di Galois  $G(K/F(\beta))$  è un sottogruppo di un gruppo diedrale  $D_4$ .* ■

Dunque il polinomio  $x^2 - D$ , dove  $D$  è il discriminante, e il polinomio cubico risolvente  $g(x)$  sono quasi sufficienti per descrivere il gruppo di Galois. I risultati sono riassunti nella tabella seguente:

	$D$ è un quadrato in $F$	$D$ non è un quadrato in $F$
$g$ riducibile	$G = V$	$G = D_4 \circ C_4$
$g$ irriducibile	$G = A_4$	$G = S_4$ .

I calcoli esplicativi per un generico polinomio di quarto grado diventano piuttosto laboriosi; possiamo però calcolare facilmente il discriminante di un polinomio di quarto grado della forma:

$$(6.15) \quad x^4 + rx + s.$$

Il discriminante è un polinomio simmetrico di grado 12 e pertanto ha grado ponderato 12 nelle funzioni simmetriche elementari  $s_1, \dots, s_4$ . Sostituendo  $(0, 0, -r, s)$  a  $(s_1, s_2, s_3, s_4)$  nell'espressione incognita del discriminante, verranno eliminati tutti i monomi contenenti  $s_1$  o  $s_2$ . Gli unici monomi di grado ponderato 12 in cui non compaiono  $s_1$  e  $s_2$  sono  $s_3^4$  e  $s_4^3$ . Il discriminante del polinomio (6.15) avrà dunque la forma

$$D = \Delta(0, 0, -r, s) = cr^4 + c's^3.$$

Possiamo determinare i coefficienti  $c, c'$  calcolando il discriminante di due polinomi particolari. Il risultato è il seguente:

$$(6.16) \quad D = -27r^4 + 256s^3.$$

Per esempio, il discriminante di

$$(6.17) \quad f(x) = x^4 + 8x + 12$$

è  $3^4 \cdot 2^{12}$ , che è un quadrato in  $\mathbb{Q}$ . Il gruppo di Galois del campo di spezzamento del polinomio (6.17) su  $\mathbb{Q}$  è pertanto un sottogruppo di  $A_4$ .

Per calcolare il polinomio cubico risolvente  $g(x)$  del polinomio (6.15), scriviamo il polinomio cubico risolvente del polinomio generale, le cui radici sono  $u_1, \dots, u_4$ , nella forma:

$$g(x) = x^3 - b_1x^2 + b_2x - b_3;$$

dato che  $\beta_i$  è una funzione quadratica nelle  $u_j$ ,  $b_i$  ha grado  $2i$  nelle  $u_j$  e grado ponderato  $2i$  nelle funzioni simmetriche. Procedendo come sopra, otteniamo

$$(6.18) \quad g(x) = x^3 - 4sx - r^2.$$

Il polinomio cubico risolvente del particolare polinomio di quarto grado (6.17) è  $x^3 - 48x - 64$ . Il polinomio (6.17) e il suo polinomio cubico risolvente sono entrambi irriducibili su  $\mathbb{Q}$ . Ne segue che  $G = A_4$  per il polinomio (6.17).

## 7 Estensioni di Kummer

Consideriamo ora il campo di spezzamento su un campo  $F$  di un polinomio della forma:

$$(7.1) \quad f(x) = x^p - a,$$

dove  $p$  è un numero primo. Supponiamo che il campo base  $F$  sia un sottocampo di  $\mathbb{C}$  che contiene la radice  $p$ -esima primitiva dell'unità  $\zeta_p = e^{2\pi i/p}$ . Le radici complesse di  $f(x)$  sono le radici  $p$ -esime di  $a$ , e se  $\alpha$  denota una radice  $p$ -esima particolare, allora le radici di  $f(x)$  sono:

$$(7.2) \quad \alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{p-1}\alpha,$$

dove  $\zeta = \zeta_p$ . Pertanto il campo di spezzamento è generato da una sola radice:  $K = F(\alpha)$ .

(7.3) PROPOSIZIONE *Sia  $F$  un sottocampo di  $\mathbb{C}$  contenente la radice  $p$ -esima dell'unità  $\zeta_p$ , e sia  $a$  un elemento di  $F$  che non sia una potenza  $p$ -esima in  $F$ . Allora il campo di spezzamento di  $f(x) = x^p - a$  ha grado  $p$  su  $F$  e il suo gruppo di Galois è un gruppo ciclico di ordine  $p$ .*

*Dimostrazione.* Sia  $K$  un campo di spezzamento di  $f$  e sia  $\alpha$  una delle sue radici in  $K$ . Supponiamo che  $\alpha$  non stia in  $F$ . Allora esiste un automorfismo  $\sigma$  di  $K/F$  che non lascia fisso  $\alpha$ . Poiché le radici di  $f$  sono  $\zeta^i\alpha$ , con  $i = 0, \dots, p-1$ , si ha  $\sigma(\alpha) = \zeta^\nu\alpha$  per qualche  $\nu \neq 0$ . Calcoliamo ora le potenze di  $\sigma$ . Ricordando che  $\sigma$  è un automorfismo e che  $\sigma(\zeta) = \zeta$  poiché  $\zeta \in F$ , otteniamo che

$$\sigma^2(\alpha) = \sigma(\zeta^\nu\alpha) = \zeta^\nu\sigma(\alpha) = \zeta^{2\nu}\alpha.$$

Analogamente,  $\sigma^i(\alpha) = \zeta^{i\nu}\alpha$  per ogni  $i$ . Poiché  $\zeta$  è una radice  $p$ -esima dell'unità, la più piccola potenza positiva di  $\sigma$  che lascia fisso  $\alpha$  è  $\sigma^p$ . Pertanto l'ordine di  $\sigma$  nel gruppo di Galois è almeno  $p$ . D'altra parte,  $\alpha$  genera  $K$  su  $F$  ed è una radice del polinomio  $x^p - a$  di grado  $p$ , sicché  $[K : F] \leq p$ . Ciò prova nello stesso tempo che  $[K : F] = p$ , che  $x^p - a$  è irriducibile su  $F$  e che  $G(K/F)$  è ciclico di ordine  $p$ . ■

Dimostriamo ora un risultato sorprendente che inverte la proposizione (7.3):

(7.4) TEOREMA *Sia  $F$  un sottocampo di  $\mathbb{C}$  contenente la radice  $p$ -esima dell'unità  $\zeta$  e sia  $K/F$  un'estensione di Galois di grado  $p$ . Allora  $K$  si ottiene aggiungendo a  $F$  una radice  $p$ -esima.*

Le estensioni di questo tipo sono chiamate spesso *estensioni di Kummer*. Per  $p = 2$ , il teorema si riduce a un risultato ben noto, secondo cui ogni estensione di grado 2 può essere ottenuta aggiungendo una radice quadrata. Ma supponiamo che  $p = 3$  e che  $F$  contenga  $\zeta_3$ . Se il discriminante del polinomio di terzo grado irriducibile (2.3) è un quadrato in  $F$ , il campo di spezzamento di  $f$  ha grado 3 [cfr. (2.16)], sicché il suo gruppo di Galois è un gruppo ciclico. Pertanto il campo di spezzamento di un polinomio siffatto ha la forma  $F(\sqrt[3]{a})$ , per qualche  $a \in F$ , e ciò non è ovvio.

*Dimostrazione del teorema (7.4).* Il gruppo di Galois  $G$  ha ordine primo  $p = [K : F]$ , e pertanto è un gruppo ciclico. Ogni elemento  $\sigma$  diverso dall'identità genererà  $G$ . Se consideriamo  $K$  come un  $F$ -spazio vettoriale,  $\sigma$  è un operatore lineare su  $K$ . Infatti, poiché  $\sigma$  è un  $F$ -automorfismo, si ha:

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \quad \text{e} \quad \sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha),$$

per ogni  $c \in F$  e per ogni  $\alpha, \beta \in K$ . Poiché  $G$  è un gruppo ciclico di ordine  $p$ ,  $\sigma^p = 1$ . Un autovalore  $\lambda$  di tale operatore deve soddisfare la relazione  $\lambda^p = 1$ , il che significa che  $\lambda$  è una potenza di  $\zeta$ . Per ipotesi, questi autovalori appartengono al campo  $F$ ; inoltre, esiste almeno un autovalore diverso da 1. Questa è una proprietà che riguarda ogni operatore lineare  $T$  tale che qualche potenza di  $T$  è l'identità, perché può essere diagonalizzato [cap. 9 (2.3)]. I suoi autovalori sono gli elementi della matrice diagonale  $A$  che lo rappresenta. Se  $T$  non è l'identità, come in questo caso, allora  $A \neq I$ , sicché qualche elemento diagonale è diverso da 1.

Scegliamo un autovettore  $\alpha$  associato a un autovalore  $\zeta^i \neq 1$ . Allora  $\sigma(\alpha) = \zeta^i\alpha$ , e quindi

$$\sigma(\alpha^p) = \sigma(\alpha)^p = (\zeta^i\alpha)^p = \zeta^{ip}\alpha^p = \alpha^p.$$

Pertanto  $\sigma$  lascia fisso  $\alpha^p$ . Poiché  $\sigma$  genera  $G$ , l'elemento  $\alpha^p$  appartiene al campo  $K^G$  lasciato fisso da  $G$ , che è  $F$  (1.9). Abbiamo così trovato un elemento  $\alpha \in K$ , la cui potenza  $p$ -esima sta in  $F$ . Poiché  $\sigma(\alpha) \neq \alpha$ , l'elemento  $\alpha$  non sta in  $F$ . Essendo  $[K : F]$  un numero primo,  $\alpha$  genera  $K$ . ■

### (7.5) Esempio

Consideriamo il polinomio di terzo grado ciclico (2.12)  $x^3 - 3x + 1$  e indichiamo con  $\eta_1, \eta_2, \eta_3$  le sue radici. Allora esiste un elemento  $\sigma G(K/F)$  che agisce come

una permutazione ciclica. Scegiamo la base  $(1, \eta_1, \eta_2)$  per  $K$  su  $F = \mathbb{Q}(\zeta_3)$ . (Perché è una base?) Rispetto a tale base, la matrice dell'operatore lineare  $\sigma$  è:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}.$$

perché  $\sigma(1) = 1$ ,  $\sigma(\eta_1) = \eta_2$ ,  $\sigma(\eta_2) = \eta_3 = -\eta_1 - \eta_2$ . Il vettore  $(0, 1, -\zeta_3)^t$  è un autovettore con autovalore  $\zeta_3$ . Pertanto, se  $\alpha = \eta_1 - \zeta_3\eta_2$ , allora  $\alpha^3$  è un elemento di  $F$  e  $\alpha$  genera il campo di spezzamento di  $x^3 - 3x + 1$  su  $F$ . Possiamo calcolare esplicitamente  $\alpha^3$ , utilizzando il fatto che  $\eta_1 = \zeta_9 + \zeta_9^8$  e  $\eta_2 = \zeta_9^2 + \zeta_9^7$ . Osservando che  $\zeta_3 = \zeta_9^3$ , otteniamo  $\alpha = \zeta_9^8 - \zeta_9^5$  e  $\alpha^3 = 3(1 - \zeta_3)$ . ■

### (7.6) Esempio

Sia  $f(x)$  un polinomio di terzo grado irriducibile arbitrario su un campo  $F$  e sia  $K$  un campo di spezzamento di  $f(x)(x^3 - 1)$  su  $F$ . Sia  $L \subset K$  il campo intermedio generato da  $\zeta$  e  $\delta = \sqrt[3]{D}$ , dove  $D$  è il discriminante di  $f$ . Allora  $[L : F]$  divide 4 e  $[K : L] = 3$ , in virtù di (2.16). I quattro elementi  $1, \sqrt[3]{D}, \sqrt{-3}, \sqrt{-3D}$  generano in ogni caso  $L$  come  $F$ -spazio vettoriale. In base al teorema (7.4) si ha  $K = L(\sqrt[3]{b})$  per qualche  $b \in L$ . Pertanto le radici di  $f(x)$  possono essere espresse per mezzo di una radice cubica della forma:

$$\sqrt[3]{c_1 + c_2\sqrt{D} + c_3\sqrt{-3} + c_4\sqrt{-3D}}, \quad \text{con } c_i \in F. \blacksquare$$

## 8 Estensioni ciclotomiche

Il sottocampo  $K$  del campo dei numeri complessi che è generato su  $\mathbb{Q}$  da  $\zeta_n = e^{2\pi i/n}$  è chiamato un *campo ciclotomico*. Inoltre, per ogni sottocampo  $F$  di  $\mathbb{C}$ , il campo  $F(\zeta_n)$  prende il nome di *estensione ciclotomica* di  $F$ . Esso è il campo di spezzamento su  $F$  del polinomio

$$(8.1) \quad x^n - 1.$$

Se denotiamo  $\zeta_n$  con  $\zeta$ , le radici di questo polinomio sono le potenze di  $\zeta$ , ossia, le radici  $n$ -esime dell'unità  $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ . In questo paragrafo concentreremo la nostra attenzione sul caso in cui  $n$  è un numero primo  $p$  diverso da 2.

Il polinomio  $x^{p-1} + \dots + x + 1$  è irriducibile su  $\mathbb{Q}$  e  $\zeta = \zeta_p$  è una delle sue radici [cap. 11 (4.6)]. Pertanto esso è il polinomio minimo di  $\zeta$  su  $\mathbb{Q}$ . Le sue radici sono le potenze  $\zeta, \zeta^2, \dots, \zeta^{p-1}$ , e quindi il gruppo di Galois di  $\mathbb{Q}(\zeta)$  su  $\mathbb{Q}$  ha ordine  $p - 1$ .

(8.2) PROPOSIZIONE Sia  $p$  un numero primo, e poniamo  $\zeta = \zeta_p$ .

- (a) Il gruppo di Galois di  $\mathbb{Q}(\zeta)$  su  $\mathbb{Q}$  è isomorfo al gruppo moltiplicativo  $\mathbb{F}_p^*$  degli elementi non nulli del campo primo  $\mathbb{F}_p$ , che è un gruppo ciclico di ordine  $p - 1$ .
- (b) Per ogni sottocampo  $F$  di  $\mathbb{C}$ , il gruppo di Galois di  $F(\zeta)$  su  $F$  è ciclico.

*Dimostrazione.* Sia  $G$  il gruppo di Galois di  $F(\zeta)$  su  $F$ . Definiamo un'applicazione  $v : G \rightarrow \mathbb{F}_p^*$  nel modo seguente. Sia  $\sigma \in G$  un automorfismo. Esso porterà  $\zeta$  in un'altra radice del polinomio  $x^p + \dots + x + 1$ , diciamo in  $\zeta^i$ . L'esponente  $i$  è un intero, che è determinato modulo  $p$ , perché  $\zeta$  ha ordine  $p$  rispetto alla moltiplicazione. Per definizione, poniamo  $v(\sigma) = i$ . Verifichiamo che  $v$  è compatibile con la moltiplicazione. Infatti, se  $\tau$  è un altro elemento di  $G$  tale che  $v(\tau) = j$ , o equivalentemente,  $\tau(\zeta) = \zeta^j$ , allora si ha:

$$(8.3) \quad \sigma\tau(\zeta) = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij}.$$

Inoltre, l'automorfismo banale manda  $\zeta$  in  $\zeta$ , e quindi  $v(1) = 1$ . Poiché  $v$  è compatibile con la moltiplicazione e  $v(\sigma) \neq 0$ ,  $v$  è un omomorfismo da  $G$  a  $\mathbb{F}_p^*$ . Questo omomorfismo è iniettivo poiché, essendo  $K$  generato da  $\zeta$ , l'azione di un automorfismo è determinata dalla sua azione su  $\zeta$ . Dunque  $G$  è isomorfo alla sua immagine in  $\mathbb{F}_p^*$ . Poiché  $\mathbb{F}_p^*$  è un gruppo ciclico, tale risulta ogni suo sottogruppo, e quindi  $G$  è ciclico. Se  $F = \mathbb{Q}$ , allora  $|G| = |\mathbb{F}_p^*| = p - 1$  e quindi questi due gruppi sono isomorfi. ■

Supponiamo che  $F = \mathbb{Q}$ . Allora il gruppo di Galois  $G$  di  $K = \mathbb{Q}(\zeta_p)$ , essendo ciclico e di ordine  $p - 1$ , possiede uno e un solo sottogruppo di ordine  $k$ , per ciascun intero  $k$  che divide  $p - 1$ . Se  $(p - 1)/k = r$  e se  $\sigma$  è un generatore di  $G$ , il sottogruppo di ordine  $k$  è generato da  $\sigma^r$ . Pertanto, in base al teorema fondamentale della teoria di Galois, esisterà uno e un solo campo intermedio  $L$  con  $[L : \mathbb{Q}] = r$ . Questi campi sono generati da certe somme di potenze di  $\zeta = \zeta_p$ . Illustreremo ciò con alcuni esempi semplici.

Il caso più semplice è  $p = 5$ . Allora  $[K : \mathbb{Q}] = 4$ , ed esiste un campo intermedio di grado 2 su  $\mathbb{Q}$ , generato da  $\eta = \zeta + \zeta^4 = 2 \cos \frac{2\pi}{5}$ . Poiché  $2 \cos \frac{2\pi}{5} = \frac{1}{2}(-1 + \sqrt{5})$ , il campo intermedio è il campo quadratico di numeri  $\mathbb{Q}(\sqrt{5})$ .

(8.4) PROPOSIZIONE Il sottocampo  $L$  di  $K = \mathbb{Q}(\zeta_p)$ , il cui grado su  $\mathbb{Q}$  è  $\frac{1}{2}(p - 1)$ , è generato su  $\mathbb{Q}$  dall'elemento  $\eta = \zeta + \zeta^{p-1} = 2 \cos \frac{2\pi}{p}$ . Inoltre,  $L = K \cap \mathbb{R}$ .

Poiché  $L = K \cap \mathbb{R}$ ,  $L$  è chiamato anche il *sottocampo reale* di  $K$ .

*Dimostrazione.* Si noti che  $\zeta$  è una radice del polinomio di secondo grado  $x^2 - \eta x + 1$ , che ha i coefficienti in  $\mathbb{Q}(\eta)$ . Pertanto  $[K : \mathbb{Q}(\eta)] \leq 2$ . D'altra parte,  $\eta$  è un numero reale, mentre  $\zeta$  non è reale, e quindi  $\mathbb{Q}(\eta) < K$ . Ne segue che  $[K : \mathbb{Q}(\eta)] = 2$ ,  $\mathbb{Q}(\eta) = K \cap \mathbb{R}$ , e infine  $[\mathbb{Q}(\eta) : \mathbb{Q}] = \frac{1}{2}(p-1)$ . ■

Quando  $p = 7$ ,  $\eta = \zeta + \zeta^6$  ha grado 3 su  $\mathbb{Q}$ . Il suo polinomio minimo su  $\mathbb{Q}$  può essere calcolato con un metodo che abbiamo usato in precedenza (2.12). Proviamo a congetturare che le altre radici siano  $\eta_2 = \zeta^2 + \zeta^5$  e  $\eta_3 = \zeta^3 + \zeta^4$ . Queste sono le altre somme di una radice  $p$ -esima e della sua inversa. Non è difficile dimostrare che  $\{\eta_1, \eta_2, \eta_3\}$  è la  $G$ -orbita di  $\eta = \eta_1$ , sicché la nostra congettura può essere giustificata formalmente. Sviluppiamo il prodotto  $(x - \eta_1)(x - \eta_2)(x - \eta_3)$  e utilizziamo la relazione  $\zeta^6 + \cdots + \zeta + 1 = 0$  ottenendo il polinomio minimo  $x^3 + x^2 - 2x - 1$  di  $\eta$  su  $\mathbb{Q}$ .

Il campo ciclotomico  $\mathbb{Q}(\zeta_7)$  contiene inoltre un'estensione quadratica di  $\mathbb{Q}$  generata da  $\epsilon = \zeta + \zeta^2 + \zeta^4$ . Se poniamo  $\epsilon' = \zeta^3 + \zeta^5 + \zeta^6$ , allora  $(x - \epsilon)(x - \epsilon') = x^2 + x + 2$  è il suo polinomio minimo. Il discriminante di questo polinomio è  $-7$ , e pertanto  $\mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{-7})$ . Ne segue che  $\mathbb{Q}(\zeta_7)$  contiene  $\sqrt{-7}$ .

Supponiamo che  $p = 17$ . Allora  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 16$ . Un gruppo ciclico di ordine 16 contiene una catena di sottogruppi  $C_{16} \supset C_8 \supset C_4 \supset C_2 \supset C_1$ . In base al teorema fondamentale della teoria di Galois, esiste una catena corrispondente di campi intermedi  $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3 \subset \mathbb{Q}(\zeta)$  di gradi, rispettivamente, 1, 2, 4, 8, 16 su  $\mathbb{Q}$ . Il campo  $F_3$  di grado 8 è il sottocampo reale generato da  $\eta = 2 \cos \frac{2\pi}{17}$ , come nella proposizione (8.4). Poiché ciascuna estensione in questa catena ha grado 2,  $F_3$  può essere ottenuto aggiungendo, una dopo l'altra, tre radici quadrate. Ciò dimostra che  $2 \cos \frac{2\pi}{17}$ , e quindi il poligono regolare di 17 lati, può essere costruito con riga e compasso [cap. 13 (4.9)].

Le altre estensioni di campi che descriveremo per tutti i primi sono quelle di grado 2 su  $\mathbb{Q}$ . Il teorema fondamentale della teoria di Galois ci dice che esiste un unico campo intermedio  $L$  di grado 2 su  $\mathbb{Q}$ , corrispondente al sottogruppo  $H$  di  $G$  di ordine  $\frac{1}{2}(p-1)$ . Se  $\sigma$  genera  $G$ , allora  $H$  è generato da  $\sigma^2$ .

(8.5) TEOREMA Sia  $p$  un numero primo dispari, e sia  $L$  l'unica estensione quadratica di  $\mathbb{Q}$  contenuta nel campo ciclotomico  $\mathbb{Q}(\zeta_p)$ . Allora si ha:

$$L = \mathbb{Q}(\sqrt{\pm p}),$$

dove il segno è  $(-1)^{1/2(p-1)}$ .

*Dimostrazione.* Dobbiamo scegliere un generatore di  $L$  la cui equazione sia facile da determinare. Il metodo di Gauss consiste nel prendere la somma di metà delle potenze di  $\zeta$ , scelte opportunamente.

Vi è tuttavia un'altra scelta, un po' più semplice da utilizzare. Sia  $D$  il discriminante del polinomio

$$(8.6) \quad x^p - 1.$$

Esso può essere calcolato direttamente per mezzo delle radici  $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ , ma è più facile utilizzare la formula seguente, semplice ed elegante:

(8.7) LEMMA Sia  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ . Il discriminante di  $f$  è:

$$D = \pm f'(\alpha_1) \cdots f'(\alpha_n) = \pm \prod_i f'(\alpha_i),$$

dove  $f'$  è la derivata di  $f$ .

*Dimostrazione.* In base alla regola di derivazione del prodotto, si ha:

$$f'(x) = \sum_{i=1}^n (x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_n).$$

Pertanto

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_n).$$

Questo è il prodotto delle differenze  $(\alpha_i - \alpha_j)$ , con l'indice  $i$  fissato e con  $j \neq i$ . Dunque

$$\prod_i f'(\alpha_i) = \prod_{i \neq j} (\alpha_i - \alpha_j) = \pm D. \blacksquare$$

Applichiamo il lemma precedente al nostro polinomio  $x^p - 1$ . La sua derivata è  $px^{p-1}$ , sicché il discriminante è:

$$D = \pm \prod_i p \zeta^{i(p-1)} = \pm \zeta^N p^p,$$

dove l'esponente  $N$  è un intero opportuno. Per determinare  $\zeta^N$ , osserviamo che  $D$  è un numero razionale, perché i coefficienti di  $x^p - 1$  sono numeri razionali. L'unica potenza di  $\zeta$  che sia un numero razionale è 1. Pertanto  $\zeta^N = 1$  e quindi risulta:

$$(8.8) \quad D = \pm p^p.$$

La radice quadrata di questo discriminante è  $\delta = \sqrt{\pm p^p}$ , che appartiene al campo  $\mathbb{Q}(\zeta)$ . Poiché  $p$  è dispari e poiché i fattori quadratici possono essere portati fuori dal segno di radice, si ha:

$$(8.9) \quad \mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{\pm p}).$$

Pertanto questo campo è un sottocampo quadratico di  $\mathbb{Q}(\zeta)$ , e poiché  $L$  è l'unico sottocampo quadratico, è proprio  $L$ . La determinazione del segno è lasciata come esercizio. ■

Il risultato seguente, enunciato per la prima volta da Kronecker, è uno dei teoremi più belli della teoria algebrica dei numeri. Purtroppo, ci vorrebbe troppo tempo per dimostrarlo qui.

(8.10) TEOREMA *Ogni estensione di Galois  $K$  di  $\mathbb{Q}$  tale che il suo gruppo di Galois è abeliano è contenuta in uno dei campi ciclotomici  $\mathbb{Q}(\zeta_n)$ .* ■

## 9 Equazioni di quinto grado

La motivazione principale per il lavoro di Galois era il problema della risoluzione delle equazioni di quinto grado. Ci proponiamo in questo paragrafo di studiare la sua soluzione. Poco tempo prima, Abel aveva dimostrato che l'equazione generale di quinto grado

$$(9.1) \quad x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0,$$

a coefficienti  $a_i$  variabili, non era risolubile per radicali (ossia eseguendo sui coefficienti solo un numero finito di operazioni razionali e di estrazioni di radice di indice intero); tuttavia, rimaneva da trovare un'equazione esplicita a coefficienti razionali che non potesse essere risolta. In ogni caso, poiché il problema era vecchio più di duecento anni, continuò a destare interesse. Nel frattempo, le idee di Galois si sono rivelate molto più importanti della questione che le aveva originate.

Un'espressione mediante radicali può diventare molto complicata, e io non conosco una buona notazione per un'espressione nel caso generale. Tuttavia, è facile dare una definizione ricorsiva precisa.

(9.2) DEFINIZIONE *Sia  $F$  un sottocampo del campo dei numeri complessi. Si dice che un numero complesso  $\alpha$  è esprimibile mediante radicali su  $F$  se esiste una catena di sottocampi  $F = F_0 \subset F_1 \subset \dots \subset F_r$  di  $\mathbb{C}$  tali che:*

- (i)  $\alpha \in F_r$ ;
- (ii) per ogni  $j = 1, \dots, r$ ,  $F_j$  è generato su  $F_{j-1}$  da un radicale  $\beta_j$ . In altre parole,  $F_j = F_{j-1}(\beta_j)$ , con  $\beta_j^{n_j} \in F_{j-1}$ , per qualche intero  $n_j$ .

Questa definizione è formalmente simile alla descrizione [cap. 13 (4.9)] dei numeri reali che possono essere costruiti con riga e compasso. In quella descrizione, erano ammesse soltanto le radici quadrate di numeri reali positivi.

(9.3) PROPOSIZIONE *Sia  $\alpha$  una radice di un polinomio  $f(x) \in F[x]$  di grado  $\leq 4$ . Allora  $\alpha$  è esprimibile mediante radicali su  $F$ .*

*Dimostrazione.* Per i polinomi di secondo grado, la soluzione è data dalla formula ben nota. Per i polinomi di terzo grado, la formula di Cardano dà la soluzione. Supponiamo che  $f(x)$  sia un polinomio di quarto grado. Se  $f$  è riducibile  $\alpha$  è una radice di un polinomio di grado più basso, e quindi il problema è risolto. Altrimenti,  $f$  ha radici distinte in un campo di spezzamento  $K$ , e pertanto il suo discriminante  $D$  è diverso da zero. Sia  $g(x)$  il polinomio cubico risolvente di  $f$ . Procediamo aggiungendo la radice quadrata  $\delta$  di  $D$ , ottenendo un campo  $F_1$  (eventualmente uguale a  $F$ ), e poi usiamo la formula di Cardano per trovare le radici del polinomio cubico risolvente. Ciò richiederà un'estensione  $F_2$  mediante una radice quadrata, seguita da un'estensione  $F_3$  mediante una radice cubica. A questo punto, la tabella (6.14) mostra che il gruppo di Galois di  $K/F_3$  è un sottogruppo del gruppo quadrinomio di Klein; quindi  $K$  può essere ottenuto mediante una successione di al più due ulteriori estensioni con radici quadrate  $F_3 \subset F_4 \subset F_5 = K$ . ■

Le radici  $n$ -esime dell'unità  $\zeta_n = e^{2\pi i/n}$  sono ammissibili in un'espressione per radicali. Inoltre, se  $n = rs$ , allora  $\sqrt[n]{b} = \sqrt[r]{\sqrt[s]{b}}$ . Pertanto, a meno di aggiungere altri passi nella catena di campi, possiamo supporre che tutte le radici siano radici  $p$ -esime, per vari primi  $p$ .

Si noti che vi è una notevole ambiguità in un'espressione per radicali, poiché per ciascun radicale  $\sqrt[n]{b}$  vi sono  $n$  possibilità di scelta. La notazione  $(-3 + \sqrt[5]{2})^{1/4}$  può indicare uno qualsiasi di 20 numeri complessi, e quindi la catena di campi  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{2}) \subset \mathbb{Q}((-3 + \sqrt[5]{2})^{1/4})$  non è definita univocamente. Questa ambiguità è insita nella notazione. Poiché la notazione è comunque ingombrante, non tenteremo di renderla più precisa. In ogni caso, non la useremo molto.

(9.4) PROPOSIZIONE *Sia  $f(x)$  un polinomio irriducibile su un campo  $F$ . Se una radice di  $f$  in  $K$  è esprimibile per radicali, tale risulta qualsiasi altra radice.*

*Dimostrazione.* Supponiamo che una radice  $\alpha$  sia esprimibile per radicali, ad esempio mediante la catena  $F = F_0 \subset \dots \subset F_r$ . Scegliamo un campo  $L$  che contenga  $F_r$  e che sia un campo di spezzamento di qualche polinomio della forma  $f(x)g(x)$  su  $F$ . Allora  $L$  è anche il campo di spezzamento di  $fg$  su  $F(\alpha)$ . Sia  $\alpha'$  una radice di  $f$  in un altro campo  $K'$  e sia  $L'$  un campo di spezzamento di  $fg$  su  $F(\alpha')$ . Allora possiamo estendere l'isomorfismo  $F(\alpha) \rightarrow F(\alpha')$  a un isomorfismo  $\varphi : L \rightarrow L'$  (5.2). La catena di campi  $F = \varphi(F_0) \subset \dots \subset \varphi(F_r)$  mostra che  $\alpha'$  è esprimibile per radicali. ■

(9.5) PROPOSIZIONE *Sia  $\alpha$  un numero complesso esprimibile per radicali su  $F$ . Allora è possibile trovare una catena di campi  $F = F_0 \subset \dots \subset F_r = K$  tale che valgano le condizioni (i) e (ii) di (9.2), nonché la condizione seguente:*

- (iii) per ogni indice  $j$   $F_j$  è un'estensione di Galois di  $F_{j-1}$  e il gruppo di Galois  $G(F_j/F_{j-1})$  è un gruppo ciclico.

*Dimostrazione.* Consideriamo la catena data nella definizione (9.2), in cui  $F_r = F(\beta_1, \dots, \beta_r)$ . Come abbiamo osservato, si può supporre che

$$\beta_j^{p_j} \in F_{j-1}$$

per qualche primo  $p_j$ . Sia  $\zeta_{p_j} = e^{2\pi i/p_j}$  la radice  $p_j$ -esima di 1. Formiamo una nuova catena di campi aggiungendo gli elementi  $(\zeta_{p_1}, \dots, \zeta_{p_r}; \beta_1, \dots, \beta_r)$ , in quest'ordine. Il teorema (7.4) e la proposizione (8.2) mostrano che ciascuna di tali estensioni è un'estensione di Galois, con gruppo di Galois ciclico. Alcune estensioni in questa catena possono risultare banali, nel qual caso accorciamo la catena. Poiché l'ultimo campo  $F(\{\zeta_{p_j}\}, \{\beta_j\})$  della catena contiene  $F_r$ , esso contiene  $\alpha$ . ■

Consideriamo il gruppo di Galois di un prodotto di polinomi  $f(x)g(x)$  su  $F$ . Sia  $K'$  un campo di spezzamento di  $fg$ . Allora  $K'$  contiene un campo di spezzamento  $K$  di  $f$ , poiché  $f$  si scomponete in fattori lineari in  $K'$ . Analogamente,  $K'$  contiene un campo di spezzamento  $F'$  di  $g$ . Pertanto abbiamo un diagramma di campi della forma:

$$(9.6) \quad \begin{array}{ccc} & K' & \\ & \swarrow \quad \searrow & \\ K & & F' \\ & \nwarrow \quad \nearrow & \\ & F & \end{array}$$

(9.7) PROPOSIZIONE *Con le notazioni appena introdotte, poniamo:  $G = G(K/F)$ ,*

*$H = G(F'/F)$  e  $\mathcal{G} = G(K'/F)$ . Allora si ha che:*

- (a)  $G$  e  $H$  sono quozienti di  $\mathcal{G}$ ;
- (b)  $\mathcal{G}$  è isomorfo ad un sottogruppo del gruppo prodotto  $G \times H$ .

*Dimostrazione.* La prima asserzione segue dal fatto che  $K$  e  $F'$  sono campi intermedi che risultano estensioni di Galois di  $F$  (5.6b). Denotiamo gli omomorfismi canonici  $\mathcal{G} \rightarrow G$ ,  $\mathcal{G} \rightarrow H$  con indici in basso:  $\sigma \mapsto \sigma_f$  e  $\sigma \mapsto \sigma_g$ . Allora  $\sigma_f$  descrive il modo in cui  $\sigma$  agisce sulle radici di  $f$ , e  $\sigma_g$  descrive il modo in cui  $\sigma$  agisce sulle radici di  $g$ . Consideriamo l'applicazione da  $\mathcal{G}$  a  $G \times H$  definita da  $\sigma \mapsto (\sigma_f, \sigma_g)$ . Se  $\sigma_f$  e  $\sigma_g$  sono entrambe l'identità, allora  $\sigma$  agisce in modo banale sulle radici di  $fg$ , e quindi  $\sigma = 1$ . Ciò dimostra che l'applicazione  $\mathcal{G} \rightarrow G \times H$  è iniettiva e che  $\mathcal{G}$  è isomorfo a un sottogruppo di  $G \times H$ . ■

(9.8) PROPOSIZIONE *Sia  $f$  un polinomio su  $F$  il cui gruppo di Galois  $G$  sia un gruppo non abeliano semplice. Sia  $F'$  un'estensione di Galois di  $F$ , con gruppo di Galois abeliano. Sia  $K'$  un campo di spezzamento di  $f$  su  $F'$ . Allora il gruppo di Galois  $G(K'/F')$  è isomorfo a  $G$ .*

Questa proposizione ha un'importanza cruciale. Essa ci dice che, se il gruppo di Galois di  $f$  è un gruppo non abeliano semplice, non faremo alcun progresso per quanto riguarda il problema dell'espressione delle radici di  $f$ , se sostituiamo  $F$  con un'estensione abeliana  $F'$ .

*Dimostrazione.* Innanzitutto ci riduciamo al caso in cui  $[F' : F]$  è un numero primo. Per fare ciò, supponiamo che il risultato sia stato dimostrato in quel caso, e scegliamo un gruppo quoziante ciclico  $H$  di  $G(F'/F)$  di ordine primo. Un tale quoziante esiste perché  $G(F'/F)$  è abeliano, e determina un campo intermedio  $F_1 \subset F'$ , che è un'estensione di Galois di  $F$ , e tale che  $G(F_1/F) = H$ , come da (5.6). Sia  $K_1$  il campo di spezzamento di  $f$  su  $F_1$ . Allora, poiché  $[F_1 : F]$  è primo,  $G(K_1/F_1) = G$ . Pertanto possiamo sostituire  $F$  con  $F_1$  e  $K$  con  $K_1$ . Procedendo per induzione su  $[F' : F]$ , si completa la dimostrazione.

Pertanto possiamo supporre che  $[F' : F] = p$  e che  $H = G(F'/F)$  sia un gruppo ciclico di ordine  $p$ . Il campo di spezzamento  $K'$  conterrà un campo di spezzamento di  $f$  su  $F$ , diciamo  $K$ . Siamo allora nella situazione della proposizione (9.7). Pertanto il gruppo di Galois  $\mathcal{G}$  di  $K'$  su  $F$  è un sottogruppo di  $G \times H$  e inoltre viene mandato in  $G$  mediante un'applicazione suriettiva. Ne segue che  $|G|$  divide  $|\mathcal{G}|$ , e  $|\mathcal{G}|$  divide  $|G \times H| = p|G|$ . Se  $|G| = |\mathcal{G}|$ , allora contando i gradi, si ottiene che  $K' = K$ . In questo caso,  $K$  contiene l'estensione di Galois  $F'$ , e quindi  $H$  è un quoziante di  $G$  (5.6b). Poiché  $G$  è un gruppo semplice non abeliano, ciò è impossibile. L'unica possibilità che rimane è che  $\mathcal{G} = G \times H$ . Applicando il teorema fondamentale alla catena di campi  $F \subset F' \subset K'$ , si conclude che  $G(K'/F') = G$ , come richiesto. ■

(9.9) TEOREMA *Le radici di un polinomio di quinto grado  $f(x)$  il cui gruppo di Galois è  $S_5$  o  $A_5$ , non possono essere espresse mediante radicali su  $F$ .*

*Dimostrazione.* Sia  $K$  un campo di spezzamento di  $f$ . Se  $G = S_5$ , il discriminante di  $f$  non è un quadrato in  $F$ . In tal caso, sostituiamo  $F$  con  $F(\delta)$ , dove  $\delta$  è una radice quadrata del discriminante in  $K$ . Il gruppo di Galois  $G(K/F(\delta))$  è  $A_5$ . Ovviamente, basta provare che le radici di  $f$  non possono essere espresse mediante radicali sul campo più grande  $F(\delta)$ . In tal modo, il caso in cui il gruppo è  $S_5$  viene ridotto al caso in cui è  $A_5$ .

Supponiamo che il gruppo di Galois di  $f$  sia  $A_5$ , e che qualche radice  $\alpha$  di  $f$  sia esprimibile per radicali su  $F$ . Supponiamo che  $\alpha \in F_r$ , dove  $F_r$  è l'ultimo elemento di una catena di estensioni di campi  $F = F_0 \subset \dots \subset F_r$ , in cui ciascuna estensione è di Galois, con il gruppo di Galois ciclico. Ora, poiché il gruppo di Galois di  $f$  su  $F$  è un gruppo semplice, dalla proposizione (9.8) si ottiene (procedendo per induzione) che il gruppo di Galois di  $f$  su  $F_i$ , per ogni  $i$ , è anch'esso  $A_5$ . D'altra parte, poiché il polinomio  $f$  ha una radice  $\alpha$  in  $F_r$ , non rimarrà irriducibile su  $F_r$ . Pertanto il gruppo di Galois di  $f$  su  $F_r$  non agirà transitivamente sulle cinque radici di  $f$  in un campo di spezzamento. In particolare, il gruppo di Galois non

può essere il gruppo alterno. Si ottiene così una contraddizione, e ciò prova che le radici di  $f$  non sono esprimibili per radicali su  $F$ . ■

Daremo ora un esempio concreto di un polinomio di quinto grado su  $\mathbb{Q}$  il cui gruppo di Galois è  $S_5$ . Queste due condizioni, che 5 sia un numero primo e che il gruppo di Galois  $G$  agisca transitivamente sull'insieme delle radici  $\{\alpha_1, \dots, \alpha_5\}$ , limitano fortemente le possibilità per i gruppi di Galois. Infatti, poiché l'azione è transitiva,  $|G|$  è divisibile per 5, e quindi  $G$  contiene un elemento di ordine 5. Gli unici elementi di ordine 5 in  $S_5$  sono le permutazioni cicliche, quale ad esempio  $\sigma = (1\ 2\ 3\ 4\ 5)$ .

(9.10) LEMMA *Se  $G$  contiene una trasposizione,  $G = S_5$ .*

*Dimostrazione.* Per trasposizione intendiamo, come sempre, una permutazione  $\tau$  che scambia tra loro due indici. Possiamo supporre che  $G$  contenga la permutazione ciclica  $\sigma = (1\ 2\ 3\ 4\ 5)$ . Rinumerando eventualmente gli indici, possiamo supporre che  $\tau$  agisca come (1i). Ora, sostituiamo  $\sigma$  con  $\sigma^{i-1}$  e rinumeriamo di nuovo gli indici, per ridurci al caso in cui  $\tau$  è la trasposizione (12). Resta soltanto da verificare che  $\sigma$  e  $\tau$  generano  $S_5$ , e ciò viene lasciato come esercizio. ■

(9.11) COROLLARIO *Supponiamo che il polinomio irriducibile (9.1) abbia radici  $\{\alpha_1, \dots, \alpha_5\}$ , e sia  $K$  il suo campo di spezzamento. Se  $F(\alpha_1, \alpha_2, \alpha_3) < K$ , allora  $G(K/F)$  è il gruppo simmetrico  $S_5$ .*

Infatti, poniamo  $F' = F(\alpha_1, \alpha_2, \alpha_3)$ . L'unica permutazione non banale che lascia fisse le radici  $\alpha_1, \alpha_2, \alpha_3$  è la trasposizione (45). Se  $F' \neq K$ , questa permutazione deve appartenere a  $G(K/F')$ . Pertanto  $G(K/F)$  contiene una trasposizione. ■

(9.12) COROLLARIO *Sia  $f(x)$  un polinomio di quinto grado irriducibile su  $\mathbb{Q}$  avente esattamente tre radici reali. Allora il suo gruppo di Galois è il gruppo simmetrico, e quindi le sue radici non possono essere espresse mediante radicali.*

Infatti, denotiamo con  $\alpha_1, \alpha_2, \alpha_3$  le radici reali. Allora  $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subset \mathbb{R}$ , ma poiché  $\alpha_4, \alpha_5$  non sono reali,  $K$  non è un sottocampo di  $\mathbb{R}$ . Pertanto possiamo applicare il corollario (9.11) per concludere che il gruppo di Galois di  $f$  è  $S_5$ . Ne segue, in base al teorema (9.9), che le radici di  $f$  non possono essere espresse mediante radicali. ■

(9.13) Esempio

Il polinomio  $x^5 - 16x = x(x^2 - 4)(x^2 + 4)$  ha tre radici reali, ma naturalmente non è irriducibile. Tuttavia possiamo aggiungere una piccola costante senza cambiare

il numero delle radici reali. Ciò si vede esaminando il grafico del polinomio. Per esempio,

$$x^5 - 16x + 2$$

ha ancora tre radici reali, ed è irriducibile in virtù del criterio di Eisenstein [cap. 10 (4.9)]. Pertanto le sue radici non possono essere espresse mediante radicali su  $\mathbb{Q}$ .

Si direbbe, da ciò, che la soluzione da noi proposta non porta alcun frutto.

Evariste Galois

### Esercizi

#### 1 Il teorema fondamentale della teoria di Galois

1. Determinare il polinomio minimo di  $i + \sqrt{2}$  su  $\mathbb{Q}$ .
2. Dimostrare che l'insieme  $(1, i, \sqrt{2}, i\sqrt{2})$  è una base di  $\mathbb{Q}(i, \sqrt{2})$  su  $\mathbb{Q}$ .
3. Determinare i campi intermedi tra  $\mathbb{Q}$  e  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ .
4. Determinare i campi intermedi di un'estensione biquadratica senza ricorrere al teorema fondamentale.
5. Dimostrare che l'automorfismo di  $\mathbb{Q}(\sqrt{2})$  che manda  $\sqrt{2}$  in  $-\sqrt{2}$  non è continuo.
6. Determinare il grado del campo di spezzamento dei seguenti polinomi su  $\mathbb{Q}$ :
  - (a)  $x^4 - 1$ ; (b)  $x^3 - 2$ ; (c)  $x^4 + 1$ .
7. Si denoti con  $\alpha$  la radice quarta reale positiva di 2. Scomporre il polinomio  $x^4 - 2$  in fattori irriducibili su ciascuno dei campi seguenti:
 
$$\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}, i), \mathbb{Q}(\alpha), \mathbb{Q}(\alpha, i).$$
8. Sia  $\zeta = e^{2\pi i/5}$ .
  - (a) Dimostrare che  $K = \mathbb{Q}(\zeta)$  è un campo di spezzamento del polinomio  $x^5 - 1$  su  $\mathbb{Q}$ , e determinare il grado  $[K : \mathbb{Q}]$ .
  - (b) Senza usare il teorema (1.11), dimostrare che  $K$  è un'estensione di Galois di  $\mathbb{Q}$ , e determinare il suo gruppo di Galois.
9. Sia  $K$  un'estensione quadratica della forma  $F(\alpha)$ , dove  $\alpha^2 = a \in F$ . Determinare tutti gli elementi di  $K$  i cui quadrati stanno in  $F$ .
10. Sia  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ . Determinare  $[K : \mathbb{Q}]$ , dimostrare che  $K$  è un'estensione di Galois di  $\mathbb{Q}$ , e determinare il suo gruppo di Galois.
11. Sia  $K$  il campo di spezzamento su  $\mathbb{Q}$  del polinomio  $f(x) = (x^2 - 2x - 1)(x^2 - 2x - 7)$ . Determinare  $G(K/\mathbb{Q})$ , e determinare esplicitamente tutti i campi intermedi.
12. Determinare tutti gli automorfismi del campo  $\mathbb{Q}(\sqrt[3]{2})$ .
13. Sia  $K/F$  un'estensione finita. Dimostrare che il gruppo di Galois  $G(K/F)$  è un gruppo finito.

14. Determinare tutti i campi di numeri quadratici  $\mathbb{Q}[\sqrt{d}]$  che contengono una radice  $p$ -esima primitiva dell'unità, per qualche primo  $p \neq 2$ .
15. Dimostrare che ogni estensione di Galois  $K/F$  il cui gruppo di Galois sia il gruppo quadrinomio di Klein è biquadratica.
16. Dimostrare o confutare l'enunciato seguente. Sia  $f(x)$  un polinomio di terzo grado irriducibile in  $\mathbb{Q}[x]$  con una sola radice reale  $\alpha$ . Le altre radici formano una coppia di numeri complessi coniugati  $\beta, \bar{\beta}$ , e pertanto il campo  $L = \mathbb{Q}(\beta)$  possiede un automorfismo  $\sigma$  che scambia tra loro  $\beta, \bar{\beta}$ .
17. Sia  $K$  un'estensione di Galois di un campo  $F$  tale che  $G(K/F) \approx C_2 \times C_{12}$ . Quanti sono i campi intermedi  $L$  tali che  
 (a)  $[L : F] = 4$ ; (b)  $[L : F] = 9$ ; (c)  $G(K/L) \approx C_4$ ?
18. Sia  $f(x) = x^4 + bx^2 + c \in F[x]$ , e sia  $K$  il campo di spezzamento di  $f$ . Dimostrare che  $G(K/F)$  è contenuto in un gruppo diedrale  $D_4$ .
19. Sia  $F = \mathbb{F}_2(u)$  il campo delle funzioni razionali sul campo di due elementi. Dimostrare che il polinomio  $x^2 - u$  è irriducibile in  $F[x]$  e ha due radici uguali in un campo di spezzamento.
20. Sia  $F$  un campo di caratteristica 2, e sia  $K$  un'estensione di  $F$  di grado 2.  
 (a) Dimostrare che  $K$  ha la forma  $F(\alpha)$ , dove  $\alpha$  è la radice di un polinomio irriducibile su  $F$  della forma  $x^2 + x + a$ , e che l'altra radice di tale polinomio è  $\alpha + 1$ .  
 (b) È vero che esiste un automorfismo di  $K$  che manda  $\alpha$  in  $\alpha + 1$ ?

## 2 Equazioni di terzo grado

1. Dimostrare che il discriminante di un polinomio di terzo grado a coefficienti reali è positivo se tutte le radici sono reali, altrimenti è negativo.
2. Determinare i gruppi di Galois dei seguenti polinomi:  
 (a)  $x^3 - 2$ ; (b)  $x^3 + 27x - 4$ ; (c)  $x^3 + x + 1$ ; (d)  $x^3 + 3x + 14$ ;  
 (e)  $x^3 - 3x^2 + 1$ ; (f)  $x^3 - 21x + 7$ ; (g)  $x^3 + x^2 - 2x - 1$ ; (h)  $x^3 + x^2 - 2x + 1$ .
3. Sia  $f$  un polinomio di terzo grado irriducibile su  $F$ , e sia  $\delta$  la radice quadrata del discriminante di  $f$ . Dimostrare che  $f$  rimane irriducibile sul campo  $F(\delta)$ .
4. Sia  $\alpha$  una radice complessa del polinomio  $x^3 + x + 1$  su  $\mathbb{Q}$ , e sia  $K$  un campo di spezzamento di questo polinomio su  $\mathbb{Q}$ .  
 (a) È vero che  $\sqrt{-3}$  appartiene al campo  $\mathbb{Q}(\alpha)$ ? È vero che  $\sqrt{-3}$  appartiene a  $K$ ?  
 (b) Dimostrare che il campo  $\mathbb{Q}(\alpha)$  non possiede automorfismi diversi dall'identità.
- \*5. Dimostrare direttamente la proposizione (2.16) per un polinomio di terzo grado della forma (2.3), determinando la formula che esprime esplicitamente  $\alpha_2$  per mezzo di  $\alpha_1, \delta, p, q$ .
6. Sia  $f \in \mathbb{Q}[x]$  un polinomio di terzo grado irriducibile con una sola radice reale e sia  $K$  il suo campo di spezzamento su  $\mathbb{Q}$ . Dimostrare che  $[K : \mathbb{Q}] = 6$ .
7. Quand'è che il polinomio  $x^3 + px + q$  ha una radice multipla?

8. Determinare i coefficienti  $p, q$  che si ottengono dalla generica equazione di terzo grado (2.1) mediante la sostituzione (2.2).
9. Dimostrare che il discriminante del polinomio di terzo grado  $x^3 + px + q$  è  $-4p^3 - 27q^2$ .
- 3 Funzioni simmetriche**
1. Ricavare l'espressione (3.10) del discriminante di un polinomio di terzo grado con il metodo dei coefficienti indeterminati.
2. Sia  $f(u)$  un polinomio simmetrico di grado  $d$  in  $u_1, \dots, u_n$ , e poniamo  $f^0(u_1, \dots, u_{n-1}) = f(u_1, \dots, u_{n-1}, 0)$ . Scriviamo allora:  $f^0(u) = g(s^0)$ , dove le  $s_i^0$  sono le funzioni simmetriche elementari in  $u_1, \dots, u_{n-1}$ . Dimostrare che, se  $n > d$ , allora  $f(u) = g(s)$ .
3. Calcolare il discriminante di un polinomio di quinto grado della forma  $x^5 + ax + b$ .
4. Per ciascuno dei seguenti polinomi, stabilire se esso è oppure no una funzione simmetrica, e, in caso affermativo, esprimere il polinomio per mezzo delle funzioni simmetriche elementari:  
 (a)  $u_1^2 u_2 + u_2^2 u_1$  ( $n = 2$ );  
 (b)  $u_1^2 u_2 + u_2^2 u_3 + u_3^2 u_1$  ( $n = 3$ );  
 (c)  $(u_1 + u_2)(u_2 + u_3)(u_1 + u_3)$  ( $n = 3$ );  
 (d)  $u_1^3 u_2 + u_2^3 u_3 + u_3^3 u_1 - u_1 u_2^3 - u_2 u_3^3 - u_3 u_1^3$  ( $n = 3$ );  
 (e)  $u_1^3 + u_2^3 + \dots + u_n^3$ .
5. Trovare due basi naturali per l'anello delle funzioni simmetriche, considerato come modulo libero sull'anello  $R$ .
- \*6. Definiamo i polinomi  $w_1, \dots, w_n$  nelle variabili  $u_1, \dots, u_n$  ponendo:  $w_k = u_1^k + \dots + u_n^k$ .  
 (a) Dimostrare le *identità di Newton*:
- $$w_k - s_1 w_{k-1} + s_2 w_{k-2} - \dots \pm s_{k-1} w_1 \mp k s_k = 0.$$
- (b) È vero che  $w_1, \dots, w_n$  generano l'anello delle funzioni simmetriche?
7. Sia  $f(x) = x^3 + a_2 x^2 + a_1 x + a_0$ . Dimostrare che la sostituzione  $x = x_1 - (a_2/3)$  lascia invariato il discriminante di un polinomio di terzo grado.
8. Dimostrare che  $[F(u) : F(s)] = n!$  per induzione, direttamente dalle definizioni.
9. Siano  $u_1, \dots, u_n$  delle variabili e denotiamo il discriminante con  $D_1$ . Definiamo:
- $$D_2 = \sum_k \prod_{\substack{i < j \\ i, j \neq k}} (u_i - u_j)^2.$$
- (a) Dimostrare che  $D_2$  è un polinomio simmetrico, e calcolare la sua espressione per mezzo dei polinomi simmetrici elementari nei casi  $n = 2, 3$ .  
 (b) Siano  $a_1, \dots, a_n$  elementi di un campo di caratteristica zero. Dimostrare che  $D_1(a_1, \dots, a_n) = D_2(a_1, \dots, a_n) = 0$  se e soltanto se il numero degli elementi distinti nell'insieme  $\{a_1, \dots, a_n\}$  è  $\leq n - 2$ .

**10.** Calcolare il discriminante dei polinomi dati nell'esercizio 2 del paragrafo 2.

**\*11. (Determinante di Vandermonde)** **(a)** Dimostrare che il determinante della matrice:

$$\begin{bmatrix} 1 & u_1 & u_1^2 & \cdots & u_1^{n-1} \\ 1 & u_2 & u_2^2 & \cdots & u_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & u_n & u_n^2 & \cdots & u_n^{n-1} \end{bmatrix}$$

è un multiplo costante di  $\delta(u)$ .

**(b)** Determinare la costante.

#### 4 Elementi primitivi

**1.** Sia  $G$  un gruppo di automorfismi di un campo  $K$ . Dimostrare che l'insieme  $K^G$  degli elementi fissi risulta un sottocampo di  $K$ .

**2.** Poniamo  $\alpha = \sqrt[3]{2}$ ,  $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ ,  $\beta = \alpha\zeta$ .

**(a)** Dimostrare che, per ogni  $c \in \mathbb{Q}$ ,  $\gamma = \alpha + c\beta$  è la radice di un polinomio di sesto grado della forma  $x^6 + ax^3 + b$ .

**(b)** Dimostrare che il polinomio minimo di  $\alpha + \beta$  è di terzo grado.

**(c)** Dimostrare che  $\alpha - \beta$  ha grado 6 su  $\mathbb{Q}$ .

**3.** Per ciascuno dei seguenti insiemi di automorfismi del campo delle funzioni razionali  $\mathbb{C}(y)$ , determinare il gruppo di automorfismi che essi generano e determinare esplicitamente il campo degli elementi fissi:

**(a)**  $\sigma(y) = y^{-1}$ ; **(b)**  $\sigma(y) = iy$ ; **(c)**  $\sigma(y) = -y$ ,  $\tau(y) = y^{-1}$ ;

**(d)**  $\sigma(y) = \zeta y$ ,  $\tau(y) = y^{-1}$ , dove  $\zeta = e^{2\pi i/3}$ ; **(e)**  $\sigma(y) = iy$ ,  $\tau(y) = y^{-1}$ .

**4.** **(a)** Dimostrare che gli automorfismi  $\sigma(y) = (y+i)/(y-i)$ ,  $\tau(y) = i(y-1)/(y+1)$  di  $\mathbb{C}(y)$  generano un gruppo isomorfo al gruppo alterno  $A_4$ .

**\*(b)** Determinare il campo fisso di tale gruppo.

**\*5.** Sia  $F$  un campo finito e sia  $f(x)$  un polinomio non costante la cui derivata sia il polinomio nullo. Dimostrare che  $f$  non è irriducibile su  $F$ .

#### 5 Dimostrazione del teorema fondamentale

**1.** Sia  $K = \mathbb{Q}(\alpha)$ , dove  $\alpha$  è una radice del polinomio  $x^3 + 2x + 1$ , e sia  $g(x) = x^3 + x + 1$ . È vero che  $g(x)$  ha una radice in  $K$ ?

**2.** Sia  $f \in F[x]$  un polinomio di grado  $n$ , e sia  $K$  un campo di spezzamento di  $f$ . Dimostrare che  $[K : F]$  divide  $n!$ .

**3.** Sia  $G$  un gruppo finito. Dimostrare che esistono un campo  $F$  e un'estensione di Galois  $K$  di  $F$  il cui gruppo di Galois è  $G$ .

**4.** Supponiamo di sapere che  $\pi$  ed  $e$  sono numeri trascendenti. Sia  $K$  il campo di spezzamento del polinomio  $x^3 + \pi x + 6$  sul campo  $F = \mathbb{Q}(\pi)$ .

**(a)** Dimostrare che  $[K : F] = 6$ .

**(b)** Dimostrare che  $K$  è isomorfo al campo di spezzamento di  $x^3 + ex + 6$  su  $\mathbb{Q}(e)$ .

**5.** Dimostrare l'isomorfismo  $F[x]/(f(x)) \approx \tilde{F}[x]/(\tilde{f}(x))$  usato nella dimostrazione del lemma (5.1) in modo formale, utilizzando la proprietà universale della costruzione dei quozienti.

**6.** Dimostrare il corollario (5.5).

**7.** Sia  $f(x)$  un polinomio di terzo grado irriducibile su  $\mathbb{Q}$ , il cui gruppo di Galois sia  $S_3$ . Determinare i gruppi di Galois possibili del polinomio  $(x^3 - 1) \cdot f(x)$ .

**8.** Si consideri il seguente diagramma di campi:



in cui  $K$  è un'estensione di Galois di  $F$  e  $K'$  è generato su  $F$  da  $K$  e  $F'$ . Dimostrare che  $K'$  è un'estensione di Galois di  $F'$  e che il suo gruppo di Galois è isomorfo ad un sottogruppo di  $G(K/F)$ .

**9.** Siano  $K \supset L \supset F$  campi. Dimostrare o confutare le affermazioni seguenti:

**(a)** Se  $K/F$  è di Galois, allora  $K/L$  è di Galois.

**(b)** Se  $K/F$  è di Galois, allora  $L/F$  è di Galois.

**(c)** Se  $L/F$  e  $K/L$  sono di Galois, allora  $K/F$  è di Galois.

**10.** Sia  $K$  un campo di spezzamento di un polinomio di terzo grado irriducibile  $f(x)$  su un campo  $F$ , avente come gruppo di Galois  $S_3$ . Determinare il gruppo di automorfismi  $G(F(\alpha)/F)$  dell'estensione  $F(\alpha)$ , essendo  $\alpha$  una radice di  $f(x)$  in  $K$ .

**11.** Sia  $K/F$  un'estensione di Galois il cui gruppo di Galois sia il gruppo simmetrico  $S_3$ . È vero che  $K$  è il campo di spezzamento di un polinomio di terzo grado irriducibile su  $F$ ?

**12.** Sia  $K/F$  un'estensione di campi di caratteristica  $p \neq 0$ , e sia  $\alpha$  una radice in  $K$  di un polinomio irriducibile  $f(x) = x^p - x - a$ , su  $F$ .

**(a)** Dimostrare che anche  $\alpha + 1$  è una radice di  $f(x)$ .

**(b)** Dimostrare che il gruppo di Galois di  $f$  su  $F$  è ciclico di ordine  $p$ .

#### 6 Equazioni di quarto grado

**1.** Calcolare il discriminante del polinomio di quarto grado  $x^4 + 1$ , e determinare il suo gruppo di Galois su  $\mathbb{Q}$ .

**2.** Sia  $K$  il campo di spezzamento di un polinomio di quarto grado irriducibile  $f(x)$  su  $F$ , e siano  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  le radici di  $f(x)$  in  $K$ . Supponiamo che il polinomio cubico

- risolvente  $g(x)$  abbia una radice, diciamo  $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$ . Esprimere esplicitamente la radice  $\alpha_1$  per mezzo di una successione di radici quadrate.
3. Cosa si può dire sul gruppo di Galois di un polinomio di quarto grado irriducibile su  $\mathbb{Q}$ , avente esattamente due radici reali?
  4. Supponiamo che un polinomio di quarto grado a coefficienti reali abbia un discriminante positivo. Cosa si può dire sul numero delle radici reali?
  5. Sia  $K$  il campo di spezzamento di un polinomio di quarto grado riducibile con radici distinte su un campo  $F$ . Quali possono essere i gruppi di Galois di  $K/F$ ?
  6. Quali sono i gruppi di Galois possibili su  $\mathbb{Q}$  di un polinomio di quarto grado irriducibile  $f(x)$  con discriminante negativo?
  7. Sia  $g$  il polinomio cubico risolvente di un polinomio di quarto grado irriducibile  $f \in F[x]$ . Determinare i possibili gruppi di Galois di  $g$  su  $F$ , e in ciascun caso, dire qualcosa sul gruppo di Galois di  $f$ .
  8. Sia  $K$  il campo di spezzamento di un polinomio  $f \in F[x]$  con radici distinte  $\alpha_1, \dots, \alpha_n$ , e poniamo  $G = G(K/F)$ . Allora  $G$  può essere considerato come un sottogruppo del gruppo simmetrico  $S_n$ . Dimostrare che, rinumerando le radici,  $G$  viene mutato in un sottogruppo coniugato.
  9. Siano  $\alpha_1, \dots, \alpha_4$  le radici di un polinomio di quarto grado. Studiare le proprietà di simmetria degli elementi  $\alpha_1\alpha_2$  e  $\alpha_1 + \alpha_2$  seguendo la trattazione sviluppata nel testo.
  10. Trovare un polinomio di quarto grado su  $\mathbb{Q}$ , il cui gruppo di Galois sia:
    - (a)  $S_4$ ; (b)  $D_4$ ; (c)  $C_4$ .
  11. Sia  $\alpha$  una radice reale di un polinomio di quarto grado  $f$  su  $\mathbb{Q}$ . Supponiamo che il polinomio cubico risolvente sia irriducibile. Dimostrare che  $\alpha$  non può essere costruito con riga e compasso.
  12. Determinare i gruppi di Galois dei seguenti polinomi su  $\mathbb{Q}$ :
    - (a)  $x^4 + 4x^2 + 2$ ; (b)  $x^4 + 2x^2 + 4$ ; (c)  $x^4 + 4x^2 - 5$ ; (d)  $x^4 - 2$ ; (e)  $x^4 + 2$ ; (f)  $x^4 + 1$ ; (g)  $x^4 + x + 1$ ; (h)  $x^4 + x^3 + x^2 + x + 1$ ; (i)  $x^4 + x^2 + 4$ .
  13. Calcolare il discriminante del polinomio di quarto grado  $x^4 + ax + b$ , utilizzando la formula data nel lemma (8.7).
  - \*14. Sia  $f$  un polinomio di quarto grado irriducibile su  $F$  della forma  $x^4 + rx + s$ , e siano  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  le radici di  $f$  in un campo di spezzamento  $K$ . Poniamo:  $\eta = \alpha_1\alpha_2$ .
    - (a) Dimostrare che  $\eta$  è una radice di un polinomio di sesto grado  $h(x)$  a coefficienti in  $F$ .
    - (b) Supponiamo che i sei prodotti  $\alpha_i\alpha_j$  siano distinti. Dimostrare che  $h(x)$  è irriducibile oppure ha un fattore quadratico irriducibile.
    - (c) Descrivere le possibilità per il gruppo di Galois  $G = G(K/F)$  nei tre casi seguenti:  $h$  è irriducibile,  $h$  è un prodotto di un polinomio di secondo grado irriducibile e di un polinomio di quarto grado irriducibile,  $h$  è un prodotto di tre polinomi di secondo grado irriducibili.
    - (d) Descrivere la situazione nel caso in cui alcuni dei prodotti  $\alpha_i\alpha_j$  sono uguali tra loro.

15. Sia  $K$  il campo di spezzamento del polinomio  $x^4 - 3$  su  $\mathbb{Q}$ .
  - (a) Dimostrare che  $[K : \mathbb{Q}] = 8$  e che  $K$  è generato da  $i$  e da una sola radice  $\alpha$  del polinomio.
  - (b) Dimostrare che il gruppo di Galois di  $K/\mathbb{Q}$  è diedrale, e descrivere esplicitamente l'azione degli elementi di  $G$  sui generatori di  $K$ .
16. Sia  $K$  il campo di spezzamento su  $\mathbb{Q}$  del polinomio  $x^4 - 2x^2 - 1$ . Determinare il gruppo di Galois  $G$  di  $K/\mathbb{Q}$ , trovare tutti i campi intermedi e metterli in corrispondenza con i sottogruppi di  $G$ .
17. Sia  $f(x)$  un polinomio di quarto grado. Dimostrare che i discriminanti di  $f$  e del suo polinomio cubico risolvente sono uguali.
18. Dimostrare l'irriducibilità del polinomio (6.17) e del suo polinomio cubico risolvente.
19. Sia  $K$  il campo di spezzamento del polinomio riducibile  $(x - 1)^2(x^2 + 1)$  su  $\mathbb{Q}$ . Dimostrare che  $\delta \in \mathbb{Q}$ , ma che  $G(K/\mathbb{Q})$  non è contenuto nel gruppo alterno.
20. Sia  $f(x)$  un polinomio di quarto grado con radici distinte, il cui polinomio cubico risolvente  $g(x)$  si spezzi completamente sul campo  $F$ . Quali sono i gruppi di Galois possibili di  $f(x)$ ?
21. Sia  $\zeta = e^{2\pi i/3}$  la radice cubica di 1, sia  $\alpha = \sqrt[3]{a + b\sqrt{2}}$ , e sia  $K$  il campo di spezzamento del polinomio minimo di  $\alpha$  su  $\mathbb{Q}(\zeta)$ . Determinare i possibili gruppi di Galois di  $K$  su  $\mathbb{Q}(\zeta)$ .
22. Sia  $\mathcal{H}$  un sottogruppo del gruppo simmetrico  $S_n$ . Dato un monomio arbitrario  $m$ , possiamo formare il polinomio
 
$$p(u) = \sum_{\sigma \in \mathcal{H}} \sigma m.$$
 Dimostrare che, se  $m = u_1u_2^2u_3^3 \cdots u_{n-1}^{n-1}$ , allora  $p(u)$  è parzialmente simmetrico rispetto a  $\mathcal{H}$ , ossia, è lasciato fisso dalle permutazioni in  $\mathcal{H}$ , ma non è lasciato fisso da nessun'altra permutazione.
23. Sia  $p(u)$  il polinomio formato come nel problema precedente, con  $\mathcal{H} = A_n$ . Allora l'orbita di  $p(u)$  contiene due elementi, diciamo  $p(u), q(u)$ . Dimostrare che  $p(u) - q(u) = \pm \delta(u)$ .
24. Determinare i gruppi di Galois possibili di un polinomio di quarto grado riducibile della forma  $x^4 + bx^2 + c$ , supponendo che il polinomio di secondo grado  $y^2 + by + c$  sia irriducibile.
25. Calcolare il discriminante del polinomio  $x^4 + rx + s$ , utilizzando il calcolo dei discriminanti di  $x^4 - x$  e  $x^4 - 1$ .
26. Usare la sostituzione  $x \mapsto y^{-1}$  per determinare il discriminante del polinomio  $x^4 + ax^3 + b$ .
27. Determinare il polinomio cubico risolvente dei polinomi:
  - (a)  $x^4 + rx + s$ ; (b)  $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ .
28. Consideriamo un polinomio della forma:  $f(x) = x^4 - 2rx^2 + (r^2 - s^2)v$ , con  $r, s, v \in F$ . Supponiamo che  $f$  sia irriducibile e denotiamo con  $G$  il suo gruppo di Galois. Poniamo  $L = F(\sqrt{v}, \delta)$ , dove  $\delta^2 = D$ . Dimostrare ciascuno dei seguenti enunciati:

- (a)  $L(\alpha) = K$ .  
(b) Se  $[L : F] = 4$ , allora  $G = D_4$ .  
(c) Se  $[L : F] = 2$  e  $\delta \notin F$ , allora  $G = C_4$ .
29. Determinare i gruppi di Galois degli ultimi due esempi di (6.5).  
30. Determinare esplicitamente l'azione del gruppo di Galois  $G$  sulle radici  $\{\alpha, \alpha', -\alpha, -\alpha'\}$  (6.7), supponendo che  
(a)  $G = C_4$ ; (b)  $G = D_4$ .
31. Stabilire se i seguenti radicali doppi possono essere espressi mediante radicali semplici, oppure no, e in caso affermativo, trovare un'espressione esplicita:  
(a)  $\sqrt{2 + \sqrt{11}}$ ; (b)  $\sqrt{6 + \sqrt{11}}$ ; (c)  $\sqrt{11 + 6\sqrt{2}}$ ; (d)  $\sqrt{11 + \sqrt{6}}$ .
- \*32. Sia  $K$  il campo di spezzamento di un polinomio di quarto grado  $f(x)$  su  $\mathbb{Q}$  il cui gruppo di Galois sia  $D_4$ , e sia  $\alpha$  una radice reale di  $f(x)$  in  $K$ . Stabilire se  $\alpha$  può essere costruito con righello e compasso, oppure no, nei casi seguenti:  
(a)  $f$  ha quattro radici reali; (b)  $f$  ha due radici reali.
33. È vero che le radici del polinomio  $x^4 + x - 5$  possono essere costruite con righello e compasso?

### 7 Estensioni di Kummer

1. Supponiamo che un'estensione di Galois  $K/F$  abbia la forma  $K = F(\alpha)$  e che  $\alpha^n \in F$ , per qualche intero  $n$ . Cosa si può dire sul gruppo di Galois di  $K/F$ ?  
\*2. Sia  $a$  un elemento di un campo  $F$ , e sia  $p$  un numero primo. Supponiamo che il polinomio  $x^p - a$  sia riducibile in  $F[x]$ . Dimostrare che esso ha una radice in  $F$ .  
3. Sia  $F$  un sottocampo di  $\mathbb{C}$  contenente  $i$ , e sia  $K$  un'estensione di Galois di  $F$  il cui gruppo di Galois sia  $C_4$ . È vero che  $K$  ha la forma  $F(\alpha)$ , dove  $\alpha^4 \in F$ ?  
4. Sia  $f(x) = x^3 + px + q$  un polinomio irriducibile su un campo  $F$ , con radici  $\alpha_1, \alpha_2, \alpha_3$ . Poniamo:  $\beta = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$ , dove  $\zeta = e^{2\pi i/3}$ . Dimostrare che  $\beta$  è un autovettore relativo alla permutazione ciclica  $\sigma$  delle radici, a meno che  $\beta = 0$ , e calcolare esplicitamente  $\beta^3$  per mezzo di  $p, q, \delta, \zeta$ .  
5. Sia  $K$  un campo di spezzamento di un polinomio irriducibile  $f(x) \in F[x]$  di grado  $p$ , il cui gruppo di Galois sia un gruppo ciclico di ordine  $p$  generato da  $\sigma$ , e supponiamo che  $F$  contenga la radice  $p$ -esima dell'unità  $\zeta = \zeta_p$ . Siano  $\alpha_1, \alpha_2, \dots, \alpha_p$  le radici di  $f$  in  $K$ . Dimostrare che

$$\beta = \alpha_1 + \zeta^\nu \alpha_2 + \zeta^{2\nu} \alpha_3 + \dots + \zeta^{(p-1)\nu} \alpha_p$$

è un autovettore di  $\sigma$ , con autovalore  $\zeta^{-\nu}$ , a meno che  $\beta = 0$ .

6. Sia  $f(x) = x^3 + px + q$  un polinomio irriducibile su un sottocampo  $F$  del campo dei numeri complessi, con radici complesse  $\alpha = \alpha_1, \alpha_2, \alpha_3$ . Poniamo  $K = F(\alpha)$ .  
(a) Esprimere esplicitamente  $(6\alpha^2 + 2p)^{-1}$  come un polinomio di grado 2 in  $\alpha$ .  
(b) Supponiamo che  $\delta = \sqrt{D}$  appartenga a  $F$ , sicché  $K$  contiene le altre radici di  $f$ . Esprimere  $\alpha_2$  come un polinomio in  $\alpha = \alpha_1$  e  $\delta$ .

- (c) Dimostrare che  $(1, \alpha_1, \alpha_2)$  è una base di  $K$ , come  $F$ -spazio vettoriale.  
(d) Sia  $\sigma$  l'automorfismo di  $K$  che permuta ciclicamente le tre radici. Scrivere la matrice di  $\sigma$  rispetto alla base sopra descritta, e trovare i suoi autovalori e autovettori.  
(e) Sia  $v$  un autovettore con autovalore  $\zeta = e^{2\pi i/3}$ . Dimostrare che, se  $\sqrt{-3} \in F$ , allora  $v^3 \in F$ . Calcolare esplicitamente  $v^3$  per mezzo di  $p, q, \delta, \sqrt{-3}$ .  
(f) Eliminando le ipotesi che  $\delta$  e  $\sqrt{-3}$  stiano in  $F$ , esprimere  $v$  per mezzo di radicali.  
(g) Determinare, senza effettuare calcoli, l'elemento  $v'$  che si ottiene da  $v$  scambiando tra loro i ruoli di  $\alpha_1, \alpha_2$ .  
(h) Esprimere la radice  $\alpha_1$  per mezzo di radicali.
- ### 8 Estensioni ciclotomiche
1. Determinare il grado di  $\zeta_7$  sul campo  $\mathbb{Q}(\zeta_3)$ .  
2. Sia  $\zeta = \zeta_{13}$ , e poniamo  $K = \mathbb{Q}(\zeta)$ . Determinare esplicitamente il campo intermedio di grado 3 su  $\mathbb{Q}$ .  
3. Sia  $\zeta = \zeta_{17}$ . Determinare esplicitamente la successione delle radici quadrate che generano il campo  $\mathbb{Q}(\zeta + \zeta^{16})$ .  
4. Sia  $\zeta = \zeta_7$ . Determinare il grado dei seguenti elementi su  $\mathbb{Q}$ :  
(a)  $\zeta + \zeta^5$ ; (b)  $\zeta^3 + \zeta^4$ ; (c)  $\zeta^3 + \zeta^5 + \zeta^6$ .  
5. Sia  $\zeta = \zeta_{13}$ . Determinare il grado dei seguenti elementi su  $\mathbb{Q}$ :  
(a)  $\zeta + \zeta^{12}$ ; (b)  $\zeta + \zeta^2$ ; (c)  $\zeta + \zeta^5 + \zeta^8$ ; (d)  $\zeta^2 + \zeta^5 + \zeta^6$ ; (e)  $\zeta + \zeta^5 + \zeta^8 + \zeta^{12}$ ; (f)  $\zeta + \zeta^2 + \zeta^5 + \zeta^{12}$ ; (g)  $\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12}$ .  
6. Sia  $\zeta = \zeta_{11}$ .  
(a) Dimostrare che  $\alpha = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$  genera un campo di grado 2 su  $\mathbb{Q}$ , e trovare il suo polinomio minimo.  
(b) Trovare un elemento che genera un sottocampo di grado 5 su  $\mathbb{Q}$ , e trovare il suo polinomio minimo.  
7. Dimostrare che ogni estensione quadratica di  $\mathbb{Q}$  è contenuta in un'estensione ciclotomica.  
8. Sia  $K = \mathbb{Q}(\zeta_n)$ .  
(a) Dimostrare che  $K$  è un'estensione di Galois di  $\mathbb{Q}$ .  
(b) Definire un omomorfismo iniettivo  $v : G(K/\mathbb{Q}) \rightarrow U$ , dove  $U$  è il gruppo delle unità nell'anello  $\mathbb{Z}/(n)$ .  
(c) Dimostrare che tale omomorfismo è biiettivo, per  $n = 6, 8, 12$ . (In realtà, tale applicazione è sempre biiettiva).  
\*9. Sia  $p$  un numero primo, e sia  $a$  un numero razionale che non sia una potenza  $p$ -esima. Sia  $K$  un campo di spezzamento del polinomio  $x^p - a$  su  $\mathbb{Q}$ .

(a) Dimostrare che  $K$  è generato su  $\mathbb{Q}$  da una radice  $p$ -esima  $\alpha$  di  $a$  e una radice  $p$ -esima primitiva  $\zeta$  dell'unità.

(b) Dimostrare che  $[K : \mathbb{Q}] = p(p - 1)$ .

(c) Dimostrare che il gruppo di Galois di  $K/\mathbb{Q}$  è isomorfo al gruppo delle matrici  $2 \times 2$  invertibili con elementi in  $\mathbb{F}_p$  della forma  $\begin{bmatrix} a & b \\ & 1 \end{bmatrix}$ , e descrivere esplicitamente le azioni degli elementi  $\begin{bmatrix} a & \\ & 1 \end{bmatrix}$  e  $\begin{bmatrix} 1 & b \\ & 1 \end{bmatrix}$  sui generatori.

**10.** Determinare il gruppo di Galois dei polinomi  $x^8 - 1$ ,  $x^{12} - 1$ ,  $x^9 - 1$ .

**11.** (a) Caratterizzare i numeri primi  $p$  tali che il poligono regolare di  $p$  lati può essere costruito con righiera e compasso.

(b) Estendere la caratterizzazione al caso di un poligono regolare di  $n$  lati, dove  $n$  non è necessariamente un numero primo.

**\*12.** Sia  $\nu$  un elemento primitivo modulo un numero primo  $p$ , e sia  $d$  un divisore di  $p - 1$ . Mostrare in che modo è possibile determinare una somma di potenze di  $\zeta = \zeta_p$  che genera il sottocampo  $L$  di  $\mathbb{Q}(\zeta)$  di grado  $d$  su  $\mathbb{Q}$ , utilizzando l'insieme delle radici dell'unità

$$\{\zeta, \zeta^\nu, \zeta^{\nu^2}, \dots, \zeta^{\nu^{p-2}}\}.$$

### 9 Equazioni di quinto grado

1. Determinare i sottogruppi transitivi di  $S_5$ .

2. Sia  $G$  il gruppo di Galois di un polinomio di quinto grado irriducibile. Dimostrare che, se  $G$  contiene un elemento di ordine 3, allora  $G = S_5$  oppure  $G = A_5$ .

**\*3.** Sia  $p$  un numero primo, e sia  $G$  un  $p$ -gruppo. Sia  $H$  un sottogruppo normale proprio di  $G$ .

(a) Dimostrare che il normalizzante  $N(H)$  di  $H$  contiene strettamente  $H$ .

(b) Dimostrare che  $H$  è contenuto in un sottogruppo di indice  $p$  e che tale sottogruppo è normale in  $G$ .

(c) Sia  $K$  un'estensione di Galois di  $\mathbb{Q}$  tale che il suo grado sia una potenza di 2 e che  $K \subset \mathbb{R}$ . Dimostrare che gli elementi di  $K$  possono essere costruiti con righiera e compasso.

4. Sia  $K \supset L \supset F$  una catena di estensioni di campi di grado 2. Dimostrare che  $K$  può essere generato su  $F$  dalla radice di un polinomio di quarto grado irriducibile della forma  $x^4 + bx^2 + c$ .

**\*5.** La formula di Cardano presenta una particolarità che ora esamineremo. Supponiamo che i coefficienti  $p, q$  del polinomio di terzo grado siano numeri reali. Un polinomio di terzo grado a coefficienti reali ha almeno una radice reale. Tuttavia, la radice quadrata che compare nella formula (2.6) sarà immaginaria, se  $(q/2)^2 + (p/3)^3 < 0$ . In tal caso, la radice reale si esprime per mezzo di un numero complesso ausiliario  $u$ .

Questa era considerata una soluzione impropria ai tempi di Cardano. Sia  $f(x)$  un polinomio di terzo grado irriducibile su un sottocampo  $F$  di  $\mathbb{R}$ , che abbia tre radici reali. Dimostrare che nessuna radice di  $f$  è esprimibile mediante radicali reali, ossia, che non esiste nessuna catena  $F = F_0 \subset \dots \subset F_r$  con le proprietà (9.2), in cui tutti i campi sono sottocampi di  $\mathbb{R}$ .

6. Sia  $f(x) \in F[x]$  un polinomio di quinto grado irriducibile, e sia  $K$  un campo di spezzamento per  $f(x)$  su  $F$ .

(a) Quali sono i possibili gruppi di Galois  $G(K/F)$ , supponendo che il discriminante  $D$  sia un quadrato in  $F$ ?

(b) Quali sono i possibili gruppi di Galois, se  $D$  non è un quadrato in  $F$ ?

7. Determinare quali sono i numeri reali  $\alpha$  di grado 4 su  $\mathbb{Q}$ , che possono essere costruiti con righiera e compasso, per mezzo del gruppo di Galois del polinomio corrispondente.

8. È vero che ogni estensione di Galois di grado 10 è “risolubile per radicali”?

**\*9.** Trovare un polinomio di grado 7 su  $\mathbb{Q}$ , il cui gruppo di Galois sia  $S_7$ .

### Esercizi vari

1. Sia  $K$  un'estensione di Galois di  $F$ , il cui gruppo di Galois sia il gruppo simmetrico  $S_4$ . Quali numeri compaiono come gradi di elementi di  $K$  su  $F$ ?

2. Dimostrare, senza effettuare calcoli, che la lunghezza del lato di un pentagono regolare inscritto nel cerchio unitario ha grado 2 su  $\mathbb{Q}$ .

3. (a) I numeri reali non negativi sono quelli che hanno una radice quadrata reale. Utilizzare questo fatto per dimostrare che il campo  $\mathbb{R}$  non ha automorfismi diversi dall'identità.

(b) Dimostrare che  $\mathbb{C}$  non ha automorfismi *continui*, al di fuori del coniugo e dell'identità.

4. Sia  $K/F$  un'estensione di Galois con gruppo di Galois  $G$ , e sia  $H$  un sottogruppo di  $G$ . Dimostrare che esiste un elemento  $\beta \in K$ , il cui stabilizzatore è  $H$ .

**\*5.** (a) Sia  $K$  un campo di caratteristica  $p$ . Dimostrare che l'applicazione di Frobenius  $\varphi$  definita da  $\varphi(x) = x^p$  è un omomorfismo di  $K$  in se stesso.

(b) Dimostrare che  $\varphi$  è un isomorfismo, se  $K$  è un campo finito.

(c) Dare un esempio di un campo infinito di caratteristica  $p$  tale che  $\varphi$  non sia un isomorfismo.

(d) Poniamo  $F = \mathbb{F}_p$  e  $K = \mathbb{F}_q$ , dove  $q = p^r$ . Dimostrare che  $G(K/F)$  è un gruppo ciclico di ordine  $r$ , generato dall'applicazione di Frobenius  $\varphi$ .

(e) Dimostrare che il teorema fondamentale della teoria di Galois vale per l'estensione di campi  $K/F$ .

6. Sia  $K$  un sottocampo di  $\mathbb{C}$ , e sia  $G$  il suo gruppo di automorfismi. Possiamo pensare che  $G$  agisca sull'insieme di punti  $K$  nel piano complesso, probabilmente in modo discontinuo. Tuttavia, possiamo definire un'azione sui segmenti  $[\alpha, \beta]$  aventi gli estremi in  $K$ , ponendo:  $g[\alpha, \beta] = [g\alpha, g\beta]$ . Allora  $G$  agisce anche sui poligoni i cui vertici stanno in  $K$ .

- (a) Sia  $K = \mathbb{Q}(\zeta)$ , dove  $\zeta$  è una radice quinta primitiva di 1. Trovare la  $G$ -orbita del pentagono regolare i cui vertici sono  $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ .
- (b) Sia  $\alpha$  la lunghezza del lato del pentagono considerato in (a). Dimostrare che  $\alpha = \alpha^2 \in K$ , e trovare il polinomio minimo di  $\alpha$  su  $\mathbb{Q}$ . È vero che  $\alpha \in K$ ?
7. Un polinomio  $f \in F[x_1, \dots, x_n]$  è chiamato  $\frac{1}{2}$ -simmetrico, se  $f(u_{\sigma 1}, \dots, u_{\sigma n}) = f(u_1, \dots, u_n)$  per ogni permutazione pari  $\sigma$  degli indici, e antisimmetrico, se  $f(u_{\sigma 1}, \dots, u_{\sigma n}) = (\text{sign } \sigma)f(u_1, \dots, u_n)$  per ogni permutazione  $\sigma$ .
- (a) Dimostrare che la radice quadrata del discriminante  $\delta = \prod_{i < j} (u_i - u_j)$  è un polinomio antisimmetrico.
- (b) Dimostrare che ogni polinomio  $\frac{1}{2}$ -simmetrico ha la forma  $f + g\delta$ , dove  $f, g$  sono polinomi simmetrici.
- \*8. Sia  $f(x, y) \in \mathbb{C}[x, y]$  un polinomio irriducibile, che noi consideriamo come un polinomio  $f(y)$  in  $y$ . Supponiamo che  $f$  sia un polinomio di terzo grado, come polinomio in  $y$ . Il suo discriminante  $D$ , calcolato rispetto alla variabile  $y$ , sarà un polinomio in  $x$ . Supponiamo che esista una radice  $x_0$  di  $D(x)$  che non sia una radice multipla.
- (a) Dimostrare che il polinomio  $f(x_0, y)$  in  $y$  ha una radice semplice e una radice doppia.
- (b) Dimostrare che il campo di spezzamento  $K$  di  $f(y)$  su  $\mathbb{C}(x)$  ha grado 6.
9. Sia  $K$  un sottocampo di  $\mathbb{C}$  che sia un'estensione di Galois di  $\mathbb{Q}$ . Dimostrare o confutare l'affermazione seguente: Il coniugio manda  $K$  in sé, e pertanto definisce un automorfismo di  $K$ .
- \*10. Sia  $K$  un'estensione finita di un campo  $F$  e sia dato un polinomio  $f(x) \in K[x]$ . Dimostrare che esiste un polinomio non nullo  $g(x) \in K[x]$  tale che  $f(x)g(x) \in F[x]$ .
- \*11. Sia  $f(x)$  un polinomio di quarto grado irriducibile in  $F[x]$ . Siano  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  le sue radici in un campo di spezzamento  $K$ . Supponiamo che il polinomio cubico risolvente abbia una radice  $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$  in  $F$ , ma che il discriminante  $D$  non sia un quadrato in  $F$ . In base al testo, il gruppo di Galois di  $K/F$  è  $C_4$  o  $D_4$ .
- (a) Determinare esplicitamente il sottogruppo  $H$  del gruppo  $S_4$ , costituito dalle permutazioni delle radici  $\alpha_i$  che lasciano fisso  $\beta$ . (Non dimenticare di dimostrare che nessun'altra permutazione, all'infuori di quelle considerate, lascia fisso  $\beta$ ).
- (b) Poniamo  $\gamma = \alpha_1\alpha_2 - \alpha_3\alpha_4$  e  $\epsilon = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$ . Descrivere l'azione di  $H$  su questi elementi.
- (c) Dimostrare che  $\gamma^2$  e  $\epsilon^2$  appartengono a  $F$ .
- (d) Sia  $\delta$  la radice quadrata del discriminante. Dimostrare che, se  $\gamma \neq 0$ , allora  $\delta\gamma$  è un quadrato in  $F$ , se e soltanto se,  $G = C_4$ . Similmente, dimostrare che, se  $\epsilon \neq 0$ , allora  $\delta\epsilon$  è un quadrato in  $F$ , se e soltanto se,  $G = C_4$ .
- (e) Dimostrare che  $\gamma$  e  $\epsilon$  non possono essere entrambi nulli.
- \*12. Sia  $F = \mathbb{F}_p(u, v)$  un campo di funzioni razionali in due variabili sul campo  $\mathbb{F}_p$  con  $p$  elementi, e poniamo  $K = F(\alpha, \beta)$ , dove  $\alpha, \beta$  sono radici, rispettivamente, dei polinomi  $x^p - u$  e  $x^p - v$ . Dimostrare che:
- (a) l'estensione  $K/F$  non ha elementi primitivi;

## Esercizi

(b) gli elementi  $\gamma = \beta + c\alpha$ , dove  $c \in F$ , generano infiniti campi intermedi distinti  $L$ .

\*13. Sia  $K$  un campo con  $p^r$  elementi. Dimostrare che l'applicazione di Frobenius definita da  $\varphi(x) = x^p$  è un operatore lineare su  $K$ , considerato come spazio vettoriale sul campo primo  $F = \mathbb{F}_p$ , e determinare i suoi autovettori e autovalori.

Solo il futuro ci dirà fin dove si spingeranno questi metodi.  
Emmy Noether

## Appendice

### Nozioni di base

Storicamente è del tutto falso, com'è ovvio, che la matematica sia priva di contraddizioni: la non-contradditorietà sembra piuttosto un obiettivo da raggiungere, che un regalo del cielo che ci sia stato dato una volta per tutte.

Nicolas Bourbaki

### 1 Teoria degli insiemi

In questo paragrafo passeremo in rassegna alcune convenzioni relative alla teoria degli insiemi utilizzate nel testo, insieme ad alcuni fatti citati occasionalmente.

Innanzitutto, cominciamo con un'osservazione sulle definizioni. Qualsiasi definizione di un termine o di un'espressione avrà approssimativamente la forma:

$$(1.1) \quad \text{xxx se } @ \# \& \$ \%,$$

dove *xxx* è il termine che viene definito e  $@ \# \& \$ \%$  è la proprietà che lo definisce. Per esempio, la frase: "Un intero  $n$  è positivo se  $n > 0$ " definisce la nozione di intero positivo. In una definizione, la parola *se* significa *se e soltanto se*. Pertanto nella definizione degli interi positivi, tutti gli interi che non verificano la condizione  $n > 0$  sono esclusi.

La notazione:

$$(1.2) \quad \{s \in S \mid @ \# \& \$ \% \}$$

indica il sottoinsieme di  $S$  costituito da tutti gli elementi  $s$  tali che la proprietà  $@ \# \& \$ \%$  è verificata. Così, se  $\mathbb{Z}$  denota l'insieme di tutti gli interi, la notazione  $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$  descrive  $\mathbb{N}$  come l'insieme degli interi positivi o *numeri naturali*.

Si dice che elementi  $a_1, \dots, a_n$  di un insieme sono *distinti*, se tra essi non vi sono due elementi uguali.

Un'applicazione  $\varphi$  da un insieme  $S$  a un insieme  $T$  è una qualunque funzione che abbia come *dominio* di definizione  $S$  e come *codominio*  $T$ . I termini *funzione* e *applicazione* vengono usati come sinonimi. Noi richiediamo che una funzione sia univoca, il che significa che ogni elemento  $s \in S$  deve avere un'immagine  $\varphi(s) \in T$  univocamente determinata. Non si richiede che il codominio  $T$  di  $\varphi$  coincida con l'insieme dei valori della funzione: in base alla definizione, ogni

elemento immagine  $\varphi(s)$  è contenuto in  $T$ ; tuttavia, ammettiamo la possibilità che qualche elemento  $t \in T$  non sia immagine, tramite  $\varphi$ , di alcun elemento di  $S$ . Si considerano inoltre il dominio e il codominio di una funzione come parte integrante della sua definizione. In particolare, se restringiamo il dominio a un sottoinsieme, o se estendiamo il codominio, la funzione così ottenuta è considerata diversa dalla funzione di partenza.

Il dominio e il codominio di un'applicazione possono essere descritti anche mediante una freccia. Così, la notazione  $\varphi : S \rightarrow T$  ci dice che  $\varphi$  è un'applicazione da  $S$  a  $T$ . L'affermazione che  $t = \varphi(s)$  può essere descritta mediante la freccia " $\mapsto$ ": precisamente,  $s \mapsto t$  significa che l'elemento  $s \in S$  viene mandato in  $t \in T$  dall'applicazione considerata. Per esempio, l'applicazione  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$  tale che  $\varphi(n) = 2n + 1$  è descritta da  $n \mapsto 2n + 1$ .

L'*immagine* dell'applicazione  $\varphi$  è il sottoinsieme di  $T$  costituito dagli elementi della forma  $\varphi(s)$ , per qualche  $s \in S$ . Essa si denoterà spesso con  $\text{im } \varphi$ , oppure con  $\varphi(S)$ :

$$(1.3) \quad \text{im } \varphi = \{t \in T \mid t = \varphi(s) \text{ per qualche } s \in S\}.$$

Nel caso in cui  $\text{im } \varphi$  è l'intero codominio  $T$ , l'applicazione si dice *suriettiva*. Pertanto  $\varphi$  è suriettiva se ogni  $t \in T$  ha la forma  $\varphi(s)$ , per qualche  $s \in S$ .

L'applicazione  $\varphi$  si dice *iniettiva*, se elementi distinti  $s_1, s_2$  di  $S$  hanno immagini distinte, ossia, se  $s_1 \neq s_2$  implica che  $\varphi(s_1) \neq \varphi(s_2)$ . Un'applicazione che sia iniettiva e suriettiva è detta *bijettiva*. Una *permutazione* di un insieme  $S$  è un'applicazione biiettiva di  $S$  in se stesso.

Siano  $\varphi : S \rightarrow T$  e  $\psi : T \rightarrow S$  due applicazioni. Allora  $\psi$  è detta *funzione inversa* di  $\varphi$  se entrambe le applicazioni composte  $\varphi \circ \psi : T \rightarrow T$  e  $\psi \circ \varphi : S \rightarrow S$  sono le applicazioni identiche, ossia se  $\varphi(\psi(t)) = t$  per ogni  $t \in T$  e  $\psi(\varphi(s)) = s$  per ogni  $s \in S$ . La funzione inversa si denota spesso con  $\varphi^{-1}$ .

(1.4) PROPOSIZIONE *Un'applicazione  $\varphi : S \rightarrow T$  ha una funzione inversa se e solo se è bijettiva.*

*Dimostrazione.* Supponiamo che  $\varphi$  abbia una funzione inversa  $\psi$ , e dimostriamo che  $\varphi$  è suriettiva e iniettiva. Sia  $t$  un elemento arbitrario di  $T$ , e poniamo  $s = \psi(t)$ . Allora  $\varphi(s) = \varphi(\psi(t)) = t$ . Pertanto  $t$  appartiene all'immagine di  $\varphi$ , e ciò dimostra che  $\varphi$  è suriettiva. Inoltre, siano  $s_1, s_2$  elementi distinti di  $S$ , e poniamo  $t_i = \varphi(s_i)$ . Allora  $\psi(t_i) = s_i$ , sicché  $t_1, t_2$  hanno immagini distinte in  $S$ , e ciò dimostra che  $t_1 \neq t_2$ . Pertanto  $\varphi$  è iniettiva.

Viceversa, supponiamo che  $\varphi$  sia bijettiva. Allora, poiché  $\varphi$  è suriettiva, ogni elemento  $t \in T$  ha la forma  $t = \varphi(s)$ , per qualche  $s \in S$ . Poiché  $\varphi$  è iniettiva, questo elemento  $s$  è unico. Definiamo allora  $\psi$  nel modo seguente:  $\psi(t)$  è l'unico elemento  $s \in S$  tale che  $\varphi(s) = t$ . Quest'applicazione è la funzione inversa richiesta. ■

Sia  $\varphi : S \rightarrow T$  un'applicazione, e sia  $U$  un sottoinsieme di  $T$ . Si definisce *immagine inversa* di  $U$  l'insieme:

$$(1.5) \quad \varphi^{-1}(U) = \{s \in S \mid \varphi(s) \in U\}.$$

Tale insieme è definito anche se  $\varphi$  non ha una funzione inversa. La notazione  $\varphi^{-1}$ , qui usata, è puramente simbolica.

Un insieme  $S$  si dice *finito* se è costituito da un numero finito di elementi. In tal caso, il numero dei suoi elementi, chiamato talvolta *cardinalità*, sarà denotato con  $|S|$ . Tale numero sarà chiamato anche l'*ordine* di  $S$ . Se  $S$  è infinito, scriveremo  $|S| = \infty$ . Il teorema seguente è del tutto elementare, tuttavia è un principio molto importante.

(1.6) TEOREMA *Sia  $\varphi : S \rightarrow T$  un'applicazione tra insiemi finiti.*

- (a) *Se  $\varphi$  è iniettiva, allora  $|S| \leq |T|$ .*
- (b) *Se  $\varphi$  è suriettiva, allora  $|S| \geq |T|$ .*
- (c) *Se  $|S| = |T|$ , allora  $\varphi$  è biiettiva, se e soltanto se,  $\varphi$  è iniettiva o suriettiva.*

L'enunciato contronomiale di (a) è chiamato spesso il *principio delle gabbie dei piccioni*: se  $|S| > |T|$ , allora  $\varphi$  non è iniettiva. Per esempio, se in 79 cassetti vi sono 87 calzini, allora qualche cassetto conterrà almeno due calzini.

Un insieme infinito  $S$  si dice *numerabile* se esiste un'applicazione biiettiva  $\varphi : \mathbb{N} \rightarrow S$  dall'insieme dei numeri naturali a  $S$ . Altrimenti,  $S$  si dice *non numerabile*.

(1.7) PROPOSIZIONE *L'insieme  $\mathbb{R}$  dei numeri reali è non numerabile.*

*Dimostrazione.* Questa dimostrazione viene citata spesso come “procedimento diagonale di Cantor”. Sia  $\varphi : \mathbb{N} \rightarrow \mathbb{R}$  un'applicazione arbitraria. Elenchiamo gli elementi dell'immagine di  $\varphi$  nell'ordine:  $\varphi(1), \varphi(2), \varphi(3), \dots$ , e scriviamo ciascuno di questi numeri reali con la notazione decimale. Per esempio, l'elenco potrebbe cominciare come segue:

$$\varphi(1) = 8 \ 2 , \underline{3} 5 \ 4 \ 7 \ 0 \ 9 \ 8 \ 4 \ 5 \ 3 \ 4 \ \dots$$

$$\varphi(2) = 0 , \underline{1} 2 \ 3 \ 9 \ 0 \ 3 \ 4 \ 5 \ 7 \ 0 \ 0 \ \dots$$

$$\varphi(3) = 5 , \underline{9} 0 \ 8 \ 4 \ 0 \ 5 \ 9 \ 8 \ 6 \ 7 \ 5 \ \dots$$

$$\varphi(4) = 1 \ 2 , \underline{8} 7 \ 4 \ 3 \ 5 \ 2 \ 6 \ 4 \ 4 \ 4 \ 4 \ \dots$$

$$\varphi(5) = 0 , \underline{0} 0 \ 1 \ 4 \ 4 \ 1 \ 0 \ 0 \ 3 \ 4 \ 9 \ \dots$$

: :

Determineremo ora un numero reale non appartenente a questo elenco. Consideriamo un numero reale  $v$ , le cui cifre decimali siano le cifre sottolineate, ad esempio:  $v = 0, \underline{3} 2 8 3 4 \dots$ . Formiamo un nuovo numero reale cambiando ciascuna di queste cifre:

$$v = 0,45142 \dots$$

Si noti che  $v \neq \varphi(1)$ , poiché la prima cifra (4) di  $v$  non è uguale alla cifra corrispondente (3) di  $\varphi(1)$ . Inoltre,  $v \neq \varphi(2)$ , poiché la seconda cifra (5) di  $v$  non è uguale alla cifra corrispondente di  $\varphi(2)$ . Analogamente,  $v \neq \varphi(n)$  per ogni  $n$ . Ciò mostra che  $\varphi$  non è suriettiva, sicché la dimostrazione è conclusa, tranne che per un punto.

Precisamente, alcuni numeri reali hanno due rappresentazioni decimali diverse: ad esempio,  $0,99999\dots$  è uguale a  $1,00000\dots$ . Ciò crea una difficoltà per la nostra argomentazione. Dobbiamo scegliere  $v$  in modo tale che, nella sua rappresentazione decimale, compaiano infinite cifre diverse da 9 e da 0. La cosa più semplice è evitare del tutto queste cifre. ■

In alcuni punti nel testo facciamo riferimento al lemma di Zorn, che è uno strumento per trattare gli insiemi non numerabili. Ora passeremo a descriverlo. Un *ordinamento parziale* di un insieme  $S$  è una relazione  $s \leq s'$  che vale tra certi elementi e che soddisfa i seguenti assiomi, per ogni  $s, s', s''$  in  $S$ :

- (1.8) (i)  $s \leq s$ ;
- (ii) se  $s \leq s'$  e  $s' \leq s''$ , allora  $s \leq s''$ ;
- (iii) se  $s \leq s'$  e  $s' \leq s$ , allora  $s = s'$ .

Un ordinamento parziale è chiamato *ordinamento totale* se vale inoltre l'assioma seguente:

- (iv) per ogni  $s, s'$  in  $S$ , si ha:  $s \leq s'$  oppure  $s' \leq s$ .

Per esempio, sia  $S$  un insieme i cui elementi siano degli insiemi. Se  $A, B$  appartengono a  $S$ , possiamo porre, per definizione,  $A \leq B$  se  $A \subset B$ . Questo è un ordinamento parziale su  $S$ , chiamato *ordinamento per inclusione*. Esso può essere un ordinamento totale oppure no, a seconda del caso particolare in esame.

Se  $A$  è un sottoinsieme di un insieme parzialmente ordinato  $S$ , un *maggiorante* di  $A$  è un elemento  $b \in S$  tale che, per ogni  $a \in A$ ,  $a \leq b$ . Un insieme parzialmente ordinato  $S$  è chiamato *induttivo* se ogni sottoinsieme totalmente ordinato  $T$  di  $S$  ha un maggiorante in  $S$ .

Un *elemento massimale*  $m \in S$  è un elemento tale che se  $s \in S$  e  $m \leq s$ , allora  $m = s$ . Ciò non significa che  $m$  è un maggiorante per  $S$ ; in particolare, vi possono essere molti elementi massimali distinti. Per esempio, l'insieme di tutti i

sottoinsiemi propri di  $\{1, \dots, n\}$  contiene  $n$  elementi massimali, uno dei quali è  $\{1, 3, 4, \dots, n\}$ .

(1.9) LEMMA DI ZORN *Un insieme parzialmente ordinato induttivo possiede un elemento massimale.* ■

Il lemma di Zorn è equivalente all'*assioma della scelta*, il quale, com'è noto, è indipendente dagli assiomi fondamentali della teoria degli insiemi. Non ci addentreremo in una trattazione ulteriore di questa equivalenza; tuttavia, mostreremo in che modo il lemma di Zorn può essere usato per dimostrare che ogni spazio vettoriale possiede una base. Considereremo qui insiemi non ordinati di vettori.

(1.10) PROPOSIZIONE *Ogni spazio vettoriale  $V$  su un campo possiede una base.*

*Dimostrazione.* Consideriamo l'insieme  $S$  di tutti i sottoinsiemi linearmente indipendenti (non ordinati) di  $V$ , parzialmente ordinato per inclusione, come sopra. Verifichiamo che  $S$  è induttivo. Sia  $T$  un sottoinsieme totalmente ordinato di  $S$ . Allora facciamo vedere che l'unione dei sottoinsiemi che appartengono a  $T$  è anch'esso un insieme linearmente indipendente, e quindi appartiene a  $S$ . Sia

$$B = \bigcup_{A \in T} A$$

l'insieme unione. Per definizione, una relazione di dipendenza lineare su  $B$  è finita, sicché essa può essere scritta nella forma:

$$(1.11) \quad c_1 v_1 + \cdots + c_n v_n = 0,$$

con  $v_i \in B$ . Poiché  $B$  è l'unione dei sottoinsiemi  $A \in T$ , ciascun vettore  $v_i$  è contenuto in uno di questi sottoinsiemi, chiamiamolo  $A_i$ . Siano  $i, j$  due degli indici in questione. Poiché  $T$  è totalmente ordinato, si ha  $A_i \subset A_j$  oppure  $A_j \subset A_i$ . Ne segue per induzione che uno dei sottoinsiemi, diciamo  $A_i$ , contiene tutti gli altri. Chiamiamo  $A$  tale insieme. Allora  $v_i \in A$  per ogni  $i = 1, \dots, n$ . Poiché  $A$  è linearmente indipendente, la (1.11) è la relazione banale. Ciò prova che  $B$  è linearmente indipendente, e quindi che esso è un elemento di  $S$ .

Abbiamo verificato l'ipotesi del lemma di Zorn. Pertanto  $S$  contiene un elemento massimale  $B$ ; vogliamo far vedere che  $B$  è una base. Per la definizione di  $S$ ,  $B$  è linearmente indipendente. Poniamo  $W = \text{Span}(B)$ . Se  $W < V$ , scegliamo un elemento  $v \in V$  che non appartenga a  $W$ . Allora l'insieme  $B \cup \{v\}$  è linearmente indipendente [cfr. cap. 3 (3.10)]. Ciò contraddice la massimalità di  $B$  e mostra che  $W = V$ , e quindi che  $B$  è una base. ■

Con un ragionamento analogo si dimostra il teorema (8.3) del capitolo 10.

(1.12) PROPOSIZIONE *Sia  $R$  un anello. Ogni ideale  $I \neq R$  è contenuto in un ideale massimale.*

La dimostrazione è lasciata come esercizio. ■

## 2 Tecniche di dimostrazione

Ciò che i matematici considerano un modo appropriato di presentare una dimostrazione non è definito con chiarezza. Di solito, non vengono date dimostrazioni complete, nel senso che ogni passo consiste nell'applicare una regola di logica al passo precedente. Una dimostrazione siffatta risulterebbe troppo lunga, e inoltre i punti principali non sarebbero messi in evidenza. D'altra parte, tutte le difficoltà nei passaggi dimostrativi sono certamente incluse. Chi legge la dimostrazione dovrebbe essere in grado di completare tutti i dettagli necessari per comprenderla. L'abilità nello scrivere una dimostrazione si acquista soltanto con l'esperienza.

Esamineremo tre tecniche importanti utilizzate per costruire dimostrazioni: la *dicotomia*, l'*induzione*, e la *contraddizione*.

La parola *dicotomia* significa divisione in due parti. Si tratta di un metodo per scomporre un problema in parti più piccole, più facilmente trattabili. Altre denominazioni per questo procedimento sono: *analisi dei casi* e *divide et impera*. Vediamo subito un esempio di dicotomia. Una definizione del *coefficiente binomiale*  $\binom{n}{k}$  (da leggere " $n$  su  $k$ ") è che  $\binom{n}{k}$  è il numero dei sottoinsiemi di ordine  $k$  nell'insieme  $\{1, 2, \dots, n\}$ . Per esempio,  $\binom{4}{2} = 6$ . Infatti, i sei sottoinsiemi di ordine 2 di  $\{1, 2, 3, 4\}$  sono:  $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$ .

(2.1) PROPOSIZIONE *Per ogni intero  $n$  e per ogni  $k \leq n$ , si ha:*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

*Dimostrazione.* Sia  $S$  un sottoinsieme di  $\{1, 2, \dots, n\}$  di ordine  $k$ . Allora o  $n \in S$  oppure  $n \notin S$ . Questa è la nostra dicotomia. Se  $n \notin S$ , allora  $S$  è in realtà un sottoinsieme di  $\{1, 2, \dots, n-1\}$ . Per definizione, vi sono  $\binom{n-1}{k}$  sottoinsiemi siffatti. Supponiamo che  $n \in S$ , e sia  $S' = S - \{n\}$  l'insieme ottenuto eliminando l'elemento  $n$  dall'insieme  $S$ . Allora  $S'$  è un sottoinsieme di  $\{1, 2, \dots, n-1\}$ , di ordine  $k-1$ . Vi sono  $\binom{n-1}{k-1}$  insiemi  $S'$  siffatti. Pertanto vi sono  $\binom{n-1}{k-1}$  sottoinsiemi di ordine  $k$  che contengono  $n$ . Ciò ci dà in totale  $\binom{n-1}{k} + \binom{n-1}{k-1}$  sottoinsiemi di ordine  $k$ . ■

La grande potenza del metodo basato sulla dicotomia si manifesta qui nel fatto che, in ciascuno dei due casi:  $n \in S$  e  $n \notin S$ , otteniamo una nuova informazione sull'insieme  $S$  in esame. Tale informazione può essere usata nella dimostrazione.

Spesso una dimostrazione richiede di distinguere parecchi casi possibili, esaminandoli uno alla volta. Questa è la dicotomia, o analisi dei casi. Per esempio, per determinare la specie di una pianta, il *Manual of Botany* di Gray procede per dicotomie successive. Una tipica dicotomia è la seguente: "foglie opposte sul ramo (caso  $h$ ), oppure foglie alternate (caso  $k$ )". Anche la classificazione delle strutture matematiche procede attraverso una serie di dicotomie. Esse non vengono necessariamente scritte in modo formale nei casi semplici, ma quando si ha a che fare con una serie complicata di possibilità è necessario esaminare accuratamente i vari casi possibili. Ecco qui un esempio semplice:

**(2.2) PROPOSIZIONE** *Ogni gruppo di ordine 4 è abeliano.*

*Dimostrazione.* Sia  $G$  un gruppo di ordine 4, e siano  $x, y$  due elementi di  $G$ . Dobbiamo dimostrare che  $xy = yx$ . Consideriamo i cinque elementi  $1, x, y, xy, yx$ . Poiché vi sono soltanto quattro elementi nel gruppo, due di questi devono essere uguali. Se  $xy = yx$ , la proposizione è verificata. Esaminiamo ora le altre possibilità:

*Caso 1:*  $x = 1$  oppure  $y = 1$ . Se  $x = 1$ , allora  $xy = y = yx$ . Se  $y = 1$ , allora  $xy = x = yx$ .

*Caso 2:*  $xy = 1$  oppure  $yx = 1$ . Allora  $y = x^{-1}$ , e  $xy = 1 = yx$ .

*Caso 3:*  $x = y$ . Allora  $xy = x^2 = yx$ .

*Caso 4:*  $xy = x$  o  $yx = x$  o  $xy = y$  o  $yx = y$ . Nei primi due casi, cancelliamo  $x$  per concludere che  $y = 1$ , ciò che ci riporta al caso 1. Negli ultimi due casi, cancelliamo  $y$ .

Ciò esaurisce tutti i casi possibili e completa la dimostrazione. ■

L'*induzione* è il metodo principale per dimostrare una successione di enunciati  $P_n$ , con  $n$  intero positivo. Per dimostrare  $P_n$  per ogni  $n$ , il principio di induzione richiede di dimostrare che

- (2.3)** (i)  $P_1$  è vero;  
(ii) se per qualche intero  $k > 1$   $P_k$  è vero, allora anche  $P_{k+1}$  è vero.

Talvolta è più conveniente dimostrare che se per qualche intero  $k \geq 1$   $P_{k-1}$  è vero, anche  $P_k$  è vero. Si tratta semplicemente di un cambiamento dell'indice.

Ecco alcuni esempi di induzione:

**(2.4) PROPOSIZIONE** *Il determinante di una matrice triangolare superiore è il prodotto dei suoi elementi diagonali.*

*Dimostrazione.* In questo caso,  $P_n$  è l'affermazione che la proposizione è vera per una matrice triangolare  $n \times n$ . Nel caso di una matrice  $1 \times 1$ , vi è un solo elemento diagonale, ed esso è uguale al determinante. Ciò significa che l'enunciato  $P_1$  è vero. Ora supponiamo che  $P_{k-1}$  sia vero, e dimostriamo  $P_k$  utilizzando questo fatto. Sia  $A$  una matrice triangolare  $k \times k$ . Calcoliamo lo sviluppo del determinante lungo la prima colonna:

$$\det A = a_{11} \det A_{11} - a_{21} \det A_{21} + \dots$$

Poiché  $A$  è triangolare, gli elementi  $a_{21}, a_{31}, \dots, a_{k1}$  sono tutti nulli, e pertanto  $\det A = a_{11} \det A_{11}$ . Osserviamo ora che  $A_{11}$  è una matrice triangolare  $(k-1) \times (k-1)$  e che i suoi elementi diagonali sono  $a_{22}, a_{33}, \dots, a_{kk}$ . Poiché  $P_{k-1}$  è vero per ipotesi, si ha:  $\det A_{11} = a_{22} \cdots a_{kk}$ . Pertanto  $\det A = a_{11} a_{22} \cdots a_{kk}$ , come richiesto. ■

**(2.5) PROPOSIZIONE**  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ .

*Dimostrazione.* In questo caso  $P_r$  è l'affermazione che  $\binom{r}{k} = \frac{r!}{k!(r-k)!}$  per ogni  $k = 1, \dots, r$ . Supponiamo che l'enunciato  $P_{r-1}$  sia vero. Allora la formula è vera quando sostituiamo  $n$  con  $r-1$  e  $k$  con  $k$  e anche quando sostituiamo  $n$  con  $r-1$  e  $k$  con  $k-1$ :

$$\binom{r-1}{k} = \frac{(r-1)!}{k!(r-1-k)!} \quad \text{e} \quad \binom{r-1}{k-1} = \frac{(r-1)!}{(k-1)!(r-k)!}.$$

In base alla proposizione (2.1), si ha:  $\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}$ . Pertanto risulta:

$$\begin{aligned} \binom{r}{k} &= \binom{r-1}{k} + \binom{r-1}{k-1} = \frac{(r-1)!}{k!(r-1-k)!} + \frac{(r-1)!}{(k-1)!(r-k)!} = \\ &= \frac{r-k}{r} \frac{r!}{k!(r-k)!} + \frac{k}{r} \frac{r!}{k!(r-k)!} = \frac{r!}{k!(r-k)!}. \end{aligned}$$

Ciò prova che l'enunciato  $P_r$  è vero, come richiesto. ■

Come ulteriore esempio, dimostriamo il principio delle gabbie dei piccioni (1.6a), secondo cui se un'applicazione  $\varphi : S \rightarrow T$  tra insiemi finiti è iniettiva, allora  $|S| \leq |T|$ . Procediamo per induzione su  $n = |T|$ . L'affermazione è vera, se  $n = 0$ , ossia se  $T = \emptyset$ , poiché l'unico insieme che ammette un'applicazione nell'insieme vuoto è l'insieme vuoto.

Supponiamo che il teorema sia stato dimostrato per  $n = k - 1$ , e dimostriamolo per  $n = k$ , con  $k > 0$ . Supponiamo che  $|T| = k$ , e scegliamo un elemento  $t \in T$ .

*Caso 1:*  $t \in \text{im } \varphi$ . Poiché  $\varphi$  è iniettiva, esiste un unico elemento  $s \in S$  tale che  $\varphi(s) = t$ . Poniamo  $S' = S - \{s\}$  e  $T' = T - \{t\}$ . Restringendo  $\varphi$  a  $S'$ , otteniamo un'applicazione iniettiva  $\varphi' : S' \rightarrow T'$ . Poiché  $|T'| = |T| - 1 = k - 1$ , l'ipotesi induttiva implica  $|S'| \leq |T'|$ . Pertanto  $|S| = |S'| + 1 \leq |T'| + 1 = |T|$ .

*Caso 2:*  $t \notin \text{im } \varphi$ . In tal caso, l'immagine di  $\varphi$  è contenuta in  $T' = T - \{t\}$ . Pertanto  $\varphi$  definisce un'applicazione iniettiva  $S \rightarrow T'$ . Di nuovo, l'ipotesi induttiva implica che  $|S| \leq |T'| = |T| - 1$ . ■

Esiste un'altra forma del principio di induzione, chiamata *induzione completa*. Anche qui vogliamo dimostrare un enunciato  $P_n$  per ogni intero positivo  $n$ . Il principio di induzione completa afferma che basta dimostrare l'enunciato seguente:

(2.6) *Se  $n$  è un intero positivo, e se  $P_k$  è vero per ogni intero positivo  $k < n$ , allora  $P_n$  è vero.*

Per  $n = 1$ , non esistono interi positivi  $k < n$ . Ne segue che l'ipotesi di (2.6) è automaticamente soddisfatta per  $n = 1$ . Pertanto una dimostrazione di (2.6) deve includere una dimostrazione di  $P_1$ .

Il principio di induzione completa si usa quando esiste un procedimento per ridurre  $P_n$  a  $P_k$  per qualche intero più piccolo  $k$ , ma non necessariamente a  $P_{n-1}$ . Ecco un esempio:

(2.7) TEOREMA *Ogni intero  $n > 1$  è un prodotto di numeri primi.*

Innanzitutto, diamo una dimostrazione informale, la quale fornisce anche un algoritmo per trovare una scomposizione in fattori primi. Se  $n$  è un numero primo, allora è un prodotto con un solo fattore primo, e la tesi è dimostrata. Altrimenti,  $n$  ha un divisore diverso da 1 e da  $n$ . Se  $n$  ci viene assegnato esplicitamente, saremo in grado di verificare se esiste o no un divisore proprio. In caso affermativo,  $n$  può essere scritto come un prodotto di interi, diciamo  $n = ab$ , con  $1 < a, b < n$ . Continuiamo, se possibile, a fattorizzare  $a$  e  $b$ . Poiché ad ogni passo i fattori diventano più piccoli, tale procedimento non può continuare indefinitamente, e pertanto alla fine otteniamo una decomposizione in fattori primi di  $n$ .

Il principio di induzione completa formalizza il fatto che è impossibile continuare indefinitamente a sostituire un intero positivo con uno più piccolo. Per applicare il principio, sia  $P_n$  l'enunciato che  $n$  è un prodotto di numeri primi, e supponiamo che  $P_k$  sia vero per ogni  $k < n$ . Riprendiamo di nuovo l'argomentazione. Precisamente, o  $n$  è primo, nel qual caso non vi è nulla da dimostrare, oppure  $n = ab$ , con  $a, b < n$ . In quest'ultimo caso, l'ipotesi induttiva ci dice che  $P_a$  e  $P_b$  sono entrambi veri, ossia, che  $a$  e  $b$  sono prodotti di numeri primi. Scrivendo questi prodotti uno accanto all'altro, otteniamo la fattorizzazione richiesta di  $n$ .

Le due dimostrazioni appaiono leggermente diverse l'una dall'altra, poiché l'algoritmo non è menzionato nell'enunciato del teorema ed in parte è stato tenuto nascosto nella dimostrazione formale. Un enunciato migliore del teorema metterebbe in evidenza l'algoritmo:

(2.8) TEOREMA *Il procedimento di fattorizzazione di un intero  $> 1$  termina dopo un numero finito di passi.*

Con questa formulazione, la dimostrazione formale diventa identica a quella informale. ■

La *dimostrazione per assurdo* procede supponendo che la conclusione desiderata sia falsa e ricavando una contraddizione da tale ipotesi. Pertanto la conclusione deve essere vera. Ad esempio, possiamo riscrivere la dimostrazione precedente del fatto che ogni gruppo di ordine 4 è abeliano, nel modo seguente:

*Dimostrazione della (2.2) (riscritta).* Supponiamo che  $G$  sia un gruppo non abeliano di ordine 4, e deduciamo da ciò una contraddizione. Poiché  $G$  è non abeliano, esistono elementi  $x, y \in G$  tali che  $xy \neq yx$ . Allora  $y$  è necessariamente diverso dagli elementi  $1, x, x^{-1}$ , poiché questi elementi commutano con  $x$ . Analogamente,  $x$  è diverso da  $1, y, y^{-1}$ . Ne segue che gli elementi  $1, x, y, xy, yx$  sono distinti, in contraddizione con l'ipotesi che  $|G| = 4$ . Pertanto non esiste un gruppo non abeliano di ordine 4. ■

Si noti che non vi è una reale differenza tra le due dimostrazioni di (2.2). La dimostrazione appena data è infatti una falsa argomentazione per assurdo e inoltre, pur essendo logicamente corretta, è poco elegante. Si dovrebbero evitare dimostrazioni di questo tipo. Per contro, vi sono vere dimostrazioni per assurdo in cui non è facile rigirare le cose per eliminare la contraddizione. Un esempio è dato dalla dimostrazione della proposizione (1.13) (cap. 6) secondo cui un gruppo di ordine  $p^2$ , con  $p$  primo, è abeliano; un altro esempio è dato dalla dimostrazione della proposizione (3.11), più avanti.

### 3 Topologia

In questo paragrafo vengono passati in rassegna alcuni concetti di topologia, di cui avremo bisogno di tanto in tanto. Gli insiemi che vogliamo studiare sono sottoinsiemi dello spazio euclideo  $\mathbb{R}^k$ .

Sia  $r$  un numero reale positivo. Il *disco aperto* di raggio  $r$  intorno a un punto  $X \in \mathbb{R}^k$  è l'insieme di tutti i punti la cui distanza da  $X$  è minore di  $r$ :

$$(3.1) \quad B_{X,r} = \{X' \in \mathbb{R}^k \mid |X' - X| < r\}.$$

Un sottoinsieme  $U$  di  $\mathbb{R}^k$  si dice *aperto* se ogni volta che un punto  $X$  appartiene a  $U$ , anche i punti abbastanza vicini a  $X$  appartengono a  $U$ . In altre parole,  $U$  è aperto se soddisfa la seguente condizione:

- (3.2) *Se  $X \in U$  e se  $r$  è abbastanza piccolo, allora  $B_{X,r} \subset U$ .  
Il raggio  $r$  dipenderà dal punto  $X$ .*

Gli insiemi aperti hanno le seguenti proprietà:

- (3.3) (i) *L'unione di una famiglia arbitraria di insiemi aperti è un insieme aperto.*  
(ii) *L'intersezione di un numero finito di insiemi aperti è un insieme aperto.*

L'intero spazio  $\mathbb{R}^k$  e l'insieme vuoto  $\emptyset$  sono gli esempi più semplici di insiemi aperti. Alcuni insiemi aperti più interessanti si ottengono nel modo seguente: sia  $f$  una funzione continua  $\mathbb{R}^k \rightarrow \mathbb{R}$ . Allora gli insiemi:

$$(3.4) \quad \{f > 0\}, \quad \{f < 0\}, \quad \{f \neq 0\}$$

sono aperti. Per esempio, se  $f(X) > 0$ , allora  $f(X') > 0$  per ogni  $X'$  vicino a  $X$ , poiché  $f$  è continua. Ciò prova che il gruppo lineare generale  $GL_2(\mathbb{R})$  è un sottoinsieme aperto dello spazio  $\mathbb{R}^4$  di tutte le matrici  $2 \times 2$ , poiché esso è l'insieme  $\{\det P \neq 0\}$ . Inoltre, il disco aperto  $B_{X,r}$  è un insieme aperto in  $\mathbb{R}^k$ , poiché è definito dalla diseguaglianza  $|X' - X| - r < 0$ .

Sia  $S$  un insieme in  $\mathbb{R}^k$ . Avremo bisogno anche della nozione di sottoinsieme aperto di  $S$ . Per definizione, un sottoinsieme  $V$  di  $S$  si dice *aperto in  $S$* , se ogni volta che esso contiene un punto  $X$ , esso contiene anche tutti i punti di  $S$  che sono abbastanza vicini a  $X$ . Tale condizione è illustrata dal seguente lemma:

(3.5) **LEMMA** *Sia  $V$  un sottoinsieme di un insieme  $S$  in  $\mathbb{R}^k$ . Le seguenti condizioni su  $V$  sono equivalenti, e inoltre, se vale una di esse, allora  $V$  è chiamato un sottoinsieme aperto di  $S$ :*

- (i)  $V = U \cap S$ , per qualche insieme aperto  $U$  di  $\mathbb{R}^k$ ;
- (ii) per ogni punto  $X \in V$ , esiste un numero reale  $r > 0$  tale che  $V$  contiene l'insieme  $B_{X,r} \cap S$ .

*Dimostrazione.* Supponiamo che  $V = U \cap S$  per qualche insieme aperto  $U$  di  $\mathbb{R}^k$ . Sia  $X \in V$ . Allora  $X \in U$  e, in base a (3.2), esiste un numero reale  $r > 0$  tale che  $B_{X,r} \subset U$ . Pertanto  $B_{X,r} \cap S \subset U \cap S = V$ , e (ii) è verificata. Viceversa, supponiamo che valga la condizione (ii). Per ogni  $X \in V$ , scegliamo un disco aperto  $B_{X,r}$  tale che

$$B_{X,r} \cap S \subset V,$$

dove il raggio  $r$  dipende, come al solito, dal punto  $X$ . Sia  $U$  l'unione di questi dischi aperti. Allora  $U$  è un insieme aperto in  $\mathbb{R}^k$  (3.3i), e  $U \cap S \subset V$ . D'altra parte,  $X \in B_{X,r} \cap S \subset U \cap S$ , per ogni  $X \in V$ . Pertanto  $V \subset U \cap S$ , e quindi  $V = U \cap S$  come richiesto. ■

I sottoinsiemi aperti di  $S$  godono delle proprietà (3.3), le quali discendono dalle stesse proprietà dei sottoinsiemi aperti di  $\mathbb{R}^k$ , in virtù di (3.5i).

Di solito si parla di un sottoinsieme aperto  $V$  di  $S$  che contiene un punto  $p$  assegnato come di un *intorno* di  $p$  in  $S$ .

Un sottoinsieme  $C$  di un insieme  $S$  si dice *chiuso*, se il suo complementare  $(S - C)$  è un sottoinsieme aperto. Per esempio, siano  $f_i : \mathbb{R}^k \rightarrow \mathbb{R}$  ( $i = 1, \dots, k$ ) funzioni continue. Allora il luogo:

$$(3.6) \quad \{f_1 = f_2 = \dots = f_k = 0\}$$

delle soluzioni del sistema formato dalle equazioni  $f_i = 0$  è un insieme chiuso in  $\mathbb{R}^k$ , poiché il suo complementare è l'unione degli insiemi aperti  $\{f_i \neq 0\}$ . La 2-sfera  $\{x_1^2 + x_2^2 + x_3^2 = 1\}$  è un esempio di un insieme chiuso in  $\mathbb{R}^3$ . Tale è anche il gruppo delle rotazioni  $SO_2$ . Esso è il luogo in  $\mathbb{R}^{2 \times 2}$  definito dalle cinque equazioni:

$$\begin{aligned} x_{11}x_{22} - x_{12}x_{21} &= 1, & x_{11}^2 + x_{12}^2 &= 1, & x_{11}x_{21} + x_{12}x_{22} &= 0, \\ x_{21}x_{11} + x_{22}x_{12} &= 0, & x_{21}^2 + x_{22}^2 &= 1. \end{aligned}$$

Gli insiemi chiusi hanno proprietà duali rispetto alle (3.3):

- (3.7) (i) *L'intersezione di una famiglia arbitraria di insiemi chiusi è un insieme chiuso.*  
(ii) *L'unione di un numero finito di insiemi chiusi è un insieme chiuso.*

Queste proprietà si ottengono dalle (3.3), mediante il passaggio ai sottoinsiemi complementari.

Un sottoinsieme  $C$  di  $\mathbb{R}^k$  si dice *limitato* se le coordinate dei punti in  $C$  sono limitate, ossia se esiste un numero reale positivo  $b$  tale che, per ogni  $X = (x_1, \dots, x_n) \in C$ , risulta

$$(3.8) \quad |x_i| \leq b, \quad \text{per } i = 1, \dots, n.$$

Se  $C$  è chiuso e limitato, esso è chiamato un sottoinsieme *compatto* di  $\mathbb{R}^k$ . La 2-sfera unitaria è un insieme compatto in  $\mathbb{R}^3$ .

Siano  $S, T$  sottoinsiemi, rispettivamente, di  $\mathbb{R}^m, \mathbb{R}^n$ . Un'applicazione  $f : S \rightarrow T$  si dice *continua* se manda punti vicini di  $S$  in punti vicini di  $T$ . Formalmente, la proprietà di continuità si enuncia nel modo seguente:

$$(3.9) \quad \begin{aligned} &\text{Sia } s \in S. \text{ Per ogni numero reale } \epsilon > 0, \text{ esiste un numero} \\ &\text{reale } \delta > 0 \text{ tale che, se } s' \in S \text{ e } |s' - s| < \delta, \text{ allora } |f(s') - f(s)| < \epsilon. \end{aligned}$$

Il modo più facile per ottenere un'applicazione continua da  $S$  a  $T$  è quello di restringere un'applicazione continua  $F : \mathbb{R}^m \rightarrow \mathbb{R}^n$  che manda  $S$  in  $T$ . La maggior parte delle applicazioni che usiamo sono di questa forma. Per esempio, il determinante è un'applicazione continua da uno qualsiasi dei gruppi classici a  $\mathbb{R}$  o a  $\mathbb{C}$ .

Un'applicazione  $f : S \rightarrow S'$  è chiamata *omeomorfismo*, se essa è biettiva ed è continua insieme con la sua inversa  $f^{-1}$ .

Per esempio, la circonferenza unitaria  $S^1$  in  $\mathbb{R}^2$  è omeomorfa al gruppo delle rotazioni  $SO_2$ . L'omeomorfismo  $f : S^1 \rightarrow SO_2$  è dato dalla restrizione dell'applicazione:

$$F(x_1, x_2) = \begin{bmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{bmatrix},$$

che manda  $\mathbb{R}^2$  nello spazio  $\mathbb{R}^4$  delle matrici  $2 \times 2$ . L'applicazione  $F$  non è biettiva e pertanto non è un omeomorfismo; tuttavia, essa si restringe ad un omeomorfismo  $f$  sui sottoinsiemi  $S^1$  e  $SO_2$ . La sua inversa è la restrizione a  $SO_2$  della proiezione  $G : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ , che manda una matrice  $2 \times 2$  nella sua prima riga. (La parola *omeomorfismo* non va confusa con *omomorfismo*!).

Un *cammino* o *arco* è un'applicazione continua  $f : [0, 1] \rightarrow \mathbb{R}^k$  dall'intervallo unitario allo spazio  $\mathbb{R}^k$ , e si dice che il cammino giace in  $S$ , se  $f(t) \in S$  per ogni  $t \in [0, 1]$ . Un sottoinsieme  $S$  di  $\mathbb{R}^k$  si dice *connesso per cammini* o *per archi*, se ogni coppia di punti  $p, q \in S$  può essere congiunta mediante un cammino giacente in  $S$ . In altre parole, per ogni coppia di punti  $p, q \in S$ , esiste un cammino  $f$  tale che:

$$(3.10) \quad \begin{aligned} &\text{(i) } f(t) \in S \text{ per ogni } t \in [0, 1]; \\ &\text{(ii) } f(0) = p \text{ e } f(1) = q. \end{aligned}$$

Ecco la proprietà più importante degli insiemi connessi per archi:

(3.11) PROPOSIZIONE *Un insieme connesso per archi  $S$  non è l'unione disgiunta di sottoinsiemi aperti propri. In altre parole, supponiamo che*

$$S = \bigcup_i V_i,$$

*dove i  $V_i$  sono insiemi aperti in  $S$  e  $V_i \cap V_j = \emptyset$ , se  $i \neq j$ . Allora tutti gli insiemi  $V_i$ , tranne uno, sono vuoti.*

*Dimostrazione.* Supponiamo che due dei sottoinsiemi assegnati siano non vuoti, diciamo  $V_0$  e  $V_1$ . Mettiamo da parte  $V_0$  e sostituiamolo  $V_1$  con l'unione dei sottoinsiemi rimanenti, che è un insieme aperto, in base a (3.3). Allora  $V_0 \cup V_1 = S$  e  $V_0 \cap V_1 = \emptyset$ . Ciò riduce il problema al caso in cui vi sono esattamente due insiemi aperti.

Scegliamo un punto  $p \in V_0$  e un punto  $q \in V_1$ , e sia  $f : [0, 1] \rightarrow S$  un cammino in  $S$  congiungente  $p$  con  $q$ . Otterremo una contraddizione, esaminando il cammino nel punto in cui esso lascia  $V_0$  per l'ultima volta.

Sia  $b$  l'estremo superiore dell'insieme costituito da tutti i numeri reali  $t \in [0, 1]$  tali che  $f(t) \in V_0$ , e poniamo  $X = f(b)$ . Se  $X \in V_0$ , tutti i punti di  $B_{X,r} \cap S$  stanno in  $V_0$  se  $r$  è abbastanza piccolo. Poiché  $f$  è continua,  $f(t) \in B_{X,r}$  per ogni  $t$  abbastanza vicino a  $b$ . Pertanto  $f(t) \in V_0$  per tali punti. Ora, se  $t$  è leggermente più grande di  $b$ , ciò contraddice il fatto che  $b$  è un maggiorante dell'insieme dei punti che vengono mandati in  $V_0$ . Pertanto  $X$  non sta in  $V_0$ , sicché  $X \in V_1$ . Ma, procedendo nello stesso modo, troviamo che  $f(t) \in V_1$  per ogni  $t$  abbastanza vicino a  $b$ . Pertanto, se  $t$  è leggermente più piccolo di  $b$ , ciò contraddice il fatto che  $b$  è l'estremo superiore dell'insieme dei punti che vengono mandati in  $V_0$ . Questa contraddizione completa la dimostrazione. ■

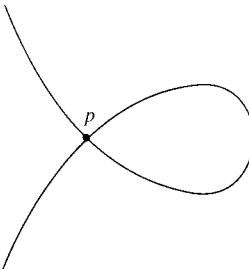
L'ultimo concetto di topologia di cui abbiamo bisogno è quello di varietà.

(3.12) DEFINIZIONE *Un sottoinsieme  $S$  di  $\mathbb{R}^n$  è chiamato una varietà di dimensione  $d$  se ogni punto  $p$  di  $S$  ha un intorno in  $S$  che è omeomorfo a un insieme aperto in  $\mathbb{R}^d$ .*

Per esempio, la sfera  $\{(x, y, z) \mid x^2 + y^2 + z^2 = 1\}$  è una varietà di dimensione 2. La semisfera  $U = \{z > 0\}$  è un insieme aperto in  $S^3$  (3.4, 3.5) e si proietta, mediante un'applicazione continua, sul disco unitario  $B_{0,1} = \{x_1^2 + x_2^2 + x_3^2 < 1\}$  in  $\mathbb{R}^3$ . La funzione inversa  $z = \sqrt{1 - x^2 - y^2}$  è continua. Pertanto  $U$  è omeomorfa a  $B_{0,1}$ . Poiché la 3-sfera è ricoperta da tali semisfere, essa è una varietà.

La figura qui sotto mostra un insieme che non è una varietà. Esso diventa una varietà di dimensione 1 se viene privato del punto  $p$ . Si noti che questo insieme

non gode della proprietà di omogeneità. Esso appare vicino a  $p$  in modo diverso rispetto a come appare vicino agli altri punti.



(3.13)

Un insieme che non è una varietà.

#### 4 Il teorema delle funzioni implicate

Il teorema delle funzioni implicate è usato in due punti nel testo, e pertanto viene enunciato qui esplicitamente.

(4.1) TEOREMA (Teorema delle funzioni implicate) *Siano  $f(x, y) = (f_1(x, y), \dots, f_r(x, y))$   $r$  funzioni di  $n+r$  variabili reali  $(x, y) = (x_1, \dots, x_n, y_1, \dots, y_r)$  di classe  $C^1$ , ossia dotate di derivate parziali prime continue, in un insieme aperto di  $\mathbb{R}^{n+r}$  contenente il punto  $(a, b)$ . Supponiamo che il determinante jacobiano:*

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial y_1} & \dots & \frac{\partial f_1}{\partial y_r} \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial y_1} & \dots & \frac{\partial f_r}{\partial y_r} \end{bmatrix}$$

*sia diverso da zero nel punto  $(a, b)$ . Allora esiste un intorno  $U$  del punto  $a$  in  $\mathbb{R}^n$  tale che su  $U$  esistono e sono univocamente determinate  $r$  funzioni di classe  $C^1$   $Y_1(x), \dots, Y_r(x)$ , soddisfacenti alle seguenti condizioni:*

$$f(x, Y(x)) = 0 \quad \text{e} \quad Y(a) = b.$$

Il teorema delle funzioni implicate è strettamente collegato al teorema della funzione inversa, che è usato nel capitolo 8 (5.8):

(4.2) TEOREMA DELLA FUNZIONE INVERSA *Sia  $f = (f_1, \dots, f_n)$  un'applicazione di classe  $C^1$  (ossia, tale che  $f_1, \dots, f_n$  siano di classe  $C^1$ ) da un insieme aperto  $U$*

*di  $\mathbb{R}^n$  a  $\mathbb{R}^n$ . Supponiamo che il determinante jacobiano*

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1} & \dots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

*sia diverso da zero in un punto  $a \in \mathbb{R}^n$ . Allora esiste un intorno di  $a$  sul quale  $f$  ha una funzione inversa di classe  $C^1$ .*

Per le dimostrazioni di questi due teoremi rimandiamo al testo di Rudin, *Principles of Mathematical Analysis* (vedi "Suggerimenti per ulteriori letture" a fine volume). ■

Usiamo anche il seguente risultato, che è l'analogo nel caso complesso del teorema delle funzioni implicate, in un punto [cap. 10 (8.15)]:

(4.3) TEOREMA *Sia  $f(x, y)$  un polinomio complesso. Supponiamo che, per qualche punto  $(a, b) \in \mathbb{C}^2$ , si abbia:  $f(a, b) = 0$  e  $\frac{\partial f}{\partial y}(a, b) \neq 0$ . Allora esiste un intorno  $U$  di  $x$  in  $\mathbb{C}$  tale che esiste ed è univocamente determinata una funzione continua  $Y(x)$  avente le seguenti proprietà:*

$$f(x, Y(x)) = 0 \quad \text{e} \quad Y(a) = b.$$

Poiché non è facile trovare nella letteratura un riferimento per questo teorema, daremo una dimostrazione che rimanda al teorema delle funzioni implicate nel caso reale. Si tratterà semplicemente di scrivere ogni cosa per mezzo della sua parte reale e della sua parte immaginaria e poi di verificare le ipotesi di (4.1). La stessa argomentazione si applica nel caso di più variabili.

*Dimostrazione.* Scriviamo  $x = x_0 + x_1 i$ ,  $y = y_0 + y_1 i$ ,  $f = f_0 + f_1 i$ , dove  $f_i = f_i(x_0, x_1, y_0, y_1)$  è una funzione di quattro variabili reali a valori reali. Dobbiamo risolvere il sistema formato dalle due equazioni  $f_0 = f_1 = 0$ , esprimendo  $y_0, y_1$  come funzioni di  $x_0, x_1$ . In base a (4.1), dobbiamo dimostrare che il determinante jacobiano:

$$\det \begin{bmatrix} \frac{\partial f_0}{\partial y_0} & \frac{\partial f_0}{\partial y_1} \\ \frac{\partial f_1}{\partial y_0} & \frac{\partial f_1}{\partial y_1} \end{bmatrix}$$

è diverso da zero in  $(a, b)$ . Poiché  $f$  è un polinomio in  $x, y$ , le funzioni reali  $f_i$  sono anch'esse polinomi in  $x_i, y_j$ . Pertanto esse hanno derivate continue.

(4.4) LEMMA *Sia  $f(x, y)$  un polinomio a coefficienti complessi. Con le notazioni sopra introdotte, si ha:*

(i)  $\frac{\partial f}{\partial y} = \frac{\partial f_0}{\partial y_0} + \frac{\partial f_1}{\partial y_0} i$ , e inoltre

(ii) valgono le equazioni di Cauchy-Riemann:  $\frac{\partial f_0}{\partial y_0} = \frac{\partial f_1}{\partial y_1}$ ,  $\frac{\partial f_0}{\partial y_1} = -\frac{\partial f_1}{\partial y_0}$ .

*Dimostrazione.* Poiché  $f$  è un polinomio e poiché la derivata di una somma è la somma delle derivate, basta dimostrare il lemma per i monomi  $cy^n = (c_0 + c_1 i)(y_0 + y_1 i)^n$ . Per questi monomi, la tesi si ottiene utilizzando la regola per la derivata di un prodotto, procedendo per induzione su  $n$ . ■

Ritorniamo alla dimostrazione del teorema (4.3). Per ipotesi,  $f_i(a_0, a_1, b_0, b_1) = 0$ . Inoltre, poiché  $\frac{\partial f}{\partial y}(a, b) \neq 0$ , sappiamo da (4.4i) che  $\frac{\partial f_0}{\partial y_0} = d_0$  e  $\frac{\partial f_1}{\partial y_0} = d_1$  non sono entrambe nulle. In base a (4.4ii), il determinante jacobiano è:

$$\det \begin{bmatrix} d_0 & -d_1 \\ d_1 & d_0 \end{bmatrix} = d_0^2 + d_1^2 > 0.$$

Pertanto le ipotesi del teorema delle funzioni implicite (4.1) sono soddisfatte. ■

## Esercizi

### 1 Teoria degli insiemi

1. Sia  $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$  l'applicazione definita da  $\varphi(n) = n^3 - 3n + 1$ .

- (a) È vero che  $\varphi$  è iniettiva?
- (b) Determinare  $\varphi^{-1}(U)$ , dove  $U$  è l'intervallo:
  - (i)  $[0, \infty)$ ; (ii)  $[2, 4]$ ; (iii)  $[4, 12]$ .

2. Dare un esempio di un'applicazione  $\varphi : S \rightarrow S$  di un insieme infinito in sé, che sia suriettiva ma non iniettiva, e di una che sia iniettiva ma non suriettiva.

3. Sia  $\varphi : S \rightarrow T$  un'applicazione tra insiemi.

- (a) Sia  $U$  un sottoinsieme di  $S$ . Dimostrare che  $\varphi(\varphi^{-1}(U)) \subset U$  e che, se  $\varphi$  è suriettiva, allora  $\varphi(\varphi^{-1}(U)) = U$ .
- (b) Sia  $V$  un sottoinsieme di  $T$ . Dimostrare che  $\varphi^{-1}(\varphi(V)) \supset V$  e che, se  $\varphi$  è iniettiva, allora  $\varphi^{-1}(\varphi(V)) = V$ .
- 4. Sia  $\varphi : S \rightarrow T$  un'applicazione tra insiemi. Un'applicazione  $\psi : T \rightarrow S$  è chiamata *inversa sinistra* di  $\varphi$ , se  $\psi \circ \varphi : S \rightarrow S$  è l'identità, e un'*inversa destra* di  $\varphi$ , se

$\varphi \circ \psi : T \rightarrow T$  è l'identità. Dimostrare che  $\varphi$  ha un'inversa sinistra se, e soltanto se, essa è iniettiva e che  $\varphi$  ha un'inversa destra se, e soltanto se, essa è suriettiva.

5. Sia  $S$  un insieme parzialmente ordinato.

(a) Dimostrare che, se  $S$  contiene un maggiorante  $b$  per  $S$ , allora  $b$  è unico, e inoltre  $b$  è un elemento massimale.

(b) Dimostrare che, se  $S$  è totalmente ordinato, allora un elemento massimale  $m$  è un maggiorante per  $S$ .

6. (a) Descrivere con precisione quali sono i numeri reali che hanno più di una rappresentazione decimale e quante rappresentazioni possiede un numero siffatto.

(b) Completare la dimostrazione della proposizione (1.7).

7. Utilizzare il lemma di Zorn per dimostrare che ogni ideale  $I \neq R$  è contenuto in un ideale massimale. Fare ciò, provando che l'insieme  $S$  di tutti gli ideali  $I \neq R$ , ordinato per inclusione, è induttivo.

### 2 Tecniche di dimostrazione

1. Usare l'induzione per trovare una forma chiusa per ciascuna delle seguenti espressioni:

(a)  $1 + 3 + 5 + \dots + (2n + 1)$ ,

(b)  $1^2 + 2^2 + 3^2 + \dots + n^2$ ,

(c)  $1 + 1/2 + 1/3 + \dots + 1/n$ ,

(d)  $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)}$ .

2. Dimostrare che  $1^3 + 2^3 + \dots + n^3 = (n(n+1)/2)^2$ .

3. Dimostrare che  $1/(1 \cdot 2) + 1/(2 \cdot 3) + \dots + 1/(n(n+1)) = n/(n+1)$ .

4. Siano  $S, T$  insiemi finiti.

(a) Sia  $\varphi : S \rightarrow T$  un'applicazione iniettiva. Dimostrare per induzione che  $|S| \leq |T|$  e che, se  $|S| = |T|$ , allora  $\varphi$  è biiettiva.

(b) Sia  $\varphi : S \rightarrow T$  un'applicazione suriettiva. Dimostrare per induzione che  $|S| \geq |T|$  e che, se  $|S| = |T|$ , allora  $\varphi$  è biiettiva.

5. Sia  $n$  un intero positivo. Dimostrare che, se  $2^n - 1$  è un numero primo, allora  $n$  è primo.

6. Posto  $a_n = 2^{2^n} + 1$ , dimostrare che  $a_n = a_0 a_1 \dots a_{n-1} + 2$ .

7. Un polinomio a coefficienti razionali si dice irriducibile, se non è costante e se non è un prodotto di due polinomi non costanti a coefficienti razionali. Usare l'induzione completa per dimostrare che ogni polinomio a coefficienti razionali può essere scritto come un prodotto di polinomi irriducibili.

8. Dimostrare le parti (b) e (c) del teorema (1.6).

### 3 Topologia

1. Sia  $S$  un sottoinsieme di  $\mathbb{R}^k$ , e siano  $f, g$  applicazioni continue da  $S$  a  $\mathbb{R}$ . Stabilire se i seguenti sottoinsiemi risultano oppure no aperti o chiusi in  $S$ :
  - (a)  $\{f(X) \geq 0\}$ ; (b)  $\{f(X) \neq 2\}$ ; (c)  $\{f(X) < 0, g(X) > 0\}$ ;
  - (d)  $\{f(X) \leq 0, g(X) < 0\}$ ; (e)  $\{f(X) \neq 0, g(X) = 0\}$ ; (f)  $\{f(X) \in \mathbb{Z}\}$ ;
  - (g)  $\{f(X) \in \mathbb{Q}\}$ .
2. Sia  $X \in \mathbb{R}^n$ . Stabilire se i seguenti sottoinsiemi risultano oppure no aperti o chiusi in  $\mathbb{R}^n$ :
  - (a)  $\{rX \mid r \in \mathbb{R}, r > 0\}$ ; (b)  $\{rX \mid r \in \mathbb{R}, r \geq 0\}$ .
3. (a) Sia  $P = (p_{ij})$  una matrice invertibile, e sia  $d = \det P$ . Possiamo definire un'applicazione  $GL_n(\mathbb{R}) \rightarrow \mathbb{R}^{n^2+1}$  mandando  $P$  in  $(p_{ij}, d)$ . Dimostrare che tale applicazione immerge  $GL_n(\mathbb{R})$  come un insieme chiuso in  $\mathbb{R}^{n^2+1}$ .
   
(b) Illustrare tale applicazione nel caso di  $GL_1(\mathbb{R})$ .
4. Dimostrare che il prodotto  $M \times M'$  di due varietà  $M, M'$  è una varietà.
5. Dimostrare che  $SL_2(\mathbb{R})$  non è un gruppo compatto.
6. (a) Disegnare sommariamente la curva  $C$  di equazione:  $x_2^2 = x_1^3 - x_1^2$  in  $\mathbb{R}^2$ .
   
(b) Dimostrare che questo luogo di punti, privato dell'origine, è una varietà di dimensione 1.

### 4 Il teorema delle funzioni implicite

1. Dimostrare il lemma (4.4).
2. Dimostrare che  $SL_2(\mathbb{R})$  è una varietà, e determinare la sua dimensione.
3. Sia  $f(x, y)$  un polinomio complesso. Supponiamo che le equazioni:

$$f = 0, \quad \frac{\partial f}{\partial x} = 0, \quad \frac{\partial f}{\partial y} = 0,$$

non abbiano soluzioni comuni in  $\mathbb{C}^2$ . Dimostrare che il luogo  $f = 0$  è una varietà di dimensione 2.

### Notazioni

$A_n$	gruppo alterno, cap. 2 (4.7)
$B_{x,r}$	disco aperto di raggio $r$ centrato nel punto $x$ , app. (3.1)
$\mathbb{C}$	campo dei numeri complessi, cap. 2 (1.11)
$C_n$	gruppo ciclico di ordine $n$ , cap. 5 (3.4)
$D_n$	gruppo diedrale, cap. 5 (3.4)
$\det$	determinante, cap. 1 (3.4)
$F_p$	campo primo $\mathbb{Z}/(p)$ , cap. 3 (2.4)
$GL_n$	gruppo lineare generale, cap. 2 (1.13)
$I$	matrice identica, cap. 1 (1.14)
$I$	gruppo icosaedrale, cap. 5 (9.1)
$\text{im } \varphi$	immagine dell'applicazione $\varphi$ , app. (1.3)
$\ker \varphi$	nucleo dell'omomorfismo $\varphi$ , cap. 2 (4.5)
$\ell^\infty$	spazio delle successioni limitate, cap. 3 (5.2)
$M$	gruppo dei movimenti del piano, cap. 4 (5.15)
$N(H)$	normalizzante di $H$ , cap. 6 (3.7)
$\mathbb{N}$	insieme degli interi positivi, o numeri naturali, cap. 10 (2.1)
$O_n$	gruppo ortogonale, cap. 5 (5.3), cap. 8 (1.3)
$O_{3,1}$	gruppo di Lorentz, cap. 8 (1.4)
$PSL_n$	gruppo proiettivo, cap. 8 (8.2)
$\mathbb{R}$	campo dei numeri reali, cap. 2 (1.11)
$\mathbb{R}^n$	spazio dei vettori $n$ -dimensionali, cap. 3 (1.1)
$S_n$	gruppo simmetrico, cap. 2 (1.14)
$S^n$	sfera $n$ -dimensionale, cap. 8 (2.6)
$SL_n$	gruppo lineare speciale, cap. 2 (4.6), cap. 8 (1.8)
$SO_n$	gruppo ortogonale speciale, cap. 4 (5.4), cap. 8 (1.8)
$SP_{2n}$	gruppo simplettico, cap. 8 (1.6)
$SU_n$	gruppo unitario speciale, cap. 8 (1.8)
$T$	gruppo tetraedrale, cap. 5 (9.1)
$t$	(apice $t$ ) trasposizione di una matrice, cap. 1 (2.24)
$\text{tr}$	traccia, cap. 4 (4.18)
$U_n$	gruppo unitario, cap. 7 (4.15), cap. 8 (1.8)
$Z$	centro di un gruppo, cap. 2 (4.10)
$\mathbb{Z}$	anello degli interi, cap. 2 (1.11)
$Z(x)$	centralizzante di $x$ , cap. 6 (1.5)

*	Se $A$ è una matrice complessa, $A^* = \overline{A}^\dagger$
$\oplus$	l'apice * indica un gruppo moltiplicativo
$!$	nel diagramma di una matrice, * indica un elemento generico, cap. 1 (1.15)
$\binom{n}{k}$	somma diretta, cap. 3 (6.4), cap. 12 (6.3)
$[\mu]$	fattoriale, $n!$ è il prodotto degli interi $1, \dots, n$
	coefficiente binomiale, app. (2.1)
	parte intera di $\mu$ , il più grande intero $\leq \mu$ , cap. 11 (10.23).

Se  $S$  e  $T$  sono insiemi, usiamo le seguenti notazioni:

$ S $	il numero degli elementi, ovvero l'ordine, di $S$
$s \in S$	$s$ è un elemento di $S$ .
$S \subset T$	$S$ è un sottoinsieme di $T$ , ovvero $S$ è contenuto in $T$ . In altre parole, ogni elemento di $S$ è anche un elemento di $T$ .
$T \supset S$	$T$ contiene $S$ , cioè $S \subset T$ .
$S < T$	$S$ è un sottoinsieme proprio di $T$ , cioè è un sottoinsieme, e $T$ contiene un elemento che non appartiene a $S$ .
$T > S$	significa $S < T$ .
$T - S$	questa notazione è usata quando $S$ è un sottoinsieme di $T$ , e denota l'insieme degli elementi che sono in $T$ ma non in $S$ :

$$T - S = \{x \mid x \in T \text{ ma } x \notin S\}.$$

$S \cap T$	l'intersezione degli insiemi $S$ e $T$ , cioè l'insieme degli elementi in comune tra $S$ e $T$ .
$S \cup T$	l'unione degli insiemi $S$ e $T$ , cioè l'insieme degli elementi contenuti in almeno uno degli insiemi $S$ e $T$ .
$S \times T$	l'insieme prodotto. I suoi elementi sono le coppie ordinate $(s, t)$ :

$$S \times T = \{(s, t) \mid s \in S, t \in T\}.$$

$\varphi : S \rightarrow T$	un'applicazione $\varphi$ da $S$ a $T$ , o una funzione il cui dominio è $S$ e il codominio è $T$ .
$s \mapsto t$	indica che l'applicazione in questione manda l'elemento $s$ nell'elemento $t$ , cioè $\varphi(s) = t$ .
■	indica che una digressione nel testo, come un esempio o una dimostrazione, è finita, e si riprende il filo del discorso.

## Suggerimenti per ulteriori letture

### OPERE GENERALI

- G. Birkhoff e S. MacLane, *A Survey of Modern Algebra*, Macmillan, New York 3<sup>a</sup> ed. 1965.  
 I.N. Herstein, *Topics in Algebra*, Wiley, New York 2<sup>a</sup> ed. 1975 [trad. it. *Algebra*, Editori Riuniti, Roma 1982].  
 N. Jacobson, *Basic Algebra I, II*, Freeman, San Francisco 1974, 1980.  
 S. Lang, *Algebra*, Addison-Wesley, Reading (MA) 2<sup>a</sup> ed. 1965.  
 H. Paley e P.M. Weichsel, *Elements of Abstract and Linear Algebra*, Holt, Reinhart & Winston, New York 1972.  
 B.L. van der Waerden, *Modern Algebra*, Ungar, New York 1970.

### STORIA DELLA MATEMATICA

- N. Bourbaki, *Éléments d'histoire des mathématiques*, Hermann, Paris 1960 [trad. it. *Elementi di storia della matematica*, Feltrinelli, Milano 1963].  
 H. Edwards, *Fermat's Last Theorem*, Springer, New York 1977.  
 H. Edwards, *Galois Theory*, Springer, New York 1984.  
 Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford, New York 1972 [trad. it. *Storia del pensiero matematico*, a cura di A. Conte, Einaudi, Torino 1991].  
 B.L. van der Waerden, *A History of Algebra*, Springer, Berlin, New York 1985.

### CAPITOLO 1

- T. Muir, *A Treatise on the Theory of Determinants*, Dover, New York 1960.

### CAPITOLO 2

- I.N. Herstein, *Topics in Algebra*, Wiley, New York 2<sup>a</sup> ed. 1975.

### CAPITOLI 3 E 4

- G. Strang, *Linear Algebra and Its Applications*, Harcourt Brace Jovanovich, San Diego 3<sup>a</sup> ed. 1988.

## CAPITOLO 5

- C.T. Benson e L.C. Grove, *Finite Reflection Groups*, Springer, New York 2<sup>a</sup> ed. 1985.  
 H.M.S. Coxeter, *Introduction to Geometry*, Wiley, New York 1961.  
 L. Ford, *Automorphic Functions*, Chelsea, New York 1929.  
 B. Grünbaum e G.C. Sheppard, *Tilings and Patterns*, Freeman, New York 1967.  
 H.W. Guggenheimer, *Plane Geometry and Its Groups*, Holden-Day, San Francisco 1967.

## CAPITOLO 7

- B. Noble, *Applied Linear Algebra*, Prentice Hall, Englewood Cliffs (NJ) 2<sup>a</sup> ed. 1977.

## CAPITOLO 8

- R. Howe, *Very Basic Lie Theory*, Math. Monthly, **90** (1983) 600-23.  
 F. Warner, *Foundations of Differential Geometry and Lie Groups*, Springer, New York 1983.  
 H. Weyl, *The Classical Groups*, Princeton University Press, Princeton 1946.

## CAPITOLO 9

- J.-P. Serre, *Linear Representations of Finite Groups*, Springer, New York 1977.

## CAPITOLO 10

- K. Kendig, *Elementary Algebraic Geometry*, Springer, New York 1976.  
 E. Landau, *Foundations of Analysis*, Chelsea, New York 1960.

## CAPITOLO 11

- Z.I. Borevič e I.R. Šafarevitč, *Number Theory*, Academic Press, New York 1966.  
 H. Edwards, *Fermat's Last Theorem*, Springer, New York 1977.  
 K.F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801.  
 H. Hasse, *Number Theory*, Springer, New York 1980.  
 J.-P. Serre, *A Course in Arithmetic*, Springer, New York 1973.  
 H. Stark, *An Introduction to Number Theory*, MIT. Press, Cambridge (MA) 1978.

## CAPITOLO 13

- G.A. Bliss, *Algebraic Functions*, AMS Colloquium Publications No. XVI, New York 1933.

## CAPITOLO 14

- H. Edwards, *Galois Theory*, Springer, New York 1984.

## APPENDICE

- J.R. Munkres, *Topology; A First Course*, Prentice Hall, Englewood Cliffs (NJ) 1975.  
 W. Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, New York 3<sup>a</sup> ed. 1976.

## Indice analitico

- Abel, 668
- Addizione:
  - in un anello, 411
  - in un campo, 99
  - di matrici, 2
  - in un modulo, 532
  - di vettori, 94, 103
- Aggiunzione:
  - di un elemento, 431
  - simbolica, 596
- Algebra di Lie, 346
- Algebra, teorema fondamentale dell', 619
- Algebricamente dipendente, 617
- Algebricamente indipendente, 617
- Algoritmo di Todd-Coxeter, 265
- Analisi dei casi, 691
- Anello, 410
  - commutativo, 411
  - degli interi, 413, 489
  - noetheriano, 552
  - non commutativo, 412
  - nullo, 412
  - prodotto, 450
  - quoziente, 426
- Angolo:
  - tra vettori, 150, 295
  - trisezione, 594
- Annulatore:
  - di una forma, 290
  - di un  $R$ -modulo, 570
- Antilinearità, 297
- Antipodale, punto, 329
- Applicazione, 686
- Applicazione:
  - biettiva, 687
  - continua, 698
  - identica, 47
  - iniettiva, 687
- lineare, 131
- nulla, 419
- suriettiva, 687
- Arco, 92
- Aritmetica modulare, 75
- Aritmetica, teorema fondamentale dell', 462
- Assioma:
  - di induzione, 413
  - della scelta, 121, 443, 690
- Assiomi di Peano, 413
- Automorfismo:
  - di un'estensione di campi, 631
  - di un gruppo, 59
- Autovalore, 140
- Autovettore, 140
- Azione:
  - di un gruppo, 209, 367
  - fedele, 217
  - parziale, 270
  - transitiva, 210
  - a sinistra, 209
- Baker, 492
- Base:
  - cambiamento di, 117
  - canonica, 30, 108, 536
  - di un modulo, 536
  - ortogonale, 291
  - ortonormale, 151, 286, 300
  - di un reticolato, 200
  - simplettica, 310
  - di uno spazio vettoriale, 107
  - teorema della, di Hilbert, 553
  - di trascendenza, 617
- Bezout, numero di, 445
- Büezione, 687
- Blocchi:
  - di Jordan, 565
  - moltiplicazione per, 9