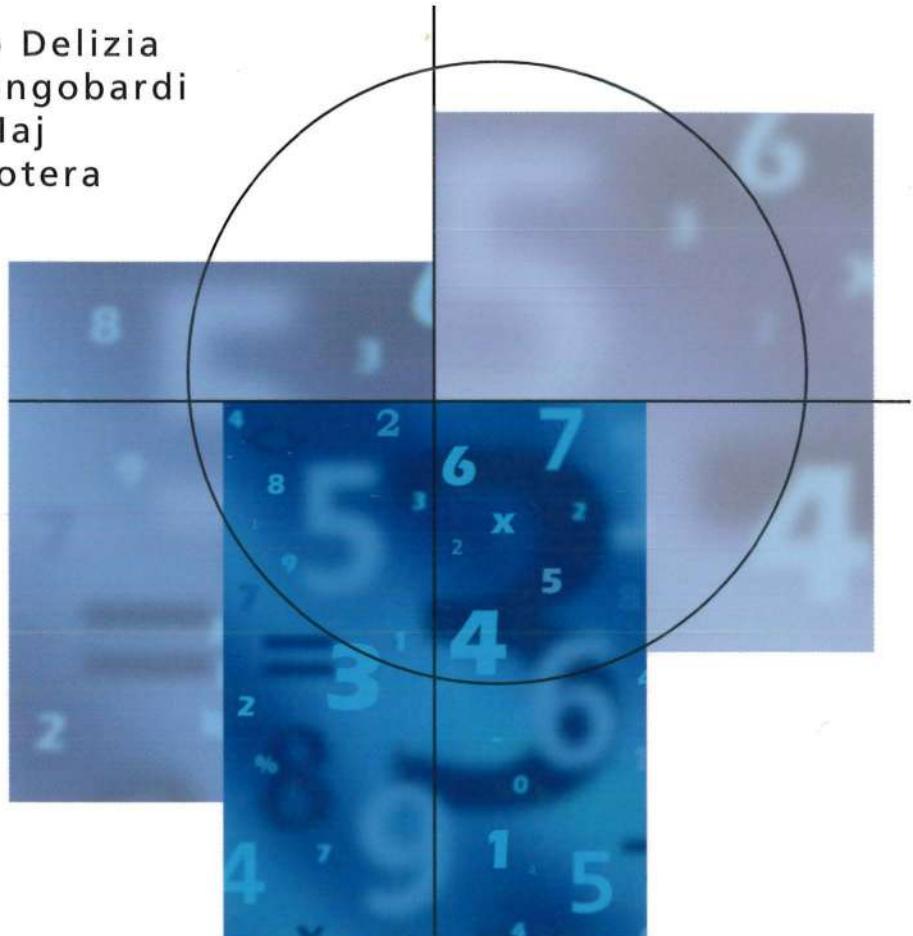


Costantino Delizia  
Patrizia Longobardi  
Mercede Maj  
Chiara Nicotera



# Matematica discreta

---

---

**McGraw-Hill**

web site 

**collana di istruzione scientifica**  
**serie di matematica**

# **Analisi matematica**



Costantino Delizia  
Patrizia Longobardi  
Mercede Maj  
Chiara Nicotera

# Matematica discreta

McGraw-Hill

---

**Milano • New York • San Francisco • Washington D.C. • Auckland**  
**Bogotá • Lisboa • London • Madrid • Mexico City • Montreal**  
**New Delhi • San Juan • Singapore • Sydney • Tokyo • Toronto**

McGraw-Hill  
Publishing Group Italia  
via Ripamonti, 89 - 20139 Milano

Copyright © 2009 The McGraw-Hill Companies, srl  
Publishing Group Italia  
via Ripamonti, 89 - 20139 Milano

**McGraw-Hill**  
A Division of The McGraw-Hill Companies



I diritti di traduzione, di riproduzione, di memorizzazione elettronica  
e di adattamento totale e parziale con qualsiasi mezzo (compresi i microfilm  
e le copie fotostatiche) sono riservati per tutti i Paesi.

Nomi e marchi citati nel testo sono generalmente depositati o registrati  
dalle rispettive case produttrici.

Editor: Paolo Roncoroni  
Produzione: Donatella Giuliani  
Grafica di copertina: G&G  
Stampa: Arti Grafiche Murelli, Fizzonasco di Pieve Emanuele (MI)

ISBN 978-88-386-6512-7

Printed in Italy  
123456789AGMLIL32109

# Indice

---

Prefazione	ix
Ringraziamenti dell'Editore	xi
Elenco dei simboli e delle notazioni	xiii
<b>1 Teoria degli insiemi</b>	<b>1</b>
1.1 Nozioni fondamentali . . . . .	1
1.2 Alcuni insiemi numerici notevoli . . . . .	8
1.3 Il principio d'induzione . . . . .	20
1.4 Operazioni tra insiemi . . . . .	25
1.5 Prodotto cartesiano . . . . .	42
1.6 Esercizi di riepilogo . . . . .	47
<b>2 Relazioni tra insiemi</b>	<b>51</b>
2.1 Nozioni fondamentali . . . . .	51
2.2 Applicazioni . . . . .	60
2.3 Relazioni d'equivalenza e partizioni . . . . .	79
2.4 Relazioni d'ordine . . . . .	89
2.5 Esercizi di riepilogo . . . . .	105
<b>3 Elementi di calcolo combinatorio</b>	<b>111</b>
3.1 I principi di addizione e di inclusione-esclusione . . . . .	111
3.2 Il principio di moltiplicazione . . . . .	113
3.3 Il principio dei cassetti . . . . .	115
3.4 Permutazioni semplici e con ripetizioni . . . . .	118
3.5 Disposizioni semplici e con ripetizioni . . . . .	121
3.6 Combinazioni semplici e con ripetizioni . . . . .	123
3.7 I numeri di Stirling di seconda specie . . . . .	129
3.8 Cenni sulla teoria di Ramsey . . . . .	135
3.9 Esercizi di riepilogo . . . . .	138
<b>4 Strutture algebriche</b>	<b>143</b>
4.1 Generalità . . . . .	143
4.2 Sottostrutture e strutture quoziente . . . . .	156
4.3 Omomorfismi tra strutture . . . . .	162
4.4 Esercizi di riepilogo . . . . .	166

---

<b>5 Elementi di aritmetica</b>	<b>169</b>
5.1 I numeri naturali e la seconda forma del principio d'induzione . . . . .	169
5.2 Rappresentazione dei numeri naturali in base fissata . . . . .	173
5.3 I numeri interi . . . . .	175
5.4 Divisibilità tra interi . . . . .	178
5.5 Congruenze tra interi . . . . .	182
5.6 La funzione di Eulero . . . . .	188
5.7 Sistemi di equazioni congruenziali lineari . . . . .	191
5.8 I numeri razionali . . . . .	197
5.9 I numeri reali . . . . .	200
5.10 I numeri complessi . . . . .	206
5.11 Metodi di fattorizzazione . . . . .	209
5.12 Esercizi di riepilogo . . . . .	213
<b>6 Alcune strutture algebriche notevoli</b>	<b>215</b>
6.1 Semigruppi . . . . .	215
6.2 Monoidi . . . . .	218
6.3 Gruppi . . . . .	220
6.4 Gruppi di permutazioni . . . . .	231
6.5 Anelli, corpi e campi . . . . .	235
6.6 Anelli di polinomi . . . . .	244
6.7 Esercizi di riepilogo . . . . .	251
<b>7 L'algebra delle matrici</b>	<b>257</b>
7.1 Generalità . . . . .	257
7.2 Operazioni con le matrici . . . . .	261
7.3 Matrici a scala . . . . .	266
7.4 Determinante di una matrice quadrata . . . . .	273
7.5 Matrici invertibili . . . . .	278
7.6 Rango di una matrice . . . . .	282
7.7 Sistemi di equazioni lineari . . . . .	285
7.8 Autovalori e autovettori di una matrice . . . . .	295
7.9 Esercizi di riepilogo . . . . .	298
<b>8 Spazi vettoriali</b>	<b>305</b>
8.1 Generalità . . . . .	305
8.2 Sottospazi e generatori . . . . .	309
8.3 Dipendenza lineare, basi e dimensione . . . . .	314
8.4 Applicazioni lineari . . . . .	324
8.5 Somma diretta di sottospazi . . . . .	332
8.6 Matrice associata a un'applicazione lineare . . . . .	336
8.7 Ancora sui sistemi di equazioni lineari . . . . .	345
8.8 Diagonalizzazione di una matrice . . . . .	351
8.9 Esercizi di riepilogo . . . . .	360

---

<b>9 Elementi di geometria analitica</b>	<b>367</b>
9.1 Riferimenti affini nel piano e nello spazio . . . . .	367
9.2 Equazioni vettoriali di rette e piani . . . . .	374
9.3 Equazioni parametriche di rette e piani . . . . .	376
9.4 Equazioni cartesiane di rette e piani . . . . .	385
9.5 Equazione cartesiana della circonferenza . . . . .	388
9.6 Spazi vettoriali metrici . . . . .	391
9.7 Esercizi di riepilogo . . . . .	396
<b>10 Reticoli, grafi, alberi</b>	<b>399</b>
10.1 Reticoli . . . . .	399
10.2 Omomorfismi di reticolati . . . . .	403
10.3 Reticoli distributivi . . . . .	405
10.4 Algebre di Boole . . . . .	407
10.5 Anelli booleani . . . . .	409
10.6 Grafi . . . . .	413
10.7 Alberi . . . . .	420
10.8 Esercizi di riepilogo . . . . .	422
<b>A Cenni di logica proposizionale e predicativa</b>	<b>425</b>
<b>Bibliografia</b>	<b>435</b>
<b>Indice analitico</b>	<b>437</b>

# Prefazione

---

Questo testo nasce dalla nostra esperienza nei corsi di Matematica discreta per il Corso di laurea in Informatica e illustra gli argomenti che di solito vengono presentati in tali corsi o in corsi analoghi. In realtà esso si presta bene a essere utilizzato per qualunque corso che si ponga come obiettivo quello di fornire agli studenti conoscenze matematiche di base, abituandoli ad adottare un'impostazione rigorosa nell'approccio ai problemi.

I contenuti del libro sono per lo più di carattere elementare e spaziano da argomenti da sempre peculiari della Matematica discreta (insiemi, insiemi numerici, induzione, operazioni tra insiemi, corrispondenze, applicazioni, relazioni d'equivalenza, relazioni d'ordine, aritmetica, congruenze, aritmetica modulo  $m$ , reticolati, algebre di Boole, grafi, alberi), ad argomenti di Combinatoria (principi di addizione, di inclusione-esclusione e di moltiplicazione, permutazioni, disposizioni e combinazioni, con e senza ripetizioni), di Algebra (strutture algebriche con una o più operazioni, semigruppi, monoidi, gruppi, anelli, corpi, campi, anelli di polinomi), di Algebra Lineare (matrici, sistemi di equazioni lineari, spazi vettoriali, diagonalizzazione), di Geometria (equazioni vettoriali, parametriche e cartesiane di rette e piani, equazione cartesiana della circonferenza, spazi metrici).

La trattazione è sempre rigorosa ma non eccessivamente formale: per evitare di appesantire la presentazione, a volte abbiamo preferito illustrare solo l'idea fondamentale rinunciando a fornire tutti i dettagli. Per aiutare ulteriormente lo studente, abbiamo accompagnato la trattazione con esempi, numerosi e particolarmente curati, completando ciascun capitolo con un ricchissimo apparato di esercizi che ammontano a quasi 900: di alcuni esercizi inoltre viene presentato lo svolgimento completo, per altri viene fornito un suggerimento. In questo modo lo studente è guidato passo passo nella comprensione degli argomenti attraverso l'applicazione dei concetti appena studiati.

Il libro termina con un'appendice contenente cenni di logica proposizionale e predicativa. Anch'essa si chiude con una sezione di esercizi.

Con piacere ringraziamo i colleghi Francesco Bottacin e Luca Esposito: oltre a interessanti discussioni sui contenuti del testo, ci hanno fornito preziosi consigli su come risolvere numerosi problemi tecnici incontrati nella stesura del libro. Ringraziamo inoltre la collega Brunella Gerla, che con amicizia ha visionato l'Appendice A. Un grazie di cuore va poi ai giovani dottori Diana Imperatore, Carmela Sica, Antonio Tortora e Maria Tota, che con scrupolo, maturità e affetto hanno attentamente riletto tutti i capitoli, evitandoci tante imprecisioni e incongruenze.

Ovviamente il testo non sarà esente da imperfezioni, di cui ci scusiamo preventivamente; saremo sinceramente grati a chi vorrà segnalarcele.

Desideriamo infine ringraziare l'Editore per aver voluto fortemente questo progetto e il suo ufficio editoriale, in particolare Filippo Aroffo che, con simpatia e precisione, ci ha pazientemente assistito durante la preparazione del volume.

*Costantino Delizia  
Patrizia Longobardi  
Mercede Maj  
Chiara Nicotera*

**Informazioni per il Lettore.** All'interno di ciascun capitolo, i paragrafi sono numerati progressivamente: 2.5 indica al solito il quinto paragrafo del secondo capitolo. Per i risultati e gli esempi si è utilizzata una numerazione tripla: 2.5.3 indica il terzo risultato che compare nel quinto paragrafo del secondo capitolo. L'introduzione di esempi è sempre preceduta dalla scritta “Esempio” (talvolta “Esempi”). Un'analogia numerazione tripla è stata usata per le formule matematiche nel testo, quando queste devono essere successivamente richiamate. In tal caso però essa è racchiusa tra parentesi tonde: (2.5.3) indica pertanto una formula che compare nel quinto paragrafo del secondo capitolo, dopo (2.5.2), ed è quindi cosa ben distinta da 2.5.3. Infine, un'ulteriore numerazione tripla utilizzata per gli esercizi: questa si distingue facilmente dalle precedenti in quanto i numeri sono sempre preceduti dalla dicitura “Esercizio”.

## Ringraziamenti dell'Editore

---

L'Editore ringrazia i revisori che con le loro preziose indicazioni hanno contribuito alla realizzazione di *Matematica discreta*:

Francesco Bottacin, *Università degli Studi di Salerno*  
Cinzia Cerroni, *Università degli Studi di Palermo*  
Michele Crismale, *Università degli Studi di Bari*  
Mario Mainardis, *Università degli Studi di Udine*

# Elenco dei simboli e delle notazioni

---

$\in$	appartiene	1.1
$\subseteq$	incluso	1.1
$\subset$	incluso strettamente	1.1
$ , :$	tale che	1.1
$\emptyset$	insieme vuoto	1.1
$\Rightarrow$	implica	1.1, A
$\iff$	equivale a	1.1, A
$::=$	uguale per definizione	1.1
$: \iff$	se e solo se per definizione	1.1
$\forall$	per ogni	1.1, A
$\exists$	esiste	1.1, A
$\exists!$	esiste ed è unico	1.1, A
$ S $	ordine dell'insieme finito $S$	1.1
$\mathcal{P}(S), 2^S$	insieme delle parti dell'insieme $S$	1.1
$\mathbb{N}_0$	insieme dei numeri naturali	1.1, 1.2, 5.1
$\mathbb{N}$	insieme dei numeri naturali positivi	1.1, 1.2, 5.1
$\mathbb{Z}$	insieme dei numeri interi	1.1, 1.2, 5.3
$\mathbb{Q}$	insieme dei numeri razionali	1.1, 1.2, 5.8
$\mathbb{R}$	insieme dei numeri reali	1.1, 5.9
$\mathbb{C}$	insieme dei numeri complessi	1.1, 5.10
$\mathbb{P}$	insieme dei numeri naturali primi	1.2
$a b$	$a$ divide $b$	1.2
$ a $	valore assoluto di $a$	1.2
$m\mathbb{Z}$	insieme dei multipli interi di $m$	1.2
$\mathbb{N}_p, 2\mathbb{N}_0$	insieme dei numeri naturali pari	1.2

$\mathbb{N}_d$	insieme dei numeri naturali dispari	1.2
$S \cup T$	unione degli insiemi $S$ e $T$	1.4
$S \cap T$	intersezione degli insiemi $S$ e $T$	1.4
$S \setminus T$	complemento dell'insieme $T$ rispetto all'insieme $S$	1.4
$S \oplus T, S \Delta T$	unione disgiunta degli insiemi $S$ e $T$	1.4
$(x, y)$	coppia ordinata di prima componente $x$ e seconda componente $y$	1.5
$S \times T$	prodotto cartesiano degli insiemi $S$ e $T$	1.5
$S^n$	prodotto cartesiano di $n$ copie di $S$	1.5
$\Delta_S$	diagonale dell'insieme $S$	1.5
$\mathcal{R}$	relazione tra insiemi	2.1
$\mathcal{R}^{\text{op}}$	relazione opposta	2.1
$f : S \rightarrow T$	applicazione di $S$ in $T$	2.1
$f(x)$	immagine di $x$ nell'applicazione $f$	2.1, 2.2
$\text{id}_S$	applicazione identica dell'insieme $S$	2.2
$T^S$	insieme delle applicazioni di $S$ in $T$	2.2
$f(X)$	immagine dell'insieme $X$ nell'applicazione $f$	2.2
$\text{Im } f$	immagine dell'applicazione $f$	2.2
$f^{-1}(Y)$	controimmagine dell'insieme $Y$ nell'applicazione $f$	2.2
$f^{-1}$	inversa dell'applicazione biettiva $f$	2.2
$g \circ f$	applicazione composta di $f$ e $g$	2.2
$[x]_{\mathcal{R}}$	classe d'equivalenza di $x$ modulo $\mathcal{R}$	2.3
$S/\mathcal{R}$	insieme quoziente di $S$ modulo $\mathcal{R}$	2.3
$\mathcal{R}_f$	relazione determinata dall'applicazione $f$	2.3
$\min S$	minimo dell'insieme ordinato $S$	2.4
$\max S$	massimo dell'insieme ordinato $S$	2.4
$\inf X,$ $\inf_S X$	estremo inferiore di $X$ in $S$	2.4
$\sup X,$ $\sup_S X$	estremo superiore di $X$ in $S$	2.4

$n!$	fattoriale del numero naturale $n$	3.4
$\mathbb{S}_X$	insieme delle permutazioni dell'insieme $X$	3.4
$\mathbb{S}_n$	insieme delle permutazioni di $n$ oggetti	3.4
$d_{n,h}$	numero delle disposizioni di $n$ elementi su $h$ posti	3.5
$c_{n,h}$	numero delle combinazioni semplici di $n$ elementi ad $h$ ad $h$	3.6
$\binom{n}{h}$	coefficiente binomiale $n$ su $h$	3.6
$S(n, k)$	numero di Stirling di seconda specie relativo a $n$ e $k$	3.7
$B_n$	numero di Bell relativo a $n$	3.7
$[S]^k$	sottoinsieme di $\mathcal{P}(S)$ costituito dai sottoinsiemi di ordine $k$ di $S$	3.7
$U(S)$	insieme degli elementi simmetrizzabili del monoide $S$	4.2
$\simeq$	strutture algebriche isomorfe	4.3
$\overline{X}$	parte stabile generata da $X$	4.2, 6.1
$(c_s \dots c_1 c_0)_b$	rappresentazione di un numero naturale in base $b \geq 2$	5.2
$\text{rest}(a, b)$	resto della divisione euclidea tra i numeri interi $a$ e $b$	5.3
$D(a)$	insieme dei divisori del numero intero $a$	5.4
$\text{MCD}(a, b), (a, b)$	massimo comune divisore non negativo tra i numeri interi $a$ e $b$	5.4
$\text{mcm}(a, b)$	minimo comune multiplo non negativo tra i numeri interi $a$ e $b$	5.4
$a \equiv b \pmod{m}$	$a$ congruo a $b$ modulo $m$	5.5
$[x]_m$	classe d'equivalenza di $x$ modulo $m$	5.5
$\overline{x}$	classe di congruenza dell'intero $x$	5.5
$\mathbb{Z}_m$	insieme degli interi modulo $m$	5.5
$\mathbb{Z}_m^*$	insieme degli interi invertibili modulo $m$	5.5
$\varphi(m)$	indicatore di Gauss-Eulero	5.5
$\lfloor x \rfloor$	parte intera del numero reale $x$	5.8, 5.9
$[a, b]$	intervallo reale chiuso	5.9

$]a, b[$	intervallo reale aperto	5.9
$[a, b[, \ ]a, b]$	intervallo reale semiaperto	5.9
$]-\infty, a[, \ ]-\infty, a]$	intervallo reale inferiormente illimitato	5.9
$]a, +\infty[, \ [a, +\infty[$	intervallo reale superiormente illimitato	5.9
$\bar{\alpha}$	coniugato del numero complesso $\alpha$	5.10
$N(\alpha)$	norma del numero complesso $\alpha$	5.10
$A^+$	semigruppo delle parole sull'alfabeto $A$	6.1
$S^{(1)}$	monoide associato al semigruppo $S$	6.1
$A^*$	monoide delle parole sull'alfabeto $A$	6.2
$[X]$	sottomonoide generato da $X$	6.2
$\langle X \rangle$	sottogruppo (o sottospazio) generato da $X$	6.3, 8.2
$H \leq G$	$H$ sottogruppo di $G$	6.3
$\text{Ker } f, \ N_f$	nucleo dell'omomorfismo $f$	6.3
$xH, \ Hx$	laterali di $H$ in $G$ individuati da $x$	6.3
$ G : H $	indice di $H$ in $G$	6.3
$H \trianglelefteq G$	$H$ sottogruppo normale di $G$	6.3
$V_4$	gruppo di Klein	6.3
$\text{supp}(f)$	supporto della permutazione $f$	6.4
$\text{sign}(f)$	segnatura della permutazione $f$	6.4
$\mathbb{A}_n$	insieme delle permutazioni pari di $n$ oggetti	6.4
$\text{car } R, \ \text{char } R$	caratteristica dell'anello unitario $R$	6.5
$\text{GL}(2, R)$	gruppo generale lineare di dimensione 2 sull'anello $R$	6.5
$f(x)$	polinomio nell'indeterminata $x$	6.6
$v(f(x))$	grado del polinomio non nullo $f(x)$	6.6
$R[x]$	insieme dei polinomi in $x$ sull'anello $R$	6.6
$f'(x)$	polinomio derivato del polinomio $f(x)$	6.6
$(a_{ij})$	matrice in cui l'elemento di posto $(i, j)$ è $a_{ij}$	7.1
$A^{(i)}$	$i$ -esima riga della matrice $A$	7.1

$A_{(i)}$	$i$ -esima colonna della matrice $A$	7.1
$A^T$	matrice trasposta della matrice $A$	7.1
$M_{n,m}(R)$	insieme delle matrici $n \times m$ sull'anello $R$	7.2
$M_n(R)$	insieme delle matrici quadrate di ordine $n$ sull'anello $R$	7.2
$\delta_{ij}$	simbolo di Kronecker	7.2
$I_n$	matrice identica di ordine $n$ su un anello unitario	7.2
$A^r$	potenza non negativa della matrice quadrata $A$	7.2
$\sim$	matrici equivalenti	7.3
$E_h^\lambda, E_{hk}, E_{hk}^\lambda$	matrici elementari	7.3
$A_{hk}$	matrice che si ottiene da $A$ eliminandone la $h$ -esima riga e la $k$ -esima colonna	7.4
$\det A$	determinante della matrice quadrata $A$	7.4
$A^{-1}$	inversa della matrice non singolare $A$	7.5
$A_{j_1, \dots, j_h}^{i_1, \dots, i_h}$	sottomatrice quadrata di ordine $h$ della matrice $A$	7.6
$\rho(A)$	rango della matrice $A$	7.6
$p_A(x)$	polinomio caratteristico della matrice quadrata $A$	7.8, 8.8
$W_1 + W_2$	somma dei sottospazi $W_1$ e $W_2$	8.2
$\text{tr}(A)$	traccia della matrice quadrata $A$	8.3
$\dim_F V$	dimensione dello spazio vettoriale $V$ sul campo $F$	8.3
$W_1 \oplus W_2$	somma diretta dei sottospazi $W_1$ e $W_2$	8.5
$\text{Hom}_F(V_1, V_2)$	insieme degli $F$ -omomorfismi di $V_1$ in $V_2$	8.6
$v_\lambda$	molteplicità algebrica dell'autovalore $\lambda$	8.8
$\mu_\lambda$	molteplicità geometrica dell'autovalore $\lambda$	8.8
$W_\lambda$	autospazio relativo all'autovalore $\lambda$	8.8
$\mathcal{E}^2$	insieme dei punti del piano euclideo	9.1
$\mathcal{E}^3$	insieme dei punti dello spazio euclideo	9.1

$\overrightarrow{OA}$	vettore applicato nel punto $O$	9.1
$\mathcal{V}_O^2$	insieme dei vettori applicati nel punto $O$ di $\mathcal{E}^2$	9.1
$\mathcal{V}_O^3$	insieme dei vettori applicati nel punto $O$ di $\mathcal{E}^3$	9.1
$\overline{PQ}$	segmento di estremi $P$ e $Q$	9.1
$ PQ $	lunghezza del segmento $\overline{PQ}$	9.1
$PQ$	retta per i punti $P$ e $Q$	9.1
$A\widehat{OB}$	angolo convesso di vertice $O$ e lati $\overline{OA}$ e $\overline{OB}$	9.1
$\mathcal{RA}(O, \underline{i}, \underline{j})$	riferimento affine del piano	9.1
$\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$	riferimento affine dello spazio	9.1
$\mathcal{V}_O$	insieme dei vettori del piano o dello spazio applicati nel punto $O$	9.1
$\tau_v$	traslazione relativa al vettore $\underline{v}$	9.1
$\ \underline{v}\ $	norma del vettore $\underline{v}$	9.5, 9.6
$d(P, Q)$	distanza tra i punti $P$ e $Q$	9.5, 9.6
$\Gamma(P, r)$	circonferenza di centro $P$ e raggio $r$	9.5
$\langle \underline{v}_1, \underline{v}_2 \rangle$	prodotto scalare dei vettori $\underline{v}_1$ e $\underline{v}_2$	9.6
$V^\perp$	nucleo di un prodotto scalare in $V$	9.6
$d(\underline{v}, \underline{w})$	distanza tra i vettori $\underline{v}$ e $\underline{w}$	9.6
$\vee$	unione reticolare, “OR”	10.1, A
$\wedge$	intersezione reticolare, “AND”	10.1, A
$L(G)$	insieme dei sottogruppi del gruppo $G$	10.1
$i$	unità immaginaria	10.5
$d(v)$	grado del vertice $v$ di un grafo finito	10.6
$\neg$	negazione, “NOT”	A

# Teoria degli insiemi

---

*In questo capitolo vengono presentati elementi della cosiddetta “teoria ingenua” degli insiemi, in cui si danno per intuitivi i concetti principali, evitando di ricorrere ad assiomi (come si fa invece nella cosiddetta “teoria assiomatica” degli insiemi) per i quali si rimanda a testi e a corsi più indicati. Per gli scopi che ci si prefigge tale teoria ingenua non preclude alcuno sviluppo e permette di evitare al Lettore difficoltà formali al momento non essenziali.*

## 1.1 Nozioni fondamentali

Col termine **insieme** si intende una collezione di oggetti, che vengono detti gli **elementi** dell’insieme. Di solito un insieme viene indicato con una lettera maiuscola:  $S$  (dal termine inglese “set”),  $T$ ,  $W$ , ..., mentre gli elementi vengono spesso denotati con lettere minuscole:  $x$ ,  $y$ ,  $z$ , .... Per indicare che  $x$  è elemento dell’insieme  $S$  si scrive:  $x \in S$  (o  $S \ni x$ ) e si legge: “ $x$  appartiene a  $S$ ”. In caso contrario si barra il simbolo:  $x \notin S$  (o  $S \not\ni x$ ) e si dice che “ $x$  non appartiene a  $S$ ”.

Spesso si assegna un insieme elencando tra parentesi graffe i suoi elementi, per esempio  $V = \{a, e, i, o, u\}$  è l’insieme i cui elementi sono:  $a, e, i, o, u$ ; si ha cioè  $a \in V$ ,  $e \in V$ ,  $i \in V$ ,  $o \in V$ ,  $u \in V$  e, per esempio,  $b \notin V$ . Gli elementi di uno stesso insieme possono essere di natura diversa, per esempio si può considerare l’insieme i cui elementi sono: questo testo, colui che lo sta leggendo in questo momento e il numero 6; o anche  $K = \{7, d, \Delta, i, *\}$ . Inoltre non è importante l’ordine con cui gli elementi sono elencati, per esempio  $\{d, \Delta, *, 7, i\}$  è ancora l’insieme  $K$ , in quanto gli elementi che lo costituiscono sono sempre  $7, d, \Delta, i, *$ . Né ripetizioni di uno stesso elemento alterano l’insieme: per esempio  $K = \{d, i, \Delta, 7, \Delta, *\}$ , in quanto gli elementi di  $\{d, i, \Delta, 7, \Delta, *\}$  sono  $7, d, \Delta, i, *$ .

Un insieme costituito da un solo elemento viene detto **singleton**: per esempio  $\{c\}$  è il singleton di  $c$ , cioè l’insieme costituito dal solo  $c$ , e si ha:  $c \in \{c\}$ ,  $x \notin \{c\}$ , per qualunque  $x \neq c$ .

Risulta opportuno considerare l’insieme privo di elementi: questo viene indicato con  $\emptyset$  e detto l’**insieme vuoto**. Si ha quindi  $x \notin \emptyset$ , per ogni  $x$ .

Insiemi numerici di utilizzo molto frequente vengono convenzionalmente denotati con lettere particolari. Per esempio  $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$  è l'insieme dei numeri naturali,  $\mathbb{N} = \{1, 2, 3, \dots\}$  l'insieme dei numeri naturali diversi da 0,  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$  l'insieme dei numeri interi (dal tedesco "Zahlen", che significa "numeri"),  $\mathbb{Q}$  l'insieme dei numeri razionali,  $\mathbb{R}$  l'insieme dei numeri reali,  $\mathbb{C}$  l'insieme dei numeri complessi.

Per assegnare un insieme, invece di elencarne gli elementi, il che non è sempre possibile o conveniente, si può precisare una proprietà di cui godono tutti e soli gli elementi dell'insieme. Per esempio, l'insieme  $V$  prima considerato può essere descritto come l'insieme costituito da tutti e soli gli elementi che sono vocali dell'alfabeto italiano, cioè da tutti gli  $x$  tali che  $x$  è una vocale dell'alfabeto italiano, e denotato nel seguente modo:

$$V = \{x : x \text{ vocale dell'alfabeto italiano}\}.$$

Pertanto  $u \in V$  in quanto vocale dell'alfabeto italiano,  $s \notin V$  non essendo vocale dell'alfabeto italiano. L'espressione "tale che" è di solito denotata con uno dei simboli ":" oppure "|".

Se l'insieme  $S$  è assegnato mediante la proprietà  $P$ , ossia

$$S = \{x : x \text{ gode di } P\},$$

gli elementi di  $S$  sono tutti e soli quelli che godono di  $P$ . In particolare:

$$\begin{aligned} \mathbb{N}_0 &= \{x : x \text{ numero naturale}\}, \\ \mathbb{N} &= \{x : x \text{ numero naturale, } x \neq 0\}, \\ \mathbb{Z} &= \{x : x \text{ numero intero relativo}\}, \\ \mathbb{Q} &= \{x : x \text{ numero razionale}\}, \\ \mathbb{R} &= \{x : x \text{ numero reale}\}, \\ \mathbb{C} &= \{x : x \text{ numero complesso}\}, \end{aligned}$$

e, per esempio:  $-6 \notin \mathbb{N}_0$  in quanto  $-6$  non è un numero naturale,  $-15 \in \mathbb{Z}$  in quanto  $-15$  è un numero intero.

È facile osservare che una tale proprietà  $P$  non è univocamente determinata; per esempio si ha:

$$\begin{aligned} V &= \{x : x \text{ vocale della parola "aiuole"}\} \\ &= \{x : x \text{ I o V o IX o XIII o XIX lettera dell'alfabeto italiano}\}, \end{aligned}$$

e così

$$\begin{aligned} \emptyset &= \{x : x \text{ triangolo con quattro lati}\} \\ &= \{x : x \text{ vocale in "pff"}\}. \end{aligned}$$

Anche la nozione di insieme **finito** viene qui assunta come intuitiva. Se  $S$  è un insieme finito, col simbolo  $|S|$  viene denotato l'**ordine** di  $S$ , cioè il numero dei

suoi elementi. Pertanto  $|\emptyset| = 0$ ,  $|\{x\}| = 1$ ,  $|V| = 5$  con  $V$  insieme prima considerato, e, se con  $A$  si indica l'insieme delle lettere dell'alfabeto italiano,  $|A| = 21$ . Un insieme non finito viene detto **infinito**; tali risultano per esempio gli insiemi:  $\mathbb{N}_0, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

Si noti che un insieme può avere elementi che sono a loro volta insiemi. Per esempio ha senso considerare l'insieme:  $\mathcal{H} = \{1, 2, b, \{a\}, \mathbb{Z}, \sqrt{3}, \emptyset\}$ , e si ha  $2 \in \mathcal{H}, \mathbb{Z} \in \mathcal{H}, -3 \notin \mathcal{H}, \mathbb{N} \notin \mathcal{H}, a \notin \mathcal{H}, \{a\} \in \mathcal{H}$ .

Insiemi  $S$  e  $T$  sono detti **uguali**, e si scrive  $S = T$ , se hanno gli stessi elementi, cioè se si ha:  $x \in S$  se e solo se  $x \in T$ . L'espressione "se e solo se" viene spesso sostituita dal simbolo  $\iff$ , che si legge anche "equivale a", "è equivalente a". Pertanto:

$$S = T \iff (x \in S \iff x \in T).$$

Per negare l'equivalenza, come al solito, si barra il simbolo:

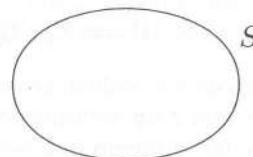
$$\not\iff.$$

Qualora si stia dando una definizione, il simbolo  $\iff$  viene preceduto da ":" , dando luogo al simbolo

$$:\iff$$

un'analogia convenzione si usa con il simbolo  $=$ , che diventa  $:=$ .

Per rappresentare un insieme si usano a volte i cosiddetti **diagrammi di Venn**: si indica un insieme  $S$  con la parte di piano racchiusa nella figura seguente:



Tale rappresentazione ovviamente è ben lungi dall'essere rigorosa, ma risulta spesso efficace per evidenziare graficamente alcune definizioni e legami tra insiemi.

Se  $S$  e  $T$  sono insiemi, si dice che  $S$  è **contenuto** (o **incluso**) in  $T$  se ogni elemento di  $S$  è elemento di  $T$ . Si dice anche che  $S$  è un **sottoinsieme** di  $T$  o una **parte** di  $T$ , e si scrive  $S \subseteq T$ , o ancora che  $T$  **contiene**  $S$ , e si scrive anche  $T \supseteq S$ . Quindi riesce:

$$S \subseteq T : \iff \text{per ogni } x \in S, x \in T.$$

Le espressioni "per ogni", "qualunque sia" vengono di solito rappresentate col simbolo  $\forall$ , detto anche il **quantificatore universale**. Pertanto:

$$S \subseteq T : \iff \forall x \in S, x \in T.$$

Per esempio, con  $V$  e  $A$  definiti come sopra, risulta  $V \subseteq A$ , in quanto  $a \in A$ ,  $e \in A$ ,  $i \in A$ ,  $o \in A$ ,  $u \in A$ , o anche in quanto ogni  $x \in V$  è una vocale dell'alfabeto italiano, e dunque è anche una lettera dell'alfabeto italiano, sicché  $x \in A$ . Così  $\mathbb{N} \subseteq \mathbb{N}_0$  perché ogni numero naturale  $\neq 0$  è un numero naturale,  $\mathbb{N}_0 \subseteq \mathbb{Z}$  perché ogni numero naturale è un numero intero,  $\mathbb{Z} \subseteq \mathbb{Q}$ ,  $\mathbb{Q} \subseteq \mathbb{R}$ ,  $\mathbb{R} \subseteq \mathbb{C}$ .

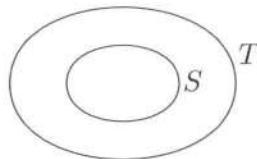
Ovviamente, qualunque sia l'insieme  $S$ , si ha:

$$\emptyset \subseteq S, \quad (1.1.1)$$

$$S \subseteq S, \quad (1.1.2)$$

$$\{x\} \subseteq S, \text{ per ogni } x \in S. \quad (1.1.3)$$

Se gli insiemi  $S$  e  $T$  sono indicati con diagrammi di Venn, l'essere  $S \subseteq T$  ha la seguente efficace rappresentazione:



Le espressioni “*implica*”, “*comporta*” sono spesso indicate col simbolo  $\implies$ , che si legge appunto “*implica*”, “*comporta*”. Che valga l'inclusione  $V \subseteq A$  può essere allora dimostrato nel seguente modo:  $x \in V \implies x$  vocale dell'alfabeto italiano  $\implies x$  lettera dell'alfabeto italiano  $\implies x \in A$ .

Proprietà  $P$  e  $Q$  tali che  $P \implies Q$  e  $Q \implies P$  sono equivalenti, cioè è soddisfatta l'una se e solo se è soddisfatta l'altra e si scrive  $P \iff Q$ . Pertanto

$$(P \iff Q) : \iff (P \implies Q \text{ e } Q \implies P).$$

Il negare che un'implicazione sussista si indica, come al solito, col simbolo barato  $\not\implies$ ; e così, se l'insieme  $S$  non è un sottoinsieme di  $T$  si scrive  $S \not\subseteq T$  (o  $T \not\supseteq S$ ). Per esempio:  $x$  lettera dell'alfabeto italiano  $\not\implies x$  vocale dell'alfabeto italiano.

In generale, se  $S$  e  $T$  sono insiemi, si ha:

$$S \not\subseteq T \iff \text{esiste } x \text{ tale che } x \in S \text{ e } x \notin T.$$

Si osservi che  $P \not\implies Q$  non equivale a ( $P$  vera  $\implies Q$  falsa): invero, ovviamente da ( $P$  vera  $\implies Q$  falsa) segue  $P \not\implies Q$ , ma non vale il viceversa. Per esempio,  $x \in A \not\implies x \in V$ , ma non è vero che  $x \in A \implies x \notin V$ . Pertanto, se si vuole dimostrare che  $P \not\implies Q$ , non è necessario provare che se  $P$  è vera allora  $Q$  è falsa (cioè, in generale, non è vero!), ma basta esibire un **controesempio**, ossia una situazione in cui  $P$  è vera ma  $Q$  è falsa. Così, per provare che  $x \in A \not\implies x \in V$  basta osservare che per esempio  $b \in A$  ma  $b \notin V$ .

Anche per l'espressione “*esiste*” c'è un simbolo particolare:  $\exists$ , detto il **quantificatore esistenziale**. E così, invece di “*non esiste*” spesso si usa  $\nexists$ . Quindi:

$$S \not\subseteq T \iff \exists x : x \in S \text{ e } x \notin T.$$

E, per esempio:

$$\begin{aligned} (\exists 0 : 0 \in \mathbb{N}_0 \text{ e } 0 \notin \mathbb{N}) &\implies \mathbb{N}_0 \not\subseteq \mathbb{N}, \\ (\exists -4 : -4 \in \mathbb{Z} \text{ e } -4 \notin \mathbb{N}_0) &\implies \mathbb{Z} \not\subseteq \mathbb{N}_0. \end{aligned}$$

A volte interviene l'espressione "esiste uno e un solo"; per questa si usa il simbolo  $\exists!$ .

Si osservi inoltre che, con  $S$  e  $T$  insiemi, si ha:

$$S = T \iff S \subseteq T \text{ e } T \subseteq S, \quad (1.1.4)$$

in quanto  $S$  e  $T$  hanno gli stessi elementi se e solo se ogni elemento di  $S$  è elemento di  $T$  e ogni elemento di  $T$  è elemento di  $S$ . Si ha allora:

$$S \neq T \iff S \not\subseteq T \text{ o } T \not\subseteq S.$$

Con  $S$ ,  $T$  e  $V$  insiemi, sussiste:

$$(S \subseteq T, T \subseteq V) \implies S \subseteq V \quad (\text{proprietà transitiva dell'inclusione}). \quad (1.1.5)$$

Infatti, se  $x \in S$ , si ha  $x \in T$  in quanto  $S \subseteq T$ , e da  $T \subseteq V$  segue poi  $x \in V$ .

Per esempio  $\mathbb{N} \subseteq \mathbb{Q}$  in quanto  $\mathbb{N} \subseteq \mathbb{N}_0$ ,  $\mathbb{N}_0 \subseteq \mathbb{Z}$ ,  $\mathbb{Z} \subseteq \mathbb{Q}$ .

Come immediata conseguenza di (1.1.4) e (1.1.5) si ha, con  $S$ ,  $T$  e  $V$  insiemi:

$$(S = T, T = V) \implies S = V \quad (\text{proprietà transitiva dell'uguaglianza}).$$

Se  $S$  e  $T$  sono insiemi, si dice che  $S$  è **contenuto strettamente** (o **incluso strettamente**) in  $T$ , e si scrive  $S \subset T$  o anche  $T \supset S$ , se  $S$  è contenuto in  $T$  ma è distinto da  $T$ :

$$S \subset T : \iff (S \subseteq T \text{ e } S \neq T).$$

Di conseguenza:

$$S \not\subset T \iff (S \not\subseteq T \text{ o } S = T).$$

È immediato verificare che:

$$S \subset T \iff (S \subseteq T \text{ e } T \not\subseteq S).$$

Pertanto:

$$S \subset T \iff (\forall x \in S, x \in T) \text{ e } (\exists y : y \in T \text{ e } y \notin S).$$

Per esempio  $\mathbb{N} \subset \mathbb{N}_0$ ,  $\mathbb{N}_0 \subset \mathbb{Z}$ . Ovviamente  $\emptyset \subset T$ , per ogni insieme  $T \neq \emptyset$ .

### 1.1.1. Con $S$ , $T$ e $V$ insiemi, risulta:

$$\begin{aligned} (S \subset T, T \subseteq V) &\implies S \subset V, \\ (S \subseteq T, T \subset V) &\implies S \subset V. \end{aligned}$$

*Dimostrazione.* Da  $S \subset T$  e  $T \subseteq V$  o da  $S \subseteq T$  e  $T \subset V$  segue  $S \subseteq T$ ,  $T \subseteq V$ , sicché  $S \subseteq V$  per la (1.1.5). Si supponga ora  $S \subset T$ . Allora esiste  $y$  tale che  $y \in T$  e  $y \notin S$ ; da  $T \subseteq V$  segue  $y \in V$  sicché esiste  $y$  tale che  $y \in V$  e  $y \notin S$ . Pertanto  $V \not\subseteq S$  e dunque  $S \subset V$ . Nell'ipotesi  $T \subset V$  si ha che esiste  $w$  tale che  $w \in V$  e  $w \notin T$ . Ovviamente  $w \notin S$  altrimenti da  $w \in S$  e  $S \subseteq T$  seguirebbe  $w \in T$  contro le ipotesi. Pertanto esiste  $w$  tale che  $w \in V$  e  $w \notin S$  e quindi  $V \not\subseteq S$  come volevasi.  $\square$

Sia  $S$  un insieme. L'**insieme delle parti** di  $S$ , denotato con  $\mathcal{P}(S)$ , è l'insieme costituito da tutti e soli i sottoinsiemi di  $S$ :

$$\mathcal{P}(S) := \{X : X \subseteq S\}.$$

Tale insieme viene anche detto l'**insieme potenza** di  $S$  e denotato con  $2^S$ . Ciò per evidenziare che, se  $S$  è un insieme finito, l'insieme  $\mathcal{P}(S)$ , ovviamente finito, ha ordine  $2^{|S|}$ , come verrà successivamente provato nel Capitolo 3. Quindi:

$$X \in \mathcal{P}(S) \iff X \subseteq S.$$

Per esempio, per ogni insieme  $S$ , da (1.1.1), (1.1.2) e (1.1.3) segue:

$$\emptyset \in \mathcal{P}(S), \tag{1.1.6}$$

$$S \in \mathcal{P}(S), \tag{1.1.7}$$

$$\{x\} \in \mathcal{P}(S), \text{ per ogni } x \in S. \tag{1.1.8}$$

Si noti in particolare che si ha  $\mathcal{P}(S) \neq \emptyset$ , per ogni insieme  $S$ .

## Esercizi

**Esercizio 1.1.1.** Siano  $A = \{a\}$ ,  $B = \{a, b\}$ ,  $C = \{a, b, c\}$ . Si determinino gli insiemni  $\mathcal{P}(A)$ ,  $\mathcal{P}(B)$ ,  $\mathcal{P}(C)$ .

*Svolgimento.* Si ha:

$$\mathcal{P}(A) = \{\emptyset, A\},$$

$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, B\},$$

$$\mathcal{P}(C) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, C\}.$$

**Esercizio 1.1.2.** Si verifichi che:

$$\mathcal{P}(\emptyset) = \{\emptyset\},$$

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\},$$

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

**Esercizio 1.1.3.** Si provi che, con  $S$  e  $T$  insiemni, si ha:

$$S \subseteq T \iff \mathcal{P}(S) \subseteq \mathcal{P}(T). \tag{1.1.9}$$

Se ne deduca che:

$$S = T \iff \mathcal{P}(S) = \mathcal{P}(T). \tag{1.1.10}$$

*Svolgimento.* Si supponga  $S \subseteq T$  e sia  $X \in \mathcal{P}(S)$ . Da  $X \subseteq S$  e  $S \subseteq T$  segue allora  $X \subseteq T$  per la (1.1.5) e dunque  $X \in \mathcal{P}(T)$ .

Viceversa, si supponga  $\mathcal{P}(S) \subseteq \mathcal{P}(T)$ . Da  $S \in \mathcal{P}(S)$  per la (1.1.7) e dalle ipotesi segue  $S \in \mathcal{P}(T)$  e dunque  $S \subseteq T$ .

La (1.1.10) segue poi subito da (1.1.9) e (1.1.4).

**Esercizio 1.1.4.** Si determinino i seguenti insiemi:

$$\begin{aligned} C &= \{x : x \text{ intero} : x^2 = 1\}, \\ D &= \{x : x \text{ intero} : x^2 = -1\}, \\ E &= \{x : x \text{ numero complesso} : x^2 = -1\}, \\ F &= \{x : x \text{ lettera di "nonno"}\}. \end{aligned}$$

**Esercizio 1.1.5.** Considerati gli insiemi

$$A = \{c, 4, \Delta, \emptyset, \{12\}, 12\}, \quad B = \{1, 0, f, \{\emptyset\}, \{d, 5\}, d\},$$

si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{llll} c \in A, & 1 \in A, & \{\Delta\} \in A, & \{12\} \in A, \\ 12 \in A, & \emptyset \in A, & \{\emptyset\} \in A, & \{12\} \subseteq A, \\ \{\{12\}\} \subseteq A, & \{c, 12\} \subseteq A, & \emptyset \subseteq A, & \{\emptyset\} \subseteq A, \\ \{\{\emptyset\}\} \subseteq A, & c \in B, & 1 \in B, & \{d, 5\} \in B, \\ \{d\} \in B, & f \in B, & \emptyset \in B, & \{\emptyset\} \in B, \\ \{1\} \subseteq B, & \{\{d\}\} \subseteq B, & \{c, 12\} \subseteq B, & \emptyset \subseteq B, \\ \{\emptyset\} \subseteq B, & \{\{\emptyset\}\} \subseteq B, & \{1, \{d, 5\}\} \subseteq B, & \{\{f\}\} \subseteq B, \\ \{\{1\}, 0\} \subseteq B, & \{f, \{\emptyset\}\} \subseteq B, & \{f, \emptyset\} \subseteq B, & \{f, d\} \subseteq B. \end{array}$$

**Esercizio 1.1.6.** Con  $S$  e  $T$  insiemi, si precisi se le seguenti affermazioni sono vere:

$$\begin{aligned} S \not\subseteq T &\iff \forall x \in S, x \notin T, \\ S \not\subseteq T &\iff \exists x \in S : x \notin T, \\ S \not\subseteq T &\iff \exists x \in T : x \notin S, \\ S \not\subseteq T &\iff \forall x \in T, x \notin S, \\ S \not\subset T &\iff S \neq T \text{ e } S \subseteq T, \\ S \not\subset T &\iff S \neq T \text{ o } S \not\subseteq T, \\ S \not\subset T &\iff S = T \text{ o } S \not\subseteq T, \\ S \not\subset T &\iff S \not\subseteq T \text{ e } T \subseteq S, \\ S \not\subset T &\iff S \subseteq T \text{ e } T \not\subseteq S, \\ S \not\subset T &\iff S \not\subseteq T \text{ o } T \subseteq S. \end{aligned}$$

**Esercizio 1.1.7.** Considerati gli insiemi  $L = \{11, 7\}$  e  $M = \{s, 8, \pi\}$  si determinino gli insiemi  $\mathcal{P}(L)$  e  $\mathcal{P}(M)$ .

**Esercizio 1.1.8.** Si verifichi se le seguenti affermazioni sono vere:

$$\begin{array}{lll} \mathbb{N} \in \mathcal{P}(\mathbb{N}_0), & \emptyset \in \mathcal{P}(\mathbb{N}_0), & \{\emptyset\} \in \mathcal{P}(\mathbb{N}_0), \\ \{0\} \in \mathcal{P}(\mathbb{N}_0), & \mathbb{N}_0 \in \mathcal{P}(\mathbb{N}_0), & 3 \in \mathcal{P}(\mathbb{N}_0), \\ \{3, \{4\}\} \in \mathcal{P}(\mathbb{N}_0), & 0 \in \mathcal{P}(\mathbb{N}_0), & \{10, 100\} \in \mathcal{P}(\mathbb{N}_0), \\ \{2, -3, 5\} \in \mathcal{P}(\mathbb{N}_0), & \mathbb{Z} \in \mathcal{P}(\mathbb{N}_0), & -3 \in \mathcal{P}(\mathbb{N}_0). \end{array}$$

**Esercizio 1.1.9.** Con  $S$  e  $T$  insiemi, si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{lll} \mathcal{P}(S) \not\subseteq \mathcal{P}(T) & \iff & \exists X \subseteq T : X \not\subseteq S, \\ \mathcal{P}(S) \not\subseteq \mathcal{P}(T) & \iff & \exists X \subseteq S : X \not\subseteq T, \\ \mathcal{P}(S) \not\subseteq \mathcal{P}(T) & \iff & \forall X \subseteq T, X \not\subseteq S, \\ \mathcal{P}(S) \not\subseteq \mathcal{P}(T) & \iff & \forall X \subseteq S, X \not\subseteq T. \end{array}$$

**Esercizio 1.1.10.** Si verifichi che, con  $S$  e  $T$  insiemi, si ha:

$$S \subseteq T \subseteq V \subseteq S \iff S = T = V.$$

**Esercizio 1.1.11.** Con  $S$  e  $T$  insiemi, si verifichi che  $\mathcal{P}(S) \subseteq \mathcal{P}(T) \implies S \subseteq T$  senza utilizzare la (1.1.7), provando che da  $x \in S$  segue  $x \in T$ .

**Esercizio 1.1.12.** Con  $S$  e  $T$  insiemi, si provi che  $S \subset T \iff \mathcal{P}(S) \subset \mathcal{P}(T)$  senza utilizzare la (1.1.10).

**Esercizio 1.1.13.** Si descriva l'insieme  $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ .

## 1.2 Alcuni insiemi numerici notevoli

Nei paragrafi seguenti del presente capitolo e nei successivi quattro capitoli saranno spesso utilizzate, in esempi ed esercizi, proprietà ben note dei numeri naturali o, più in generale, dei numeri interi o dei numeri razionali. Per agevolare il Lettore, queste vengono ora evidenziate senza alcuna pretesa di rigore o di completezza. Per uno studio più organico si rimanda al Capitolo 5.

### L'insieme $\mathbb{N}_0$ dei numeri naturali

Come già indicato nel precedente paragrafo, con i simboli  $\mathbb{N}_0$  ed  $\mathbb{N}$  si denotano rispettivamente l'insieme dei numeri naturali e quello dei numeri naturali diversi da 0:

$$\begin{aligned} \mathbb{N}_0 &= \{0, 1, 2, 3, \dots\}, \\ \mathbb{N} &= \{1, 2, 3, \dots\}. \end{aligned}$$

Si richiameranno ora alcune proprietà dei numeri naturali, certamente ben familiari al Lettore.

In  $\mathbb{N}_0$  sono definite una somma e un prodotto, denotate rispettivamente con i simboli  $+$  e  $\cdot$ , che godono delle seguenti notevoli proprietà:

$$a + b = b + a, \text{ per ogni } a, b \in \mathbb{N}_0 \quad (1.2.1)$$

(proprietà commutativa della somma),

$$(a + b) + c = a + (b + c), \text{ per ogni } a, b, c \in \mathbb{N}_0 \quad (1.2.2)$$

(proprietà associativa della somma),

$$0 + a = a + 0 = a, \text{ per ogni } a \in \mathbb{N}_0 \quad (1.2.3)$$

(0 elemento neutro per la somma),

$$a + b = 0 \text{ se e solo se } a = b = 0, \quad (1.2.4)$$

$$\text{da } a + c = b + c \text{ segue } a = b \quad (1.2.5)$$

(cancellabilità a destra rispetto alla somma),

$$\text{da } a + b = a + c \text{ segue } b = c \quad (1.2.6)$$

(cancellabilità a sinistra rispetto alla somma),

$$a \cdot b = b \cdot a, \text{ per ogni } a, b \in \mathbb{N}_0 \quad (1.2.7)$$

(proprietà commutativa del prodotto),

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \text{ per ogni } a, b, c \in \mathbb{N}_0 \quad (1.2.8)$$

(proprietà associativa del prodotto),

$$1 \cdot a = a \cdot 1 = a, \text{ per ogni } a \in \mathbb{N}_0 \quad (1.2.9)$$

(1 elemento neutro per il prodotto),

$$0 \cdot a = a \cdot 0 = 0, \text{ per ogni } a \in \mathbb{N}_0, \quad (1.2.10)$$

$$a \cdot b = 0 \text{ se e solo se } a = 0 \text{ o } b = 0 \quad (1.2.11)$$

(legge di annullamento del prodotto),

$$a \cdot b = 1 \text{ se e solo se } a = b = 1, \quad (1.2.12)$$

da  $a \cdot c = b \cdot c$ , con  $c \neq 0$ , segue  $a = b$  (1.2.13)  
*(cancellabilità a destra rispetto al prodotto),*

da  $a \cdot b = a \cdot c$ , con  $a \neq 0$ , segue  $b = c$  (1.2.14)  
*(cancellabilità a sinistra rispetto al prodotto),*

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ , per ogni  $a, b, c \in \mathbb{N}_0$  (1.2.15)  
*(proprietà distributiva a sinistra del prodotto rispetto alla somma),*

$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ , per ogni  $a, b, c \in \mathbb{N}_0$  (1.2.16)  
*(proprietà distributiva a destra del prodotto rispetto alla somma).*

Si noti che la commutatività della somma rende (1.2.5) e (1.2.6) equivalenti e, analogamente, la commutatività del prodotto fa sì che (1.2.13) e (1.2.14), e così (1.2.15) e (1.2.16), siano equivalenti. Si noti altresì che la (1.2.10) è contenuta nella (1.2.11). Infine si osservi che dalla (1.2.4) segue che:

$$\forall a \in \mathbb{N}, \nexists b \in \mathbb{N}_0 : a + b = 0, \quad (1.2.17)$$

e così, dalla (1.2.12) segue che:

$$\forall a \in \mathbb{N}_0, a \neq 1, \nexists b \in \mathbb{N}_0 : a \cdot b = 1. \quad (1.2.18)$$

Le proprietà (1.2.4) e (1.2.11) rispettivamente assicurano inoltre che:

$$\text{da } a, b \in \mathbb{N} \text{ segue } a + b \in \mathbb{N}, \quad (1.2.19)$$

$$\text{da } a, b \in \mathbb{N} \text{ segue } a \cdot b \in \mathbb{N}. \quad (1.2.20)$$

È poi opportuno evidenziare che le proprietà (1.2.2) e (1.2.8) permettono di scrivere  $a + b + c$  e  $a \cdot b \cdot c$  senza ambiguità, intendendo, rispettivamente,  $(a + b) + c$  o  $a + (b + c)$  e  $(a \cdot b) \cdot c$  o  $a \cdot (b \cdot c)$ .

Inoltre per ogni  $n \in \mathbb{N}$  e per ogni  $a \in \mathbb{N}_0$  si definisce **potenza**  $n$ -esima di  $a$  il prodotto

$$a^n := \underbrace{a \cdot a \cdot \dots \cdot a}_n.$$

Per convenzione si pone anche  $a^0 := 1$ . È immediato verificare che per ogni  $n, m, a, b \in \mathbb{N}_0$  si ha:

$$a^n \cdot a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad (1.2.21)$$

e

$$(ab)^n = a^n \cdot b^n. \quad (1.2.22)$$

Di solito, nel seguito, si preferirà scrivere  $ab$  in luogo di  $a \cdot b$  e, per esempio,  $ab + ac$  in luogo di  $(a \cdot b) + (a \cdot c)$ .

Nell'insieme  $\mathbb{N}_0$  è definito il cosiddetto “*ordine usuale*”, indicato col simbolo  $\leq$ . Con  $a, b \in \mathbb{N}_0$ , si pone

$$a \leq b : \iff \exists t \in \mathbb{N}_0 : b = a + t.$$

Si scrive anche  $b \geq a$ . Si noti che, per la (1.2.6), un tale  $t$ , quando esiste, è unico. È facile verificare che valgono le seguenti proprietà:

$$a \leq a, \text{ per ogni } a \in \mathbb{N}_0 \quad (\text{proprietà riflessiva}), \quad (1.2.23)$$

$$\text{da } a \leq b \text{ e } b \leq a \text{ segue } a = b \quad (\text{proprietà asimmetrica}), \quad (1.2.24)$$

$$\text{da } a \leq b \text{ e } b \leq c \text{ segue } a \leq c \quad (\text{proprietà transitiva}). \quad (1.2.25)$$

La (1.2.23) segue subito da (1.2.3), in quanto esiste  $0 \in \mathbb{N}_0$  tale che  $a = a + 0$ . Si supponga ora  $a \leq b$  e  $b \leq a$ , esistano quindi  $t, s \in \mathbb{N}_0$  tali che  $b = a + t, a = b + s$ ; ciò comporta  $b = (b + s) + t = b + (s + t)$ , per la (1.2.2), sicché  $b + 0 = b + (s + t)$ , da cui  $s + t = 0$  per la (1.2.6), pertanto  $s = t = 0$  per la (1.2.4) e quindi  $a = b$  per la (1.2.3): vale così la (1.2.24). Da  $a \leq b$  e  $b \leq c$  segue poi  $b = a + h$  e  $c = b + k$ , per opportuni  $h, k \in \mathbb{N}_0$ , sicché  $c = (a + h) + k = a + (h + k)$ , per la (1.2.2), pertanto  $a \leq c$ , il che prova la (1.2.25).

Si noti che:

$$0 \leq a, \text{ per ogni } a \in \mathbb{N}_0, \quad (1.2.26)$$

poiché  $a = a + 0$ , per la (1.2.3); ciò si esprime dicendo che 0 è “minimo” per l'ordine usuale. Ovviamente risulta poi:

$$a \leq a + 1, \text{ per ogni } a \in \mathbb{N}_0. \quad (1.2.27)$$

Si noti inoltre che:

$$\text{da } a \leq b, c \leq d \text{ segue } a + c \leq b + d, \quad (1.2.28)$$

$$\text{da } a \leq b, c \leq d \text{ segue } ac \leq bd. \quad (1.2.29)$$

Infatti, si supponga  $b = a + t$  e  $d = c + s$ , per opportuni  $t, s \in \mathbb{N}_0$ . Si ha allora  $b + d = (a + t) + (c + s) = a + (t + c) + s = a + (c + t) + s = (a + c) + (t + s)$ , per le (1.2.1) e (1.2.2), sicché  $a + c \leq b + d$ . Inoltre si ha  $bd = (a + t)(c + s) = ac + (as + tc + ts)$ , sicché  $ac \leq bd$ .

Per la (1.2.23), la (1.2.28) e la (1.2.29) comportano rispettivamente che:

$$\text{da } a \leq b \text{ segue } a + c \leq b + c \text{ e } c + a \leq b + c, \forall c \in \mathbb{N}_0, \quad (1.2.30)$$

$$\text{da } a \leq b \text{ segue } ac \leq bc \text{ e } ca \leq cb, \forall c \in \mathbb{N}_0. \quad (1.2.31)$$

Con  $a, b \in \mathbb{N}_0$ , si pone inoltre:

$$a < b : \iff (a \leq b \text{ e } a \neq b).$$

Ovviamente si ha  $a < b$  se e solo se esiste  $t \in \mathbb{N}$  tale che  $b = a + t$ . Per esempio  $0 < n$ , per ogni  $n \in \mathbb{N}$ , e  $a < a + 1$ , per ogni  $a \in \mathbb{N}_0$ .

Una notevole proprietà dell'ordine usuale in  $\mathbb{N}_0$  è la seguente: per ogni  $a, b \in \mathbb{N}_0$  risulta  $a \leq b$  oppure  $b \leq a$ . Più precisamente, vale la seguente:

**1.2.1. Proprietà di tricotomia.** *Per ogni  $a, b \in \mathbb{N}_0$  sussiste una e una sola delle seguenti:  $a < b$ ,  $b < a$ ,  $a = b$ .*

Se  $a, b \in \mathbb{N}_0$  sono tali che  $a \leq b$  è possibile definire  $b - a$  come quell'unico  $t \in \mathbb{N}_0$  tale che  $b = a + t$ . Si noti che:

$$a - a = 0, \text{ per ogni } a \in \mathbb{N}_0, \quad (1.2.32)$$

e che

$$b - 0 = b, \text{ per ogni } b \in \mathbb{N}_0. \quad (1.2.33)$$

**1.2.2.** *Se  $a, b, c \in \mathbb{N}_0$  sono tali che  $a \leq b$ , allora hanno senso  $bc - ac$  e  $cb - ca$  e si ha:*

$$(b - a)c = bc - ac \quad (1.2.34)$$

$$c(b - a) = cb - ca. \quad (1.2.35)$$

*Dimostrazione.* Per la (1.2.31) risulta  $ac \leq bc$  e  $ca \leq cb$ , sicché hanno senso  $bc - ac$  e  $cb - ca$ . Posto poi  $b = a + t$ , si ha che  $bc = (a + t)c = ac + tc$  per la (1.2.16) e  $cb = c(a + t) = ca + ct$  per la (1.2.15), pertanto  $bc - ac = tc = (b - a)c$  e  $cb - ca = ct = c(b - a)$ .  $\square$

Se  $a, b \in \mathbb{N}_0$ , si dice che  $a$  **divide**  $b$  se esiste  $k \in \mathbb{N}_0$  tale che  $b = ak$ . In tal caso si scrive  $a|b$ , e si dice anche che  $a$  è un **divisore** di  $b$ , o che  $b$  è un **multiplo** di  $a$  in  $\mathbb{N}_0$ . Si osservi in primo luogo che:

$$a|0, \text{ per ogni } a \in \mathbb{N}_0, \quad (1.2.36)$$

essendo  $0 = a0$  per la (1.2.10), e che:

$$0|b \text{ se e solo se } b = 0, \quad (1.2.37)$$

sempre per la (1.2.10). Si osservi poi che se  $b \neq 0$  e  $a|b$ , si ha  $a \neq 0$ , sicché, per la (1.2.14), risulta univocamente determinato l'elemento  $k \in \mathbb{N}_0$  tale che  $b = ak$ . Valgono le seguenti proprietà:

$$1|a, \text{ per ogni } a \in \mathbb{N}_0, \quad (1.2.38)$$

$$a|a, \text{ per ogni } a \in \mathbb{N}_0, \quad (\text{proprietà riflessiva}) \quad (1.2.39)$$

$$\text{da } a|b \text{ e } b|a \text{ segue } a = b, \quad (\text{proprietà asimmetrica}) \quad (1.2.40)$$

$$\text{da } a|b \text{ e } b|c \text{ segue } a|c, \quad (\text{proprietà transitiva}) \quad (1.2.41)$$

$$\text{se } a|b \text{ e } a|c, \text{ allora } a|b + c, \quad (1.2.42)$$

$$\text{se } a|b + c \text{ e } a|b, \text{ allora } a|c. \quad (1.2.43)$$

La (1.2.38) e la (1.2.39) sono ovvie conseguenze della (1.2.9). Si supponga ora  $b = ak$  e  $a = bh$ , per opportuni  $k, h \in \mathbb{N}_0$ . Dalla (1.2.10) segue subito che si ha  $a = 0$  se e solo se  $b = 0$ . Si suppongano pertanto  $a, b \neq 0$ . Da  $b1 = b = (bh)k = b(hk)$  segue allora  $hk = 1$  per la (1.2.14), sicché anche in tal caso  $a = b$ , e vale la (1.2.40). Da  $b = ak$  e  $c = bt$ , per opportuni  $k, t \in \mathbb{N}_0$  segue  $c = (ak)t = a(kt)$ , pertanto  $a|c$  e vale (1.2.41). Se poi  $b = ak$  e  $c = av$ , per opportuni  $k, v \in \mathbb{N}_0$ , riesce  $b+c = ak+av = a(k+v)$  per (1.2.15) e vale (1.2.42). Infine se  $b+c = as$  e  $b = ak$ , per opportuni  $s, k \in \mathbb{N}_0$ , si ha  $as = ak+c$ , sicché  $ak \leq as$  e  $c = as - ak = a(s-k)$  per la (1.2.35), e dunque  $a|c$ .

**1.2.3.** Con  $a, b, c, d \in \mathbb{N}_0$ , se  $a|b$  e  $c|d$  allora  $ac|bd$ . Ne segue che se  $a|b$  e  $n \in \mathbb{N}_0$  allora  $an|bn$ , e quindi anche  $a|bn$ .

*Dimostrazione.* Esercizio. □

Un numero naturale positivo  $p$  è detto un **numero primo** se è  $p \neq 1$  e gli unici divisori di  $p$  sono 1 e  $p$ . Un numero naturale non primo è detto **composto**. L'insieme dei numeri naturali primi viene di solito denotato col simbolo  $\mathbb{P}$ .

Notevoli proprietà relative ai primi, ben note al Lettore, e che saranno provate nel Capitolo 5, sono le seguenti:

**1.2.4.** Se  $p$  è un primo e  $p$  divide il prodotto  $ab$ , con  $a, b \in \mathbb{N}$ , allora  $p$  divide  $a$  o  $p$  divide  $b$ .

**1.2.5. Teorema fondamentale dell'aritmetica (in  $\mathbb{N}$ ).** Sia  $n \geq 2$  un numero naturale. Allora si ha  $n = p_1 p_2 \dots p_t$ , con  $t \geq 1$  e  $p_1, p_2, \dots, p_t$  primi. Inoltre tale scrittura è unica a meno dell'ordine dei fattori.

**Osservazione.** Da 1.2.5 segue in particolare che ogni  $n \in \mathbb{N}, n \geq 2$ , è sempre divisibile per un numero primo, e che ogni naturale ha un numero finito di divisori.

## L'insieme $\mathbb{Z}$ dei numeri interi

Con il simbolo  $\mathbb{Z}$  si denota l'insieme dei numeri interi:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}.$$

Come ben noto in  $\mathbb{Z}$  sono definite una somma e un prodotto, che, rispettivamente, estendono la somma e il prodotto in  $\mathbb{N}_0$  e che godono delle proprietà analoghe alle proprietà (1.2.1) – (1.2.3), (1.2.5) – (1.2.11), (1.2.13) – (1.2.16). Inoltre continuano a valere considerazioni e notazioni introdotte in  $\mathbb{N}_0$ . Si noti però che in  $\mathbb{Z}$  non valgono le analoghe della (1.2.4) e della (1.2.12). Infatti risulta

$$a + b = 0 \iff b = -a,$$

con la usuale convenzione che  $-0 = 0$  e  $-(-a) = a$ , per ogni  $a \in \mathbb{N}$ , e si ha inoltre

$$ab = 1 \iff a = b = 1 \text{ o } a = b = -1. \quad (1.2.44)$$

In particolare si ha che

$$\forall a \in \mathbb{Z}, \exists! b \in \mathbb{Z} : a + b = 0, \text{ con } b = -a. \quad (1.2.45)$$

Se  $a$  e  $b$  sono interi, è sempre possibile definire  $b - a$  ponendo:

$$b - a := b + (-a),$$

e valgono le proprietà analoghe a (1.2.32) e (1.2.33).

Si osservi che, se  $a, b \in \mathbb{N}_0$  e  $a \leq b$ , cioè  $b = a + t$  con  $t \in \mathbb{N}_0$ , si ha  $b + (-a) = a + t + (-a) = t + (a + (-a)) = t + 0 = t$ . Pertanto la definizione di sottrazione in  $\mathbb{Z}$  appena data generalizza quella data in  $\mathbb{N}_0$ .

**1.2.6.** Con  $a, b \in \mathbb{Z}$ , risulta:  $a(-b) = -(ab) = (-a)b$ .

*Dimostrazione.* Si ha:  $0 = a0 = a(b + (-b)) = ab + a(-b)$ , sicché da (1.2.45) segue  $a(-b) = -(ab)$ . Da  $0 = 0b = (a + (-a))b$  segue in maniera del tutto analoga  $(-a)b = -(ab)$ .  $\square$

**1.2.7.** Con  $a, b, c \in \mathbb{Z}$ , risulta:

$$a(b - c) = ab - ac, \quad (a - b)c = ac - bc \\ (\text{proprietà distributiva del prodotto rispetto alla sottrazione}).$$

*Dimostrazione.* Si ha  $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + ((-ac)) = ab - ac$ . Analogamente si prova l'altra uguaglianza.  $\square$

Per ogni  $n \in \mathbb{N}$  e per ogni  $a \in \mathbb{Z}$  si definisce la **potenza  $n$ -esima** di  $a$  il prodotto

$$a^n := \underbrace{a \cdot a \cdot \dots \cdot a}_n.$$

Per convenzione si pone anche  $a^0 := 1$ .

Ancora valgono le proprietà:  $a^n a^m = a^{n+m}$ ,  $(a^n)^m = a^{nm}$  e  $(ab)^n = a^n b^n$ , per ogni  $a, b \in \mathbb{Z}$  e  $n, m \in \mathbb{N}_0$ .

Anche in  $\mathbb{Z}$  è definito un “ordine usuale”, denotato ancora con  $\leq$ , e che estende l'ordine usuale di  $\mathbb{N}_0$ . Precisamente, con  $a, b \in \mathbb{Z}$ :

$$a \leq b : \iff \exists t \in \mathbb{N}_0 : b = a + t.$$

In tal caso si scrive anche  $b \geq a$ .

**1.2.8.** L'ordine usuale di  $\mathbb{Z}$  soddisfa proprietà analoghe alle (1.2.23) – (1.2.25), (1.2.27), (1.2.28) e (1.2.30).

*Dimostrazione.* Esercizio. □

Come in  $\mathbb{N}_0$ , così in  $\mathbb{Z}$  si pone:

$$a < b : \iff (a \leq b \text{ e } a \neq b),$$

sicché

$$a < b \iff \exists k \in \mathbb{N} : b = a + k.$$

In tal caso si scrive anche  $b > a$ . Si osservi che per ogni  $a \in \mathbb{Z}$  si ha:

$$a - 1 < a < a + 1. \quad (1.2.46)$$

Perciò in  $\mathbb{Z}$  non esiste un elemento “minimo”, non vale cioè l’analoga di (1.2.26). Continua però a valere la proprietà analoga di 1.2.1. Ciò comporta in particolare che l’ordine usuale di  $\mathbb{Z}$  è un ordine totale (vedi Paragrafo 2.4).

Da notare che in  $\mathbb{Z}$  non vale l’analoga di (1.2.29): per esempio si ha  $1 \leq 3$ ,  $-4 \leq -3$  e  $1(-4) \not\leq 3(-3)$ ; né l’analoga di (1.2.31), per esempio  $2 \leq 3$  ma  $3(-5) < 2(-5)$ . Più precisamente si ha:

**1.2.9.** Con  $a, b, c \in \mathbb{Z}$ , risulta:

$$a \leq b, 0 \leq c \implies ac \leq bc,$$

$$a \leq b, c < 0 \implies bc \leq ac,$$

$$a < b, 0 < c \implies ac < bc,$$

$$a < b, c < 0 \implies bc < ac.$$

Ne segue che:

$$0 \leq a \iff -a \leq 0,$$

e quindi anche:

$$a \leq 0 \iff 0 \leq -a,$$

e che:

$$0 \leq a, 0 \leq b \implies 0 \leq ab,$$

$$0 < a, 0 < b \implies 0 < ab,$$

$$0 \leq a, b \leq 0 \implies ab \leq 0,$$

$$0 < a, b < 0 \implies ab < 0,$$

$$a \leq 0, b \leq 0 \implies 0 \leq ab,$$

$$a < 0, b < 0 \implies 0 < ab.$$

*Dimostrazione.* Esercizio. □

Un numero intero  $a \neq 0$  viene detto **positivo** se  $a > 0$ , **negativo** se  $a < 0$ .

Di notevole interesse è la ben nota seguente definizione. Con  $a \in \mathbb{Z}$ , si pone:

$$|a| := \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$$

e  $|a|$  vien detto il **valore assoluto** di  $a$ .

Banalmente, per ogni  $a \in \mathbb{Z}$ , risulta  $|a| \geq 0$  e  $|a| = |-a|$ . È facile poi verificare che, per ogni  $a, b \in \mathbb{Z}$ :

$$|ab| = |a||b|, \quad (1.2.47)$$

$$|a+b| \leq |a| + |b|. \quad (1.2.48)$$

Anche il concetto del “divide” si estende a  $\mathbb{Z}$ , precisamente si pone:

$$a|b : \iff \exists k \in \mathbb{Z} : b = ak.$$

**1.2.10.** In  $\mathbb{Z}$  valgono le analoghe delle proprietà (1.2.36) – (1.2.39) e le analoghe delle (1.2.41) – (1.2.43). Inoltre, per ogni  $a, b \in \mathbb{Z}$ , si ha:

$$-1|a \iff (-a)|a, \quad (1.2.49)$$

$$a|b \iff (-a)|b, \quad (1.2.50)$$

$$a|b \iff a|(-b). \quad (1.2.51)$$

Non vale invece l’analoga di (1.2.40).

*Dimostrazione.* Esercizio. □

**1.2.11.** Con  $a, b \in \mathbb{Z}$ , risulta  $a|b$  e  $b|a \iff b = a$  oppure  $b = -a$ .

*Dimostrazione.* Si supponga  $b = ak$ ,  $a = bh$ , per opportuni  $k, h \in \mathbb{Z}$ . Si ottiene  $a = 0$  se e solo se  $b = 0$ . Se poi  $a, b \neq 0$ , si ottiene  $b1 = b = bhk$  da cui  $hk = 1$  e poi  $h = k = 1$  oppure  $h = k = -1$  per la (1.2.44), da cui  $b = a$  oppure  $b = -a$ . Il viceversa segue subito dalla proprietà riflessiva, da (1.2.49) e da (1.2.50). □

Se  $m \in \mathbb{Z}$  e  $X \subseteq \mathbb{Z}$  si pone:

$$mX := \{mx : x \in X\}.$$

Per esempio  $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\} = \{z \in \mathbb{Z} : m \text{ divide } z\}$ .

L’insieme  $2\mathbb{N}_0$  viene detto l’insieme dei **numeri naturali pari** e denotato anche con il simbolo  $\mathbb{N}_p$ . L’insieme dei numeri naturali che non sono pari è detto

insieme dei **numeri naturali dispari** ed è denotato con il simbolo  $\mathbb{N}_d$ . Pertanto si ha:

$$\mathbb{N}_p = \{2n : n \in \mathbb{N}_0\}, \quad \mathbb{N}_d = \{2n + 1 : n \in \mathbb{N}_0\}.$$

Da 1.2.9 e dalla definizione di potenza di un numero intero segue subito che la potenza  $n$ -esima di un numero intero negativo è positiva se  $n$  è pari, negativa se  $n$  è dispari.

### L'insieme $\mathbb{Q}$ dei numeri razionali

Come già precisato nel paragrafo precedente, il simbolo  $\mathbb{Q}$  denota l'insieme dei numeri razionali, cioè:

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\},$$

con l'usuale convenzione di identificare ogni intero  $m$  con il numero razionale  $\frac{m}{1}$ .

Nel Paragrafo 5.8 sarà illustrata una costruzione di tale insieme a partire da  $\mathbb{Z}$ . Per il momento ci si limita a evidenziare che:

$$\frac{m}{n} = \frac{a}{b} \text{ se e solo se } mb = na,$$

da cui segue facilmente:

$$\frac{m}{n} = \frac{mr}{nr}, \text{ per ogni } r \in \mathbb{Z}, r \neq 0.$$

Nell'insieme  $\mathbb{Q}$  sono definite un'operazione di somma e un'operazione di prodotto con le seguenti posizioni:

$$\frac{m}{n} + \frac{s}{t} := \frac{mt + ns}{nt}, \text{ per ogni } \frac{m}{n}, \frac{s}{t} \in \mathbb{Q},$$

$$\frac{m}{n} \cdot \frac{s}{t} := \frac{ms}{nt}, \text{ per ogni } \frac{m}{n}, \frac{s}{t} \in \mathbb{Q}.$$

Con l'identificazione prima introdotta tali operazioni estendono quelle di  $\mathbb{Z}$ .

### Esercizi

**Esercizio 1.2.1.** Si verifichi che, con  $a, b, c, d \in \mathbb{N}_0$ , risulta:

$$\begin{aligned} &\text{da } a \leq b, b < c \text{ segue } a < c, \\ &\text{da } a < b, b \leq c \text{ segue } a < c. \end{aligned}$$

Se ne deduca che  $a < b$  e  $b < c$  implicano  $a < c$ . Si provi poi che:

$$\text{da } a < b, c \leq d \text{ segue } a + c < b + d,$$

da  $a < b, c < d$  segue  $ac < bd$ ,

e inoltre:

da  $a < b$  segue  $a + k < b + k$ , per ogni  $k \in \mathbb{N}_0$ ,

da  $a < b$  segue  $ak < bk$ , per ogni  $k \in \mathbb{N}$ .

**Esercizio 1.2.2.** Si provi 1.2.3.

**Esercizio 1.2.3.** Siano  $a, b, c, d \in \mathbb{N}_0$  con  $a \leq b, c \leq b, a \leq d$ . Si provi che:

$$b - a = b - c \implies a = c,$$

$$b - a = d - a \implies b = d.$$

**Esercizio 1.2.4.** Si provi che in  $\mathbb{Z}$  la cancellabilità rispetto alla somma può essere derivata dalla (1.2.45).

**Esercizio 1.2.5.** Siano  $a, b, c \in \mathbb{Z}$ . Si verifichi che:

$$b - a = b - c \implies a = c,$$

$$b - a = c - a \implies b = c.$$

**Esercizio 1.2.6.** Siano  $a, b, c, d \in \mathbb{Z}$ . Si verifichi che:

$$\text{da } a \leq b, b < c \text{ segue } a < c,$$

$$\text{da } a < b, b \leq c \text{ segue } a < c.$$

Se ne deduca che  $a < b$  e  $b < c$  implicano  $a < c$ . Inoltre si provi che:

$$\text{da } a < b, c \leq d \text{ segue } a + c < b + d,$$

e quindi che:

$$\text{da } a < b \text{ segue } a + k < b + k, \text{ per ogni } k \in \mathbb{Z}.$$

**Esercizio 1.2.7.** Si provi 1.2.9.

**Esercizio 1.2.8.** Si provi 1.2.10.

**Esercizio 1.2.9.** Si provino (1.2.47) e (1.2.48).

**Esercizio 1.2.10.** Si provi che:

$$x, y \in \mathbb{N}_p \implies x + y \in \mathbb{N}_p, xy \in \mathbb{N}_p,$$

$$x, y \in \mathbb{N}_d \implies x + y \in \mathbb{N}_p, xy \in \mathbb{N}_d,$$

$$x \in \mathbb{N}_p, y \in \mathbb{N}_d \implies x + y \in \mathbb{N}_d, xy \in \mathbb{N}_p.$$

**Esercizio 1.2.11.** Si provi che, con  $a, b, c, d \in \mathbb{Z}$ , da  $a|b$  e  $c|d$  segue  $ac|bd$ . Se ne deduca che se  $a|b$  allora per ogni  $z \in \mathbb{Z}$  risulta  $az|bz$ , e quindi anche  $a|bz$ .

**Esercizio 1.2.12.** Si verifichi che, con  $s, t \in \mathbb{N}_0$  e  $h, k \in \mathbb{Z}$ , si ha:

$$\begin{aligned} s\mathbb{N}_0 \subseteq t\mathbb{N}_0 &\iff t|s, \\ h\mathbb{Z} \subseteq k\mathbb{Z} &\iff k|h, \end{aligned}$$

e si deduca che:

$$\begin{aligned} s\mathbb{N}_0 = t\mathbb{N}_0 &\iff t = s, \\ h\mathbb{Z} = k\mathbb{Z} &\iff h = k \text{ oppure } h = -k. \end{aligned}$$

**Esercizio 1.2.13.** Si provi che, per ogni  $\frac{m}{n}, \frac{a}{b}, \frac{s}{t}, \frac{c}{d} \in \mathbb{Q}$ ,

$$\frac{m}{n} = \frac{a}{b}, \quad \frac{s}{t} = \frac{c}{d} \implies \frac{mt+ns}{nt} = \frac{ad+bc}{bd} \quad \text{e} \quad \frac{ms}{nt} = \frac{ac}{bd}.$$

**Esercizio 1.2.14.** Si provi che valgono le seguenti proprietà:

$$\frac{m}{n} + \frac{s}{t} = \frac{s}{t} + \frac{m}{n}, \quad \text{per ogni } \frac{m}{n}, \frac{s}{t} \in \mathbb{Q},$$

(proprietà commutativa della somma);

$$\left(\frac{m}{n} + \frac{s}{t}\right) + \frac{u}{v} = \frac{m}{n} + \left(\frac{s}{t} + \frac{u}{v}\right), \quad \text{per ogni } \frac{m}{n}, \frac{s}{t}, \frac{u}{v} \in \mathbb{Q},$$

(proprietà associativa della somma);

$$\frac{m}{n} \frac{s}{t} = \frac{s}{t} \frac{m}{n}, \quad \text{per ogni } \frac{m}{n}, \frac{s}{t} \in \mathbb{Q},$$

(proprietà commutativa del prodotto);

$$\left(\frac{m}{n} \frac{s}{t}\right) \frac{u}{v} = \frac{m}{n} \left(\frac{s}{t} \frac{u}{v}\right), \quad \text{per ogni } \frac{m}{n}, \frac{s}{t}, \frac{u}{v} \in \mathbb{Q},$$

(proprietà associativa del prodotto);

$$\left(\frac{m}{n} + \frac{s}{t}\right) \frac{u}{v} = \frac{m}{n} \frac{u}{v} + \frac{s}{t} \frac{u}{v}, \quad \text{per ogni } \frac{m}{n}, \frac{s}{t}, \frac{u}{v} \in \mathbb{Q},$$

(proprietà distributiva a destra del prodotto rispetto alla somma);

$$\frac{m}{n} \left(\frac{s}{t} + \frac{u}{v}\right) = \frac{m}{n} \frac{s}{t} + \frac{m}{n} \frac{u}{v}, \quad \text{per ogni } \frac{m}{n}, \frac{s}{t}, \frac{u}{v} \in \mathbb{Q},$$

(proprietà distributiva a sinistra del prodotto rispetto alla somma).

**Esercizio 1.2.15.** Si provi che:

$$\frac{0}{n} = \frac{0}{t} = 0, \quad \text{per ogni } n, t \in \mathbb{Z}, n, t \neq 0,$$

$$\frac{m}{m} = \frac{s}{s} = 1, \quad \text{per ogni } m, s \in \mathbb{Z}, m, s \neq 0,$$

e che:

$$\frac{m}{n} + 0 = \frac{m}{n}, \quad \text{per ogni } \frac{m}{n} \in \mathbb{Q},$$

$$\frac{m}{n} 1 = \frac{m}{n}, \quad \text{per ogni } \frac{m}{n} \in \mathbb{Q}.$$

**Esercizio 1.2.16.** Si provi che:

$$\frac{m}{n} + \frac{-m}{n} = 0, \quad \text{per ogni } \frac{m}{n} \in \mathbb{Q},$$

$$\frac{m}{n} \frac{n}{m} = 1, \quad \text{per ogni } \frac{m}{n} \in \mathbb{Q}, \frac{m}{n} \neq 0.$$

### 1.3 Il principio d'induzione

Verrà ora illustrata una proprietà fondamentale dell'insieme dei numeri naturali, che fornisce un metodo dimostrativo insostituibile.

L'insieme  $\mathbb{N}_0$  è caratterizzato dalla proprietà che, partendo da 0 e considerando il successivo  $n + 1$  di ogni numero naturale  $n$ , si descrive tutto l'insieme. Vale cioè la seguente proprietà: con  $X \subseteq \mathbb{N}_0$ ,

$$\left. \begin{array}{l} (i) \quad 0 \in X \\ (ii) \quad s \in X \implies s + 1 \in X \end{array} \right\} \implies X = \mathbb{N}_0.$$

Più in generale, se  $\bar{n}$  è un fissato numero naturale e  $Y$  è un sottoinsieme di  $\mathbb{N}_0$  cui appartiene  $\bar{n}$  e tale che a  $Y$  appartiene  $t + 1$  ognqualvolta  $t \geq \bar{n}$  appartiene a  $Y$ , si ha che a  $Y$  appartiene ogni naturale  $n \geq \bar{n}$ : con  $Y \subseteq \mathbb{N}_0$ ,

$$\left. \begin{array}{l} (i) \quad \bar{n} \in Y \\ (ii) \quad t \in Y, t \geq \bar{n} \implies t + 1 \in Y \end{array} \right\} \implies n \in Y, \forall n \geq \bar{n}. \quad (1.3.1)$$

Tale proprietà dei naturali, nota come “principio d'induzione”, si applica in particolare nella dimostrazione di enunciati relativi ai numeri naturali.

**1.3.1. Prima forma del principio d'induzione.** Sia  $\bar{n}$  un numero naturale e sia  $P$  una proprietà relativa ai numeri naturali  $n \geq \bar{n}$ . La proprietà  $P$  è vera per ogni naturale  $n \geq \bar{n}$  se  $P$  è vera per  $\bar{n}$  e  $P$  è vera per  $t + 1$  ognqualvolta è vera per  $t$  (con  $t \geq \bar{n}$ ). Si ha cioè:

$$\left. \begin{array}{l} (j) \quad P \text{ vera per } \bar{n} \\ (jj) \quad t \geq \bar{n}, P \text{ vera per } t \implies P \text{ vera per } t + 1 \end{array} \right\} \implies P \text{ vera per } n, \forall n \geq \bar{n}.$$

*Dimostrazione.* Posto:

$$Y = \{n \in \mathbb{N}_0 : n \geq \bar{n} \text{ e } P \text{ vera per } n\},$$

si ha che:  $\bar{n} \in Y$  per la (j), e  $t \in Y \implies t + 1 \in Y$  per la (jj). Pertanto (1.3.1) assicura che  $n \in Y$  per ogni  $n \geq \bar{n}$ , e dunque  $P$  è vera per ogni  $n \geq \bar{n}$ .  $\square$

La condizione (j) è detta la **base dell'induzione**, l'implicazione (jj) il **passo induttivo**.

**1.3.2. Esempio.** Si consideri la seguente proprietà:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \text{ per ogni } n \geq 1.$$

Per provare che tale uguaglianza è soddisfatta per ogni numero naturale  $n \geq 1$  è necessario utilizzare il principio d'induzione. Si può dapprima osservare che

è soddisfatta la base dell'induzione in quanto, per  $n = 1$ , il primo membro dell'uguaglianza si riduce all'addendo 1, e il secondo è

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1,$$

sicché la proprietà è vera per  $n = 1$ . Si supponga ora vera la proprietà per  $t$ , si assuma quindi l'ipotesi induttiva che

$$1 + 2 + \cdots + t = \frac{t(t+1)}{2}.$$

Si vuole provare che

$$1 + 2 + \cdots + t + (t+1) = \frac{(t+1)(t+1+1)}{2}.$$

Si ha

$$1 + 2 + \cdots + t + (t+1) = (1 + 2 + \cdots + t) + (t+1),$$

sicché, utilizzando l'ipotesi d'induzione,

$$\begin{aligned} 1 + 2 + \cdots + t + (t+1) &= \frac{t(t+1)}{2} + (t+1) \\ &= \frac{t(t+1) + 2(t+1)}{2} \\ &= \frac{(t+1)(t+2)}{2}, \end{aligned}$$

come volevasi. Per il principio d'induzione l'uguaglianza considerata è vera per ogni  $n \geq 1$ .

Si noti che affermare che sussiste l'uguaglianza  $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ , per ogni  $n \geq 1$ , equivale a sostenere la veridicità di infinite uguaglianze, una per ogni numero naturale  $n$ ; tale proprietà, senza il principio d'induzione, sarebbe suscettibile solo di un numero finito di verifiche.

Si noti che la condizione (jj) può anche essere scritta nel seguente modo:  
con  $h > \bar{n}$ ,

$$P \text{ vera per } h - 1 \implies P \text{ vera per } h.$$

Ciò dipende dall'ovvia uguaglianza:

$$\{t \in \mathbb{N}_0 : t \geq \bar{n}\} = \{h - 1 : h \in \mathbb{N}, h > \bar{n}\}$$

e dall'essere  $(h - 1) + 1 = h$ .

**1.3.3. Esempio.** Si consideri la seguente proprietà:

$$2|n(n+1), \text{ per ogni } n \geq 0.$$

La si proverà utilizzando il principio d'induzione. È soddisfatta la base dell'induzione, in quanto per  $n = 0$  si ha  $n(n+1) = 0(0+1) = 0$  e  $2|0$ . Si supponga ora  $h > 0$  e la proprietà vera per  $h - 1$ , si assuma quindi l'ipotesi induttiva che:  $2|(h-1)((h-1)+1)$ , cioè  $2|(h-1)h$ . Si vuole provare che:  $2|h(h+1)$ . Ovviamente  $2|2h$ , pertanto per la (1.2.42) e per l'ipotesi induttiva si ha che 2 divide  $(h-1)h + 2h = h^2 + h = h(h+1)$ , come volevasi. Per il principio d'induzione la proprietà considerata è vera per ogni  $n \geq 0$ .

**1.3.4. Algoritmo della divisione in  $\mathbb{N}_0$ .** Considerato un numero naturale  $b \neq 0$ , per ogni  $n \in \mathbb{N}_0$  esistono (e sono univocamente determinati) naturali  $q$  ed  $r$  tali che  $n = bq + r$ , con  $r < b$ .

*Dimostrazione.* Si ragiona per induzione su  $n$ . Per  $n = 0$ , si ha  $0 = b \cdot 0 + 0$ , con  $0 < b$ . Si supponga ora  $n > 0$  e, per ipotesi d'induzione,  $n - 1 = bq' + r'$ , con  $r' < b$ , sicché  $n = bq' + r' + 1$ . Se si ha  $r' + 1 < b$ , basta allora porre  $q = q'$  e  $r = r' + 1$ . Altrimenti, da  $r' + 1 = b$  segue  $n = bq' + b = b(q' + 1) + 0$ , e si ha l'asserto con  $q = q' + 1$  e  $r = 0$ . Il fatto che tali interi  $q$  ed  $r$  sono univocamente determinati sarà provato nel Capitolo 5.  $\square$

Si noti che, nelle dimostrazioni per induzione, è essenziale provare in primo luogo che vale la condizione (j), verificare cioè la base dell'induzione.

**1.3.5. Esempio.** Si consideri la seguente proprietà P:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} + 3, \text{ per ogni } n \geq 1.$$

Tale uguaglianza è falsa per ogni  $n$ . Si verifica però facilmente che se si suppone P vera per  $h$ , allora si ottiene P vera per  $h + 1$ . Ma non sussiste la base dell'induzione: infatti per  $n = 1$  l'uguaglianza non è soddisfatta.

Per ben visualizzare la situazione, si può pensare a (infiniti) tasselli di un domino ritti uno davanti l'altro in modo tale che la caduta di ciascuno provochi la caduta del successivo. Questa condizione "rappresenta" la proprietà (jj). Facendo cadere il primo tassello, e solo allora (il che ha il significato della base d'induzione), si provoca la caduta di tutti i tasselli.

**1.3.6. Esempio.** Per ogni  $n \geq 1$ , si ha:

$$8 \text{ non divide } 3^{2n} + 5.$$

Si proceda per induzione su  $n$ . Per  $n = 1$  si ha  $3^{2 \cdot 1} + 5 = 9 + 5 = 14$  e 8 non divide 14, sicché la base d'induzione è soddisfatta. Si supponga che 8 non divida

$3^{2t} + 5$ . Risulta  $3^{2(t+1)} + 5 = 3^{2t+2} + 5 = 3^{2t}3^2 + 5 = 3^{2t}9 + 5 = 3^{2t}(8+1) + 5 = 3^{2t} \cdot 8 + 3^{2t} \cdot 1 + 5 = 3^{2t} \cdot 8 + (3^{2t} + 5)$ . Se per assurdo 8 dividesse  $3^{2(t+1)} + 5$ , allora da  $8|3^{2t} \cdot 8$  e da (1.2.43) seguirebbe  $8|3^{2t} + 5$ , contro l'ipotesi d'induzione. Ciò comporta che 8 non divide  $3^{2(t+1)} + 5$ . Il principio d'induzione assicura l'asserto.

Questa proprietà dei numeri naturali permette anche di fornire le cosiddette "definizioni per ricorrenza": volendo dare significato all'espressione  $E_n$ , con  $n$  numero naturale, è sufficiente precisare  $E_0$ , e poi definire  $E_{n+1}$  in funzione di  $E_n$ .

**1.3.7. Esempio.** Se  $a$  è un numero intero e  $n$  è un numero naturale, la posizione

$$a^0 := 1, \quad a^{n+1} := a^n \cdot a$$

definisce la potenza  $n$ -ma di  $a$  (vedi Paragrafo 1.2).

## Esercizi

**Esercizio 1.3.1.** Si dimostri, per induzione su  $n$ , che:

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}, \text{ per ogni } n \geq 1.$$

*Svolgimento.* È soddisfatta la base dell'induzione in quanto, per  $n = 1$ , si ha  $1^3 = 1$  e  $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ . Si supponga ora la proprietà vera per  $t$ , si assuma quindi l'ipotesi induttiva che:  $1^3 + \cdots + t^3 = \frac{t^2(t+1)^2}{4}$ . Si vuole dimostrare che  $1^3 + \cdots + t^3 + (t+1)^3 = \frac{(t+1)^2(t+1+1)^2}{4} = \frac{(t+1)^2(t+2)^2}{4}$ . Risulta ovviamente  $1^3 + \cdots + t^3 + (t+1)^3 = \frac{t^2(t+1)^2}{4} + (t+1)^3$  per l'ipotesi induttiva, e inoltre  $\frac{t^2(t+1)^2}{4} + (t+1)^3 = \frac{t^2(t+1)^2 + 4(t+1)^3}{4} = \frac{(t+1)^2(t^2+4t+4)}{4} = \frac{(t+1)^2(t+2)^2}{4}$ , pertanto  $1^3 + \cdots + t^3 + (t+1)^3 = \frac{(t+1)^2(t+2)^2}{4}$ , come volevasi. Per il principio d'induzione la proprietà considerata è vera per ogni  $n \geq 1$ .

**Esercizio 1.3.2.** Si dimostri, per induzione su  $n$ , che:

$$3|n(n+1)(n+2), \text{ per ogni } n \geq 0.$$

*Svolgimento.* È soddisfatta la base dell'induzione in quanto, per  $n = 0$ , si ha  $0(0+1)(0+2) = 0$  e  $3|0$ . Si supponga ora la proprietà vera per  $t$ , si assuma quindi l'ipotesi induttiva che:  $3|(t+1)(t+2)(t+3)$ . Si proverà che  $3|(t+1)(t+2)(t+3)$ . Si ha:

$$\begin{aligned} (t+1)(t+2)(t+3) &= (t+1)(t+2)t + (t+1)(t+2)3 \\ &= t(t+1)(t+2) + 3(t+1)(t+2); \end{aligned}$$

ovviamente 3 divide il secondo addendo e inoltre divide il primo addendo per ipotesi induttiva, pertanto  $3|(t+1)(t+2)(t+3)$  per (1.2.42), come volevasi. Per il principio d'induzione la proprietà considerata è vera per ogni  $n \geq 0$ .

**Esercizio 1.3.3.** Si dimostri, per induzione su  $n$ , che:

$$15|4^{2n} - 1, \text{ per ogni } n \geq 0.$$

*Svolgimento.* È soddisfatta la base dell'induzione in quanto, per  $n = 0$ , si ha  $4^0 - 1 = 1 - 1 = 0$  e  $15|0$ . Si supponga ora  $h > 0$  e la proprietà vera per  $h - 1$ , si assuma quindi l'ipotesi induttiva che  $15|4^{2(h-1)} - 1$ . Si vuole provare che  $15|4^{2h} - 1$ . Risulta  $4^{2h} - 1 = 4^2 \cdot 4^{2(h-1)} - 1 = 4^2 \cdot 4^{2(h-1)} - 4^2 + 4^2 - 1 = 4^2(4^{2(h-1)} - 1) + (4^2 - 1)$ , e si ha che  $15|4^2(4^{2(h-1)} - 1)$  per l'ipotesi induttiva e ovviamente  $15|4^2 - 1$ . Pertanto  $15|4^{2h} - 1$ , come volevasi. Per il principio d'induzione la proprietà considerata è vera per ogni  $n \geq 0$ .

**Esercizio 1.3.4.** Per induzione su  $k$ , si provi che, se  $p$  è un numero naturale primo e se  $p$  divide il prodotto  $a_1 \dots a_k$ , con  $a_1, \dots, a_k \in \mathbb{N}$ , allora esiste  $i \in \{1, \dots, k\}$  tale che  $p$  divide  $a_i$ .

Se ne deduca l'unicità della fattorizzazione in prodotto di primi di ogni numero naturale  $n \geq 2$ , come enunciato in 1.2.5.

**Esercizio 1.3.5.** Si dimostri, per induzione su  $n$ , che:

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.6.** Si dimostri, per induzione su  $n$ , che:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n \cdot (n+1)} = 1 - \frac{1}{n+1}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.7.** Si dimostri per induzione che per ogni  $n \geq 1$ :

$$1 + 3 + 5 + \dots + (2n-1) = n^2.$$

**Esercizio 1.3.8.** Si dimostri per induzione che per ogni  $n \geq 1$ :

$$2 + 4 + 6 + 8 + \dots + 2n = n(n+1).$$

**Esercizio 1.3.9.** Si dimostri che:

$$1 \cdot 2^1 + 2 \cdot 2^2 + \dots + n \cdot 2^n = (n-1) \cdot 2^{n+1} + 2, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.10.** Si dimostri che:

$$2 + 2^2 + \dots + 2^n = 2(2^n - 1), \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.11.** Si dimostri per induzione su  $n$  che:

$$3 + 3^2 + 3^3 + \dots + 3^n = \frac{3(3^n - 1)}{2}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.12.** Si dimostri che:

$$-1^2 + 2^2 - 3^2 + \cdots + (-1)^n n^2 = (-1)^n \frac{n(n+1)}{2}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.13.** Si dimostri per induzione che:

$$11|12^n - 1, \text{ per ogni } n \geq 0.$$

**Esercizio 1.3.14.** Si dimostri per induzione che:

$$7|2^{3n} - 1, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.15.** Si dimostri per induzione che:

$$124|5^{3n} - 1, \text{ per ogni } n \geq 1.$$

**Esercizio 1.3.16.** Si dimostri che, per  $n \geq 1$ , le affermazioni:

$$1 + 3 + 5 + \dots + (2n-1) = n^2 - 3$$

sono tutte false.

## 1.4 Operazioni tra insiemi

In questo paragrafo saranno illustrate alcune notevoli operazioni tra insiemi: si introduciranno cioè nuovi insiemi a partire da insiemi dati. Se ne studieranno poi le principali proprietà.

Siano  $S$  e  $T$  insiemi, si definisce **unione** di  $S$  e  $T$ , e si indica con il simbolo  $S \cup T$ , l'insieme i cui elementi sono tutti e soli gli elementi appartenenti a  $S$  o a  $T$ :

$$S \cup T := \{x : x \in S \text{ o } x \in T\}.$$

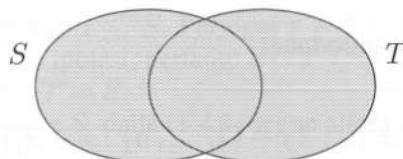
Si ha cioè:

$$x \in S \cup T : \iff x \in S \text{ o } x \in T,$$

e quindi:

$$x \notin S \cup T \iff x \notin S \text{ e } x \notin T.$$

Se gli insiemi  $S$  e  $T$  sono rappresentati mediante diagrammi di Venn, l'unione  $S \cup T$  è la parte ombreggiata nella figura seguente:



Per esempio: se  $A = \{1, a, b, -6, \star\}$ ,  $B = \{b, \triangle, \star, 1, -7, f\}$  e  $C = \{a, -6\}$ , risulta:

$$\begin{aligned} A \cup B &= \{1, a, b, -6, \star, \triangle, -7, f\}, \\ A \cup C &= \{1, a, b, -6, \star\} = A, \\ B \cup C &= \{a, b, \triangle, \star, 1, -6, -7, f\}. \end{aligned}$$

Si noti che riesce sempre:

$$\begin{aligned} S &\subseteq S \cup T, \\ T &\subseteq S \cup T. \end{aligned} \tag{1.4.1}$$

È immediato inoltre verificare che, qualunque siano gli insiemi  $S$ ,  $T$  e  $V$ , risulta sempre:

$$\begin{aligned} S \cup T &= T \cup S \\ (\text{proprietà commutativa dell'unione}), \end{aligned} \tag{1.4.2}$$

$$\begin{aligned} (S \cup T) \cup V &= S \cup (T \cup V) \\ (\text{proprietà associativa dell'unione}), \end{aligned} \tag{1.4.3}$$

$$\begin{aligned} S \cup \emptyset &= S = \emptyset \cup S \\ (\emptyset \text{ elemento neutro per l'unione}), \end{aligned} \tag{1.4.4}$$

$$\begin{aligned} S \cup S &= S \\ (\text{proprietà iterativa dell'unione}). \end{aligned} \tag{1.4.5}$$

Si noti che la (1.4.3) permette di denotare l'insieme  $(S \cup T) \cup V = S \cup (T \cup V)$  col simbolo  $S \cup T \cup V$ ; si ha  $S \cup T \cup V = \{x : x \in S \cup T \cup V\}$ .

Più in generale, se  $S_1, S_2, \dots, S_n$  ( $n \geq 2$ ), sono insiemi, riesce:

$$S_1 \cup S_2 \cup \dots \cup S_n = \{x : x \in S_1 \cup S_2 \cup \dots \cup S_n\}.$$

Il primo membro dell'uguaglianza precedente è spesso denotato con il simbolo:

$$\bigcup_{i=1}^n S_i$$

e si ha, con le notazioni già introdotte:

$$\bigcup_{i=1}^n S_i = \{x : \exists j \in \{1, \dots, n\} : x \in S_j\}.$$

Pertanto:

$$x \notin \bigcup_{i=1}^n S_i \iff x \notin S_j, \forall j \in \{1, \dots, n\}.$$

Se  $\mathcal{F}$  è un insieme di insiemi, si dà poi significato all'unione degli elementi di  $\mathcal{F}$  ponendo:

$$\bigcup_{X \in \mathcal{F}} X := \{x : \exists Y \in \mathcal{F} : x \in Y\}.$$

Si ha cioè

$$x \in \bigcup_{X \in \mathcal{F}} X \iff \exists Y \in \mathcal{F} : x \in Y,$$

$$x \notin \bigcup_{X \in \mathcal{F}} X \iff x \notin X, \forall X \in \mathcal{F}.$$

Si noti che se  $\mathcal{F} = \{S, T\}$ , risulta

$$\bigcup_{X \in \mathcal{F}} X = S \cup T;$$

più in generale, se  $\mathcal{F} = \{S_1, \dots, S_n\}$ , si ha

$$\bigcup_{X \in \mathcal{F}} X = S_1 \cup \dots \cup S_n = \bigcup_{i=1}^n S_i.$$

Si osservi inoltre che la proprietà commutativa dell'unione (1.4.2) evita ogni ambiguità nella definizione appena data.

Ovviamente per ogni  $Y \in \mathcal{F}$  si ha:

$$Y \subseteq \bigcup_{X \in \mathcal{F}} X.$$

Una notevole proprietà dell'unione è la seguente:

**1.4.1.** *Con  $S$  e  $T$  insiemi, si ha:*

$$T \subseteq S \iff S \cup T = S.$$

*Dimostrazione.* Si supponga  $T \subseteq S$ . Per ogni  $x \in S \cup T$  risulta allora  $x \in S$  o  $x \in T$ , da cui  $x \in S$  per le ipotesi; pertanto  $S \cup T \subseteq S$ . L'inclusione  $S \subseteq S \cup T$  è sempre vera, sicché  $S \cup T = S$ .

Viceversa, sia  $S \cup T = S$ , dalla (1.4.1) segue allora  $T \subseteq S \cup T = S$ , sicché  $T \subseteq S$ .  $\square$

**1.4.2.** Siano  $S, T, V$  e  $W$  insiemi. Allora:

$$S \subseteq T, V \subseteq W \implies S \cup V \subseteq T \cup W,$$

quindi:

$$\begin{aligned} S \subseteq T &\implies S \cup V \subseteq T \cup V, \\ S \subseteq T, V \subseteq T &\implies S \cup V \subseteq T. \end{aligned}$$

*Dimostrazione.* Esercizio. □

**1.4.3.** Con  $S, T, V$  e  $W$  insiemi, si ha:

$$\begin{aligned} S \subset T, V \subset W &\not\implies S \cup V \subset T \cup W, \\ S \subset T &\not\implies S \cup V \subset T \cup V, \\ S \subset T, V \subset T &\not\implies S \cup V \subset T. \end{aligned}$$

*Dimostrazione.* Per provare che un'inclusione non vale, basta esibire un controsenso, cioè descrivere un caso in cui valgono le ipotesi ma non la tesi. Per esempio, con  $A = \{1, 2\}$ ,  $B = \{1, 2, 3\}$ ,  $C = \{1, 3, 4\}$ ,  $D = \{1, 2, 3, 4\}$ , si ha  $A \subset B, C \subset D$ , ma  $A \cup C = \{1, 2, 3, 4\} = B \cup D$ , pertanto non vale la prima implicazione. Il Lettore individui controsensi per le altre due implicazioni. □

Siano  $S$  e  $T$  insiemi, si definisce **intersezione** di  $S$  e  $T$ , e si indica con il simbolo  $S \cap T$ , l'insieme i cui elementi sono tutti e soli gli elementi appartenenti sia a  $S$  che a  $T$ :

$$S \cap T := \{x : x \in S \text{ e } x \in T\}.$$

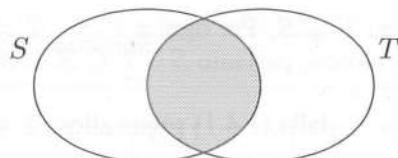
Si ha cioè:

$$x \in S \cap T \iff x \in S \text{ e } x \in T,$$

e quindi:

$$x \notin S \cap T \iff x \notin S \text{ o } x \notin T.$$

Se gli insiemi  $S$  e  $T$  sono rappresentati mediante diagrammi di Venn, l'intersezione  $S \cap T$  è la parte ombreggiata nella figura seguente:



Per esempio: se  $A = \{1, a, b, -6, \star\}$ ,  $B = \{b, \triangle, \star, 1, -7, f\}$  e  $C = \{a, -6\}$ , risulta:

$$\begin{aligned} A \cap B &= \{1, b, \star\}, \\ A \cap C &= \{a, -6\} = C, \\ B \cap C &= \emptyset. \end{aligned}$$

Insiemi  $S$  e  $T$  tali che  $S \cap T = \emptyset$  sono detti **disgiunti**; per esempio sono disgiunti gli insiemi  $B$  e  $C$  dell'esempio precedente.

Si noti che riesce sempre:

$$\begin{aligned} S \cap T &\subseteq S, \\ S \cap T &\subseteq T. \end{aligned} \tag{1.4.6}$$

Valgono inoltre proprietà analoghe a quelle enunciate per l'unione. Qualunque siano gli insiemi  $S$ ,  $T$  e  $V$ , si ha infatti:

$$\begin{aligned} S \cap T &= T \cap S \\ (\text{proprietà commutativa dell'intersezione}), \end{aligned} \tag{1.4.7}$$

$$\begin{aligned} (S \cap T) \cap V &= S \cap (T \cap V) \\ (\text{proprietà associativa dell'intersezione}), \end{aligned} \tag{1.4.8}$$

$$\begin{aligned} S \cap S &= S \\ (\text{proprietà iterativa dell'intersezione}). \end{aligned} \tag{1.4.9}$$

La proprietà associativa permette di denotare l'insieme  $(S \cap T) \cap V = S \cap (T \cap V)$  più brevemente col simbolo  $S \cap T \cap V$ ; si ha

$$S \cap T \cap V = \{x : x \in S \text{ e } x \in T \text{ e } x \in V\}.$$

Più in generale, se  $S_1, S_2, \dots, S_n$  ( $n \geq 2$ ), sono insiemi, riesce:

$$S_1 \cap S_2 \cap \dots \cap S_n = \{x : x \in S_1 \text{ e } x \in S_2 \dots \text{ e } x \in S_n\}.$$

Il primo membro dell'uguaglianza precedente è spesso denotato con il simbolo:

$$\bigcap_{i=1}^n S_i,$$

e si ha, con le notazioni già introdotte:

$$\bigcap_{i=1}^n S_i = \{x : x \in S_j, \forall j \in \{1, \dots, n\}\}.$$

Pertanto:

$$x \notin \bigcap_{i=1}^n S_i \iff \exists j \in \{1, \dots, n\} : x \notin S_j.$$

Se  $\mathcal{F}$  è un insieme di insiemi, si dà poi significato all'intersezione degli elementi di  $\mathcal{F}$  ponendo:

$$\bigcap_{X \in \mathcal{F}} X := \{x : x \in X, \forall X \in \mathcal{F}\}.$$

Si ha cioè

$$x \in \bigcap_{X \in \mathcal{F}} X : \iff x \in X, \forall X \in \mathcal{F},$$

$$x \notin \bigcap_{X \in \mathcal{F}} X \iff \exists Y \in \mathcal{F} : x \notin Y.$$

Si noti che se  $\mathcal{F} = \{S, T\}$ , risulta

$$\bigcap_{X \in \mathcal{F}} X = S \cap T;$$

più in generale, se  $\mathcal{F} = \{S_1, \dots, S_n\}$ , si ha

$$\bigcap_{X \in \mathcal{F}} X = S_1 \cap \dots \cap S_n = \bigcap_{i=1}^n S_i.$$

La proprietà commutativa dell'intersezione (1.4.7) evita ancora ogni ambiguità nella definizione prima data.

Ovviamente per ogni  $Y \in \mathcal{F}$  si ha:

$$\bigcap_{X \in \mathcal{F}} X \subseteq Y.$$

“Duale” della 1.4.1 è la seguente:

**1.4.4. Con  $S$  e  $T$  insiemi, si ha:**

$$T \subseteq S \iff S \cap T = T.$$

*Dimostrazione.* Si supponga  $T \subseteq S$ . Per ogni  $x \in T$  risulta allora  $x \in S$  per le ipotesi; pertanto  $T \subseteq S \cap T$ . L'inclusione  $S \cap T \subseteq T$  è sempre vera, sicché  $S \cap T = T$ . Viceversa, sia  $S \cap T = T$ , dalla (1.4.6) segue allora  $T = S \cap T \subseteq S$ , sicché  $T \subseteq S$ .  $\square$

**1.4.5.** Con  $S, T, V$  e  $W$  insiemi, si ha:

$$S \subseteq T, V \subseteq W \implies S \cap V \subseteq T \cap W,$$

quindi:

$$\begin{aligned} S \subseteq T &\implies S \cap V \subseteq T \cap V, \\ S \subseteq T, S \subseteq W &\implies S \subseteq T \cap W. \end{aligned}$$

*Dimostrazione.* Esercizio. □

Proprietà che legano l'unione e l'intersezione sono le seguenti:

**1.4.6.** Con  $S, T$  e  $V$  insiemi si ha:

$$\begin{aligned} S \cup (T \cap V) &= (S \cup T) \cap (S \cup V) \\ (S \cap T) \cup V &= (S \cup V) \cap (T \cup V) \end{aligned} \tag{1.4.10}$$

(proprietà distributiva dell'unione rispetto all'intersezione);

$$\begin{aligned} S \cap (T \cup V) &= (S \cap T) \cup (S \cap V) \\ (S \cup T) \cap V &= (S \cap V) \cup (T \cap V) \end{aligned} \tag{1.4.11}$$

(proprietà distributiva dell'intersezione rispetto all'unione).

*Dimostrazione.* Si proverà la prima uguaglianza delle (1.4.10) verificando che

$$x \in S \cup (T \cap V) \iff x \in (S \cup T) \cap (S \cup V).$$

Si ha infatti:

$$\begin{aligned} x \in S \cup (T \cap V) &\iff x \in S \circ (x \in T \cap V) \\ &\iff x \in S \circ (x \in T \text{ e } x \in V) \\ &\iff (x \in S \circ x \in T) \text{ e } (x \in S \circ x \in V) \\ &\iff (x \in S \cup T) \text{ e } (x \in S \cup V) \\ &\iff x \in (S \cup T) \cap (S \cup V). \end{aligned}$$

La seconda uguaglianza delle (1.4.10) discende da quanto appena provato e dalla proprietà commutativa dell'unione (1.4.2), infatti:  $(S \cap T) \cup V = V \cup (S \cap T) = (V \cup S) \cap (V \cup T) = (S \cup V) \cap (T \cup V)$ .

Per dimostrare la prima uguaglianza delle (1.4.11) si proverà che

$$x \in S \cap (T \cup V) \iff x \in (S \cap T) \cup (S \cap V).$$

Si ha infatti:

$$\begin{aligned}
 x \in S \cap (T \cup V) &\iff x \in S \text{ e } (x \in T \cup V) \\
 &\iff x \in S \text{ e } (x \in T \text{ o } x \in V) \\
 &\iff (x \in S \text{ e } x \in T) \text{ o } (x \in S \text{ e } x \in V) \\
 &\iff x \in S \cap T \text{ o } x \in S \cap V \\
 &\iff x \in (S \cap T) \cup (S \cap V).
 \end{aligned}$$

La seconda uguaglianza delle (1.4.11) discende dalla proprietà commutativa dell'intersezione (1.4.7), ragionando come in precedenza.  $\square$

**1.4.7.** Siano  $S$  e  $T$  insiemi. Allora:

$$S \cup (S \cap T) = S = S \cap (S \cup T) \quad (\text{leggi di assorbimento}).$$

*Dimostrazione.* Esercizio.  $\square$

**1.4.8.** Sia  $\mathcal{F}$  un insieme di insiemi e sia  $T$  un insieme. Si ha:

$$X \subseteq T, \text{ per ogni } X \in \mathcal{F} \implies \bigcup_{X \in \mathcal{F}} X \subseteq T,$$

$$T \subseteq X, \text{ per ogni } X \in \mathcal{F} \implies T \subseteq \bigcap_{X \in \mathcal{F}} X.$$

*Dimostrazione.* Esercizio.  $\square$

**1.4.9.** Siano  $S$  un insieme e  $\mathcal{F}$  un insieme di insiemi. Si ha:

$$S \cup \left( \bigcap_{X \in \mathcal{F}} X \right) = \bigcap_{X \in \mathcal{F}} (S \cup X)$$

(proprietà distributiva dell'unione rispetto all'intersezione),

$$S \cap \left( \bigcup_{X \in \mathcal{F}} X \right) = \bigcup_{X \in \mathcal{F}} (S \cap X)$$

(proprietà distributiva dell'intersezione rispetto all'unione).

*Dimostrazione.* Esercizio. □

Con  $S$  e  $T$  insiemi, si definisce **complemento** di  $T$  rispetto a  $S$  (o **differenza** tra  $S$  e  $T$ ), e si indica con il simbolo  $S \setminus T$ , l'insieme costituito da tutti e soli gli elementi di  $S$  che non appartengono a  $T$ :

$$S \setminus T := \{x : x \in S \text{ e } x \notin T\}.$$

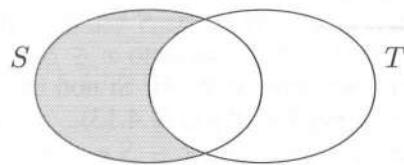
Si ha cioè:

$$x \in S \setminus T \iff x \in S \text{ e } x \notin T.$$

Pertanto:

$$x \notin S \setminus T \iff x \notin S \text{ o } x \in T.$$

Utilizzando i diagrammi di Venn si ha la seguente rappresentazione di  $S \setminus T$ :



Per esempio, con  $A = \{1, a, b, -6, *\}$ ,  $B = \{b, \Delta, *, 1, -7, f\}$  e  $C = \{a, -6\}$ , si ha:

$$\begin{array}{ll} A \setminus B = \{a, -6\}, & B \setminus A = \{\Delta, -7, f\}, \\ A \setminus C = \{1, b, *\}, & C \setminus A = \emptyset, \\ B \setminus C = B, & C \setminus B = C, \\ (A \setminus B) \setminus C = \emptyset, & A \setminus (B \setminus C) = A \setminus B. \end{array}$$

Come evidenziato negli esempi precedenti, per il complemento non vale la proprietà commutativa né la proprietà associativa. È poi facile verificare che qualunque siano gli insiemi  $S$  e  $T$  riesce:

$$S \setminus T \subseteq S, \tag{1.4.12}$$

$$S \setminus \emptyset = S, \tag{1.4.13}$$

$$\emptyset \setminus S = \emptyset, \tag{1.4.14}$$

$$S \setminus S = \emptyset, \tag{1.4.15}$$

$$S \cap (T \setminus S) = \emptyset. \tag{1.4.16}$$

Si noti che, con  $S \neq \emptyset$ , la (1.4.13) e la (1.4.14) evidenziano ancora la non commutatività del complemento.

**1.4.10.** Con  $S$  e  $T$  insiemi, risulta:  $S \setminus T = S \setminus (S \cap T)$ .

*Dimostrazione.* Infatti se  $x \in S \setminus T$ , allora  $x \in S$  e  $x \notin T$ , sicché  $x \in S$  e  $x \notin S \cap T$ ; pertanto  $x \in S \setminus (S \cap T)$ . Viceversa, se  $x \in S \setminus (S \cap T)$ , si ha  $x \in S$  e  $x \notin S \cap T$ , da cui  $x \in S$  e ( $x \notin S$  o  $x \notin T$ ), sicché  $x \in S$  e  $x \notin T$ , il che implica  $x \in S \setminus T$ .  $\square$

**1.4.11.** Con  $S$  e  $T$  insiemi, si ha:

$$\begin{aligned} S \setminus T = S &\iff S \cap T = \emptyset, \\ S \setminus T = \emptyset &\iff S \subseteq T. \end{aligned}$$

*Dimostrazione.* Sia  $S \setminus T = S$  e si supponga per assurdo che  $S \cap T \neq \emptyset$ . Esiste allora  $x$  tale che  $x \in S$  e  $x \in T$ , pertanto  $x \in S$  e  $x \notin S \setminus T$ , in contrasto con le ipotesi.

Viceversa si supponga  $S \cap T = \emptyset$ . Si ha  $S \setminus T \subseteq S$  per la (1.4.12), se poi  $x \in S$ , allora  $x \notin S \cap T$ , cioè  $x \notin T$ , pertanto  $x \in S \setminus T$  e  $S \subseteq S \setminus T$ . Ne segue  $S = S \setminus T$ , per la (1.1.4), come volevasi. Si noti che, più rapidamente, se  $S \cap T = \emptyset$ , risulta  $S \setminus T = S$  per 1.4.10 e la (1.4.13).

Sia ora  $S \setminus T = \emptyset$ . Se  $x \in S$ , allora  $x \in S$  e  $x \notin S \setminus T$ , sicché  $x \in S$  e ( $x \notin S$  o  $x \in T$ ), da cui  $x \in T$ , come volevasi.

Viceversa, supposto  $S \subseteq T$ , si ha  $S \setminus T = \emptyset$ , altrimenti esisterebbe  $x$  tale che  $x \in S$  e  $x \notin T$  e dunque  $x \notin T$ , contro le ipotesi. Alla stessa conclusione si giunge applicando 1.4.4, 1.4.10 e (1.4.15): da  $S \subseteq T$  segue  $S \cap T = S$ , quindi  $S \setminus T = S \setminus (S \cap T) = S \setminus S = \emptyset$ .  $\square$

Rispetto alle operazioni di unione e di intersezione valgono le seguenti proprietà:

**1.4.12.** Con  $S$ ,  $T$  e  $V$  insiemi, si ha:

$$(S \cup T) \setminus V = (S \setminus V) \cup (T \setminus V) \quad (1.4.17)$$

(proprietà distributiva a destra del complemento rispetto all'unione),

$$(S \cap T) \setminus V = (S \setminus V) \cap (T \setminus V) \quad (1.4.18)$$

(proprietà distributiva a destra del complemento rispetto all'intersezione).

*Dimostrazione.* Per provare la (1.4.17) si ragioni nel modo seguente:

$$\begin{aligned} x \in (S \cup T) \setminus V &\iff x \in S \cup T \text{ e } x \notin V \\ &\iff (x \in S \text{ o } x \in T) \text{ e } x \notin V \\ &\iff (x \in S \text{ e } x \notin V) \text{ o } (x \in T \text{ e } x \notin V) \\ &\iff x \in S \setminus V \text{ o } x \in T \setminus V \\ &\iff x \in (S \setminus V) \cup (T \setminus V). \end{aligned}$$

La (1.4.18) si prova in maniera analoga.  $\square$

**1.4.13. Formule di De Morgan.** Con  $S, T$  e  $V$  insiemi, si ha:

$$\begin{aligned} S \setminus (T \cup V) &= (S \setminus T) \cap (S \setminus V) \\ S \setminus (T \cap V) &= (S \setminus T) \cup (S \setminus V). \end{aligned}$$

*Dimostrazione.* Si ha:

$$\begin{aligned} x \in S \setminus (T \cup V) &\iff x \in S \text{ e } x \notin T \cup V \\ &\iff x \in S \text{ e } (x \notin T \text{ e } x \notin V) \\ &\iff (x \in S \text{ e } x \notin T) \text{ e } (x \in S \text{ e } x \notin V) \\ &\iff x \in S \setminus T \text{ e } x \in S \setminus V \\ &\iff x \in (S \setminus T) \cap (S \setminus V). \end{aligned}$$

Pertanto  $S \setminus (T \cup V) = (S \setminus T) \cap (S \setminus V)$ . Si ha poi:

$$\begin{aligned} x \in S \setminus (T \cap V) &\iff x \in S \text{ e } x \notin T \cap V \\ &\iff x \in S \text{ e } (x \notin T \text{ o } x \notin V) \\ &\iff (x \in S \text{ e } x \notin T) \text{ o } (x \in S \text{ e } x \notin V) \\ &\iff x \in S \setminus T \text{ o } x \in S \setminus V \\ &\iff x \in (S \setminus T) \cup (S \setminus V). \end{aligned}$$

Pertanto  $S \setminus (T \cap V) = (S \setminus T) \cup (S \setminus V)$ .  $\square$

Con  $S$  e  $T$  insiemi si definisce **unione disgiunta** o **differenza simmetrica** di  $S$  e  $T$ , e si denota con il simbolo  $S \dot{\cup} T$  (o  $S \Delta T$ ), l'insieme costituito dagli elementi che appartengono all'unione di  $S$  e  $T$  ma non alla loro intersezione:

$$S \dot{\cup} T := (S \cup T) \setminus (S \cap T).$$

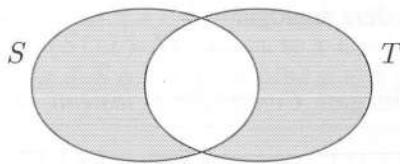
Si noti subito che:

$$S \dot{\cup} T = (S \setminus T) \cup (T \setminus S). \quad (1.4.19)$$

Infatti:

$$\begin{aligned} x \in S \dot{\cup} T &\iff x \in (S \cup T) \setminus (S \cap T) \\ &\iff x \in S \cup T \text{ e } x \notin S \cap T \\ &\iff (x \in S \text{ o } x \in T) \text{ e } (x \notin S \text{ o } x \notin T) \\ &\iff (x \in S \text{ e } x \notin T) \text{ o } (x \in T \text{ e } x \notin S) \\ &\iff x \in S \setminus T \text{ o } x \in T \setminus S \\ &\iff x \in (S \setminus T) \cup (T \setminus S). \end{aligned}$$

Pertanto  $S \dot{\cup} T$  è l'insieme degli elementi che appartengono a uno solo degli insiemi  $S$  e  $T$ . Graficamente:



Per esempio, se  $A = \{1, a, b, -6, \star\}$ ,  $B = \{b, \triangle, \star, 1, -7, f\}$  e  $C = \{a, -6\}$ , risulta:  $A \dot{\cup} B = \{a, -6, \triangle, -7, f\} = B \dot{\cup} A$ ,  $A \dot{\cup} C = \{1, b, \star\}$ ,  $B \dot{\cup} C = \{b, \triangle, \star, 1, -7, a, -6, f\}$ . Si osservi che:

$$x \notin S \dot{\cup} T \iff (x \notin S \text{ o } x \in T) \text{ e } (x \notin T \text{ o } x \in S) \quad (1.4.20)$$

Infatti  $x \notin (S \setminus T) \cup (T \setminus S) \iff x \notin S \setminus T \text{ e } x \notin T \setminus S$ . Si noti anche che:

$$S \dot{\cup} T = S \cup T \iff S \cap T = \emptyset$$

Valgono le seguenti proprietà:

**1.4.14.** Con  $S, T, V$  insiemi si ha:

$$S \dot{\cup} T = T \dot{\cup} S \quad (1.4.21)$$

(proprietà commutativa dell'unione disgiunta);

$$(S \dot{\cup} T) \dot{\cup} V = S \dot{\cup} (T \dot{\cup} V) \quad (1.4.22)$$

(proprietà associativa dell'unione disgiunta);

$$S \dot{\cup} \emptyset = S \quad (1.4.23)$$

( $\emptyset$  elemento neutro rispetto all'unione disgiunta);

$$S \dot{\cup} S = \emptyset. \quad (1.4.24)$$

*Dimostrazione.* La (1.4.21) segue subito dalle analoghe proprietà dell'unione e dell'intersezione. Per provare la (1.4.22) si osservi che ciascuno degli insiemi in questione è costituito dagli elementi che appartengono o a tutti e tre gli insiemi o a uno e uno solo dei tre. Infatti per esempio si ha, per la (1.4.19) e la (1.4.20):

$$\begin{aligned} x \in (S \dot{\cup} T) \dot{\cup} V &\iff x \in ((S \dot{\cup} T) \setminus V) \cup (V \setminus (S \dot{\cup} T)) \\ &\iff (x \in S \dot{\cup} T \text{ e } x \notin V) \text{ o } (x \in V \text{ e } x \notin S \dot{\cup} T) \\ &\iff (((x \in S \text{ e } x \notin T) \text{ o } (x \in T \text{ e } x \notin S)) \text{ e } x \notin V) \text{ o} \\ &\quad (x \in V \text{ e } ((x \notin S \text{ o } x \in T) \text{ e } (x \notin T \text{ o } x \in S))) \\ &\iff (x \in S \text{ e } x \notin T \text{ e } x \notin V) \text{ o } (x \in T \text{ e } x \notin S \text{ e } x \notin V) \text{ o} \\ &\quad (x \in V \text{ e } x \notin S \text{ e } x \notin T) \text{ o } (x \in V \text{ e } x \in T \text{ e } x \in S). \end{aligned}$$

Le altre uguaglianze seguono subito dalla definizione e da proprietà studiate in precedenza.  $\square$

**1.4.15.** Con  $S, T, V$  insiemi si ha:

$$\begin{aligned} S \cap (T \cup V) &= (S \cap T) \cup (S \cap V) \\ (S \cup T) \cap V &= (S \cap V) \cup (T \cap V) \end{aligned}$$

(distributività dell'intersezione rispetto all'unione disgiunta).

*Dimostrazione.* Per la proprietà distributiva dell'intersezione rispetto all'unione (vedi (1.4.11)) e al complemento (vedi Esercizio 1.4.15) si ha:

$$\begin{aligned} S \cap (T \cup V) &= S \cap ((T \setminus V) \cup (V \setminus T)) \\ &= (S \cap (T \setminus V)) \cup (S \cap (V \setminus T)) \\ &= ((S \cap T) \setminus (S \cap V)) \cup ((S \cap V) \setminus (S \cap T)) \\ &= (S \cap T) \cup (S \cap V). \end{aligned}$$

L'altra uguaglianza segue dalla commutatività dell'intersezione.  $\square$

## Esercizi

**Esercizio 1.4.1.** Si provi 1.4.2.

**Esercizio 1.4.2.** Con  $S, T$  e  $V$  insiemi, si stabilisca se è sempre vero che

$$S \cup V \subseteq T \cup V \implies S \subseteq T.$$

**Esercizio 1.4.3.** Si provi 1.4.5.

**Esercizio 1.4.4.** Con  $S, T$  e  $V$  insiemi, si stabilisca se è sempre vero che

$$S \cap V \subseteq T \cap V \implies S \subseteq T.$$

**Esercizio 1.4.5.** Con  $S, T, V$  e  $W$  insiemi, si ha:

$$\begin{aligned} S \subset T, V \subset W &\not\Rightarrow S \cap V \subset T \cap W, \\ S \subset T &\not\Rightarrow S \cap V \subset T \cap V, \\ S \subset T, S \subset W &\not\Rightarrow S \subset T \cap W. \end{aligned}$$

**Esercizio 1.4.6.** Si provi 1.4.7.

**Esercizio 1.4.7.** Si provi 1.4.8.

**Esercizio 1.4.8.** Si provi 1.4.9.

**Esercizio 1.4.9.** Considerati gli insiemi

$$G = \{a, b, c, 2, m, n\}, H = \{b, d, 3, m, 0\}, K = \{d, 3, 0\},$$

si determinino i seguenti insiemi e il loro ordine:

$$\begin{array}{ccccccc} G \cup H, & G \cup K, & H \cup K, & G \cap H, & G \cap K, & H \cap K, \\ G \setminus H, & H \setminus G, & G \setminus K, & K \setminus G, & H \setminus K, & K \setminus H. \end{array}$$

**Esercizio 1.4.10.** Si provi che, con  $S, T, V$  e  $W$  insiemi, si ha:

$$S \subseteq V, T \subseteq W \implies S \setminus W \subseteq V \setminus T,$$

o equivalentemente

$$S \subseteq V, T \subseteq W \implies W \setminus S \supseteq T \setminus V,$$

e se ne deduca che

$$\begin{aligned} S \subseteq V &\implies S \setminus T \subseteq V \setminus T, \\ S \subseteq V &\implies T \setminus S \supseteq T \setminus V. \end{aligned}$$

**Esercizio 1.4.11.** Si provi che, con  $S, T, V$  e  $W$  insiemi, si ha:

$$\begin{aligned} S \subset V, T \subset W &\not\implies S \setminus W \subset V \setminus T, \\ S \subset V, T \subset W &\not\implies W \setminus S \supseteq T \setminus V, \end{aligned}$$

da cui

$$\begin{aligned} S \subset V &\not\implies S \setminus T \subset V \setminus T, \\ S \subset V &\not\implies T \setminus S \supseteq T \setminus V. \end{aligned}$$

**Esercizio 1.4.12.** Si provi con un esempio che, con  $S, T$  e  $V$  insiemi, le ugualanze:

$$\begin{aligned} S \setminus (T \cup V) &= (S \setminus T) \cup (S \setminus V), \\ S \setminus (T \cap V) &= (S \setminus T) \cap (S \setminus V) \end{aligned}$$

non sono sempre soddisfatte.

*Suggerimento.* Si considerino gli insiemi:  $\{a, b, c\}$ ,  $\{a, b\}$  e  $\{a, c\}$ .

**Esercizio 1.4.13.** Si provi che, con  $S$  e  $T$  insiemi, si ha:

$$S \setminus (S \setminus T) = S \cap T,$$

e, utilizzando (1.4.15) e (1.4.14), si ritrovi che non vale la proprietà associativa del complemento.

Più in generale si ha:

**Esercizio 1.4.14.** Si provi che, con  $S, T$  e  $V$  insiemi, si ha:

$$\begin{aligned} S \setminus (T \setminus V) &= (S \setminus T) \cup (S \cap V), \\ (S \setminus T) \setminus V &= S \setminus (T \cup V). \end{aligned}$$

*Svolgimento.* Si ha:

$$\begin{aligned} x \in S \setminus (T \setminus V) &\iff x \in S \text{ e } x \notin T \setminus V \\ &\iff x \in S \text{ e } (x \notin T \text{ o } x \in V) \\ &\iff (x \in S \text{ e } x \notin T) \text{ o } (x \in S \text{ e } x \in V) \\ &\iff x \in S \setminus T \text{ o } x \in S \cap V \\ &\iff x \in (S \setminus T) \cup (S \cap V). \end{aligned}$$

Inoltre:

$$\begin{aligned} x \in (S \setminus T) \setminus V &\iff x \in S \setminus T \text{ e } x \notin V \\ &\iff (x \in S \text{ e } x \notin T) \text{ e } x \notin V \\ &\iff (x \in S) \text{ e } (x \notin T \text{ e } x \notin V) \\ &\iff x \in S \text{ e } x \notin T \cup V \\ &\iff x \in S \setminus (T \cup V). \end{aligned}$$

**Esercizio 1.4.15.** Con  $S, T$  e  $V$  insiemi, si provi che:

$$S \cap (T \setminus V) = (S \cap T) \setminus (S \cap V)$$

$$(S \setminus T) \cap V = (S \cap V) \setminus (T \cap V)$$

(proprietà distributiva dell'intersezione rispetto al complemento).

**Esercizio 1.4.16.** Si descrivano i seguenti insiemi:

$$\begin{array}{lll} \mathbb{N} \cup \{3, -4, a\}, & \mathbb{N} \cap \{3, -4, a\}, & \mathbb{N} \setminus \{3, -4, a\}, \\ \mathbb{Z} \cup \{3, -4, a\}, & \mathbb{Z} \cap \{3, -4, a\}, & \mathbb{Z} \setminus \{3, -4, a\}, \\ \{3, -4, a\} \setminus \mathbb{N}, & \{3, -4, a\} \setminus \mathbb{N}_0, & \{3, -4, a\} \setminus \mathbb{Z}, \\ \mathbb{N} \dot{\cup} \{3, -4, a\}, & \mathbb{N}_0 \dot{\cup} \{3, -4, a\}, & \mathbb{Z} \dot{\cup} \{3, -4, a\}. \end{array}$$

**Esercizio 1.4.17.** Si descrivano i seguenti insiemi:  $6\mathbb{N} \cup 9\mathbb{Z}$ ,  $6\mathbb{N} \cap 9\mathbb{Z}$ ,  $6\mathbb{N} \setminus 9\mathbb{Z}$ ,  $9\mathbb{Z} \setminus 6\mathbb{N}$ ,  $9\mathbb{Z} \dot{\cup} 6\mathbb{N}$ ,  $9\mathbb{Z} \dot{\cup} 6\mathbb{N}_0$ .

**Esercizio 1.4.18.** Con  $M, N$  e  $L$  insiemi, si rappresentino mediante i diagrammi di Venn gli insiemi:

$$\begin{array}{lll} L \setminus (L \setminus M), & L \dot{\cup} M, & L \setminus (M \setminus L), \\ (M \dot{\cup} N) \setminus (L \cap N), & (L \cap N) \setminus (N \setminus M), & (L \setminus M) \cup (M \setminus N), \\ (M \dot{\cup} N) \setminus L, & (L \cap N) \cup (M \setminus L), & (L \setminus M) \cap N, \\ L \setminus (M \dot{\cup} N), & (L \cup N) \cap (M \setminus L), & (L \setminus M) \cup N. \end{array}$$

**Esercizio 1.4.19.** Con  $S$  e  $T$  insiemi, si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{ll} x \notin S \cup T \iff x \notin S \text{ o } x \notin T; & x \notin S \cap T \iff x \notin S \text{ o } x \notin T; \\ x \notin S \cup T \iff x \notin S \text{ e } x \notin T; & x \notin S \cap T \iff x \notin S \text{ e } x \notin T; \\ x \notin S \setminus T \iff x \notin S \text{ o } x \in T; & x \notin S \setminus T \iff x \notin S \text{ e } x \notin T; \\ x \notin S \setminus T \iff x \notin S \text{ e } x \in T; & x \notin S \setminus T \iff x \notin S \text{ o } x \notin T. \end{array}$$

**Esercizio 1.4.20.** Si provi con un esempio che l'uguaglianza  $A \cup B = A \cup (B \setminus C)$ , con  $A, B, C$  insiemi, non è sempre soddisfatta.

**Esercizio 1.4.21.** Si provi con un esempio che l'uguaglianza  $A \cap B = A \cap (B \setminus C)$ , con  $A, B, C$  insiemi, non è sempre soddisfatta.

**Esercizio 1.4.22.** Si provi con un esempio che l'uguaglianza  $S \setminus T = S \setminus (T \cap V)$ , con  $S, T, V$  insiemi, non è sempre soddisfatta.

**Esercizio 1.4.23.** Si dimostri che, con  $S, T, V$  insiemi, si ha:

$$\begin{aligned} S \setminus (T \setminus V) &= S \iff S \cap T \subseteq V, \\ S \setminus T &= S \setminus V \iff S \cap T = S \cap V. \end{aligned}$$

**Esercizio 1.4.24.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{lllll} -3 \in \mathbb{Z} \setminus \mathbb{N}, & 3 \in \mathbb{Z} \setminus \mathbb{N}, & -3 \in 2\mathbb{Z} \setminus \mathbb{N}, & 3 \in 2\mathbb{Z} \setminus \mathbb{N}, & 0 \in \mathbb{Z} \setminus \mathbb{N}, \\ 5 \in 2\mathbb{Z} \cup \mathbb{N}, & -5 \in 2\mathbb{Z} \cup \mathbb{N}, & 0 \in 2\mathbb{Z} \cup \mathbb{N}, & -4 \in 2\mathbb{Z} \cup \mathbb{N}, & 4 \in 2\mathbb{Z} \cup \mathbb{N}, \\ 0 \in 2\mathbb{Z} \cap \mathbb{N}, & -4 \in 2\mathbb{Z} \cap \mathbb{N}, & 4 \in 2\mathbb{Z} \cap \mathbb{N}, & -5 \in 2\mathbb{Z} \cap \mathbb{N}, & 5 \in 2\mathbb{Z} \cap \mathbb{N}. \end{array}$$

**Esercizio 1.4.25.** Con  $V$  insieme, si precisino i seguenti insiemi:

$$\begin{array}{lll} V \cup (\emptyset \setminus V), & V \cap (\emptyset \setminus V), & V \cup (V \setminus V), \\ V \cap (V \setminus V), & V \setminus (\emptyset \cup V), & V \setminus (\emptyset \cap V), \\ V \cap (V \setminus \emptyset), & V \setminus (V \setminus \emptyset), & V \setminus (\emptyset \setminus V), \\ V \cup (V \cap \emptyset), & V \setminus (V \setminus V), & V \cup (V \setminus \emptyset). \end{array}$$

**Esercizio 1.4.26.** Posto

$$A = \{a, 4, c, \frac{1}{3}, \sqrt{5}\}, \quad B = \{b, 7, i, \frac{1}{3}\}, \quad C = \{a, b, c, \frac{1}{3}, 7, \sqrt{15}\},$$

si determinino gli insiemi  $A \cup (B \setminus C)$  e  $(A \cup B) \setminus (A \cup C)$  e se ne deduca che, con  $S, T, V$  insiemi, l'uguaglianza  $S \cup (T \setminus V) = (S \cup T) \setminus (S \cup V)$  non sempre sussiste. Si verifichi poi che vale comunque:  $S \cup (T \setminus V) \supseteq (S \cup T) \setminus (S \cup V)$ .

**Esercizio 1.4.27.** Si provi che, con  $S, T, V$  insiemi, si ha:

$$(S \setminus T) \cap V = (S \cap V) \setminus T.$$

**Esercizio 1.4.28.** Si provi che, con  $S, T, V$  insiemi, si ha:

$$(S \cup T) \setminus (T \cap V) = (S \setminus T) \cup (T \setminus V).$$

**Esercizio 1.4.29.** Con  $L, M, N$  insiemi, si confrontino gli insiemi  $L \cup (M \setminus N)$  e  $(L \cup M) \setminus N$ . Si dimostri poi che  $L \cup (M \setminus N) = (L \cup M) \setminus (N \setminus L)$ .

**Esercizio 1.4.30.** Si provi che:

$$S \cap T \neq \emptyset, T \cap V \neq \emptyset, S \cap V \neq \emptyset \Rightarrow S \cap T \cap V \neq \emptyset.$$

**Esercizio 1.4.31.** Si dimostri che, con  $L, M$  e  $N$  insiemi, si ha:

$$L \setminus (M \cap N) = L \setminus (L \cap M \cap N).$$

**Esercizio 1.4.32.** Si dimostri che, con  $L, M$  e  $N$  insiemi, si ha:

$$L \setminus (N \setminus (L \cap M)) = L \iff L \cap N \subseteq M.$$

**Esercizio 1.4.33.** Si dimostri che, con  $L, M$  e  $N$  insiemi, si ha:

$$(L \setminus M) \cup (L \cap N) = L \iff (L \cap M) \setminus N = \emptyset.$$

**Esercizio 1.4.34.** Si provi che, con  $S$  e  $T$  insiemi, si ha  $S = (S \setminus T) \cup (S \cap T)$ , e  $(S \setminus T) \cap (S \cap T) = \emptyset$ .

**Esercizio 1.4.35.** Si provi che, con  $S$  e  $T$  insiemi, si ha:

$$S \cup T = (S \setminus T) \cup (T \setminus S) \cup (S \cap T),$$

dove gli insiemi  $S \setminus T, T \setminus S$  e  $S \cap T$  sono a due a due disgiunti.

**Esercizio 1.4.36.** Si ritrovi l'uguaglianza  $S \dot{\cup} T = (S \setminus T) \cup (T \setminus S)$  utilizzando le formule di De Morgan.

**Esercizio 1.4.37.** Si provi con un esempio che non sempre vale l'uguaglianza

$$S \cup (T \dot{\cup} V) = (S \cup T) \dot{\cup} (S \cup V).$$

Si provi però che riesce sempre  $S \cup (T \dot{\cup} V) \supseteq (S \cup T) \dot{\cup} (S \cup V)$ .

**Esercizio 1.4.38.** Siano  $S$  un insieme e  $\mathcal{F}$  un insieme di insiemi. Si provi che:

$$\left( \bigcup_{X \in \mathcal{F}} X \right) \setminus S = \bigcup_{X \in \mathcal{F}} (X \setminus S)$$

(proprietà distributiva a destra del complemento rispetto all'unione),

$$\left( \bigcap_{X \in \mathcal{F}} X \right) \setminus S = \bigcap_{X \in \mathcal{F}} (X \setminus S)$$

(proprietà distributiva a destra del complemento rispetto all'intersezione).

**Esercizio 1.4.39** (Formule di De Morgan). *Siano  $S$  un insieme e  $\mathcal{F}$  un insieme di insiemi. Si provi che:*

$$\begin{aligned} S \setminus \left( \bigcup_{X \in \mathcal{F}} X \right) &= \bigcap_{X \in \mathcal{F}} (S \setminus X) \\ S \setminus \left( \bigcap_{X \in \mathcal{F}} X \right) &= \bigcup_{X \in \mathcal{F}} (S \setminus X). \end{aligned}$$

## 1.5 Prodotto cartesiano

Si presenterà ora un'ulteriore operazione tra insiemi: il prodotto cartesiano.

Il simbolo  $(x, y)$  sta a denotare la **coppia** (ordinata) di prima **coordinata**  $x$  e seconda coordinata  $y$ , con la convenzione che:

$$(x, y) = (x', y') \iff x = x' \text{ e } y = y'. \quad (1.5.1)$$

Con  $S$  e  $T$  insiemi, il **prodotto cartesiano**  $S \times T$  di  $S$  e  $T$  è l'insieme costituito da tutte le coppie di prima coordinata un elemento di  $S$  e seconda coordinata un elemento di  $T$ :

$$S \times T := \{(x, y) : x \in S, y \in T\}.$$

Pertanto:

$$(x, y) \in S \times T : \iff x \in S \text{ e } y \in T,$$

$$(x, y) \notin S \times T \iff x \notin S \text{ o } y \notin T.$$

Per esempio, se  $A = \{a, b, c\}$  e  $B = \{1, 2\}$ , si ha:

$$\begin{aligned} A \times B &= \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}, \\ B \times A &= \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}, \\ A \times A &= \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}, \\ B \times B &= \{(1, 1), (1, 2), (2, 1), (2, 2)\}, \end{aligned}$$

con

$$|A \times B| = 6 = |B \times A|, |A \times A| = 9, |B \times B| = 4.$$

Per ogni insieme  $S$  si ha:

$$\emptyset \times S = \emptyset = S \times \emptyset. \quad (1.5.2)$$

Il sottoinsieme di  $S \times S$  costituito da tutte e sole le coppie di coordinate uguali è denotato con  $\Delta_S$  e chiamato la **diagonale** di  $S$ . Per esempio, se  $A$  e  $B$  sono gli insiemi prima definiti, si ha:

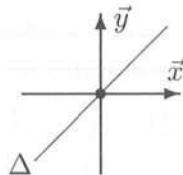
$$\Delta_A = \{(a, a), (b, b), (c, c)\},$$

$$\Delta_B = \{(1,1), (2,2)\}.$$

Ovviamente, se  $S$  e  $T$  sono insiemi finiti, si ha:

$$|S \times T| = |S| \cdot |T| = |T \times S|, \quad |\Delta_S| = |S|.$$

Il termine “*prodotto cartesiano*” prende origine dall’usuale rappresentazione come coppie di numeri reali dei punti di un piano in cui è assegnato un riferimento cartesiano. Se tale riferimento è monometrico ortogonale, i punti del piano rappresentati da coppie con coordinate uguali sono esattamente i punti della cosiddetta “*diagonale principale*”, cioè della bisettrice del primo e del terzo quadrante:



Ciò giustifica il termine utilizzato per  $\Delta_S$ .

**Osservazione.** È possibile definire la coppia  $(x, y)$  nel seguente modo:

$$(x, y) := \{x, \{x, y\}\}.$$

Tale posizione assicura, come è facile verificare, che è soddisfatta la proprietà (1.5.1), che non deve, quindi, essere imposta. Queste considerazioni comunque esulano dagli scopi prefissi.

Con  $S, T, V, W$  insiemi, si ha:

$$S \subseteq V, T \subseteq W \implies S \times T \subseteq V \times W. \quad (1.5.3)$$

Supposto  $S, T \neq \emptyset$ , si ha anche:

$$S \times T \subseteq V \times W \implies S \subseteq V, T \subseteq W. \quad (1.5.4)$$

Quindi:

**1.5.1.** *Se  $S, T, V$  e  $W$  sono insiemi non vuoti, si ha:*

$$S \times T = V \times W \iff S = V \text{ e } T = W.$$

*Dimostrazione.* Per provare la (1.5.3) basta osservare che, se  $(x, y) \in S \times T$ , allora  $x \in S$  e  $y \in T$ , sicché, per le ipotesi,  $x \in V$  e  $y \in W$ , da cui segue, per definizione,  $(x, y) \in V \times W$ .

Supposto ora  $S \times T \subseteq V \times W$  con  $S, T \neq \emptyset$ , si ha che esistono  $\bar{x} \in S$  e  $\bar{y} \in T$ . Pertanto per ogni  $x \in S$  si ha  $(x, \bar{y}) \in S \times T$  e dunque  $(x, \bar{y}) \in V \times W$ , da cui  $x \in V$ . Analogamente  $T \subseteq W$ . Ciò prova la (1.5.4).  $\square$

Ne segue che:

**1.5.2.** Se  $S$  e  $T$  sono insiemi si ha:

$$S \times T = T \times S \iff S = \emptyset \text{ o } T = \emptyset \text{ o } S = T.$$

*Dimostrazione.* Esercizio □

Si noti che un sottoinsieme di un prodotto cartesiano può non essere un prodotto cartesiano; si ha cioè, con  $S$  e  $T$  insiemi:

$$U \subseteq S \times T \not\Rightarrow (\exists X \subseteq S, Y \subseteq T : U = X \times Y).$$

Come esempio si possono considerare gli insiemi:

$$S = \{a, b, c\}, T = \{1, 2\}, U = \{(a, 1), (b, 2)\}.$$

È facile verificare che:

**1.5.3.** Con  $S, T$  e  $V$  insiemi, si ha:

$$(S \cup V) \times T = (S \times T) \cup (V \times T)$$

(proprietà distributiva a destra del prodotto rispetto all'unione),

$$(S \cap V) \times T = (S \times T) \cap (V \times T)$$

(proprietà distributiva a destra del prodotto rispetto all'intersezione),

$$(S \setminus V) \times T = (S \times T) \setminus (V \times T)$$

(proprietà distributiva a destra del prodotto rispetto al complemento).

*Dimostrazione.* Per la prima uguaglianza, si osservi che:

$$\begin{aligned} (x, y) \in (S \cup V) \times T &\iff x \in S \cup V \text{ e } y \in T \\ &\iff (x \in S \text{ o } x \in V) \text{ e } y \in T \\ &\iff (x \in S \text{ e } y \in T) \text{ o } (x \in V \text{ e } y \in T) \\ &\iff (x, y) \in S \times T \text{ o } (x, y) \in V \times T \\ &\iff (x, y) \in (S \times T) \cup (V \times T). \end{aligned}$$

La seconda uguaglianza si prova analogamente. Infine si ha:

$$\begin{aligned} (x, y) \in (S \setminus V) \times T &\iff x \in S \setminus V \text{ e } y \in T \\ &\iff (x \in S \text{ e } x \notin V) \text{ e } y \in T \\ &\iff (x \in S \text{ e } y \in T) \text{ e } (x \notin V \text{ e } y \in T) \\ &\iff (x, y) \in S \times T \text{ e } (x, y) \notin V \times T \\ &\iff (x, y) \in (S \times T) \setminus (V \times T). \end{aligned}$$

Si noti che la penultima equivalenza discende dalla seguente ovvia osservazione: se  $y \in T$  allora  $(x, y) \notin V \times T \iff x \notin V$ . □

In maniera analoga si prova che:

**1.5.4.** Con  $S, T$  e  $V$  insiemi, si ha:

$$S \times (T \cup V) = (S \times T) \cup (S \times V)$$

(proprietà distributiva a sinistra del prodotto rispetto all'unione),

$$S \times (T \cap V) = (S \times T) \cap (S \times V)$$

(proprietà distributiva a sinistra del prodotto rispetto all'intersezione),

$$S \times (T \setminus V) = (S \times T) \setminus (S \times V)$$

(proprietà distributiva a sinistra del prodotto rispetto al complemento).

Con  $S_1, S_2, \dots, S_n$  ( $n \geq 2$ ) insiemi, si parla anche del prodotto cartesiano

$$S_1 \times S_2 \times \cdots \times S_n,$$

intendendo l'insieme di tutte e sole le cosiddette  **$n$ -uple**

$$(x_1, x_2, \dots, x_n),$$

con  $x_1 \in S_1, x_2 \in S_2, \dots, x_n \in S_n$ , dove per le  $n$ -uple si fanno considerazioni analoghe a quelle fatte per le coppie. Pertanto:

$$(x_1, x_2, \dots, x_n) = (y_1, y_2, \dots, y_n) \iff x_1 = y_1, x_2 = y_2, \dots, x_n = y_n.$$

Inoltre:

$$(x_1, x_2, \dots, x_n) \in S_1 \times S_2 \times \cdots \times S_n \iff x_1 \in S_1, x_2 \in S_2, \dots, x_n \in S_n,$$

$$(x_1, x_2, \dots, x_n) \notin S_1 \times S_2 \times \cdots \times S_n \iff \exists i \in \{1, 2, \dots, n\} : x_i \notin S_i.$$

Se  $S_1 = S_2 = \cdots = S_n = S$ , il prodotto cartesiano  $S_1 \times S_2 \times \cdots \times S_n$  viene detto "prodotto cartesiano di  $n$  copie di  $S$ " e denotato col simbolo  $S^n$ . Quindi si ha:

$$S^n := \underbrace{S \times S \times \cdots \times S}_{n \text{ volte}} = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in S\}.$$

## Esercizi

**Esercizio 1.5.1.** Si verifichi che nella (1.5.4) è essenziale l'ipotesi  $S, T \neq \emptyset$ .

**Esercizio 1.5.2.** Si provi 1.5.2.

**Esercizio 1.5.3.** Considerati gli insiemi  $V = \{9, \infty\}, W = \{m, \diamond, 9, \alpha\}$ , si determinino i seguenti insiemi:  $V \times W, V \times V, W \times V, W \times W, \Delta_V, \Delta_W$ .

**Esercizio 1.5.4.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{aligned} (-1, 3) &\in \mathbb{Z} \times \mathbb{N}; & (-1, 3) &\in \mathbb{N} \times \mathbb{Z}; & (-1, 3) &\in \mathbb{Z} \times \mathbb{Z}; & (-1, 3) &\in \mathbb{N} \times \mathbb{N}; \\ (1, 0) &\in \mathbb{Z} \times \mathbb{N}_0; & (1, 0) &\in \mathbb{N} \times \mathbb{Z}; & (1, 0) &\in \mathbb{N} \times \mathbb{N}_0; & (1, 0) &\in \mathbb{N} \times \mathbb{N}; \\ (0, 0) &\in \mathbb{Z} \times \mathbb{Z}; & (0, 0) &\in \mathbb{N}_0 \times \mathbb{N}_0; & (0, 0) &\in \mathbb{N}_0 \times \mathbb{Z}; & (0, 0) &\in \mathbb{N} \times \mathbb{Z}; \\ (4, -5) &\in 2\mathbb{Z} \times \mathbb{Z}; & (4, -5) &\in 2\mathbb{Z} \times \mathbb{N}; & (4, -5) &\in \mathbb{N} \times 2\mathbb{Z}; & (4, -5) &\in 2\mathbb{N} \times \mathbb{Z}. \end{aligned}$$

**Esercizio 1.5.5.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{aligned} (\mathbb{N}_0, \emptyset) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (\emptyset, \mathbb{N}_0) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); \\ (\emptyset, \mathbb{Z}) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (\mathbb{N}, \mathbb{N}_0) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); \\ (\mathbb{N}, \mathbb{N}) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (2, 7) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); \\ (\{\emptyset\}, \{\emptyset\}) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (1, -5) &\in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}). \end{aligned}$$

**Esercizio 1.5.6.** Si provi che, con  $S, T, V$  e  $W$  insiemi, si ha:

- (i)  $(S \cup V) \times (T \cup W) = (S \times T) \cup (S \times W) \cup (V \times T) \cup (V \times W)$ ,
- (ii)  $(S \cap V) \times (T \cap W) = (S \times T) \cap (V \times W)$ ,
- (iii)  $(S \setminus V) \times (T \setminus W) = (S \times T) \setminus ((S \times W) \cup (V \times T))$ ,
- (iv)  $(S \times T) \setminus (V \times W) = ((S \setminus V) \times T) \cup (S \times (T \setminus W))$ .

*Svolgimento.* Si ha:

$$\begin{aligned} (x, y) \in (S \cup V) \times (T \cup W) &\iff x \in S \cup V \text{ e } y \in T \cup W \\ &\iff (x \in S \text{ o } x \in V) \text{ e } (y \in T \text{ o } y \in W) \\ &\iff (x \in S \text{ e } y \in T) \text{ o } (x \in S \text{ e } y \in W) \text{ o} \\ &\quad (x \in V \text{ e } y \in T) \text{ o } (x \in V \text{ e } y \in W) \\ &\iff (x, y) \in S \times T \text{ o } (x, y) \in S \times W \text{ o} \\ &\quad (x, y) \in V \times T \text{ o } (x, y) \in V \times W \\ &\iff (x, y) \in (S \times T) \cup (S \times W) \cup \\ &\quad \cup (V \times T) \cup (V \times W). \end{aligned}$$

e ciò prova la (i). Inoltre:

$$\begin{aligned} (x, y) \in (S \cap V) \times (T \cap W) &\iff x \in S \cap V \text{ e } y \in T \cap W \\ &\iff (x \in S \text{ e } x \in V) \text{ e } (y \in T \text{ e } y \in W) \\ &\iff (x \in S \text{ e } y \in T) \text{ e } (x \in V \text{ e } y \in W) \\ &\iff (x, y) \in S \times T \text{ e } (x, y) \in V \times W \\ &\iff (x, y) \in (S \times T) \cap (V \times W). \end{aligned}$$

e la (ii) è dimostrata.

Infine per dimostrare la (iii) e la (iv) si osservi che:

$$\begin{aligned}
 (x, y) \in (S \setminus V) \times (T \setminus W) &\iff x \in S \setminus V \text{ e } y \in T \setminus W \\
 &\iff (x \in S \text{ e } x \notin V) \text{ e } (y \in T \text{ e } y \notin W) \\
 &\iff (x, y) \in S \times T \text{ e } (x, y) \notin S \times W \text{ e} \\
 &\qquad\qquad\qquad (x, y) \notin V \times T \\
 &\iff (x, y) \in (S \times T) \setminus ((S \times W) \cup (V \times T)),
 \end{aligned}$$

e

$$\begin{aligned}
 (x, y) \in (S \times T) \setminus (V \times W) &\iff (x, y) \in S \times T \text{ e } (x, y) \notin V \times W \\
 &\iff (x \in S \text{ e } y \in T) \text{ e } (x \notin V \text{ o } y \notin W) \\
 &\iff (x \in S \text{ e } x \notin V \text{ e } y \in T) \text{ o} \\
 &\qquad\qquad\qquad (x \in S \text{ e } y \in T \text{ e } y \notin W) \\
 &\iff (x \in S \setminus V \text{ e } y \in T) \text{ o} \\
 &\qquad\qquad\qquad (x \in S \text{ e } y \in T \setminus W) \\
 &\iff (x, y) \in (S \setminus V) \times T \text{ o} \\
 &\qquad\qquad\qquad (x, y) \in S \times (T \setminus W) \\
 &\iff (x, y) \in ((S \setminus V) \times T) \cup (S \times (T \setminus W)).
 \end{aligned}$$

## 1.6 Esercizi di riepilogo

**Esercizio 1.6.1.** Si dimostri per induzione su  $n$  che:

$$4 + 6 + 8 + \cdots + 2n = n(n+1) - 2, \text{ per ogni } n \geq 2.$$

**Esercizio 1.6.2.** Si dimostri per induzione su  $n$  che:

$$12 + 14 + \cdots + 2n = n(n+1) - 30, \text{ per ogni } n \geq 6.$$

**Esercizio 1.6.3.** Si dimostri per induzione su  $n$  che:

$$3 \cdot 2^3 + 4 \cdot 2^4 + \cdots + n \cdot 2^n = 8(2^{n-2}(n-1) - 1), \text{ per ogni } n \geq 3.$$

**Esercizio 1.6.4.** Si dimostri per induzione su  $n$  che:

$$2^5 + 2^6 + \cdots + 2^n = 2^{n+1} - 32, \text{ per ogni } n \geq 5.$$

**Esercizio 1.6.5.** Si dimostri per induzione su  $n$  che:

$$6^0 + 6^1 + 6^2 + \cdots + 6^n = \frac{6^{(n+1)} - 1}{5}, \text{ per ogni } n \geq 0.$$

**Esercizio 1.6.6.** Si dimostri per induzione su  $n$  che:

$$4^3 + 5^3 + 6^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} - 36, \text{ per ogni } n \geq 4.$$

**Esercizio 1.6.7.** Si dimostri per induzione su  $n$  che:

$$1 + 7 + 13 + \cdots + (6n-5) = 3n^2 - 2n, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.8.** Si dimostri per induzione su  $n$  che:

$$\frac{1}{5} + \frac{1}{5^2} + \cdots + \frac{1}{5^n} = \frac{5^n - 1}{4 \cdot 5^n}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.9.** Si dimostri per induzione che:

$$43|44^n - 1, \text{ per ogni } n \geq 0.$$

**Esercizio 1.6.10.** Si dimostri per induzione che:

$$63|8^{2n} - 1, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.11.** Si dimostri per induzione su  $n$  che:

$$10 + 15 + \cdots + 5n = \frac{5(n^2 + n - 2)}{2}, \text{ per ogni } n \geq 2.$$

**Esercizio 1.6.12.** Si dimostri per induzione su  $n$  che:

$$10 + 19 + 28 + \cdots + (9n+1) = \frac{9n^2 + 11n}{2}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.13.** Si dimostri per induzione su  $n$  che:

$$35|6^{2n} - 1, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.14.** Si dimostri per induzione su  $n$  che:

$$26|3^{3n} - 1, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.15.** Si dimostri per induzione su  $n$  che:

$$4^2 + 5^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} - 14, \text{ per ogni } n \geq 4.$$

**Esercizio 1.6.16.** Si dimostri per induzione su  $n$  che:

$$4 \cdot 2^4 + 5 \cdot 2^5 + \cdots + n \cdot 2^n = 16(2^{n-3}(n-1) - 2), \text{ per ogni } n \geq 4.$$

**Esercizio 1.6.17.** Si dimostri per induzione su  $n$  che:

$$1 + \frac{1}{10} + \frac{1}{100} + \cdots + \frac{1}{10^{n-1}} = \frac{10^n - 1}{9 \cdot 10^{n-1}}, \text{ per ogni } n \geq 1.$$

**Esercizio 1.6.18.** Con  $V$  insieme, si precisino i seguenti insiemi:

$$\begin{array}{llll} V \cup V, & V \cup \emptyset, & \emptyset \cup V, & \emptyset \cup \emptyset, \\ V \cap V, & V \cap \emptyset, & \emptyset \cap V, & \emptyset \cap \emptyset, \\ V \setminus V, & V \setminus \emptyset, & \emptyset \setminus V, & \emptyset \setminus \emptyset, \\ V \dot{\cup} V, & V \dot{\cup} \emptyset, & \emptyset \dot{\cup} V, & \emptyset \dot{\cup} \emptyset. \end{array}$$

**Esercizio 1.6.19.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{llll} -4 \in \mathbb{N} \cup 4\mathbb{Z}, & 8 \in \mathbb{N} \cup 4\mathbb{Z}, & -15 \in \mathbb{N} \cup 4\mathbb{Z}, & 15 \in \mathbb{N} \cup 4\mathbb{Z}, \\ -4 \in \mathbb{N} \cap 4\mathbb{Z}, & 8 \in \mathbb{N} \cap 4\mathbb{Z}, & -15 \in \mathbb{N} \cap 4\mathbb{Z}, & 15 \in \mathbb{N} \cap 4\mathbb{Z}, \\ -4 \in \mathbb{N} \setminus 4\mathbb{Z}, & 8 \in \mathbb{N} \setminus 4\mathbb{Z}, & -15 \in \mathbb{N} \setminus 4\mathbb{Z}, & 15 \in \mathbb{N} \setminus 4\mathbb{Z}, \\ -4 \in \mathbb{N} \dot{\cup} 4\mathbb{Z}, & 8 \in \mathbb{N} \dot{\cup} 4\mathbb{Z}, & -15 \in \mathbb{N} \dot{\cup} 4\mathbb{Z}, & 15 \in \mathbb{N} \dot{\cup} 4\mathbb{Z}. \end{array}$$

**Esercizio 1.6.20.** Sia  $A = \{a \in \mathbb{Z} : -6 \leq a \leq 6\}$ . Elencandone gli elementi, si descrivano i seguenti insiemi:

$$(2\mathbb{Z} \cup 3\mathbb{Z}) \cap A, \quad (2\mathbb{Z} \cap 3\mathbb{Z}) \cap A, \quad (2\mathbb{Z} \setminus 3\mathbb{Z}) \cap A, \quad (2\mathbb{Z} \dot{\cup} 3\mathbb{Z}) \cap A.$$

**Esercizio 1.6.21.** Si provi che, con  $S$  e  $T$  insiemi, si ha:

$$\begin{aligned} \mathcal{P}(S \cap T) &= \mathcal{P}(S) \cap \mathcal{P}(T) \\ \mathcal{P}(S) \cup \mathcal{P}(T) &\subseteq \mathcal{P}(S \cup T) \end{aligned}$$

e si verifichi con un esempio che quest'ultima inclusione può essere stretta.

**Esercizio 1.6.22.** Si dimostri che, con  $L, M$  e  $N$  insiemi, si ha:

$$(L \cup M) \setminus N = (L \setminus N) \cup (M \setminus (L \cup N)).$$

**Esercizio 1.6.23.** Si dimostri che, con  $L, M$  e  $N$  insiemi, si ha:

$$L \setminus (M \cup N) = L \setminus M \iff L \cap N \subseteq M.$$

**Esercizio 1.6.24.** Si provi che, con  $S$  e  $T$  insiemi, si ha  $S \cup T = S \cup (T \setminus S)$ , e  $S \cap (T \setminus S) = \emptyset$ .

**Esercizio 1.6.25.** Si provi che, con  $S$  e  $T$  insiemi, si ha:

$$S \subseteq T \iff T = S \cup (T \setminus S).$$

**Esercizio 1.6.26.** Si provi che, con  $S$ ,  $T$  e  $V$  insiemi, si ha:

$$(S \cup T) \setminus (S \cup V) = T \setminus (S \cup V).$$

**Esercizio 1.6.27.** Si provi l'associatività dell'unione disgiunta mostrando che, con  $S$ ,  $T$  e  $V$  insiemi, si ha che  $(S \dot{\cup} T) \dot{\cup} V$  e  $S \dot{\cup} (T \dot{\cup} V)$  coincidono con l'insieme  $(S \setminus (T \cup V)) \cup (T \setminus (S \cup V)) \cup (V \setminus (S \cup T)) \cup (S \cap T \cap V)$ .

*Suggerimento.* Si faccia uso della (1.4.19), della (1.4.18) e dell'Esercizio 1.4.14 per provare che:  $(S \dot{\cup} T) \setminus V = (S \setminus (T \cup V)) \cup (T \setminus (S \cup V))$ ,  $V \setminus (S \dot{\cup} T) = (V \setminus (S \cup T)) \cup (S \cap T \cap V)$ .

**Esercizio 1.6.28.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{ll} (\emptyset, 3) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0; & (\{-4\}, 3) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0; \\ (\{\emptyset\}, 3) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0; & (\mathbb{N}_0, 6) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0; \\ (\emptyset, 4) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); & (\{-4\}, 3) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); \\ (\mathbb{Z}, \emptyset) \in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (\mathbb{N}, \mathbb{Z}) \in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); \\ (\{1, -1\}, 3\mathbb{N}) \in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); & (3\mathbb{N}, \{1, -1\}) \in \mathcal{P}(\mathbb{N}_0) \times \mathcal{P}(\mathbb{Z}); \\ (3\mathbb{Z}, -3) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0; & (\mathbb{N}, 3) \in \mathcal{P}(\mathbb{Z}) \times \mathbb{N}_0. \end{array}$$

**Esercizio 1.6.29.** Si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{ll} (5\mathbb{Z}, \{\mathbb{N}\}) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); & (\{-9\}, 2) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); \\ (\emptyset, 8) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); & (\{\emptyset\}, 2) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); \\ (\mathbb{N}_0, 6) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); & (\mathbb{N}, 2) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); \\ (\{-4\}, 2) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0); & (2\mathbb{Z}, -2) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{N}_0). \end{array}$$

**Esercizio 1.6.30.** Con  $S$ ,  $T$  e  $V$  insiemi, si rappresentino mediante i diagrammi di Venn gli insiemi:

$$\begin{array}{lll} T \setminus (S \cup V), & S \cup (T \setminus V), & V \setminus (S \cap T), \\ T \setminus (S \cap V), & S \cap (T \setminus V), & V \setminus (S \cup T), \\ T \setminus (S \dot{\cup} V), & (S \dot{\cup} T) \setminus (S \dot{\cup} V), & (S \cup T) \setminus (S \cup V), \\ (S \setminus V) \cup (T \cap V), & V \setminus (S \dot{\cup} T), & (S \setminus T) \cup (V \setminus S). \end{array}$$

**Esercizio 1.6.31.** Con  $S$  e  $T$  insiemi, si precisi se le seguenti affermazioni sono vere:

$$\begin{array}{ll} S \cup T = T \iff S \subseteq T, & S \cup T = T \iff T \subseteq S, \\ S \cup T = T \iff T \not\subseteq S, & S \cup T = T \iff S = T, \\ S \cup T = T \iff S \not\subseteq T, & S \cup T = T \iff S = \emptyset, \\ S \setminus T = S \iff S \subseteq T, & S \setminus T = S \iff T \subseteq S, \\ S \setminus T = S \iff S \cap T = \emptyset, & S \setminus T = S \iff T = \emptyset, \\ S \setminus T = S \iff S \cap T \neq \emptyset, & S \setminus T = S \iff S = \emptyset. \end{array}$$

# 2

## Relazioni tra insiemi

In questo capitolo verrà introdotto e studiato un concetto fondamentale, quello di relazione tra insiemi, che formalizza la naturale esigenza di legare tra loro elementi di insiemi.

### 2.1 Nozioni fondamentali

Siano  $S$  e  $T$  insiemi. Un sottoinsieme  $\mathcal{R}$  di  $S \times T$  è detto una **relazione** o **corrispondenza** tra  $S$  e  $T$ . Se  $x \in S$  e  $y \in T$  sono tali che  $(x, y) \in \mathcal{R}$  si scrive  $x \mathcal{R} y$  e si dice che “ $x$  è **nella relazione  $\mathcal{R}$**  con  $y$ ”, o che “ $y$  è **corrispondente in  $\mathcal{R}$**  di  $x$ ”. In caso contrario si scrive  $x \not\mathcal{R} y$ . Pertanto:

$$\begin{aligned} x \mathcal{R} y &: \iff (x, y) \in \mathcal{R}, \\ x \not\mathcal{R} y &\iff (x, y) \notin \mathcal{R}. \end{aligned}$$

**Osservazione.** Nell’assegnare una relazione vanno sempre precisati gli insiemi  $S$  e  $T$  coinvolti, in quanto, ovviamente, un insieme di coppie è sottoinsieme di più prodotti cartesiani. Per tale motivo a volte si preferisce definire una relazione  $\mathcal{R}$  tra insiemi  $S$  e  $T$  come una coppia  $(S \times T, G)$ , con  $S$  e  $T$  insiemi e  $G$  sottoinsieme di  $S \times T$ , ponendo poi  $x \mathcal{R} y \iff (x, y) \in G$ . Se  $S$  e  $T$  sono insiemi non vuoti, si ha dunque, con  $\mathcal{R} = (S \times T, G)$ ,  $\mathcal{R}_1 = (V \times W, G_1)$ ,

$$\mathcal{R} = \mathcal{R}_1 \iff S = V, \quad T = W, \quad G = G_1,$$

per 1.5.1 e (1.5.1). Si è qui preferito evitare questa formalizzazione, con l’intesa, appunto, che, nel considerare una relazione, gli insiemi  $S$  e  $T$  vengano sempre precisati in precedenza.

Si noti che, se  $\mathcal{R}$  e  $\mathcal{R}'$  sono relazioni tra  $S$  e  $T$ , tali relazioni coincidono se e solo se, con  $x \in S$  e  $y \in T$ , si ha:

$$x \mathcal{R} y \iff x \mathcal{R}' y.$$

Assegnare una relazione tra insiemi  $S$  e  $T$  significa quindi individuare un sottoinsieme di  $S \times T$ , cioè “privilegiare” particolari coppie di elementi di  $S \times T$ .

Studiarla vuol dire investigare quali elementi di  $S$  hanno corrispondenti in  $T$  e descrivere questi ultimi.

Considerati gli insiemi  $A = \{a, b, c\}$  e  $B = \{1, 2\}$ , esempi di relazioni tra  $A$  e  $B$  sono i seguenti:

$$\begin{aligned}\mathcal{R}_1 &= \{(a, 1), (a, 2)\}, \\ \mathcal{R}_2 &= \{(a, 2), (b, 2), (c, 1)\}, \\ \mathcal{R}_3 &= \emptyset, \\ \mathcal{R}_4 &= A \times B, \\ \mathcal{R}_5 &= \{(b, 1)\},\end{aligned}$$

e si ha, per esempio:

$$a \mathcal{R}_1 1, b \not\mathcal{R}_1 1, a \mathcal{R}_2 2, c \mathcal{R}_2 2, b \mathcal{R}_5 1, c \not\mathcal{R}_5 1.$$

Si noti che, se  $S$  e  $T$  sono insiemi, ponendo  $\mathcal{R}_0 = \emptyset$  si individua una relazione tra  $S$  e  $T$ , detta la **relazione vuota**, e si ha:

$$x \not\mathcal{R}_0 y, \text{ per ogni } x \in S, y \in T.$$

Così, ponendo  $\mathcal{R}_t = S \times T$ , si ottiene la cosiddetta **relazione totale** (o **piena**) tra  $S$  e  $T$ , caratterizzata dall'essere:

$$x \mathcal{R}_t y, \text{ per ogni } x \in S, y \in T.$$

Ovviamente, per la (1.5.2),  $\mathcal{R}_0 = \mathcal{R}_t$  se e solo se  $S = \emptyset$  o  $T = \emptyset$ .

Si noti inoltre che se  $S = \emptyset$  o  $T = \emptyset$ , da  $S \times T = \emptyset$  segue che la relazione vuota è l'unica relazione tra  $S$  e  $T$ . Pertanto spesso nel seguito si supporrà, a volte tacitamente, che gli insiemi  $S$  e  $T$  in questione siano entrambi non vuoti.

Se  $S$  e  $T$  sono insiemi finiti non vuoti, esiste ovviamente solo un numero finito di relazioni tra  $S$  e  $T$ , e tale numero è:

$$|\mathcal{P}(S \times T)| = 2^{|S \times T|} = 2^{|S| \cdot |T|}.$$

Spesso, per assegnare una relazione  $\mathcal{R}$  tra insiemi  $S$  e  $T$ , si precisa una proprietà che individua tale sottoinsieme di  $S \times T$ , si evidenzia cioè quando una coppia, elemento di  $S \times T$ , appartiene a  $\mathcal{R}$ . Per esempio, ponendo:

$$x \mathcal{R}_1 y : \iff x = y^2,$$

con  $x \in \mathbb{N}_0$  e  $y \in \mathbb{Z}$ , si individua, in maniera forse più efficace, la relazione:

$$\mathcal{R}_1 = \{(x, y) \in \mathbb{N}_0 \times \mathbb{Z} : x = y^2\}.$$

Si noti che tale relazione  $\mathcal{R}_1$  è ben distinta dalla relazione  $\mathcal{R}_2$  definita ponendo:

$$x \mathcal{R}_2 y : \iff x^2 = y,$$

con  $x \in \mathbb{Z}$  e  $y \in \mathbb{N}_0$ .

Se  $\mathcal{R}$  è una relazione tra insiemi  $S$  e  $T$ , si definisce **relazione opposta** (o **inversa** di  $\mathcal{R}$ ) e si indica con  $\mathcal{R}^{\text{op}}$ , la relazione tra  $T$  e  $S$  definita ponendo:

$$\mathcal{R}^{\text{op}} := \{(y, x) : (x, y) \in \mathcal{R}\}.$$

Si ha quindi, con  $y \in T$  e  $x \in S$ :

$$y(\mathcal{R}^{\text{op}})x : \iff x \mathcal{R} y.$$

Ovviamente:

$$(\mathcal{R}^{\text{op}})^{\text{op}} = \mathcal{R}$$

e

$$\mathcal{R} \subseteq \mathcal{R}' \implies \mathcal{R}^{\text{op}} \subseteq (\mathcal{R}')^{\text{op}}.$$

Si noti per esempio che le relazioni  $\mathcal{R}_1$  e  $\mathcal{R}_2$  prima definite sono l'una l'opposta dell'altra. Se  $S$  e  $T$  sono insiemi non vuoti e  $\mathcal{R}$  è una relazione tra  $S$  e  $T$ , può avversi  $\mathcal{R} = \mathcal{R}^{\text{op}}$  solo se  $S = T$ .

Se  $S, T, V$  e  $W$  sono insiemi, con  $V \subseteq S$  e  $W \subseteq T$ , considerata una qualunque relazione  $\mathcal{R}$  tra  $S$  e  $T$ , la relazione  $\mathcal{R} \cap (V \times W)$  tra  $V$  e  $W$  viene detta la **relazione indotta** da  $\mathcal{R}$  su  $V \times W$  e denotata con  $\mathcal{R}|_{V \times W}$ . Si ha pertanto, con  $x \in V$  e  $y \in W$ :

$$x(\mathcal{R}|_{V \times W})y : \iff x \mathcal{R} y.$$

Una relazione tra insiemi  $S$  e  $T$  con  $S = T$  viene detta anche una **relazione binaria** in  $S$ . Un esempio notevole di relazione binaria in un insieme  $S$  è la diagonale  $\Delta_S$ ; tale relazione è detta l'**identità** di  $S$  o l'**uguaglianza** in  $S$  ed è denotata anche con  $\text{id}_S$  o  $1_S$ . Pertanto, con  $x, y \in S$ , si ha:

$$x(\text{id}_S)y : \iff x = y.$$

**2.1.1. Esempio.** Si considerino le seguenti relazioni tra  $\mathbb{N}_0$  e  $\mathbb{Z}$ :

$$\begin{aligned} x \mathcal{R}_1 y &: \iff x + y = 3; \\ x \mathcal{R}_2 y &: \iff x + 4 = y; \\ x \mathcal{R}_3 y &: \iff x = y^3; \\ x \mathcal{R}_4 y &: \iff y = -x^2; \\ x \mathcal{R}_5 y &: \iff x = |y|; \\ x \mathcal{R}_6 y &: \iff x + 4 > y; \\ x \mathcal{R}_7 y &: \iff y + 11 = x. \end{aligned}$$

La relazione  $\mathcal{R}_1$  è tale che ogni  $x \in \mathbb{N}_0$  ha corrispondente e ne ha uno solo, precisamente  $y = 3 - x$ ; dell'analogia proprietà gode  $\mathcal{R}_2$  in quanto ogni  $x \in \mathbb{N}_0$  è in relazione con il solo intero  $y = x + 4$ . Nella relazione  $\mathcal{R}_3$  hanno corrispondenti solo i numeri naturali  $x$  che sono cubi di un intero, per esempio  $0 \mathcal{R}_3 0, 1 \mathcal{R}_3 1, 8 \mathcal{R}_3 2$ , mentre  $2 \not\mathcal{R}_3 y$ , qualunque sia  $y \in \mathbb{Z}$ ; è facile però osservare che se  $x$

ha corrispondente, ne ha uno solo. Ogni  $x \in \mathbb{N}_0$  ha in  $\mathcal{R}_4$  uno e un solo corrispondente, precisamente l'intero  $y = -x^2$ . Nella relazione  $\mathcal{R}_5$  ogni naturale ha corrispondenti, 0 solo 0, ogni  $x \neq 0$  ne ha esattamente due, se stesso e il suo opposto. Anche nella relazione  $\mathcal{R}_6$  ogni naturale  $x$  ha corrispondenti, precisamente ha infiniti corrispondenti, per esempio ogni intero negativo. Infine in  $\mathcal{R}_7$  ogni  $x \in \mathbb{N}_0$  ha uno e un solo corrispondente, l'intero  $x - 11$ .

Con  $S$  e  $T$  insiemi, una relazione  $\mathcal{R}$  tra  $S$  e  $T$  tale che ogni elemento  $x$  di  $S$  ha in  $T$  uno e un solo corrispondente è detta **applicazione o funzione** di  $S$  in  $T$ :

$$\mathcal{R} \text{ applicazione di } S \text{ in } T : \iff \forall x \in S, \exists! y \in T : x \mathcal{R} y.$$

L'insieme  $S$  viene detto il **dominio** dell'applicazione  $\mathcal{R}$ ,  $T$  il **codomino** dell'applicazione  $\mathcal{R}$ . L'unico elemento  $y$  corrispondente di  $x$  viene detto l'**immagine** di  $x$  mediante  $\mathcal{R}$  e denotato con  $\mathcal{R}(x)$ . Si scrive anche:

$$\mathcal{R} : x \in S \longmapsto \mathcal{R}(x) \in T.$$

Una relazione tra  $S$  e  $T$  che sia un'applicazione viene di solito indicata con una lettera minuscola:  $f$  (da “funzione”),  $g, h, \dots$  e si usa la scrittura:  $f : S \longrightarrow T$ .

Per esempio, delle relazioni  $\mathcal{R}_1, \dots, \mathcal{R}_7$  di  $\mathbb{N}_0$  in  $\mathbb{Z}$  esaminate in 2.1.1, sono applicazioni  $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_4, \mathcal{R}_7$  e si ha:

$$\begin{aligned}\mathcal{R}_1 : x \in \mathbb{N}_0 &\longmapsto 3 - x \in \mathbb{Z}, \\ \mathcal{R}_2 : x \in \mathbb{N}_0 &\longmapsto x + 4 \in \mathbb{Z}, \\ \mathcal{R}_4 : x \in \mathbb{N}_0 &\longmapsto -x^2 \in \mathbb{Z}, \\ \mathcal{R}_7 : x \in \mathbb{N}_0 &\longmapsto x - 11 \in \mathbb{Z}.\end{aligned}$$

Il concetto di applicazione tra insiemi, di fondamentale importanza, verrà ripreso e approfondito nel successivo Paragrafo 2.2.

Le relazioni binarie in un insieme possono ovviamente soddisfare la proprietà che definisce le applicazioni, ma possono anche soddisfare altre proprietà di notevole interesse. Queste verranno ora introdotte e analizzate e porteranno a concetti che saranno poi approfonditi nei Paragrafi 2.3 e 2.4.

Sia  $S$  un insieme. Una relazione binaria  $\mathcal{R}$  in  $S$  è detta **riflessiva** se ogni  $x \in S$  è in relazione con se stesso:

$$\mathcal{R} \text{ riflessiva} : \iff (x \mathcal{R} x, \forall x \in S).$$

Ciò significa che:

$$\mathcal{R} \text{ riflessiva} \iff ((x, x) \in \mathcal{R}, \forall x \in S),$$

e quindi:

$$\mathcal{R} \text{ riflessiva} \iff \Delta_S \subseteq \mathcal{R}.$$

Si noti che:

$$\mathcal{R} \text{ non riflessiva} \iff (\exists y \in S : y \not\mathcal{R} y).$$

La relazione  $\mathcal{R}$  è detta **simmetrica** se, con  $x, y \in S$ , da  $x \mathcal{R} y$  segue  $y \mathcal{R} x$ :

$$\mathcal{R} \text{ simmetrica} : \iff (x \mathcal{R} y \implies y \mathcal{R} x).$$

Equivalentemente:

$$\mathcal{R} \text{ simmetrica} \iff ((x, y) \in \mathcal{R} \implies (y, x) \in \mathcal{R}).$$

$\mathcal{R}$  è detta **asimmetrica** se, con  $x, y \in S$ , da  $x \mathcal{R} y$  e  $y \mathcal{R} x$  segue  $x = y$ :

$$\mathcal{R} \text{ asimmetrica} : \iff ((x \mathcal{R} y \text{ e } y \mathcal{R} x) \implies x = y).$$

Si ha cioè:

$$\mathcal{R} \text{ asimmetrica} \iff ((x \mathcal{R} y \text{ e } x \neq y) \implies y \mathcal{R} x),$$

il che ovviamente equivale a:

$$((x, y) \in \mathcal{R}, x \neq y) \implies (y, x) \notin \mathcal{R}.$$

La relazione  $\mathcal{R}$  è detta **transitiva** se, con  $x, y, z \in S$ , da  $x \mathcal{R} y$  e  $y \mathcal{R} z$  segue  $x \mathcal{R} z$ :

$$\mathcal{R} \text{ transitiva} : \iff ((x \mathcal{R} y, y \mathcal{R} z) \implies x \mathcal{R} z),$$

cioè

$$\mathcal{R} \text{ transitiva} \iff (((x, y) \in \mathcal{R}, (y, z) \in \mathcal{R}) \implies (x, z) \in \mathcal{R}).$$

**2.1.2. Esempio.** Sia  $A = \{a, b, c\}$  e si considerino le relazioni:

$$\begin{aligned}\mathcal{R}_1 &= \{(a, b)\}, \\ \mathcal{R}_2 &= \{(a, b), (b, a), (a, a)\}, \\ \mathcal{R}_3 &= \{(a, b), (b, a), (a, a), (b, b)\}, \\ \mathcal{R}_4 &= \{(a, a), (b, b), (c, c), (a, b)\}, \\ \mathcal{R}_5 &= \{(a, a), (b, b), (c, c), (a, b), (b, a)\}\end{aligned}$$

nell'insieme  $A$ . La relazione  $\mathcal{R}_1$  non è riflessiva perché, per esempio,  $b \mathcal{R}_1 b$ , né simmetrica in quanto  $a \mathcal{R}_1 b$  e  $b \mathcal{R}_1 a$ . Inoltre essa è asimmetrica non esistendo elementi distinti  $x, y \in A$  tali che  $x \mathcal{R}_1 y$  e  $y \mathcal{R}_1 x$ , ed è banalmente transitiva. La relazione  $\mathcal{R}_2$  non è riflessiva; è simmetrica e non è asimmetrica. È poi non transitiva in quanto, per esempio,  $b \mathcal{R}_2 a$  e  $a \mathcal{R}_2 b$  ma  $b \not\mathcal{R}_2 b$ . La relazione  $\mathcal{R}_3$  è simmetrica e transitiva, la  $\mathcal{R}_4$  è riflessiva, asimmetrica e transitiva, la  $\mathcal{R}_5$  è riflessiva, simmetrica e transitiva.

Si noti che nello studio della transitività di una relazione  $\mathcal{R}$ , supposti  $x \mathcal{R} y$  e  $y \mathcal{R} z$ , si può assumere  $x \neq y$  e  $y \neq z$ . Infatti se per esempio si ha  $x = y$ , allora banalmente riesce  $x \mathcal{R} z$  e così, se  $y = z$ , ancora ovviamente  $x \mathcal{R} z$ .

Una relazione binaria  $\mathcal{R}$  in un insieme  $S$  è detta d'**equivalenza** se è riflessiva, simmetrica e transitiva. Per esempio la relazione  $\mathcal{R}_5$  di 2.1.2 è d'equivalenza, le altre non lo sono.

Una relazione binaria  $\mathcal{R}$  è detta d'**ordine** se è riflessiva, asimmetrica e transitiva. Nell'Esempio 2.1.2 solo la relazione  $\mathcal{R}_4$  è d'ordine.

**2.1.3.** Siano  $S$  un insieme,  $X$  un suo sottoinsieme,  $\mathcal{R}$  una relazione binaria in  $S$  e  $\mathcal{R}' = \mathcal{R}|_{X \times X}$  la relazione binaria indotta da  $\mathcal{R}$  su  $X$ . Si ha:

$$\begin{aligned}\mathcal{R} \text{ riflessiva} &\implies \mathcal{R}' \text{ riflessiva}, \\ \mathcal{R} \text{ simmetrica} &\implies \mathcal{R}' \text{ simmetrica}, \\ \mathcal{R} \text{ asimmetrica} &\implies \mathcal{R}' \text{ asimmetrica}, \\ \mathcal{R} \text{ transitiva} &\implies \mathcal{R}' \text{ transitiva}.\end{aligned}$$

Ne segue che:

$$\begin{aligned}\mathcal{R} \text{ d'equivalenza in } S &\implies \mathcal{R}' \text{ d'equivalenza in } X, \\ \mathcal{R} \text{ d'ordine in } S &\implies \mathcal{R}' \text{ d'ordine in } X.\end{aligned}$$

*Dimostrazione.* Esercizio. □

## Esercizi

**Esercizio 2.1.1.** Si studi la relazione tra  $\mathbb{N}_0$  e  $\mathbb{Z}$  definita ponendo:

$$x \mathcal{R}_1 y : \iff x = y^2,$$

e la relazione tra  $\mathbb{Z}$  e  $\mathbb{N}_0$  definita ponendo:

$$x \mathcal{R}_2 y : \iff x^2 = y.$$

**Esercizio 2.1.2.** Considerata la relazione tra  $\mathbb{Q}$  e  $\mathbb{Z}$  definita ponendo:

$$x \mathcal{R} y : \iff 49x^2 = y^2,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{ccccccccc}2 \mathcal{R} 14, & 7 \mathcal{R} 1, & -10 \mathcal{R} 70, & 1 \mathcal{R} -7, & 1 \mathcal{R} 1, & -1 \mathcal{R} -7, & \frac{1}{7} \mathcal{R} -1, \\ 1 \mathcal{R} -1, & \frac{1}{4} \mathcal{R} 7, & -1 \mathcal{R} 1, & 0 \mathcal{R} 0, & 2 \mathcal{R} 7, & 1 \mathcal{R} 7, & 1 \mathcal{R} 49.\end{array}$$

*Svolgimento.* Si ha  $2 \mathcal{R} 14$  poiché  $49 \cdot 4 = 14^2$ ;  $7 \mathcal{R} 1$  essendo  $49 \cdot 7^2 \neq 1^2$ ;  $-10 \mathcal{R} 70$  in quanto  $49(-10)^2 = 4900 = 70^2$ ;  $1 \mathcal{R} -7$  perché  $49 \cdot 1^2 = (-7)^2$  e così  $-1 \mathcal{R} -7$ ,  $0 \mathcal{R} 0$ ,  $1 \mathcal{R} 7$ ,  $\frac{1}{7} \mathcal{R} -1$ , mentre  $1 \mathcal{R} 1$ ,  $1 \mathcal{R} -1$ ,  $-1 \mathcal{R} 1$ , in quanto  $49 \cdot 1 \neq 1$ , e così  $\frac{1}{4} \mathcal{R} 7$ ,  $2 \mathcal{R} 7$ ,  $1 \mathcal{R} 49$ .

**Esercizio 2.1.3.** Si consideri in  $\mathbb{Z}$  la relazione binaria definita da:

$$a \mathcal{R} b : \iff (a = b) \text{ oppure } (a, b \in \mathbb{N}).$$

Si provi che  $\mathcal{R}$  è una relazione d'equivalenza in  $\mathbb{Z}$ .

*Svolgimento.* Si ha  $x \mathcal{R} x$ , per ogni  $x \in \mathbb{Z}$  in quanto è soddisfatta la proprietà  $x = x$ . Si ha poi  $\mathcal{R}$  simmetrica poiché da  $x \mathcal{R} y$  segue  $(x = y)$  o  $(x, y \in \mathbb{N})$ , il che ovviamente equivale a  $(y = x)$  o  $(y, x \in \mathbb{N})$  sicché  $y \mathcal{R} x$ . Infine si supponga  $x \mathcal{R} y$  e  $y \mathcal{R} z$ . Se  $x = y$  o  $y = z$ , come già osservato più in generale, si ha subito  $x \mathcal{R} z$ . Se poi  $x \neq y$  e  $y \neq z$ , risulta  $x, y \in \mathbb{N}$  e  $y, z \in \mathbb{N}$  da cui  $x, z \in \mathbb{N}$  e  $x \mathcal{R} z$  come volevasi.

**Esercizio 2.1.4.** Si esibisca un esempio di relazione binaria  $\mathcal{R}$  in un opportuno insieme  $A$  che risulti non simmetrica né asimmetrica.

**Esercizio 2.1.5.** Una relazione binaria  $\mathcal{R}$  in un insieme  $S$  è detta **antiriflessiva** se si ha  $x \not\mathcal{R} x$ , per ogni  $x \in S$ . Si esibiscano un esempio di relazione antiriflessiva e un esempio di relazione contemporaneamente non riflessiva né antiriflessiva.

**Esercizio 2.1.6.** Si provi che, se  $S$  è un insieme non vuoto, la relazione totale  $\mathcal{R}_t$  è sempre riflessiva, simmetrica e transitiva; è poi asimmetrica se e solo se  $S$  è un singleton.

**Esercizio 2.1.7.** Si discutano le proprietà della relazione vuota  $\mathcal{R}_0$  in un insieme  $S$  non necessariamente non vuoto.

**Esercizio 2.1.8.** Si discutano le proprietà della relazione  $\text{id}_S$  in un qualunque insieme  $S$ .

**Esercizio 2.1.9.** Siano  $S$  un insieme e  $\mathcal{R}$  una relazione binaria in  $S$ . Si provi che si ha:

$$\mathcal{R} \text{ simmetrica} \iff \mathcal{R}^{\text{op}} \subseteq \mathcal{R} \iff \mathcal{R}^{\text{op}} = \mathcal{R}.$$

**Esercizio 2.1.10.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff 3 + 4x = 4 + 3y,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{llllll} 2 \mathcal{R} 10, & 0 \mathcal{R} 0, & 3 \mathcal{R} 3, & 10 \mathcal{R} 13, & 1 \mathcal{R} 1, & 10 \mathcal{R} 17, \\ 4 \mathcal{R} 5, & 6 \mathcal{R} 9, & 7 \mathcal{R} 9, & 13 \mathcal{R} 17, & 5 \mathcal{R} 4, & 2 \mathcal{R} 2. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva.

**Esercizio 2.1.11.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff |2x - 5| = |5y - 8|,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{cccccc} 1 \mathcal{R} 4, & -1 \mathcal{R} 3, & 4 \mathcal{R} 3, & -4 \mathcal{R} -1, & 1 \mathcal{R} 1, & -6 \mathcal{R} 5, \\ -1 \mathcal{R} -1, & 4 \mathcal{R} 1, & 9 \mathcal{R} -1, & -2 \mathcal{R} 4, & 11 \mathcal{R} 5, & 0 \mathcal{R} -2. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva e se è un'applicazione.

**Esercizio 2.1.12.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff |x - 8| = |y - 8|,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{cccc} -3 \mathcal{R} -3, & -3 \mathcal{R} 19, & 0 \mathcal{R} -8, & 0 \mathcal{R} 8, \\ 2 \mathcal{R} 14, & -2 \mathcal{R} 14, & 5 \mathcal{R} 5, & 5 \mathcal{R} -11. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva.

**Esercizio 2.1.13.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff x^2 - 5x + 6 = y^2 + 7y + 12,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{cccccc} 3 \mathcal{R} -3, & 3 \mathcal{R} 4, & 2 \mathcal{R} 5, & 2 \mathcal{R} -2, & 7 \mathcal{R} 1, & 4 \mathcal{R} 2, \\ 2 \mathcal{R} 1, & -4 \mathcal{R} 2, & 0 \mathcal{R} -1, & 0 \mathcal{R} 0, & -3 \mathcal{R} 3, & -3 \mathcal{R} 2, \\ 1 \mathcal{R} 1, & 8 \mathcal{R} 2, & 5 \mathcal{R} -1, & 4 \mathcal{R} 3, & -1 \mathcal{R} 0, & 3 \mathcal{R} 2. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva.

**Esercizio 2.1.14.** Considerate le seguenti relazioni tra  $\mathbb{Z}$  e  $8\mathbb{Z}$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned} x \mathcal{R}_1 y &: \iff x = 8y; \\ x \mathcal{R}_2 y &: \iff y = 8x; \\ x \mathcal{R}_3 y &: \iff 64x^2 = y^2; \\ x \mathcal{R}_4 y &: \iff x^2 = 64y^2. \end{aligned}$$

**Esercizio 2.1.15.** Considerate le seguenti relazioni tra  $\mathbb{N}_0$  e  $2\mathbb{N}_0$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned} x \mathcal{R}_1 y &: \iff x = y; \\ x \mathcal{R}_2 y &: \iff x = 2y; \\ x \mathcal{R}_3 y &: \iff 2x = y; \\ x \mathcal{R}_4 y &: \iff x = |y - 8|. \end{aligned}$$

**Esercizio 2.1.16.** Considerate le seguenti relazioni tra  $\mathbb{Z}$  e  $\mathbb{Q}$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned}x \mathcal{R}_1 y & : \iff 5x = 6y; \\x \mathcal{R}_2 y & : \iff x^2 = 16y^2; \\x \mathcal{R}_3 y & : \iff x = y^3; \\x \mathcal{R}_4 y & : \iff x^3 = 8y^3.\end{aligned}$$

**Esercizio 2.1.17.** Considerate le seguenti relazioni tra  $\mathbb{N}_0$  e  $\mathbb{Q}$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned}x \mathcal{R}_1 y & : \iff \frac{x}{2} = y; \\x \mathcal{R}_2 y & : \iff x = 2y; \\x \mathcal{R}_3 y & : \iff x = y^2.\end{aligned}$$

**Esercizio 2.1.18.** Considerate le seguenti relazioni tra  $\mathbb{N}$  e  $\mathbb{Q}$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned}x \mathcal{R}_1 y & : \iff 2x = 3y; \\x \mathcal{R}_2 y & : \iff 2x^2 = 3y; \\x \mathcal{R}_3 y & : \iff 2x = 3y^2; \\x \mathcal{R}_4 y & : \iff 2x = 3|y|.\end{aligned}$$

**Esercizio 2.1.19.** Con  $S = \{l, m, n\}$  e  $T = \{1, 7\}$ , si precisi quali delle seguenti relazioni tra  $S$  e  $T$  sono applicazioni:

$$\begin{aligned}\mathcal{R}_1 &= \{(l, 1), (m, 1), (n, 7)\}, \\ \mathcal{R}_2 &= \{(l, 1), (m, 1), (n, 1)\}, \\ \mathcal{R}_3 &= \{(l, 7), (m, 1)\},\end{aligned}$$

e quali tra le seguenti relazioni di  $S$  in  $S$  sono applicazioni:

$$\begin{aligned}\mathcal{R}_4 &= \{(l, m), (n, m)\}, \\ \mathcal{R}_5 &= \{(l, m), (m, n), (n, l)\}, \\ \mathcal{R}_6 &= \{(l, l), (m, n), (l, n)\}.\end{aligned}$$

**Esercizio 2.1.20.** Considerate in  $\mathbb{N}$  le seguenti relazioni, si precisi, motivando le risposte, se sono applicazioni di  $\mathbb{N}$  in  $\mathbb{N}$ :

$$\begin{aligned}x \mathcal{R}_1 y & : \iff x + y = 3; \\x \mathcal{R}_2 y & : \iff x + 4 = y; \\x \mathcal{R}_3 y & : \iff x + y > 3.\end{aligned}$$

**Esercizio 2.1.21.** Con  $n$  numero naturale positivo, si dica  $h(n)$  il massimo numero naturale  $h$  tale che  $2^h$  divide  $n$ , sia cioè  $n = 2^{h(n)}k$ , con  $k \in \mathbb{N}$  tale che 2 non divide  $k$ . Si dimostri che non è d'equivalenza né d'ordine la relazione  $\mathcal{R}$  definita in  $\mathbb{N}$  da:

$$n \mathcal{R} m : \iff h(n) \geq h(m),$$

dove  $\leq$  indica l'ordine usuale in  $\mathbb{N}_0$ .

**Esercizio 2.1.22.** Con  $n$  numero naturale positivo, si dica  $h(n)$  il massimo numero naturale  $h$  tale che  $2^h$  divide  $n$ , sia cioè  $n = 2^{h(n)}k$ , con  $k \in \mathbb{N}$  tale che 2 non divide  $k$ . Si dimostri che non è d'equivalenza né d'ordine la relazione  $\mathcal{R}$  definita in  $\mathbb{N}$  da:

$$n \mathcal{R} m : \iff |h(n) - h(m)| \leq 1,$$

dove  $\leq$  indica l'ordine usuale in  $\mathbb{N}_0$ .

**Esercizio 2.1.23.** Si dimostri 2.1.3.

## 2.2 Applicazioni

Come osservato nel paragrafo precedente, di particolare interesse nell'ambito delle relazioni tra insiemi sono le applicazioni, che verranno ora esaminate attentamente, partendo dalle notazioni già introdotte.

Siano  $S$  e  $T$  insiemi e sia  $f : S \rightarrow T$  un'applicazione di  $S$  in  $T$ . Ciò significa che  $f$  è un sottoinsieme di  $S \times T$  tale che per ogni  $x \in S$  esiste uno e un solo  $y \in T$  per cui  $(x, y) \in f$ , cioè  $x f y$ . Tale elemento  $y$  viene denotato con il simbolo  $f(x)$  e detto l'immagine di  $x$  mediante  $f$  e l'applicazione  $f$  viene descritta nel seguente modo:

$$f : x \in S \mapsto f(x) \in T$$

o anche

$$\begin{aligned} f : S &\longrightarrow T \\ x &\longmapsto f(x). \end{aligned}$$

L'insieme  $S$  è detto il dominio di  $f$ , l'insieme  $T$  è chiamato il codominio di  $f$ .

Se  $f : S \rightarrow T$  e  $g : S_1 \rightarrow T_1$  sono applicazioni, con  $S, S_1, T, T_1$  insiemi non vuoti, si ha:

$$f = g \iff \begin{cases} S = S_1 \\ T = T_1 \\ f(x) = g(x), \text{ per ogni } x \in S. \end{cases} \quad (2.2.1)$$

**2.2.1. Esempio.** Posto

$$f_1 : x \in \mathbb{Z} \mapsto x^2 \in \mathbb{N}_0,$$

$f_1$  è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  che a ogni intero  $x$  associa il suo quadrato, elemento di  $\mathbb{N}_0$ . Così

$$f_2 : x \in \mathbb{Z} \longmapsto |x| \in \mathbb{N}_0$$

è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  che a ogni intero  $x$  associa il suo valore assoluto, elemento di  $\mathbb{N}_0$ . Ancora:

$$f_3 : x \in \mathbb{Z} \longmapsto 4 \in \mathbb{N}_0$$

è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  che a ogni intero  $x$  associa il numero naturale 4;

$$f_4 : \mathbb{Z} \longrightarrow \mathbb{N}_0$$

$$x \longmapsto \begin{cases} x^2 & \text{se } x \leq 0 \\ 4 & \text{se } x > 0 \end{cases}$$

è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  che a ogni intero  $x$  associa il suo quadrato, se  $x$  è non positivo, e associa 4, se  $x$  è positivo;

$$f_5 : \mathbb{Z} \longrightarrow \mathbb{N}_0$$

$$x \longmapsto \begin{cases} -2x & \text{se } x \leq 0 \\ 2x - 1 & \text{se } x > 0 \end{cases}$$

è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  che a ogni intero  $x$  non positivo associa l'opposto del suo doppio, a ogni  $x$  positivo associa il precedente del suo doppio. Si ha per esempio:

$$\begin{aligned} f_1(0) &= 0^2 = 0, & f_1(1) &= 1^2 = 1, & f_1(-1) &= (-1)^2 = 1, \\ f_2(-1) &= |-1| = 1 & f_3(0) &= 4, & f_3(1) &= f_3(-1) = 4, \end{aligned}$$

precisamente  $f_3(x) = 4$ , per ogni  $x \in \mathbb{Z}$ ,

$$\begin{aligned} f_4(0) &= 0^2 = 0, & f_4(1) &= 4, & f_4(-1) &= 1, & f_4(2) &= 4, \\ f_5(0) &= 0, & f_5(1) &= 1, & f_5(-1) &= 2, & f_5(2) &= 3. \end{aligned}$$

Un'applicazione di dominio  $\mathbb{N}_0$  o  $\mathbb{N}$  e codominio  $T$ , con  $T$  insieme, è detta una **successione** di elementi di  $T$ . Se  $f : n \in \mathbb{N}_0 \longmapsto a_n \in T$  è una successione di elementi di  $T$ , spesso si preferisce utilizzare per  $f$  la scrittura  $(a_n)_{n \in \mathbb{N}_0}$ , che evidenzia qual è l'immagine di ciascun naturale.

Un'applicazione  $f : S \longrightarrow T$  tale che  $f(x) = f(x')$  per ogni  $x, x' \in S$  è detta **costante**. Ovviamente si ha:

$$f \text{ costante} : \iff \exists \bar{y} \in T : (f(x) = \bar{y}, \forall x \in S),$$

e  $f$  è anche detta l'applicazione di  $S$  in  $T$  **costantemente uguale** a  $\bar{y}$ . Per esempio l'applicazione  $f_3$  prima introdotta è l'applicazione di  $\mathbb{Z}$  in  $\mathbb{N}_0$  costantemente uguale a 4.

Se l'insieme  $T$  è finito, è immediato riscontrare che di applicazioni costanti di  $S$  in  $T$ , con  $S$  insieme non vuoto, ce ne sono esattamente  $|T|$ .

Se gli insiemi  $S$  e  $T$  sono entrambi finiti, il numero delle applicazioni di  $S$  in  $T$  è  $|T|^{|S|}$ , come sarà giustificato nel Capitolo 3. Ciò motiva l'uso del simbolo  $T^S$  per denotare l'insieme delle applicazioni di  $S$  in  $T$ , qualunque siano gli insiemi  $S$  e  $T$  non necessariamente finiti.

Si osservi che se  $S$  è l'insieme vuoto e  $T$  è un insieme qualsiasi, tra  $S$  e  $T$  esiste solo la relazione vuota e questa è anche un'applicazione, detta appunto l'**applicazione vuota**. Se  $S$  è un insieme non vuoto e  $T = \emptyset$ , non esistono applicazioni di  $S$  in  $T$ . Queste considerazioni illustrano perché nello studio delle applicazioni tra insiemi è lecito supporre, a volte tacitamente, che questi siano entrambi non vuoti. Si noti che, se  $S$  e  $T$  sono insiemi entrambi non vuoti, esistono sempre applicazioni di  $S$  in  $T$ , per esempio quelle costanti (che sono ovviamente le uniche se  $T$  è un singleton).

Se  $S$  e  $T$  coincidono, un'applicazione notevole è la relazione identica:

$$\text{id}_S : x \in S \mapsto x \in S,$$

detta anche l'**applicazione identica** di  $S$ .

Se  $X$  è un sottoinsieme di  $S$ , ha senso considerare l'applicazione:

$$\text{imm}_X : x \in X \mapsto x \in S,$$

di  $X$  in  $S$ , detta l'**immersione** di  $X$  in  $S$ . Si noti che è  $\text{imm}_X = \Delta_S \cap (X \times S)$ . Ovviamente si ha  $\text{imm}_S = \text{id}_S$ .

Sia  $f : S \rightarrow T$  un'applicazione. Se  $X$  è un sottoinsieme di  $S$ , l'insieme costituito dalle immagini in  $f$  degli elementi di  $X$  è detto l'**immagine** di  $X$  in  $f$  e denotato con  $f(X)$ :

$$f(X) := \{f(x) : x \in X\}.$$

Ovviamente  $f(X)$  è un sottoinsieme di  $T$ . Si ha quindi, con  $y \in T$ :

$$y \in f(X) : \iff \exists x \in X : y = f(x).$$

Se  $X$  coincide con  $S$ , si dice anche che  $f(S)$  è l'**immagine** di  $S$ , e si usa il simbolo **Im**  $f$ :

$$\text{Im } f := f(S) = \{f(x) : x \in S\}$$

$$y \in \text{Im } f : \iff \exists x \in S : y = f(x).$$

Per esempio, considerate le applicazioni  $f_1, f_3$  e  $f_4$  di 2.2.1, si ha:

$$f_1(\{0, 1, -1, 3, -3\}) = \{0, 1, 9\},$$

$$f_1(\mathbb{Z}) = \{x^2 : x \in \mathbb{Z}\} = \{x^2 : x \in \mathbb{N}_0\} = f_1(\mathbb{N}_0),$$

$$f_3(\{0\}) = \{4\} = f_3(\{0, 1\}) = f_3(\mathbb{Z}),$$

$$f_4(\mathbb{N}) = \{4\}.$$

Ovviamente si ha sempre  $f(\emptyset) = \emptyset$ , e  $f(X) \neq \emptyset$ , per ogni sottoinsieme non vuoto  $X$  di  $S$ ; cioè, con  $X \subseteq S$ :

$$f(X) = \emptyset \iff X = \emptyset.$$

Inoltre, se  $X \subseteq S$ , si ha:

$$|X| = 1 \implies |f(X)| = 1$$

in quanto, se  $X = \{\bar{x}\}$ , si ha  $f(X) = \{f(\bar{x})\}$ . Ma chiaramente

$$|f(X)| = 1 \not\implies |X| = 1,$$

come mostrato, per esempio, da applicazioni in 2.2.1. Infatti  $f_1(\{1, -1\}) = \{1\} = f_2(\{1, -1\})$ , più in generale  $|f_1(\{x, -x\})| = 1 = |f_2(\{x, -x\})|$ , per ogni  $x \in \mathbb{Z}$ . Se si considera l'applicazione  $f_3$  di 2.2.1 si ha  $f_3(\mathbb{Z}) = \{4\} = f_3(X)$ , per ogni  $X \subseteq \mathbb{Z}$ ,  $X \neq \emptyset$ . Ciò mostra anche che:

$$X \subseteq S, X \text{ infinito} \not\implies f(X) \text{ infinito.}$$

Si ha però ovviamente:

$$X \subseteq S, X \text{ finito} \implies f(X) \text{ finito e } |f(X)| \leq |X|, \quad (2.2.2)$$

in quanto se  $X = \{x, \dots, x_n\}$ , si ha  $f(X) = \{f(x_1), \dots, f(x_n)\}$ . Come già osservato, può avversi  $|f(X)| < |X|$ , cioè possono esserci coincidenze tra gli elementi  $f(x_1), \dots, f(x_n)$ .

Se  $X_1$  e  $X_2$  sono sottoinsiemi di  $S$ , si ha ovviamente:

$$\begin{aligned} X_1 \subseteq X_2 &\implies f(X_1) \subseteq f(X_2), \\ f(X_1) \subseteq f(X_2) &\not\implies X_1 \subseteq X_2. \end{aligned}$$

Infatti per ogni  $y \in f(X_1)$  esiste  $x \in X_1$  tale che  $y = f(x)$ ; da  $X_1 \subseteq X_2$  segue allora che  $x \in X_2$ , quindi per ogni  $y \in f(X_1)$  esiste  $x \in X_2$  tale che  $y = f(x)$ , e dunque  $y \in f(X_2)$ , e vale la prima implicazione. Considerata poi per esempio l'applicazione  $f_1$  di 2.2.1 si ha  $f_1(\{0, 1\}) = f_1(\{0, -1\})$  con  $\{0, 1\} \not\subseteq \{0, -1\}$ , pertanto non vale la seconda implicazione.

**2.2.2.** Sia  $f : S \rightarrow T$  un'applicazione e siano  $X_1$  e  $X_2$  sottoinsiemi di  $S$ . Si ha:

$$X_1 \subset X_2 \not\implies f(X_1) \subset f(X_2).$$

Si ha poi:

$$f(X_1 \cup X_2) = f(X_1) \cup f(X_2);$$

$f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$ , e l'inclusione può essere stretta;

$f(X_1 \setminus X_2) \supseteq f(X_1) \setminus f(X_2)$ , e l'inclusione può essere stretta.

*Dimostrazione.* Esercizio. □

Sia  $f : S \rightarrow T$  un'applicazione. Se  $Y$  è un sottoinsieme di  $T$ , l'insieme costituito dagli elementi di  $S$  la cui immagine appartiene a  $Y$  è detto la **controimmagine** di  $Y$  in  $f$  e denotato con  $f^{-1}(Y)$ :

$$f^{-1}(Y) := \{x \in S : f(x) \in Y\}.$$

Ovviamente  $f^{-1}(Y)$  è un sottoinsieme di  $S$ . Con  $x \in S$ , si ha quindi:

$$x \in f^{-1}(Y) \iff f(x) \in Y.$$

Per esempio, considerata l'applicazione  $f_1$  di 2.2.1, si ha:

$$\begin{aligned} f_1^{-1}(\{0, 1, 2, 3, 4, 5\}) &= \{x \in \mathbb{Z} : f_1(x) \in \{0, 1, 2, 3, 4, 5\}\} = \\ &\{x \in \mathbb{Z} : x^2 = 0, 1, 2, 3, 4, 5\} = \{0, 1, -1, 2, -2\}, f_1^{-1}(\{6, 7\}) = \emptyset. \end{aligned}$$

Banalmente riesce sempre:

$$f^{-1}(T) = S,$$

in quanto ogni  $x \in S$  è tale che  $f(x) \in T$ ; e si ha pure ovviamente:

$$f^{-1}(\emptyset) = \emptyset.$$

Si noti che:

$$Y \neq \emptyset \not\Rightarrow f^{-1}(Y) \neq \emptyset.$$

Per esempio, con le notazioni di 2.2.1,  $f_1^{-1}(\{6, 7\}) = \emptyset$ , in quanto non esistono interi il cui quadrato sia 6 o 7. Così:

$$Y \text{ infinito} \not\Rightarrow f^{-1}(Y) \text{ infinito},$$

$$Y \text{ finito} \not\Rightarrow f^{-1}(Y) \text{ finito};$$

e, anche nell'ipotesi che  $Y$  e  $f^{-1}(Y)$  siano entrambi finiti, non c'è alcun legame tra i loro ordini. Si considerino per esempio le applicazioni  $f_3$  e  $f_1$  di 2.2.1:  $f_3^{-1}(\mathbb{N}_0 \setminus \{4\}) = \emptyset$ ,  $f_3^{-1}(\{4\}) = \mathbb{Z}$ ,  $f_1^{-1}(\{0\}) = \{0\}$ ,  $f_1^{-1}(\{1\}) = \{1, -1\}$ ,  $f_1^{-1}(\{1, 2, 3\}) = \{1, -1\}$ .

**2.2.3.** Sia  $f : S \rightarrow T$  un'applicazione e siano  $Y_1$  e  $Y_2$  sottoinsiemi di  $T$ . Risulta:

$$\begin{aligned} Y_1 \subseteq Y_2 &\implies f^{-1}(Y_1) \subseteq f^{-1}(Y_2), \\ f^{-1}(Y_1) \subseteq f^{-1}(Y_2) &\not\implies Y_1 \subseteq Y_2. \end{aligned}$$

*Dimostrazione.* Essendo  $Y_1 \subseteq Y_2$ , da  $x \in f^{-1}(Y_1)$  segue  $f(x) \in Y_1$ , quindi  $f(x) \in Y_2$  e poi  $x \in f^{-1}(Y_2)$ .

Se poi, per esempio,  $f_1$  è l'applicazione definita in 2.2.1, si ha:  $f_1^{-1}(\{1, 2\}) = \{1, -1\} = f_1^{-1}(\{1, 3\})$ . □

**2.2.4.** Sia  $f : S \rightarrow T$  un'applicazione e siano  $Y_1$  e  $Y_2$  sottoinsiemi di  $T$ . Si ha:

$$Y_1 \subset Y_2 \not\Rightarrow f^{-1}(Y_1) \subset f^{-1}(Y_2)$$

e

$$\begin{aligned} f^{-1}(Y_1 \cup Y_2) &= f^{-1}(Y_1) \cup f^{-1}(Y_2), \\ f^{-1}(Y_1 \cap Y_2) &= f^{-1}(Y_1) \cap f^{-1}(Y_2), \\ f^{-1}(Y_1 \setminus Y_2) &= f^{-1}(Y_1) \setminus f^{-1}(Y_2). \end{aligned}$$

*Dimostrazione.* Esercizio. □

**2.2.5.** Sia  $f : S \rightarrow T$  un'applicazione, e siano  $X$  un sottoinsieme di  $S$  e  $Y$  un sottoinsieme di  $T$ . Si ha:

$$\begin{aligned} X &\subseteq f^{-1}(f(X)), \\ Y &\supseteq f(f^{-1}(Y)). \end{aligned}$$

In più:

$$f(f^{-1}(Y)) = Y \cap f(S).$$

*Dimostrazione.* Esercizio. □

Come osservato in 2.2.1, per alcune applicazioni esistono elementi distinti che hanno la stessa immagine, oppure esistono elementi del codominio dell'applicazione che non sono corrispondenti di alcun elemento del dominio. Queste considerazioni motivano le definizioni seguenti.

Un'applicazione  $f : S \rightarrow T$  è detta **iniettiva** (o più brevemente **in**) se è tale che elementi distinti di  $S$  hanno immagini distinte in  $T$ :

$$f \text{ iniettiva} : \iff (x_1, x_2 \in S, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

Equivalentemente:

$$f \text{ iniettiva} \iff (f(x_1) = f(x_2) \text{ con } x_1, x_2 \in S \Rightarrow x_1 = x_2),$$

cioè  $f$  è iniettiva se e solo se elementi di  $S$  che hanno la stessa immagine in  $f$  necessariamente coincidono.

Ovviamente l'identità  $\text{id}_S$  di  $S$  e l'immersione  $\text{imm}_X$  di  $X \subseteq S$  sono iniettive.

Le applicazioni  $f_1, f_2, f_3$  e  $f_4$  di 2.2.1 non sono iniettive, perché, per esempio:  $f_1(1) = f_1(-1), f_2(1) = f_2(-1), f_3(0) = f_3(1), f_4(1) = f_4(2)$ .

L'applicazione  $f_5$  è invece iniettiva. Infatti, se  $x$  e  $x'$  sono elementi distinti di  $\mathbb{Z}$ , entrambi non positivi, si ha  $f_5(x) = -2x \neq -2x' = f_5(x')$ ; se sono entrambi

positivi, riesce  $f_5(x) = 2x - 1 \neq 2x' - 1 = f(x')$ ; infine se, per esempio,  $x$  è positivo e  $x'$  no, si ha  $f_5(x) = 2x - 1$  non divisibile per 2 e  $f_5(x') = -2x$  divisibile per 2, sicché banalmente  $f_5(x) \neq f_5(x')$ .

Ovviamente un'applicazione costante è iniettiva se e solo se il dominio è un singleton.

**2.2.6. Esempio.** Le seguenti applicazioni:

$$g_1 : x \in \mathbb{N}_0 \longmapsto 2x \in 2\mathbb{N}_0,$$

$$g_2 : x \in \mathbb{N}_0 \longmapsto 2x + 1 \in \mathbb{N}_0 \setminus 2\mathbb{N}_0,$$

$$g_3 : x \in \mathbb{N}_0 \longmapsto x + 1 \in \mathbb{N}_0,$$

$$g_4 : x \in \mathbb{N}_0 \longmapsto x + 1 \in \mathbb{N},$$

$$g_5 : x \in \mathbb{N}_0 \longmapsto 3x + 4 \in \mathbb{N}_0,$$

$$g_6 : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

$$x \longmapsto \begin{cases} x & \text{se } x \leq 6 \\ x - 4 & \text{se } x > 6, \end{cases}$$

$$g_7 : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

$$x \longmapsto \begin{cases} x & \text{se } x \leq 6 \\ x + 4 & \text{se } x > 6, \end{cases}$$

$$g_8 : x \in \mathbb{N}_0 \longmapsto 6 \in \mathbb{N}_0,$$

$$g_9 : \mathbb{N}_0 \longrightarrow \mathbb{Z}$$

$$x \longmapsto \begin{cases} -x/2 & \text{se } x \in 2\mathbb{N}_0 \\ (x+1)/2 & \text{se } x \in \mathbb{N}_0 \setminus 2\mathbb{N}_0, \end{cases}$$

sono tutte iniettive tranne la  $g_6$  e la  $g_8$ .

Un'applicazione  $f : S \longrightarrow T$  è detta **suriettiva** (o più brevemente **su**) se l'immagine di  $f$  coincide con  $T$ , cioè  $f$  è tale che ogni elemento di  $T$  è corrispondente di almeno un elemento di  $S$ :

$$f \text{ suriettiva} : \iff f(S) = T \iff (\forall y \in T, \exists x \in S : f(x) = y).$$

L'identità  $\text{id}_S$  di un qualunque insieme  $S$  è suriettiva, mentre l'immersione  $\text{imm}_X$  di  $X$  in  $S$  lo è solo se  $X = S$  (e dunque  $\text{imm}_X = \text{id}_S$ ) in quanto  $\text{imm}_X(X) = X$ .

Ovviamente un'applicazione costante è suriettiva se e solo se il suo codominio è un singleton.

Le applicazioni  $f_1, f_3$  e  $f_4$  di 2.2.1 non sono suriettive: infatti per esempio esiste  $2 \in \mathbb{N}_0$  tale che non c'è alcun  $x \in \mathbb{Z}$  per cui risulti  $2 = f_1(x)$ ,  $2 = f_3(x)$ ,  $2 = f_4(x)$  essendo  $2 \neq x^2$ , per ogni  $x \in \mathbb{Z}$  e ovviamente  $2 \neq 4$ .

L'applicazione  $f_2$  è suriettiva poiché  $f_2(\mathbb{Z}) = \mathbb{N}_0$ , precisamente ogni  $y \in \mathbb{N}_0$  è tale che esistono  $y$  e  $-y \in \mathbb{Z}$  per cui risulti  $f_2(y) = f_2(-y) = y$ . Anche l'applicazione  $f_5$  è suriettiva poiché, per ogni  $y \in \mathbb{N}_0$ , si ha che  $y = -2(-\frac{y}{2}) = f_5(-\frac{y}{2})$  se  $y \in 2\mathbb{N}_0$  (si noti che in tal caso  $-\frac{y}{2} \in \mathbb{Z}$ ) e  $y = 2\frac{y+1}{2} - 1 = f_5(\frac{y+1}{2})$  se  $y \in \mathbb{N}_0 \setminus 2\mathbb{N}_0$  (si noti ancora che  $\frac{y+1}{2} \in \mathbb{Z}$ ).

**2.2.7. Esempio.** Considerate le applicazioni di 2.2.6, si ha che sono suriettive  $g_1, g_2, g_4, g_6$  e  $g_9$ , non lo sono  $g_3, g_5, g_7$  e  $g_8$ .

Si osserva facilmente che un'applicazione può non essere né iniettiva né suriettiva (per esempio  $f_3$  di 2.2.1), può essere iniettiva e non suriettiva (per esempio l'immersione di  $\mathbb{N}$  in  $\mathbb{Z}$ ), può essere suriettiva e non iniettiva (per esempio la  $f_2$  di 2.2.1). Situazioni analoghe si ritrovano anche con le applicazioni introdotte in 2.2.6.

**2.2.8. Siano  $S$  e  $T$  insiemi finiti non vuoti. Allora:**

$$\begin{aligned}\exists f : S \longrightarrow T \text{ iniettiva} &\iff |S| \leq |T|, \\ \exists f : S \longrightarrow T \text{ suriettiva} &\iff |S| \geq |T|.\end{aligned}$$

Ne segue che, se  $X$  è un sottoinsieme di  $S$ :

$$\begin{aligned}X \subset S \implies \#f : S \longrightarrow X \text{ iniettiva}, \\ X \subset S \implies \#f : X \longrightarrow S \text{ suriettiva}.\end{aligned}$$

*Dimostrazione.* Esercizio. □

La 2.2.8 non vale per insiemi infiniti. Nell'Esempio 2.2.6, l'applicazione  $g_1$  è iniettiva, e il suo codominio è un sottoinsieme proprio del dominio. Invece la  $g_9$  è suriettiva, e il suo dominio è un sottoinsieme proprio del codominio.

Un'applicazione  $f : S \longrightarrow T$  è detta **biettiva** (o **biezione**, o **corrispondenza biunivoca**) se è sia iniettiva che suriettiva:

$$f \text{ biettiva} : \iff f \text{ iniettiva e suriettiva.}$$

È immediato verificare che:

$$f \text{ biettiva} \iff (\forall y \in T, \exists! x \in S : f(x) = y).$$

Infatti, se  $f$  è biettiva, per la suriettività si ha che per ogni  $y \in T$  esiste  $x \in S$  tale che  $f(x) = y$ ; tale  $x$  è poi univocamente individuato per l'iniettività di  $f$ . Viceversa, se ogni elemento di  $T$  è corrispondente in  $f$  di uno e un solo elemento

di  $S$  si ha che ovviamente  $f$  è suriettiva, ed è poi iniettiva in quanto  $f(x) = f(x')$  comporta  $x = x'$  per l'unicità dell'elemento di  $S$  che ha in  $f$  immagine  $f(x) = f(x')$ .

L'applicazione  $\text{id}_S$  è biettiva. Un'applicazione costante lo è se e solo se il dominio e il codominio sono entrambi singleton. In 2.2.1 solo l'applicazione  $f_5$  è biettiva. Delle applicazioni considerate in 2.2.6 sono biettive  $g_1, g_2, g_4$  e  $g_9$ .

Se  $f : S \rightarrow T$  è un'applicazione biettiva, ha senso definire la seguente applicazione di  $T$  in  $S$ , detta l'**applicazione inversa** di  $f$  e denotata con  $f^{-1}$ . Tale applicazione associa a ogni elemento di  $T$  l'unico elemento di  $S$  di cui è immagine in  $f$ :

$$\begin{aligned} f^{-1} : T &\rightarrow S \\ y &\mapsto x \in S : f(x) = y. \end{aligned}$$

Si noti che  $f^{-1}$  è la relazione opposta della  $f$ .

Per esempio, l'inversa di  $\text{id}_S$  è  $\text{id}_S$ , l'inversa della  $f_5$  descritta in 2.2.1 è la  $g_9$  in 2.2.6, come evidenziato dallo studio della suriettività di  $f_5$ ; l'inversa di  $g_9$  è  $f_5$ . Relativamente alle altre applicazioni biettive di 2.2.6 si ha che:

$$\begin{aligned} g_1^{-1} : y \in 2\mathbb{N}_0 &\mapsto \frac{y}{2} \in \mathbb{N}_0, \\ g_2^{-1} : y \in \mathbb{N}_0 \setminus 2\mathbb{N}_0 &\mapsto \frac{y-1}{2} \in \mathbb{N}_0, \\ g_4^{-1} : y \in \mathbb{N} &\mapsto y-1 \in \mathbb{N}_0, \end{aligned}$$

in quanto per esempio ogni  $y \in 2\mathbb{N}_0$  è immagine in  $g_1$  dell'unico  $x \in \mathbb{N}_0$  tale che  $y = g_1(x) = 2x$ , cioè di  $x = \frac{y}{2}$ .

Come accade per  $\text{id}_S$ , può avversi che l'inversa di un'applicazione biettiva  $f : S \rightarrow T$  coincida con l'applicazione stessa. In tal caso ovviamente deve avversi  $S = T$ , e l'applicazione  $f$  viene detta un'**involuzione** di  $S$ . Per esempio, sono involuzioni le applicazioni:

$$h_1 : x \in \mathbb{Z} \mapsto -x \in \mathbb{Z},$$

$$\begin{aligned} h_2 : \mathbb{N}_0 &\longrightarrow \mathbb{N}_0 \\ x &\mapsto \begin{cases} x+1 & \text{se } x \in 2\mathbb{N}_0 \\ x-1 & \text{se } x \in \mathbb{N}_0 \setminus 2\mathbb{N}_0. \end{cases} \end{aligned}$$

Come conseguenza di 2.2.8 si ottiene:

**2.2.9.** *Siano  $S$  e  $T$  insiemi finiti. Allora:*

$$\exists f : S \rightarrow T \text{ biettiva} \iff |S| = |T|.$$

Pertanto non esiste mai un'applicazione biettiva tra un insieme finito e un suo sottoinsieme proprio, in contrasto con quanto avviene per insiemi infiniti (si pensi alle applicazioni  $g_1, g_2, g_4$  e  $g_9$  di 2.2.6).

**Osservazione.** Il concetto di “inversa” non va confuso con il concetto di “controimmagine”; si parla di controimmagine di un sottoinsieme  $Y$  mediante  $f$  qualunque sia l’applicazione  $f$ , si parla di inversa di  $f$  solo se  $f$  è biettiva. Si noti però che, se  $f$  è biettiva, la controimmagine del sottoinsieme  $Y$  mediante  $f$  coincide con l’immagine di  $Y$  mediante  $f^{-1}$ . Non c’è dunque ambiguità tra le due nozioni. Ciò giustifica l’utilizzo dello stesso simbolo,  $f^{-1}(Y)$ , per denotarle entrambe.

Per le applicazioni aventi come dominio e codominio insiemi finiti dello stesso ordine l’iniettività, la suriettività e la biettività sono condizioni equivalenti. Infatti:

**2.2.10.** *Siano  $S$  e  $T$  insiemi finiti dello stesso ordine  $n$ . Allora un’applicazione  $f : S \rightarrow T$  è iniettiva se e solo se è suriettiva.*

*Dimostrazione.* Sia  $S = \{x_1, x_2, \dots, x_n\}$ . Se  $f$  è iniettiva, gli elementi  $f(x_1), f(x_2), \dots, f(x_n)$  sono a due a due distinti, sicché  $f(S)$  ha ordine  $n$  e dunque coincide con  $T$ . Pertanto  $f$  è suriettiva.

Viceversa, sia  $f$  suriettiva e dunque si abbia  $f(S) = T$ . Da (2.2.2) si ottiene allora  $|T| = |S| \geq |f(S)| = |T|$ , quindi  $|f(S)| = |S|$  ed  $f$  è iniettiva.  $\square$

Si illustrerà ora come costruire ulteriori applicazioni da applicazioni date, legate da un’opportuna proprietà.

Siano  $f : S \rightarrow T$  e  $g : T \rightarrow V$  applicazioni; siano cioè  $f$  e  $g$  applicazioni tali che il codominio di  $f$  coincide con il dominio di  $g$ . Si definisce **applicazione composta o prodotto** di  $f$  e  $g$ , e si denota con  $g \circ f$ , l’applicazione di  $S$  in  $V$  che a ogni elemento  $x \in S$  associa l’elemento di  $V$  che si ottiene applicando  $g$  all’elemento  $f(x)$  di  $T$ :

$$g \circ f : x \in S \mapsto g(f(x)) \in V.$$

Si pone quindi:

$$(g \circ f)(x) := g(f(x)), \text{ per ogni } x \in S.$$

**2.2.11. Esempio.** Considerate le applicazioni:

$$k_1 : x \in \mathbb{N}_0 \mapsto x^2 + 10 \in \mathbb{N},$$

$$k_2 : n \in \mathbb{N} \mapsto -5n + 8 \in \mathbb{Z},$$

$$k_3 : z \in \mathbb{Z} \mapsto \frac{1}{4}z \in \mathbb{Q},$$

si ha:

$$k_2 \circ k_1 : x \in \mathbb{N}_0 \mapsto -5x^2 - 42 \in \mathbb{Z},$$

in quanto  $(k_2 \circ k_1)(x) = k_2(k_1(x)) = k_2(x^2 + 10) = -5(x^2 + 10) + 8 = -5x^2 - 50 + 8 = -5x^2 - 42$  per ogni  $x \in \mathbb{N}_0$ ;

$$k_3 \circ k_2 : n \in \mathbb{N} \mapsto -\frac{5}{4}n + 2 \in \mathbb{Q},$$

perché  $k_3(k_2(n)) = k_3(-5n + 8) = -\frac{5n+8}{4} = -\frac{5}{4}n + 2$  per ogni  $n \in \mathbb{N}$ .

La composizione di applicazioni è detta anche **prodotto operativo** di applicazioni. Si noti che l'esistenza di  $g \circ f$  non comporta l'esistenza di  $f \circ g$ : con le notazioni precedenti, se è  $S \neq V$ , non esiste  $f \circ g$ . Se è  $S = V \neq T$ , esistono sia  $g \circ f$  che  $f \circ g$ , ma sono in ogni caso distinte, essendo  $g \circ f : S \rightarrow S$  e  $f \circ g : T \rightarrow T$ . Anche se  $S = T = V$ , le applicazioni  $g \circ f$  e  $f \circ g$  possono essere distinte. Per esempio, considerate le applicazioni:

$$\begin{aligned} k_4 : x \in \mathbb{N}_0 &\mapsto x^3 \in \mathbb{N}_0, \\ k_5 : n \in \mathbb{N}_0 &\mapsto 3n + 2 \in \mathbb{N}_0, \end{aligned}$$

si ha:

$$\begin{aligned} k_5 \circ k_4 : x \in \mathbb{N}_0 &\mapsto 3x^3 + 2 \in \mathbb{N}_0, \\ k_4 \circ k_5 : n \in \mathbb{N}_0 &\mapsto (3n + 2)^3 \in \mathbb{N}_0, \end{aligned}$$

con  $k_5 \circ k_4 \neq k_4 \circ k_5$  (per esempio,  $(k_5 \circ k_4)(1) = 5 \neq 5^3 = (k_4 \circ k_5)(1)$ ).

Non vale dunque per il prodotto operativo la proprietà commutativa. Si ha però:

**2.2.12. Proprietà associativa del prodotto operativo di applicazioni.** *Siano  $f : S \rightarrow T$ ,  $g : T \rightarrow V$  e  $h : V \rightarrow W$  applicazioni. Allora:*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

*Dimostrazione.* Si noti innanzitutto che ha senso comporre  $g \circ f : S \rightarrow V$  con  $h$  e  $f$  con  $h \circ g : T \rightarrow W$ , e in entrambi i casi si ottengono applicazioni di  $S$  in  $W$ . Queste coincidono perché, per ogni  $x \in S$ , si ha:

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

e

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

□

Le applicazioni identiche hanno un comportamento particolare. Infatti:

**2.2.13. Sia  $f : S \rightarrow T$  un'applicazione. Si ha:**

$$\text{id}_T \circ f = f, \quad f \circ \text{id}_S = f.$$

*Dimostrazione.* Ovviamente  $\text{id}_T \circ f$  è un'applicazione di  $S$  in  $T$ , e così  $f \circ \text{id}_S$ . Inoltre, per ogni  $x \in S$ , si ha:

$$\begin{aligned} (\text{id}_T \circ f)(x) &= \text{id}_T(f(x)) = f(x), \\ (f \circ \text{id}_S)(x) &= f(\text{id}_S(x)) = f(x), \end{aligned}$$

come volevasi. □

Il prodotto operativo di applicazioni “conserva” l’iniettività e la suriettività (e quindi la biettività), nel senso che:

**2.2.14.** Siano  $f : S \rightarrow T$  e  $g : T \rightarrow V$  applicazioni. Si ha:

$$\begin{aligned} f \text{ e } g \text{ iniettive} &\implies g \circ f \text{ iniettiva;} \\ f \text{ e } g \text{ suriettive} &\implies g \circ f \text{ suriettiva;} \\ f \text{ e } g \text{ biettive} &\implies g \circ f \text{ biettiva.} \end{aligned}$$

*Dimostrazione.* Siano  $f$  e  $g$  iniettive e si supponga  $(g \circ f)(x) = (g \circ f)(x')$  con  $x, x' \in S$ . Si abbia cioè  $g(f(x)) = g(f(x'))$ . L’iniettività di  $g$  assicura allora che  $f(x) = f(x')$  e, per l’iniettività di  $f$ , si ottiene che  $x = x'$ , come volevasi.

Siano ora  $f$  e  $g$  suriettive e si consideri  $g \circ f : S \rightarrow V$ . Per ogni  $z \in V$  esiste, per la suriettività di  $g$ , un elemento  $y \in T$  tale che  $z = g(y)$ . La suriettività di  $f$  assicura che, considerato questo  $y$  esiste  $x \in S$  tale che  $y = f(x)$ . Si ha quindi:  $z = g(y) = g(f(x)) = (g \circ f)(x)$ . Pertanto  $g \circ f$  è suriettiva. Si noti che si può ottenere la suriettività di  $g \circ f$  anche osservando che  $(g \circ f)(S) = g(f(S)) = g(T) = V$ .

La biettività di  $g \circ f$  nell’ipotesi di biettività di  $f$  e  $g$  è ovvia conseguenza delle due proprietà precedenti.  $\square$

Le implicazioni di 2.2.14 non si invertono (vedi Esercizio 2.2.6). Riesce però:

**2.2.15.** Siano  $f : S \rightarrow T$  e  $g : T \rightarrow V$  applicazioni. Si ha:

$$\begin{aligned} g \circ f \text{ iniettiva} &\implies f \text{ iniettiva;} \\ g \circ f \text{ suriettiva} &\implies g \text{ suriettiva;} \\ g \circ f \text{ biettiva} &\implies f \text{ iniettiva e } g \text{ suriettiva.} \end{aligned}$$

*Dimostrazione.* Sia  $g \circ f$  iniettiva e si supponga  $f(x) = f(x')$  con  $x, x' \in S$ . Allora è anche  $g(f(x)) = g(f(x'))$  cioè  $(g \circ f)(x) = (g \circ f)(x')$  sicché l’iniettività di  $g \circ f$  comporta  $x = x'$ , come volevasi.

Sia ora  $g \circ f$  suriettiva e si consideri  $z \in V$ . Per la suriettività di  $g \circ f$  esiste  $x \in S$  tale che  $z = (g \circ f)(x) = g(f(x))$ , sicché  $z \in g(T)$  come volevasi.

Infine, se  $g \circ f$  è biettiva, essa è iniettiva e suriettiva e dunque l’asserto segue dalle precedenti implicazioni.  $\square$

Se  $f : S \rightarrow T$  è un’applicazione biettiva, allora esiste l’applicazione inversa  $f^{-1} : T \rightarrow S$  e ha senso considerare  $f^{-1} \circ f : S \rightarrow S$ , e  $f \circ f^{-1} : T \rightarrow T$ . Come si proverà ora si ha:

$$f^{-1} \circ f = \text{id}_S, \quad f \circ f^{-1} = \text{id}_T. \quad (2.2.3)$$

Più precisamente:

**2.2.16.** Sia  $f : S \rightarrow T$  un'applicazione. Si ha

$$f \text{ biettiva} \iff (\exists f' : T \rightarrow S : f' \circ f = \text{id}_S \text{ e } f \circ f' = \text{id}_T).$$

Inoltre, se tale applicazione  $f'$  esiste, essa è unica, ed è quindi l'inversa di  $f$ .

*Dimostrazione.* Sia  $f$  biettiva e si consideri la sua inversa  $f^{-1}$ . Per ogni  $x \in S$  si ha:  $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = \text{id}_S(x)$ , in quanto, per definizione di  $f^{-1}$ ,  $f^{-1}(f(x))$  è l'unico elemento di  $S$  la cui immagine in  $f$  è  $f(x)$ . Così, per ogni  $y \in T$ , si ha:  $(f \circ f^{-1})(y) = f(f^{-1}(y)) = y = \text{id}_T(y)$ , perché  $f^{-1}(y)$  è l'unico elemento di  $S$  la cui immagine in  $f$  è  $y$ .

Viceversa, sia  $f' : T \rightarrow S$  tale che  $f' \circ f = \text{id}_S$  e  $f \circ f' = \text{id}_T$ . Le identità sono biettive, in particolare  $\text{id}_S$  è iniettiva e  $\text{id}_T$  è suriettiva, sicché per 2.2.15  $f$  è iniettiva e suriettiva, quindi biettiva.

Si supponga infine:  $f', f'' : T \rightarrow S$  tali che  $f' \circ f = \text{id}_S = f'' \circ f$  e  $f \circ f' = \text{id}_T = f \circ f''$ . Per la 2.2.12 e la 2.2.13 si ha:  $f' = \text{id}_S \circ f' = (f'' \circ f) \circ f' = f'' \circ (f \circ f') = f'' \circ \text{id}_T = f''$ , come volevasi.  $\square$

Si noti che, con la verifica appena fatta, si prova che, con  $f : S \rightarrow T$  applicazione, se esistono  $f^*, f^{**} : T \rightarrow S$  tali che  $f \circ f^* = \text{id}_T$  e  $f^{**} \circ f = \text{id}_S$ , allora  $f^* = f^{**}$ .

Da 2.2.16 segue subito:

**2.2.17.** Sia  $f : S \rightarrow T$  un'applicazione. Se  $f$  è biettiva e ha per inversa  $f^{-1}$ , anche  $f^{-1}$  è biettiva e ha per inversa  $f$ , si ha cioè  $(f^{-1})^{-1} = f$ .

## Esercizi

**Esercizio 2.2.1.** Con  $f_1, f_2, f_4$  e  $f_5$  definite in 2.2.1, si calcolino:

$$\begin{array}{llll} f_1(2), & f_1(-2), & f_1(15), & f_1(-15), \\ f_2(0), & f_2(1), & f_2(2), & f_2(-2), \\ f_2(15), & f_2(-15), & f_4(-2), & f_4(15), \\ f_4(-15), & f_5(-2), & f_5(15), & f_5(-15). \end{array}$$

**Esercizio 2.2.2.** Sia  $f : S \rightarrow T$  un'applicazione. Si provi che:

$$f \text{ iniettiva} \iff |f^{-1}(\{y\})| \leq 1, \forall y \in T,$$

cioè

$$f \text{ iniettiva} \iff |f^{-1}(\{y\})| = 1, \forall y \in f(S).$$

**Esercizio 2.2.3.** Sia  $f : S \rightarrow T$  un'applicazione. Si provi che:

$$\begin{aligned} f \text{ suriettiva} &\iff f^{-1}(\{y\}) \neq \emptyset, \forall y \in T, \\ f \text{ suriettiva} &\iff f^{-1}(Y) \neq \emptyset, \forall Y \subseteq T, Y \neq \emptyset. \end{aligned}$$

**Esercizio 2.2.4.** Sia  $f : S \rightarrow T$  un'applicazione. Si provi che la relazione opposta  $f^{\text{op}}$  di  $f$  è un'applicazione se e solo se  $f$  è biettiva.

**Esercizio 2.2.5.** Siano  $S$  e  $T$  insiemi. Si provi che la relazione totale  $\mathcal{R}_t$  tra  $S$  e  $T$  è un'applicazione di  $S$  in  $T$  se e solo se  $S = \emptyset$  o  $|T| = 1$ .

**Esercizio 2.2.6.** Considerate le applicazioni

$$l_1 : x \in \mathbb{N}_0 \mapsto 4x \in \mathbb{N}_0,$$

$$l_2 : \mathbb{N}_0 \rightarrow \mathbb{Z}$$

$$n \mapsto \begin{cases} -n & \text{se } n \in 2\mathbb{N}_0 \\ -3 & \text{se } n \in \mathbb{N}_0 \setminus 2\mathbb{N}_0, \end{cases}$$

$$l_3 : \mathbb{Z} \rightarrow 2\mathbb{N}_0$$

$$z \mapsto \begin{cases} |z| & \text{se } z \in 2\mathbb{Z} \\ 4|z| & \text{se } z \in \mathbb{Z} \setminus 2\mathbb{Z}, \end{cases}$$

$$l_4 : \mathbb{N}_0 \rightarrow \mathbb{N}$$

$$n \mapsto \begin{cases} (n+4)/4 & \text{se } n \in 4\mathbb{N}_0 \\ 2 & \text{se } n \in \mathbb{N}_0 \setminus 4\mathbb{N}_0, \end{cases}$$

si provi che le implicazioni in 2.2.14 non si invertono.

**Esercizio 2.2.7.** Si dimostri quanto affermato nell'Esempio 2.2.6.

*Svolgimento.* La  $g_1$ , la  $g_2$ , la  $g_3$ , la  $g_4$  e la  $g_5$  sono iniettive. Infatti, con  $x, x' \in \mathbb{N}_0$  si ha:

$$g_1(x) = g_1(x') \implies 2x = 2x' \implies x = x', \text{ per la (1.2.14);}$$

$$g_2(x) = g_2(x') \implies 2x + 1 = 2x' + 1 \implies 2x = 2x' \implies x = x' \text{ per la (1.2.5) e la (1.2.14);}$$

$$g_3(x) = g_3(x') \implies x + 1 = x' + 1 \implies x = x', \text{ per la (1.2.5);}$$

$$g_4(x) = g_4(x') \implies x + 1 = x' + 1 \implies x = x', \text{ per la (1.2.5);}$$

$$g_5(x) = g_5(x') \implies 3x + 4 = 3x' + 4 \implies 3x = 3x' \implies x = x', \text{ sempre per la (1.2.5) e la (1.2.14).}$$

Per lo studio della  $g_7$  è conveniente osservare che da  $x \leq 6$  segue  $g_7(x) \leq 6$  e da  $x > 6$  segue  $g_7(x) = x + 4 > 6 + 4 = 10$  sicché se  $x \leq 6$  e  $x' > 6$  (o viceversa  $x > 6$  e  $x' \leq 6$ ) senz'altro si ha  $g_7(x) \neq g_7(x')$ . Se poi  $x, x' \leq 6$  con  $x \neq x'$ , banalmente  $g_7(x) = x \neq x' = g_7(x')$ ; infine se  $x > 6, x' > 6$  con  $x \neq x'$ , è anche  $x + 4 \neq x' + 4$ , per la (1.2.5). In ogni caso si ha che da  $x \neq x'$  segue

$g_7(x) \neq g_7(x')$  e dunque  $g_7$  è iniettiva. Analoghe considerazioni valgono per  $g_9$ , dopo avere osservato che  $g_9(x) \leq 0$  se  $x \in 2\mathbb{N}_0$ , e  $g_9(x) > 0$  se  $x \in \mathbb{N}_0 \setminus 2\mathbb{N}_0$ .

La  $g_6$  non è iniettiva poiché, per esempio,  $g_6(7) = 7 - 4 = 3 = g_6(3)$ , con  $7 \neq 3$ , e banalmente non lo è la  $g_8$  perché costante con dominio infinito.

**Esercizio 2.2.8.** Si dimostri 2.2.2.

**Esercizio 2.2.9.** Si dimostri 2.2.4.

**Esercizio 2.2.10.** Si dimostri 2.2.5.

**Esercizio 2.2.11.** Si dimostri 2.2.7.

**Esercizio 2.2.12.** Si dimostri 2.2.8.

**Esercizio 2.2.13.** Siano  $f : S \rightarrow T$  e  $g : T \rightarrow V$  applicazioni. Si provi che:

$$\begin{aligned} g \circ f \text{ iniettiva, } f \text{ suriettiva} &\implies g \text{ iniettiva,} \\ g \circ f \text{ suriettiva, } g \text{ iniettiva} &\implies f \text{ suriettiva.} \end{aligned}$$

**Esercizio 2.2.14.** Sia  $f : S \rightarrow T$  un'applicazione iniettiva. Se  $X$  è un sottoinsieme di  $S$ , si ha che:

$$|X| = 1 \iff |f(X)| = 1,$$

$$X \text{ finito} \iff f(X) \text{ finito};$$

più precisamente:

$$|X| = n \iff |f(X)| = n.$$

Inoltre:

$$X = f^{-1}(f(X)).$$

Se  $X_1$  e  $X_2$  sono sottoinsiemi di  $S$ , si ha che:

$$X_1 \subseteq X_2 \iff f(X_1) \subseteq f(X_2),$$

sicché

$$X_1 = X_2 \iff f(X_1) = f(X_2),$$

e dunque

$$X_1 \subset X_2 \iff f(X_1) \subset f(X_2).$$

Inoltre:

$$f(X_1 \cap X_2) = f(X_1) \cap f(X_2),$$

$$f(X_1 \setminus X_2) = f(X_1) \setminus f(X_2).$$

**Esercizio 2.2.15.** Sia  $f : S \rightarrow T$  un'applicazione e sia  $X$  un sottoinsieme di  $S$ . Si definisce **restrizione** di  $f$  a  $X$ , e si denota con  $f|_X$ , l'applicazione di  $X$  in  $T$  che a ogni elemento di  $X$  associa la sua immagine in  $f$ :

$$f|_X : x \in X \mapsto f(x) \in T.$$

Si noti che  $f|_X$  è la relazione indotta da  $f$  su  $X \times T$ . Si provi che:

$$\begin{aligned} f \text{ iniettiva} &\implies f|_X \text{ iniettiva}, \\ f|_X \text{ iniettiva} &\not\implies f \text{ iniettiva}, \\ f \text{ suriettiva} &\not\implies f|_X \text{ suriettiva}, \\ f|_X \text{ suriettiva} &\implies f \text{ suriettiva}. \end{aligned}$$

Si verifichi poi che  $\text{imm}_X = (\text{id}_S)|_X$ .

**Esercizio 2.2.16.** Siano  $f : S \rightarrow T$  un'applicazione e  $V$  un insieme contenente  $S$ . Un'applicazione  $g : V \rightarrow T$  è detta un **prolungamento** di  $f$  a  $V$  se  $g|_S = f$ , cioè se  $g(x) = f(x)$ , per ogni  $x \in S$ .

Per esempio,

$$g_1 : x \in \mathbb{N}_0 \mapsto 3x - 5 \in \mathbb{Z},$$

$$\begin{aligned} g_2 : x \in \mathbb{N}_0 &\longrightarrow \mathbb{Z} \\ x &\mapsto \begin{cases} 3x - 5 & \text{se } x \in \mathbb{N} \\ 43 & \text{se } x = 0, \end{cases} \end{aligned}$$

sono prolungamenti di  $f : x \in \mathbb{N} \mapsto 3x - 5 \in \mathbb{Z}$ .

Si scrivano altri tre prolungamenti di  $f$ .

**Esercizio 2.2.17.** Si provi che, con  $g$  prolungamento di  $f$ , si ha:

$$\begin{aligned} g \text{ iniettiva} &\implies f \text{ iniettiva}, \\ f \text{ iniettiva} &\not\implies g \text{ iniettiva}, \\ g \text{ suriettiva} &\not\implies f \text{ suriettiva}, \\ f \text{ suriettiva} &\implies g \text{ suriettiva}. \end{aligned}$$

**Esercizio 2.2.18.** Siano  $S$  e  $T$  insiemi e si consideri il prodotto cartesiano  $S \times T$ . Restano allora definite le applicazioni:

$$\pi_S : (x, y) \in S \times T \mapsto x \in S$$

e

$$\pi_T : (x, y) \in S \times T \mapsto y \in T,$$

dette, rispettivamente, la **proiezione** di  $S \times T$  su  $S$  e la proiezione di  $S \times T$  su  $T$ . Si provi che  $\pi_S$  e  $\pi_T$  sono suriettive, a meno che, rispettivamente, risultino ( $S \neq \emptyset$  e  $T = \emptyset$ ) o ( $S = \emptyset$  e  $T \neq \emptyset$ ).

Si noti che il termine “proiezione” deriva anch’esso dalla rappresentazione in coppie di numeri reali dei punti di un piano in cui sia definito un riferimento cartesiano ortogonale: infatti, se il punto  $P$  ha coordinate  $(a, b)$ , il punto di coordinate  $(a, 0)$  è la proiezione di  $P$  sull’asse  $x$  e così  $b$  individua sull’asse  $y$  la proiezione di  $P$ .

**Esercizio 2.2.19.** Siano  $S$  e  $T$  insiemi non vuoti. Un’applicazione  $f : S \rightarrow T$  è detta **cancellabile a sinistra** se da  $f \circ h = f \circ k$ , con  $h, k : V \rightarrow S$  segue  $h = k$ ;  $f$  è detta **cancellabile a destra** se da  $g \circ f = l \circ f$ , con  $g, l : T \rightarrow W$  segue che  $g = l$ . Si provi che:

$$\begin{aligned} f \text{ cancellabile a sinistra} &\iff f \text{ iniettiva}, \\ f \text{ cancellabile a destra} &\iff f \text{ suriettiva}. \end{aligned}$$

Se ne deduca che:

$$f \text{ cancellabile a destra e a sinistra} \iff f \text{ biettiva}.$$

**Esercizio 2.2.20.** Sia  $f : S \rightarrow T$  un’applicazione, con  $S$  e  $T$  non vuoti. Un’applicazione  $h : T \rightarrow S$  è detta un’**inversa sinistra** di  $f$  se  $h \circ f = \text{id}_S$ , un’**inversa destra** di  $f$  se  $f \circ h = \text{id}_T$ . Si provi che:

$$\begin{aligned} f \text{ ha inversa sinistra} &\iff f \text{ iniettiva}, \\ f \text{ ha inversa destra} &\iff f \text{ suriettiva}. \end{aligned}$$

Si provi inoltre che se  $h$  è un’inversa sinistra di  $f$  e  $k$  è un’inversa destra di  $f$  allora  $h = k$ ,  $f$  è biettiva e  $h = f^{-1}$ . Si costruiscano due inverse sinistre di:

$$f : x \in \mathbb{N} \mapsto x - 1 \in \mathbb{Z},$$

e due inverse destre di:

$$g : x \in \mathbb{Z} \mapsto |x| \in \mathbb{N}_0.$$

**Suggerimento.** Se  $f$  è iniettiva, si fissi  $\bar{x} \in S$ . Si definisca poi  $h(y)$  come l’unico elemento  $x \in S$  tale che  $y = f(x)$ , se  $y \in f(S)$ ; e  $h(y) = \bar{x}$  se  $y \notin f(S)$ .

Se  $f$  è suriettiva, per ogni  $y \in T$  si “scelga” un elemento  $x_y \in f^{-1}(\{y\})$ , e si ponga  $h(y) = x_y$  per ogni  $y \in T$ . Si noti che tale procedimento necessita della possibilità di fare “infinte scelte”, coinvolge cioè il cosiddetto “Assioma della scelta” che qui si preferisce non approfondire.

**Esercizio 2.2.21.** Considerate le applicazioni:

$$k : x \in \mathbb{N} \mapsto -x - 5 \in \mathbb{Z},$$

$$l : z \in \mathbb{Z} \mapsto 5z^2 + 4 \in \mathbb{N},$$

$$f : n \in \mathbb{N} \mapsto 1 \in \mathbb{N},$$

si stabilisca se esse sono iniettive, suriettive, biettive, e si determinino le composite:

$$l \circ k, \quad k \circ l, \quad f \circ l, \quad k \circ f.$$

**Esercizio 2.2.22.** Si considerino le applicazioni:

$$g : m \in 16\mathbb{Z} \longmapsto \frac{m}{4} \in 4\mathbb{Z},$$

$$k : x \in 4\mathbb{Z} \longmapsto x^2 \in 16\mathbb{Z}.$$

- (i) Si calcolino:  $g(\{-16, 0, 16, 32\})$ ,  $g(32\mathbb{Z})$ ,  $g^{-1}(4\mathbb{Z})$ ,  $k(\{0, 4, 12, 8, -8\})$ ,  $k(4\mathbb{Z})$ ,  $k^{-1}(\{0, 16, -16, 32\})$ .
- (ii) Si stabilisca se  $g$  e  $k$  sono iniettive o suriettive.
- (iii) Qualora una delle applicazioni (o entrambe) sia biettiva, se ne precisi l'inversa.
- (iv) Si determinino le composte  $k \circ g$  e  $g \circ k$ .

**Esercizio 2.2.23.** Si considerino le applicazioni:

$$k : t \in 5\mathbb{Z} \longmapsto t^2 \in 25\mathbb{Z},$$

$$h : z \in 25\mathbb{Z} \longmapsto \frac{z}{5} \in 5\mathbb{Z}.$$

- (i) Si calcolino:  $k(\{-5, 0, 5, 10\})$ ,  $k(50\mathbb{Z})$ ,  $k^{-1}(\{0, 25, -25, 50\})$ ,  $h^{-1}(5\mathbb{Z})$ ,  $h(\{0, 25, -50\})$ ,  $h^{-1}(\{0, 25, 50\})$ .
- (ii) Si stabilisca se  $k$  e  $h$  sono iniettive o suriettive.
- (iii) Qualora una delle applicazioni (o entrambe) sia biettiva, se ne precisi l'inversa.
- (iv) Si determinino le composte  $h \circ k$  e  $k \circ h$  e le si studi.

**Esercizio 2.2.24.** Si considerino le applicazioni:

$$g : m \in 4\mathbb{N}_0 \longmapsto \frac{m}{3} \in \mathbb{Q},$$

$$k : x \in \mathbb{Q} \longmapsto 3x \in \mathbb{Q}.$$

- (i) Si calcolino:  $g(\{0, 16, 32, 36\})$ ,  $g(12\mathbb{N}_0)$ ,  $g^{-1}(\mathbb{Q})$ ,  $k^{-1}(\{0, 16, -16, 32\})$ ,  $k(\mathbb{Q})$ ,  $k(\{0, 8, -8, 9, -9\})$ .
- (ii) Si stabilisca se  $g$  e  $k$  sono iniettive o suriettive.
- (iii) Qualora una delle applicazioni (o entrambe) sia biettiva, se ne precisi l'inversa.
- (iv) Si determini la composta  $k \circ g$ .

**Esercizio 2.2.25.** Si considerino le applicazioni:

$$g : z \in 3\mathbb{Z} \longmapsto \frac{z}{3} + 5 \in \mathbb{Z},$$

$$h : t \in \mathbb{Z} \longmapsto 9t + 3 \in 3\mathbb{Z}.$$

- (i) Si calcolino:  $g(\{0, 6, -6, 12, -12\})$ ,  $g(3\mathbb{Z})$ ,  $g^{-1}(\mathbb{Z})$ ,  $g^{-1}(\{1, 11, -11\})$ ,  $h(\{-7, -2, -1, 0, 1, 2, 7\})$ ,  $h^{-1}(\{0, -3, 24, -30\})$ ,  $h^{-1}(\{15, -21, 36\})$ .
- (ii) Si stabilisca se  $g$  e  $h$  sono iniettive o suriettive.
- (iii) Si determinino e si studino le composte  $g \circ h$  e  $h \circ g$ .

**Esercizio 2.2.26.** Si considerino le applicazioni:

$$\begin{aligned} g : m \in 3\mathbb{N}_0 &\longmapsto 2m + 6 \in 6\mathbb{N}, \\ k : x \in 6\mathbb{N} &\longmapsto (x - 6)(x - 12) \in 6\mathbb{N}. \end{aligned}$$

- (i) Si calcolino:  $g(\{0, 3, 6, 12\})$ ,  $g^{-1}(\{6, 12, 24\})$ ,  $g(3\mathbb{N})$ ,  $k(\{6, 12, 18, 24\})$ ,  $k^{-1}(\{0, 6, 72\})$ ,  $k^{-1}(6\mathbb{N})$ .
- (ii) Si stabilisca se  $g$  e  $k$  sono iniettive o suriettive.
- (iii) Qualora una delle applicazioni (o entrambe) sia biettiva, se ne precisi l'inversa.
- (iv) Si determini la composta  $k \circ g$  e la si studi.

**Esercizio 2.2.27.** Si considerino le applicazioni:

$$\begin{aligned} g : m \in \mathbb{N} &\longmapsto -(m - 1) \in \mathbb{Z}, \\ k : x \in \mathbb{Z} &\longmapsto 2|x| \in 2\mathbb{N}_0. \end{aligned}$$

- (i) Si calcolino:  $g(\{1, 3, 6, 7\})$ ,  $g(3\mathbb{N})$ ,  $g^{-1}(\{0, 1, 3, 4, -4, -7\})$ ,  $g^{-1}(\{5, 9\})$ ,  $k(\{0, 2, 3, -3, -5\})$ ,  $k^{-1}(\{10\})$ .
- (ii) Si stabilisca se  $g$  e  $k$  sono iniettive o suriettive.
- (iii) Si determini la composta  $k \circ g$ , si verifichi che è biettiva e se ne individui l'inversa.

**Esercizio 2.2.28.** Si considerino le applicazioni:

$$\begin{aligned} k : t \in \mathbb{N}_0 &\longmapsto -t \in \mathbb{Z}, \\ h : z \in \mathbb{Z} &\longmapsto 6|z| + 6 \in 6\mathbb{N}. \end{aligned}$$

- (i) Si calcolino:  $k(\{0, 2, 3, 5\})$ ,  $k(4\mathbb{N})$ ,  $k^{-1}(\{1, -1, 3, -4\})$ ,  $k^{-1}(\{5, 6, 7\})$ ,  $h(\{0, -2, 3, 4, -4\})$ ,  $h^{-1}(\{12\})$ .
- (ii) Si stabilisca se  $k$  e  $h$  sono iniettive o suriettive.
- (iii) Si determini la composta  $h \circ k$ , si verifichi che è biettiva e se ne individui l'inversa.

**Esercizio 2.2.29.** Si dimostri che l'applicazione

$$f : t \in \mathbb{Z} \longmapsto 2t - 16 \in 2\mathbb{Z}$$

è biettiva. Si determini l'inversa  $f^{-1}$ , e si calcolino:  $f^{-1}(-20)$ ,  $f^{-1}(20)$ ,  $f^{-1}(0)$ .

**Esercizio 2.2.30.** Si dimostri che l'applicazione

$$g : s \in \mathbb{Q} \longmapsto \frac{1}{5}s + \frac{3}{2} \in \mathbb{Q}$$

è biettiva. Si determini l'inversa  $g^{-1}$ , e si calcolino:  $g^{-1}(-\frac{1}{2})$ ,  $g^{-1}(\frac{1}{2})$ ,  $g^{-1}(0)$ .

**Esercizio 2.2.31.** Con  $X = \{i, m, n, v\}$  e  $Y = \{1, 7, 13, 21\}$ , osservato che l'applicazione seguente  $f$  è biettiva, se ne precisi l'inversa:

$$\begin{array}{rcl} f : & X & \longrightarrow Y \\ & i & \longmapsto 13 \\ & m & \longmapsto 1 \\ & n & \longmapsto 21 \\ & v & \longmapsto 7. \end{array}$$

## 2.3 Relazioni d'equivalenza e partizioni

Nella prima parte di questo paragrafo sarà introdotto il concetto di partizione di un insieme non vuoto, concetto strettamente legato a quello di relazione d'equivalenza cui è prevalentemente dedicato il paragrafo. Il legame in oggetto è evidenziato dal teorema fondamentale che sarà ampiamente illustrato.

Sia  $S$  un insieme non vuoto e sia  $\mathcal{F} \subseteq \mathcal{P}(S)$  un insieme di sottoinsiemi di  $S$ . L'insieme  $\mathcal{F}$  è detto una **partizione** di  $S$  se ogni elemento di  $\mathcal{F}$  è un sottoinsieme non vuoto di  $S$ , gli elementi di  $\mathcal{F}$  sono a due a due disgiunti, e la loro unione è  $S$ :

$$\mathcal{F} \text{ partizione di } S : \iff \left\{ \begin{array}{l} 1) \quad X \neq \emptyset, \forall X \in \mathcal{F}; \\ 2) \quad X, Y \in \mathcal{F}, X \neq Y \implies X \cap Y = \emptyset; \\ 3) \quad \bigcup_{X \in \mathcal{F}} X = S. \end{array} \right.$$

**2.3.1. Esempio.** Esempi di partizione sono

$$\mathcal{F}_t = \{S\},$$

la **partizione totale**, e

$$\mathcal{F}_{\text{id}} = \{\{x\} : x \in S\},$$

la **partizione identica**. Ovviamente esse coincidono se e solo se  $S$  è un singleton, e sono le sole se  $|S| \leq 2$ .

Considerato l'insieme  $A = \{a, b, c\}$ , le partizioni di  $A$  sono:

$$\mathcal{F}_t, \mathcal{F}_{\text{id}}, \mathcal{F}_3 = \{\{a\}, \{b, c\}\}, \mathcal{F}_4 = \{\{b\}, \{a, c\}\}, \mathcal{F}_5 = \{\{c\}, \{a, b\}\}.$$

Partizioni di  $\mathbb{N}_0$  sono per esempio:

$$\{\mathbb{N}_0\}, \{\mathbb{N}_p, \mathbb{N}_d\}, \{\{0\}, \mathbb{N}\}, \{\mathbb{N}_p, \{x\} : x \in \mathbb{N}_d\}.$$

Se  $S$  è un insieme non vuoto e  $\mathcal{F}$  un insieme di sottoinsiemi non vuoti di  $S$  si ha che:

$$\mathcal{F} \text{ partizione di } S \iff (\forall x \in S, \exists! Y \in \mathcal{F} : x \in Y). \quad (2.3.1)$$

Infatti, se  $\mathcal{F}$  è una partizione di  $S$ , ogni  $x \in S$  appartiene a qualche  $Y \in \mathcal{F}$  in quanto  $S = \bigcup_{X \in \mathcal{F}} X$ . Supposto poi  $x \in Y$  e  $x \in Z$  con  $Y, Z \in \mathcal{F}$ , si ha

che  $Y \cap Z \neq \emptyset$  sicché, per la 2),  $Y = Z$ , come volevasi. Viceversa, se ogni  $x \in S$  appartiene a uno e un solo  $Y \in \mathcal{F}$ , si ha ovviamente  $S = \bigcup_{X \in \mathcal{F}} X$  e poi, supposto  $Y, Z \in \mathcal{F}$  con  $Y \cap Z \neq \emptyset$ , si ha  $Y = Z$  in quanto ogni elemento di  $Y \cap Z$  appartiene sia a  $Y$  che a  $Z$ .

Come anticipato, il concetto di partizione è strettamente legato a quello di relazione d'equivalenza: ciò sarà illustrato nel seguito del paragrafo.

Come già introdotto nel Paragrafo 2.1, se  $S$  è un insieme non vuoto, una relazione binaria  $\mathcal{R}$  in  $S$  viene detta una relazione d'equivalenza se è contemporaneamente riflessiva, simmetrica e transitiva:

$$\mathcal{R} \text{ relazione d'equivalenza in } S \iff \begin{cases} \mathcal{R} \text{ riflessiva,} \\ \mathcal{R} \text{ simmetrica,} \\ \mathcal{R} \text{ transitiva.} \end{cases}$$

Si ha cioè:

$$\mathcal{R} \text{ relazione d'equivalenza in } S \iff \begin{cases} x \mathcal{R} x, \forall x \in S; \\ x \mathcal{R} y \implies y \mathcal{R} x, \forall x, y \in S; \\ x \mathcal{R} y, y \mathcal{R} z \implies x \mathcal{R} z, \forall x, y, z \in S. \end{cases}$$

**2.3.2. Esempio.** Qualunque sia l'insieme  $S$  l'identità di  $S$  è una relazione d'equivalenza in  $S$ , e così la relazione totale  $\mathcal{R}_t$ . La relazione vuota invece non è mai una relazione d'equivalenza in un insieme non vuoto  $S$ , non essendo riflessiva.

La relazione  $\mathcal{R}$  in  $\mathbb{N}_0$  definita ponendo  $x \mathcal{R} y : \iff x + y \in \mathbb{N}_p$  è una relazione d'equivalenza in  $\mathbb{N}_0$ . Infatti:  $x \mathcal{R} x$ , per ogni  $x \in \mathbb{N}_0$  poiché  $x + x = 2x$  è sempre pari; da  $x \mathcal{R} y$  segue  $x + y \in \mathbb{N}_p$ , sicché  $y + x = x + y \in \mathbb{N}_p$  e dunque  $y \mathcal{R} x$ ; infine, se  $x \mathcal{R} y$  e  $y \mathcal{R} z$ , risulta  $x + y \in \mathbb{N}_p$  e  $y + z \in \mathbb{N}_p$ , da cui  $(x + y) + (y + z) = x + 2y + z \in \mathbb{N}_p$  e  $x + z \in \mathbb{N}_p$ , il che comporta  $x \mathcal{R} z$ , come volevasi.

Siano ora  $S$  un insieme non vuoto e  $\mathcal{R}$  una relazione d'equivalenza in  $S$ . Se  $x \in S$  si dice **classe d'equivalenza** di  $x$  modulo  $\mathcal{R}$ , e si denota con il simbolo  $[x]_{\mathcal{R}}$  (o più semplicemente con il simbolo  $[x]$ , se non c'è ambiguità) il sottoinsieme di  $S$  costituito da tutti e soli gli elementi di  $S$  che sono in relazione con  $x$ :

$$[x]_{\mathcal{R}} := \{s \in S : s \mathcal{R} x\}.$$

Si parla anche di classe d'equivalenza “rappresentata da  $x$ ”.

L'insieme delle classi d'equivalenza di  $S$  modulo  $\mathcal{R}$  viene detto l'**insieme quoziente** di  $S$  modulo  $\mathcal{R}$  (o l'insieme “ $S$  su  $\mathcal{R}$ ”):

$$S/\mathcal{R} := \{[x]_{\mathcal{R}} : x \in S\}.$$

L'applicazione:

$$\pi : x \in S \mapsto [x]_{\mathcal{R}} \in S/\mathcal{R}$$

è detta la **proiezione canonica** di  $S$  in  $S/\mathcal{R}$ . Si noti che essa è sempre suriettiva, ed è iniettiva se e solo se  $\mathcal{R} = \text{id}_S$ .

**2.3.3.** Siano  $S$  un insieme e  $\mathcal{R}$  una relazione d'equivalenza in  $S$ . Allora:

$$x \in [x]_{\mathcal{R}}, \forall x \in S, \quad (2.3.2)$$

$$x \mathcal{R} y \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}}, \quad (2.3.3)$$

$$x \not\mathcal{R} y \iff [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset. \quad (2.3.4)$$

*Dimostrazione.* Per ogni  $x \in S$  si ha  $x \mathcal{R} x$  per la proprietà riflessiva di  $\mathcal{R}$ , sicché  $x \in [x]_{\mathcal{R}}$ , pertanto vale la (2.3.2).

Per provare la (2.3.3) si supponga in primo luogo  $x \mathcal{R} y$ . Se  $z \in [x]_{\mathcal{R}}$ , allora  $z \mathcal{R} x$  e da  $x \mathcal{R} y$  segue  $z \mathcal{R} y$  per la proprietà transitiva, sicché  $z \in [y]_{\mathcal{R}}$ ; viceversa sia  $z \in [y]_{\mathcal{R}}$ , allora  $z \mathcal{R} y$ , le ipotesi assicurano che  $y \mathcal{R} x$  per la proprietà simmetrica, sicché  $z \mathcal{R} x$  per la proprietà transitiva e dunque  $z \in [x]_{\mathcal{R}}$ . Pertanto  $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$ . Viceversa, sia  $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$ , allora da  $x \in [x]_{\mathcal{R}}$  segue  $x \in [y]_{\mathcal{R}}$  e  $x \mathcal{R} y$ , come volevasi. Pertanto vale la (2.3.3).

Si supponga ora  $x \not\mathcal{R} y$  e, per assurdo, esista  $z \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}}$ ; allora  $z \in [x]_{\mathcal{R}}$  e  $z \in [y]_{\mathcal{R}}$ , sicché  $z \mathcal{R} x$  e  $z \mathcal{R} y$ , da cui  $x \mathcal{R} z$ , per la proprietà simmetrica, e  $x \mathcal{R} y$ , per la proprietà transitiva, contro le ipotesi. Viceversa, se  $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$ , non può avversi  $x \mathcal{R} y$ , altrimenti risulterebbe  $x \in [y]_{\mathcal{R}}$  e  $x \in [x]_{\mathcal{R}}$  per la (2.3.2) sicché  $x \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}}$ , contro le ipotesi. Resta così provata la (2.3.4).  $\square$

Si noti che la (2.3.3) ovviamente equivale a:

$$[x]_{\mathcal{R}} = [y]_{\mathcal{R}} \iff x \in [y]_{\mathcal{R}}, \quad (2.3.5)$$

il che assicura che ogni elemento di una classe d'equivalenza è capace di rappresentarla.

**2.3.4. Esempi.** Sia  $S$  un insieme non vuoto. Considerata la relazione identica  $\text{id}_S$  in  $S$ , si ha  $[x]_{\text{id}_S} = \{x\}$  per ogni  $x \in S$ , perché ogni elemento di  $S$  è in relazione solo con se stesso. Pertanto  $S / \text{id}_S = \{\{x\} : x \in S\} = \mathcal{F}_{\text{id}}$ . Considerata la relazione totale  $\mathcal{R}_t$ , si ha  $[x]_{\mathcal{R}_t} = S$  per ogni  $x \in S$  e dunque  $S / \mathcal{R}_t = \{S\} = \mathcal{F}_t$ .

In  $\mathbb{N}_0$  si consideri la relazione d'equivalenza  $x \mathcal{R} y \iff x + y \in \mathbb{N}_p$ , già definita nell'Esempio 2.3.2. Si vede subito che  $[0]_{\mathcal{R}} = \{n \in \mathbb{N}_0 : n + 0 \in \mathbb{N}_p\} = \{n \in \mathbb{N}_0 : n \in \mathbb{N}_p\} = \mathbb{N}_p$ . Si ha poi  $[1]_{\mathcal{R}} = \{n \in \mathbb{N}_0 : n + 1 \in \mathbb{N}_p\} = \mathbb{N}_d$ . Per ogni  $n \in \mathbb{N}_p$ , da  $n \in [0]_{\mathcal{R}}$  segue allora  $[n]_{\mathcal{R}} = [0]_{\mathcal{R}} = \mathbb{N}_p$ ; analogamente, per ogni  $n \in \mathbb{N}_d$  si ha  $n \in [1]_{\mathcal{R}}$  e quindi  $[n]_{\mathcal{R}} = [1]_{\mathcal{R}} = \mathbb{N}_d$ . Quanto provato assicura che:  $\mathbb{N}_0 / \mathcal{R} = \{\mathbb{N}_p, \mathbb{N}_d\}$ .

**2.3.5.** Siano  $S$  un insieme non vuoto,  $\mathcal{R}_1$  e  $\mathcal{R}_2$  relazioni d'equivalenza in  $S$ . Sono equivalenti le seguenti proprietà:

- (i)  $\mathcal{R}_1 = \mathcal{R}_2$ ,
- (ii)  $[x]_{\mathcal{R}_1} = [x]_{\mathcal{R}_2}, \forall x \in S$ ,
- (iii)  $S / \mathcal{R}_1 = S / \mathcal{R}_2$ .

*Dimostrazione.* Ovviamente da (i) segue (ii) in quanto l'ipotesi (i) assicura che, con  $x, y \in S$ , si ha  $x \mathcal{R}_1 y$  se e solo se  $x \mathcal{R}_2 y$ . Supposto (ii), si ha subito (iii) per definizione di insieme quoziante. Si assuma ora  $S/\mathcal{R}_1 = S/\mathcal{R}_2$  e sia  $x \in S$ . Si ha  $[x]_{\mathcal{R}_1} \in S/\mathcal{R}_1 = S/\mathcal{R}_2$  sicché esiste  $x' \in S$  tale che  $[x]_{\mathcal{R}_1} = [x']_{\mathcal{R}_2}$ . Per la (2.3.2) riesce  $x \in [x]_{\mathcal{R}_1}$  e dunque  $x \in [x']_{\mathcal{R}_2}$  da cui  $[x]_{\mathcal{R}_2} = [x']_{\mathcal{R}_2}$  per la (2.3.5). Pertanto  $[x]_{\mathcal{R}_1} = [x]_{\mathcal{R}_2}$ . Ciò prova la (ii). Si ottiene subito anche la (i) in quanto, con  $x, y \in S$ , si ha:  $x \mathcal{R}_1 y$  se e solo se, per (2.3.3),  $[x]_{\mathcal{R}_1} = [y]_{\mathcal{R}_1}$ , ciò equivale, per quanto appena provato, a  $[x]_{\mathcal{R}_2} = [y]_{\mathcal{R}_2}$ , cioè a  $x \mathcal{R}_2 y$ , sempre per la (2.3.3). Pertanto  $\mathcal{R}_1 = \mathcal{R}_2$ .  $\square$

Si è ora in grado di enunciare e dimostrare il seguente:

**2.3.6. Teorema fondamentale sulle relazioni d'equivalenza.** *Sia  $S$  un insieme non vuoto.*

- (I) *Se  $\mathcal{R}$  è una relazione d'equivalenza in  $S$ , l'insieme quoziante  $S/\mathcal{R}$  è una partizione di  $S$ .*
- (II) *Se  $\mathcal{F}$  è una partizione di  $S$ , esiste una e una sola relazione d'equivalenza  $\mathcal{R}_{\mathcal{F}}$  tale che  $\mathcal{F} = S/\mathcal{R}_{\mathcal{F}}$ .*

*Dimostrazione.* Sia  $\mathcal{R}$  una relazione d'equivalenza in  $S$  e si consideri l'insieme quoziante  $S/\mathcal{R}$ . Ovviamente  $S/\mathcal{R} \subseteq \mathcal{P}(S)$  in quanto  $[x]_{\mathcal{R}} \subseteq S$ , per ogni  $x \in S$ . Da (2.3.2) segue  $[x]_{\mathcal{R}} \neq \emptyset$ , per ogni  $x \in S$ . Supposto  $[x]_{\mathcal{R}} \neq [y]_{\mathcal{R}}$ , si ha  $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$  altrimenti si avrebbe  $x \mathcal{R} y$  per (2.3.4) e poi  $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$  per (2.3.3). Infine, ovviamente,  $\bigcup_{x \in S} [x]_{\mathcal{R}} = S$  per (2.3.2). Pertanto  $S/\mathcal{R}$  è una partizione di  $S$ , e la (I) è provata.

Allo scopo di provare la (II), sia ora  $\mathcal{F}$  una partizione di  $S$  e si definisca in  $S$  la seguente relazione: con  $x, y \in S$ ,

$$x \mathcal{R}_{\mathcal{F}} y : \iff \exists Y \in \mathcal{F} : x, y \in Y.$$

La relazione  $\mathcal{R}_{\mathcal{F}}$  è riflessiva perché, con  $x \in S$ , si ha che esiste  $Y \in \mathcal{F}$  tale che  $x \in Y$ , in quanto  $\bigcup_{X \in \mathcal{F}} X = S$ . È poi banalmente simmetrica, in quanto supposto  $x \mathcal{R}_{\mathcal{F}} y$ , si ha  $x, y \in Y$  per qualche  $Y \in \mathcal{F}$  e dunque  $y, x \in Y$  con  $Y \in \mathcal{F}$ , il che comporta  $y \mathcal{R}_{\mathcal{F}} x$ . Si supponga ora  $x \mathcal{R}_{\mathcal{F}} y$  e  $y \mathcal{R}_{\mathcal{F}} z$ , esistano quindi  $Y, Z \in \mathcal{F}$  tali che  $x, y \in Y$  e  $y, z \in Z$ . Si ha allora  $y \in Y \cap Z$  e dunque  $Y \cap Z \neq \emptyset$ , sicché  $Y = Z$  per la proprietà 2) delle partizioni. Riesce quindi  $x, z \in Y$  con  $Y \in \mathcal{F}$  da cui  $x \mathcal{R}_{\mathcal{F}} z$ . Pertanto  $\mathcal{R}_{\mathcal{F}}$  è transitiva. Si è così provato che  $\mathcal{R}_{\mathcal{F}}$  è una relazione d'equivalenza. Si osservi ora che, essendo  $\mathcal{F}$  una partizione di  $S$ , la (2.3.1) assicura che per ogni  $x \in S$  esiste uno e un solo elemento di  $\mathcal{F}$ , lo si denoti con  $V_x$ , tale che  $x \in V_x$ . È facile ora provare che:

$$[x]_{\mathcal{R}_{\mathcal{F}}} = V_x.$$

Infatti, sia  $y \in [x]_{\mathcal{R}_{\mathcal{F}}}$ , sia cioè  $y \mathcal{R}_{\mathcal{F}} x$ . Allora esiste  $Y \in \mathcal{F}$  tale che  $x, y \in Y$  e si ha  $Y = V_x$  per l'unicità dell'elemento di  $\mathcal{F}$  cui  $x$  appartiene. Pertanto  $y \in V_x$ .

Viceversa, se  $y \in V_x$ , esiste proprio  $V_x \in \mathcal{F}$  tale che  $x, y \in V_x$  e dunque  $y \mathcal{R}_{\mathcal{F}} x$  e  $y \in [x]_{\mathcal{R}_{\mathcal{F}}}$ , come volevasi. Da ciò segue facilmente che :

$$S/\mathcal{R}_{\mathcal{F}} = \mathcal{F}.$$

Infatti, se  $[x]_{\mathcal{R}_{\mathcal{F}}} \in S/\mathcal{R}_{\mathcal{F}}$ , si ha  $[x]_{\mathcal{R}_{\mathcal{F}}} = V_x \in \mathcal{F}$ , dove  $V_x$  è l'elemento prima individuato. Viceversa, se  $Y \in \mathcal{F}$  si ha  $Y \neq \emptyset$  e dunque esiste  $z \in S$  tale che  $z \in Y$  sicché  $Y = V_z = [z]_{\mathcal{R}_{\mathcal{F}}} \in S/\mathcal{R}_{\mathcal{F}}$ , come richiesto. Supposto infine  $\mathcal{R}'$  relazione d'equivalenza in  $S$  tale che  $S/\mathcal{R}' = \mathcal{F}$ , si ottiene subito  $\mathcal{R}' = \mathcal{R}_{\mathcal{F}}$  da 2.3.5.  $\square$

Il Teorema 2.3.6 assicura che esiste un'applicazione biettiva tra l'insieme delle relazioni d'equivalenza in  $S$  e le partizioni di  $S$ : infatti associando a ogni  $\mathcal{R}$  l'insieme quoziante  $S/\mathcal{R}$  si ottiene per la 2.3.5 un'applicazione iniettiva, che risulta poi suriettiva per la (II) del teorema fondamentale sulle relazioni d'equivalenza (vedi 2.3.6).

Si noti che la dimostrazione del Teorema 2.3.6 è "costruttiva" nel senso che permette sia di individuare la partizione a partire dalla relazione d'equivalenza che, viceversa, determinare la relazione d'equivalenza a partire dalla partizione. Per esempio è immediato verificare che la relazione d'equivalenza in  $\mathbb{N}_0$  determinata dalla partizione  $\{\mathbb{N}_p, \mathbb{N}_d\}$  è la relazione  $\mathcal{R}$  di 2.3.2.

Ogni applicazione  $f$  tra insiemi non vuoti  $S$  e  $T$  individua una relazione d'equivalenza in  $S$ , detta la **relazione determinata o indotta** da  $f$  su  $S$  e denotata con  $\mathcal{R}_f$ . Tale relazione mette in corrispondenza gli elementi di  $S$  che hanno in  $f$  la stessa immagine: con  $x, y \in S$

$$x \mathcal{R}_f y : \iff f(x) = f(y).$$

Che tale relazione sia d'equivalenza è di immediata verifica.

**2.3.7. Esempio.** Si consideri  $f : x \in \mathbb{Z} \mapsto x^2 \in \mathbb{N}_0$ . La relazione d'equivalenza determinata da  $f$  è la seguente relazione in  $\mathbb{Z}$ :

$$x \mathcal{R}_f y \iff x^2 = y^2 \iff y = \pm x.$$

Sia ora  $g : x \in \mathbb{Z} \mapsto |x| \in \mathbb{N}_0$ . La relazione d'equivalenza determinata da  $g$  è la seguente relazione in  $\mathbb{Z}$ :

$$x \mathcal{R}_g y \iff |x| = |y| \iff y = \pm x.$$

Risulta  $\mathcal{R}_f = \mathcal{R}_g$ , pertanto applicazioni diverse possono determinare la stessa relazione d'equivalenza.

**Osservazione.** Sia  $\mathcal{R}$  una relazione d'equivalenza in  $S$  e sia

$$\pi : x \in S \mapsto [x]_{\mathcal{R}} \in S/\mathcal{R}$$

la relativa proiezione canonica. Con  $x, y \in S$  si ha:

$$x \mathcal{R}_{\pi} y \iff \pi(x) = \pi(y) \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}} \iff x \mathcal{R} y,$$

per la (2.3.3). Pertanto  $\mathcal{R} = \mathcal{R}_{\pi}$ , e dunque ogni relazione d'equivalenza è indotta da un'opportuna applicazione.

Si noti inoltre che:

**2.3.8.** Sia  $f : S \rightarrow S$  un'applicazione, con  $S \neq \emptyset$ . Allora:

$$\begin{aligned}\mathcal{R}_f \text{ totale} &\iff f \text{ costante}, \\ \mathcal{R}_f = \text{id}_S &\iff f \text{ iniettiva}.\end{aligned}$$

*Dimostrazione.* Esercizio. □

**Osservazione.** A volte si vuole definire un'applicazione di dominio un insieme quoziante, precisando il corrispondente di ciascuna classe a partire da un suo rappresentante. Per esempio, considerata la relazione  $\mathcal{R}$  di 2.3.2 in  $\mathbb{N}_0$ , si potrebbe pensare di associare a ogni classe  $[x]_{\mathcal{R}}$  il numero intero  $3x - 7$ . In tal modo resta definita una relazione tra  $\mathbb{N}_0 / \mathcal{R}$  e  $\mathbb{Z}$  che non è un'applicazione, in quanto ogni classe ha infiniti corrispondenti, per esempio  $[1]_{\mathcal{R}} = [3]_{\mathcal{R}} = [5]_{\mathcal{R}} = \dots$  ha corrispondenti  $-4, 2, 8, \dots$ , mentre  $[2]_{\mathcal{R}} = [4]_{\mathcal{R}} = [6]_{\mathcal{R}} = \dots$  ha corrispondenti  $-1, 5, 11, \dots$ . Per essere sicuri di definire una relazione che sia un'applicazione, bisogna provare che il corrispondente di ogni classe non dipende dal rappresentante considerato. Nell'esempio precedente, associando a ogni classe  $[x]_{\mathcal{R}} \in \mathbb{N}_0 / \mathcal{R}$  l'intero  $(-1)^x$  si ottiene un'applicazione di  $\mathbb{N}_0 / \mathcal{R}$  in  $\mathbb{Z}$  poiché se  $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$  allora  $x \mathcal{R} y$ , quindi  $x$  e  $y$  sono entrambi pari oppure entrambi dispari; ne segue in ogni caso  $(-1)^x = (-1)^y$ .

Nel seguito tali considerazioni saranno spesso applicate.

## Esercizi

**Esercizio 2.3.1.** Si consideri in  $\mathbb{Z}$  la relazione binaria definita da:

$$a \mathcal{R} b : \iff (a = b) \text{ o } (a, b \in \mathbb{N}_0).$$

- (i) Si provi che  $\mathcal{R}$  è una relazione d'equivalenza in  $\mathbb{Z}$ .
- (ii) Si precisi se le seguenti affermazioni sono esatte:  $17 \mathcal{R} 151$ ,  $-3 \mathcal{R} 123$ ,  $-41 \mathcal{R} -41$ ,  $-60 \mathcal{R} -20$ ,  $34 \mathcal{R} 34$ ,  $6 \mathcal{R} 0$ .
- (iii) Si determini l'insieme quoziante  $\mathbb{Z} / \mathcal{R}$ .

**Svolgimento.** Si è già provato che  $\mathcal{R}$  è una relazione d'equivalenza in  $\mathbb{Z}$  (vedi Esercizio 2.1.3). Si ha  $17 \mathcal{R} 151$ , poiché  $17$  e  $151 \in \mathbb{N}_0$ , analogamente  $6 \mathcal{R} 0$ ; inoltre ovviamente  $-41 \mathcal{R} -41$  e  $34 \mathcal{R} 34$ . Invece  $-3 \mathcal{R} 123$ , infatti  $-3 \neq 123$  e  $-3 \notin \mathbb{N}_0$ , analogamente  $-60 \mathcal{R} -20$ . Si ha:

$$[0]_{\mathcal{R}} = \{n \in \mathbb{Z} : n \mathcal{R} 0\} = \{n \in \mathbb{Z} : (n = 0) \text{ o } (n, 0 \in \mathbb{N}_0)\} = \mathbb{N}_0,$$

pertanto  $[0]_{\mathcal{R}} = \mathbb{N}_0$ , e per la (2.3.5),  $[x]_{\mathcal{R}} = \mathbb{N}_0$  per ogni  $x \in \mathbb{N}_0$ . Invece se  $x \notin \mathbb{N}_0$  allora  $x$  è in relazione solo con se stesso, dunque  $[x]_{\mathcal{R}} = \{x\}$ . L'insieme quoziante è dunque:

$$\mathbb{Z} / \mathcal{R} = \{\mathbb{N}_0, \{x\} : x \in \mathbb{Z} \setminus \mathbb{N}_0\}.$$

**Esercizio 2.3.2.** Considerati l'insieme  $W = \{-7, -4, -3, 0, 3, 6, 7\}$  e la relazione d'equivalenza  $\mathcal{R}$  in  $W$  definita da:

$$v \mathcal{R} w : \iff |v| - |w| \in \{0, 4\},$$

si determinino le classi d'equivalenza e l'insieme quoziante  $W/\mathcal{R}$ .

*Svolgimento.* Risulta  $v \mathcal{R} w \iff (|v| = |w| \text{ o } |v| - |w| = 4)$ . Si ha dunque:

$$\begin{aligned} [-7]_{\mathcal{R}} &= \{-7, 7, -3, 3\} = [7]_{\mathcal{R}} = [-3]_{\mathcal{R}} = [3]_{\mathcal{R}}, \\ [-4]_{\mathcal{R}} &= \{-4, 0\} = [0]_{\mathcal{R}}, \\ [6]_{\mathcal{R}} &= \{6\}, \\ W/\mathcal{R} &= \{\{6\}, \{-4, 0\}, \{7, -7, 3, -3\}\}. \end{aligned}$$

**Esercizio 2.3.3.** Si consideri l'insieme  $A$  costituito dai numeri naturali della forma  $2^n 3^m$ , con  $n, m \in \mathbb{N}_0$ :

$$A = \{2^n 3^m : n, m \in \mathbb{N}_0\}.$$

Si verifichi che la relazione  $\mathcal{R}$  definita in  $A$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff n + m = s + t$$

è d'equivalenza. Si determinino poi:  $[1]_{\mathcal{R}}$ ,  $[2]_{\mathcal{R}}$ ,  $[3]_{\mathcal{R}}$ ,  $[4]_{\mathcal{R}}$ ,  $[12]_{\mathcal{R}}$ . Si verifichi che la relazione  $\mathcal{R}^*$  definita ponendo:

$$2^n 3^m \mathcal{R}^* 2^s 3^t : \iff n + s = m + t$$

non è d'equivalenza.

*Svolgimento.* Si ha ovviamente  $2^n 3^m \mathcal{R} 2^n 3^m$ , per ogni  $2^n 3^m \in A$ , sicché  $\mathcal{R}$  è riflessiva; se  $2^n 3^m \mathcal{R} 2^s 3^t$ , risulta  $n + m = s + t$ , da cui  $s + t = n + m$  e  $2^s 3^t \mathcal{R} 2^n 3^m$ , pertanto  $\mathcal{R}$  è simmetrica; infine se  $2^n 3^m \mathcal{R} 2^s 3^t$  e  $2^s 3^t \mathcal{R} 2^u 3^v$  si ha  $n + m = s + t$  e  $s + t = u + v$ , da cui  $n + m = u + v$  e dunque  $2^n 3^m \mathcal{R} 2^u 3^v$ , sicché  $\mathcal{R}$  è transitiva. Quindi  $\mathcal{R}$  è una relazione d'equivalenza in  $A$ .

Risulta poi:

$$\begin{aligned} [1]_{\mathcal{R}} &= [2^0 3^0]_{\mathcal{R}} = \{2^n 3^m : n + m = 0\} = \{1\}, \\ [2]_{\mathcal{R}} &= [2^1 3^0]_{\mathcal{R}} = \{2^n 3^m : n + m = 1\} = \{2, 3\} = [3]_{\mathcal{R}}, \\ [4]_{\mathcal{R}} &= [2^2 3^0]_{\mathcal{R}} = \{2^n 3^m : n + m = 2\} = \{4, 6, 9\}, \\ [12]_{\mathcal{R}} &= [2^2 3^1]_{\mathcal{R}} = \{2^n 3^m : n + m = 3\} = \{8, 12, 18, 27\}. \end{aligned}$$

La relazione  $\mathcal{R}^*$  non è riflessiva, poiché per esempio  $2 \mathcal{R}^* 2$  in quanto  $2 = 2^{13^0}$  e  $1 + 1 \neq 0 + 0$ , pertanto non è una relazione d'equivalenza. Si noti che  $\mathcal{R}^*$  è simmetrica, e non è transitiva essendo  $2 \mathcal{R}^* 3, 3 \mathcal{R}^* 2$  e  $2 \mathcal{R}^* 2$ .

**Esercizio 2.3.4.** Si consideri l'insieme  $A = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ . Si verifichi che la relazione  $\mathcal{R}$  definita in  $A$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff n = s \text{ e } m + t \in 2\mathbb{N}_0$$

è d'equivalenza. Si descriva poi la generica classe d'equivalenza  $[2^n 3^m]_{\mathcal{R}}$  e in particolare  $[1]_{\mathcal{R}}$  e  $[2]_{\mathcal{R}}$ . Si provi che ha senso definire l'applicazione:

$$\varphi : [2^n 3^m]_{\mathcal{R}} \in S / \mathcal{R} \longmapsto (-1)^m n \in \mathbb{Z},$$

e si studi tale applicazione.

*Svolgimento.* Si ha  $2^n 3^m \mathcal{R} 2^n 3^m$ , per ogni  $2^n 3^m \in A$ , essendo  $n = n$  e  $m + m = 2m \in 2\mathbb{N}_0$ , sicché  $\mathcal{R}$  è riflessiva; se  $2^n 3^m \mathcal{R} 2^s 3^t$ , risulta  $n = s$  e  $m + t \in 2\mathbb{N}_0$ , ne segue  $s = n$  e  $t + m \in 2\mathbb{N}_0$ , cioè  $2^s 3^t \mathcal{R} 2^n 3^m$ , pertanto  $\mathcal{R}$  è simmetrica; infine se  $2^n 3^m \mathcal{R} 2^s 3^t$  e  $2^s 3^t \mathcal{R} 2^u 3^v$  si ha  $n = s$ ,  $s = u$  e  $m + t \in 2\mathbb{N}_0$ ,  $t + v \in 2\mathbb{N}_0$ , ne segue  $n = u$  e  $m + 2t + v \in 2\mathbb{N}_0$ , dunque  $m + v \in 2\mathbb{N}_0$  e quindi  $2^n 3^m \mathcal{R} 2^u 3^v$ , sicché  $\mathcal{R}$  è transitiva. Quindi  $\mathcal{R}$  è una relazione d'equivalenza in  $A$ .

Per ogni elemento  $2^n 3^m \in A$  si ha:

$$[2^n 3^m]_{\mathcal{R}} = \{2^s 3^t : n = s \text{ e } m + t \in 2\mathbb{N}_0\} = \{2^n 3^t : t \text{ ha la stessa parità di } m\}.$$

In particolare:

$$\begin{aligned}[1]_{\mathcal{R}} &= [2^0 3^0]_{\mathcal{R}} = \{2^0 3^{2j} : j \in \mathbb{N}_0\} = \{3^{2j} : j \in \mathbb{N}_0\}, \\ [2]_{\mathcal{R}} &= [2^1 3^0]_{\mathcal{R}} = \{2^1 3^{2j} : j \in \mathbb{N}_0\} = \{2 \cdot 3^{2j} : j \in \mathbb{N}_0\}.\end{aligned}$$

La  $\varphi$  è un'applicazione, infatti da  $[2^n 3^m]_{\mathcal{R}} = [2^s 3^t]_{\mathcal{R}}$  segue  $n = s$  e  $m + t \in 2\mathbb{N}_0$ , quindi  $(-1)^m n = (-1)^t s$ . Inoltre  $\varphi$  è suriettiva, infatti per ogni  $z \in \mathbb{Z}$  si ha  $z = \varphi([2^z 3^0]_{\mathcal{R}})$  se  $z \geq 0$  e  $z = \varphi([2^{(-z)} 3^1]_{\mathcal{R}})$  se  $z < 0$ . Infine  $\varphi$  non è iniettiva, infatti  $\varphi([2^0 3^0]_{\mathcal{R}}) = \varphi([2^0 3^1]_{\mathcal{R}})$ , con  $[2^0 3^0]_{\mathcal{R}} \neq [2^0 3^1]_{\mathcal{R}}$  poiché  $2^0 3^0 \not\mathcal{R} 2^0 3^1$ .

**Esercizio 2.3.5.** Con  $A = \{i, m, n, v, w\}$  e  $B = \{1, 7, 13, 21\}$  si precisi per ciascuno dei seguenti insiemi di insiemi se esso è una partizione di  $A$ :

$$\begin{aligned}\mathcal{F}_1 &= \{\{i, m, v, w\}, \{n\}\}, \\ \mathcal{F}_2 &= \{\{i\}, \{m\}, \{v\}, \{w\}\}, \\ \mathcal{F}_3 &= \{\{i, m, n, v, w\}\},\end{aligned}$$

e per ciascuno dei seguenti se è una partizione di  $B$ :

$$\begin{aligned}\mathcal{F}_4 &= \{\{1, 7\}, \emptyset, \{13, 21\}\}, \\ \mathcal{F}_5 &= \{\{1, 13, 21\}, \{7\}\}, \\ \mathcal{F}_6 &= \{\{1, 7, 13\}, \{7, 21\}\}.\end{aligned}$$

**Esercizio 2.3.6.** Con  $V = \{4, 6, 8, 10\}$  e  $W = \{a, b, c, d, e, i\}$  si precisi per ciascuno dei seguenti insiemi di insiemi se esso è una partizione di  $V$ :

$$\begin{aligned}\mathcal{F}_1 &= \{\{4\}, \{6\}, \{8\}, \{10\}\}, \\ \mathcal{F}_2 &= \{\{4, 8\}, \emptyset, \{10, 6\}\}, \\ \mathcal{F}_3 &= \{\{4, 6, 10, 8\}\},\end{aligned}$$

e per ciascuno dei seguenti se è una partizione di  $W$ :

$$\begin{aligned}\mathcal{F}_4 &= \{\{i, a, d, c\}, \{b, e\}\}, \\ \mathcal{F}_5 &= \{\{a, c, i\}, \{b, d, e, i\}\}, \\ \mathcal{F}_6 &= \{\{b\}, \{c, i\}, \{a, e\}\}.\end{aligned}$$

**Esercizio 2.3.7.** Considerata la partizione  $\mathcal{F} = \{\{2k, 2k+1\} : k \in \mathbb{N}_0\}$  dell'insieme  $\mathbb{N}_0$ , e detta  $\mathcal{R}_{\mathcal{F}}$  la relazione d'equivalenza da essa determinata, si precisi se le seguenti affermazioni sono esatte:  $15 \mathcal{R}_{\mathcal{F}} 15$ ,  $23 \mathcal{R}_{\mathcal{F}} 24$ ,  $24 \mathcal{R}_{\mathcal{F}} 25$ ,  $0 \mathcal{R}_{\mathcal{F}} 1$ ,  $6 \mathcal{R}_{\mathcal{F}} 8$ ,  $6 \mathcal{R}_{\mathcal{F}} 9$ ,  $24 \mathcal{R}_{\mathcal{F}} 24$ ,  $25 \mathcal{R}_{\mathcal{F}} 24$ .

**Esercizio 2.3.8.** Considerata la partizione  $\mathcal{F} = \{\{a, c, e\}, \{b, d\}, \{f\}\}$  dell'insieme  $S = \{a, b, c, d, e, f\}$ , e dette  $\mathcal{R}_{\mathcal{F}}$  la relazione d'equivalenza da essa determinata, si precisi se le seguenti affermazioni sono esatte:  $a \mathcal{R}_{\mathcal{F}} a$ ,  $b \mathcal{R}_{\mathcal{F}} f$ ,  $f \mathcal{R}_{\mathcal{F}} b$ ,  $c \mathcal{R}_{\mathcal{F}} e$ ,  $e \mathcal{R}_{\mathcal{F}} c$ ,  $f \mathcal{R}_{\mathcal{F}} f$ ,  $a \mathcal{R}_{\mathcal{F}} b$ ,  $e \mathcal{R}_{\mathcal{F}} f$ . Si descriva poi l'insieme quoziante  $S / \mathcal{R}_{\mathcal{F}}$ .

**Esercizio 2.3.9.** Si dimostri 2.3.8.

**Esercizio 2.3.10.** Si consideri l'insieme  $A = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ . Si verifichi che la relazione  $\mathcal{R}$  definita in  $A$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff n + t = m + s$$

è d'equivalenza. Si descriva poi la generica classe d'equivalenza  $[2^n 3^m]_{\mathcal{R}}$ , e in particolare  $[1]_{\mathcal{R}}$  e  $[2]_{\mathcal{R}}$ . Si provi che ha senso definire l'applicazione:

$$\varphi : [2^n 3^m]_{\mathcal{R}} \in S / \mathcal{R} \longmapsto n - m \in \mathbb{Z},$$

e si studi tale applicazione.

**Esercizio 2.3.11.** Si consideri l'insieme  $A = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ . Si verifichi che la relazione  $\mathcal{R}$  definita in  $A$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff n + s \in 2\mathbb{N}_0 \text{ e } m + t \in 2\mathbb{N}_0$$

è d'equivalenza. Si descriva poi la generica classe d'equivalenza  $[2^n 3^m]_{\mathcal{R}}$ , e in particolare  $[1]_{\mathcal{R}}$  e  $[2]_{\mathcal{R}}$ .

**Esercizio 2.3.12.** Si consideri in  $\mathbb{Z}$  la relazione binaria definita da:

$$a \mathcal{R} b : \iff (a = b) \text{ o } (a, b \in 2\mathbb{N}_0).$$

- (i) Si provi che  $\mathcal{R}$  è una relazione d'equivalenza in  $\mathbb{Z}$ .
- (ii) Si precisi se le seguenti affermazioni sono esatte:  $4 \mathcal{R} -6, 22 \mathcal{R} 8, 23 \mathcal{R} 46, 5 \mathcal{R} 5, 60 \mathcal{R} -20, 6 \mathcal{R} 0$ .
- (iii) Si determini l'insieme quoziante  $\mathbb{Z}/\mathcal{R}$ .

**Esercizio 2.3.13.** Si ponga  $C = \{0, 1, 2, 3, 4, 5\}$  e si consideri in  $\mathbb{N}_0$  la relazione binaria definita da:

$$a \mathcal{R} b : \iff (a = b) \text{ o } (a, b \in C).$$

- (i) Si provi che  $\mathcal{R}$  è una relazione d'equivalenza in  $\mathbb{N}_0$ .
- (ii) Si precisi se le seguenti affermazioni sono esatte:  $42 \mathcal{R} 6, 7 \mathcal{R} 7, 22 \mathcal{R} 2, 23 \mathcal{R} 46, 5 \mathcal{R} 5, 4 \mathcal{R} 10, 6 \mathcal{R} 0, 3 \mathcal{R} 4, [15]_{\mathcal{R}} = [4]_{\mathcal{R}}, [1]_{\mathcal{R}} = [2]_{\mathcal{R}}, [0]_{\mathcal{R}} = [3]_{\mathcal{R}}, [352]_{\mathcal{R}} = [7]_{\mathcal{R}}, [23]_{\mathcal{R}} = [46]_{\mathcal{R}}$ .
- (iii) Si determini l'insieme quoziante  $\mathbb{N}_0/\mathcal{R}$ .

**Esercizio 2.3.14.** Si consideri l'insieme  $V$  costituito dai numeri interi della forma  $4h + 1$ , con  $h \in \mathbb{Z}$ :

$$V = \{4h + 1 : h \in \mathbb{Z}\}.$$

Si verifichi che la relazione  $\mathcal{R}$  definita in  $V$  ponendo:

$$(4h + 1) \mathcal{R} (4k + 1) : \iff |h| = |k|$$

è d'equivalenza. Si determinino poi:  $[1]_{\mathcal{R}}, [5]_{\mathcal{R}}, [-3]_{\mathcal{R}}$ .

**Esercizio 2.3.15.** Sia  $\mathbb{P}$  l'insieme dei numeri primi in  $\mathbb{N}_0$  e si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $p_1 p_2$ , con  $p_1, p_2 \in \mathbb{P}, p_1 \leq p_2$ :

$$W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}.$$

Si dimostri che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$p_1 p_2 \mathcal{R} q_1 q_2 : \iff ((p_1 = q_1) \text{ o } (p_1 = q_2) \text{ o } (p_2 = q_1) \text{ o } (p_2 = q_2))$$

non è d'equivalenza. Osservato poi che la relazione indotta  $\mathcal{R}'$  in

$$A = \{4, 15, 21, 22, 26, 34, 35\}$$

è d'equivalenza, se ne determinino le classi d'equivalenza e l'insieme quoziante.

**Esercizio 2.3.16.** Sia  $\mathbb{P}$  l'insieme dei numeri primi in  $\mathbb{N}_0$  e si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $p_1 p_2$ , con  $p_1, p_2 \in \mathbb{P}$ ,  $p_1 \leq p_2$ :

$$W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}.$$

(i) Si dimostri che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$p_1 p_2 \mathcal{R} q_1 q_2 : \iff ((p_1 = q_1) \text{ o } (p_1 q_1 = 21))$$

è d'equivalenza.

- (ii) Si precisi se le seguenti affermazioni sono esatte:  $14 \mathcal{R} 10$ ,  $33 \mathcal{R} 39$ ,  $21 \mathcal{R} 6$ ,  $9 \mathcal{R} 77$ ,  $15 \mathcal{R} 35$ ,  $6 \mathcal{R} 21$ ,  $4 \mathcal{R} 4$ ,  $10 \mathcal{R} 14$ ,  $[51]_{\mathcal{R}} = [49]_{\mathcal{R}}$ ,  $[49]_{\mathcal{R}} = [4]_{\mathcal{R}}$ ,  $[15]_{\mathcal{R}} = [35]_{\mathcal{R}}$ ,  $[39]_{\mathcal{R}} = [91]_{\mathcal{R}}$ ,  $[15]_{\mathcal{R}} = [14]_{\mathcal{R}}$ .
- (iii) Si descrivano:  $[4]_{\mathcal{R}}$ ,  $[6]_{\mathcal{R}}$ ,  $[9]_{\mathcal{R}}$ ,  $[25]_{\mathcal{R}}$ ,  $[49]_{\mathcal{R}}$ .

**Esercizio 2.3.17.** Si consideri la relazione d'equivalenza  $\mathcal{R}$  in  $\mathbb{N}$  definita ponendo:

$$x \sim y : \iff x \text{ e } y \text{ hanno lo stesso numero di cifre distinte.}$$

- (i) Si precisi se le seguenti affermazioni sono esatte:  $115 \mathcal{R} 1000$ ,  $100 \mathcal{R} 1001$ ,  $400 \mathcal{R} 4$ ,  $123 \mathcal{R} 134$ .
- (ii) Si calcoli:  $[3]_{\mathcal{R}}$ ,  $[21]_{\mathcal{R}}$ ,  $[100]_{\mathcal{R}}$ .
- (iii) Quanti e quali sono gli elementi dell'insieme quoziante  $\mathbb{N}/\mathcal{R}$ ?
- (iv) Si spieghi per quale motivo l'applicazione

$$f : [a]_{\mathcal{R}} \in \mathbb{N}/\mathcal{R} \longmapsto [a+1]_{\mathcal{R}} \in \mathbb{N}/\mathcal{R}$$

non è ben posta.

## 2.4 Relazioni d'ordine

Si approfondiranno ora le relazioni d'ordine già definite nel Paragrafo 2.1. Esempi notevoli di tali relazioni definite nell'insieme dei numeri naturali e nell'insieme degli interi sono stati già richiamati nel Capitolo 1 anche in assenza della terminologia precisa. In realtà il concetto di relazione d'ordine prende proprio spunto dal cosiddetto "ordine usuale" illustrato negli esempi prima citati, e così altre definizioni che saranno ora introdotte.

Una relazione binaria  $\mathcal{R}$  in un insieme  $S$  è detta d'ordine (o d'ordine parziale) se è riflessiva, asimmetrica e transitiva, cioè se si ha:

$$\begin{aligned} &x \mathcal{R} x, \forall x \in S; \\ &x \mathcal{R} y, y \mathcal{R} x \implies x = y, \forall x, y \in S; \\ &x \mathcal{R} y, y \mathcal{R} z \implies x \mathcal{R} z, \forall x, y, z \in S. \end{aligned}$$

**2.4.1. Esempio.** L'ordine usuale in  $\mathbb{N}_0$  e l'ordine usuale in  $\mathbb{Z}$  sono relazioni d'ordine (vedi (1.2.23), (1.2.24), (1.2.25) e 1.2.8). E così il “divide” in  $\mathbb{N}_0$  (vedi (1.2.39), (1.2.40) e (1.2.41)). Non lo è invece il “divide” in  $\mathbb{Z}$  (vedi 1.2.11).

Con  $T$  insieme, la relazione  $\mathcal{R}$  definita in  $\mathcal{P}(T)$  ponendo:

$$X \mathcal{R} Y \iff X \subseteq Y$$

è d'ordine (vedi (1.1.2), (1.1.4) e (1.1.5)).

In analogia a quanto succede in  $\mathbb{N}_0$  e in  $\mathbb{Z}$ , si preferisce spesso denotare con “ $\leq$ ” una qualunque relazione d'ordine  $\mathcal{R}$  in  $S$ ; si pone cioè:

$$x \leq y : \iff x \mathcal{R} y$$

e si dice “ $x$  minore o uguale di  $y$ ” piuttosto che “ $x$  in relazione con  $y$ ”. Le proprietà riflessiva, asimmetrica e transitiva quindi si scrivono:

$$\begin{aligned} x \leq x, \quad & \forall x \in S; \\ x \leq y, y \leq x \implies & x = y, \quad \forall x, y \in S; \\ x \leq y, y \leq z \implies & x \leq z, \quad \forall x, y, z \in S. \end{aligned}$$

La scrittura  $y \geq x$  indica che  $x \leq y$ , cioè  $x \mathcal{R} y$ , e si legge “ $y$  maggiore o uguale di  $x$ ”.

La coppia  $(S, \leq)$  con  $S$  insieme e  $\leq$  relazione d'ordine in  $S$  è detto un **insieme ordinato** o **parzialmente ordinato**; a volte, quando è chiaro il contesto, viene denotato più brevemente col solo simbolo  $S$ . Esempi di insiemi ordinati sono allora:  $(\mathbb{N}_0, \text{usuale})$ ,  $(\mathbb{N}_0, \text{divide})$ ,  $(\mathbb{Z}, \text{usuale})$  e, con  $T$  insieme arbitrario,  $(\mathcal{P}(T), \subseteq)$ .

Sia  $(S, \leq)$  un insieme ordinato. Elementi  $x$  e  $y$  in  $S$  vengono detti **confrontabili** se si ha  $x \leq y$  o  $y \leq x$ . Ovviamente ogni elemento è confrontabile con se stesso, e si ha contemporaneamente  $x \leq y$  e  $y \leq x$  se solo se  $x = y$ .

Un insieme ordinato  $(S, \leq)$  tale che  $x$  e  $y$  sono confrontabili, per ogni  $x, y \in S$  è detto **totalmente ordinato** (o **catena**). Per esempio  $(\mathbb{N}_0, \text{usuale})$  e  $(\mathbb{Z}, \text{usuale})$  sono totalmente ordinati. Non lo è  $(\mathbb{N}_0, \text{divide})$  in quanto, per esempio, 2 non divide 3 e 3 non divide 2. L'insieme  $(\mathcal{P}(T), \subseteq)$  è totalmente ordinato se e solo se  $|T| \leq 1$  poiché, per esempio, se  $x$  e  $y$  sono elementi distinti di  $T$ , i singleton  $\{x\}$  e  $\{y\}$  non sono confrontabili.

Se  $(S, \leq)$  è un insieme ordinato, con  $x, y \in S$  si pone:

$$x < y : \iff x \leq y \text{ e } x \neq y,$$

e si legge “ $x$  minore strettamente di  $y$ ”. Si noti che anche questa notazione estende quella ben nota tra numeri interi, e che in  $(\mathcal{P}(T), \subseteq)$  il minore stretto coincide con l'inclusione stretta. Si dice anche che “ $y$  è maggiore strettamente di  $x$ ” e si scrive  $y > x$ , per indicare che  $x < y$ . Per esempio  $x \not< x$ , per ogni  $x \in S$ ,  $2 < 6$  in  $(\mathbb{N}_0, \text{divide})$ , e  $\emptyset < T$  in  $(\mathcal{P}(T), \subseteq)$ , per ogni insieme  $T \neq \emptyset$ .

**2.4.2.** Sia  $(S, \leq)$  un insieme ordinato. Si ha:

$$\begin{aligned} x < y, y \leq z &\implies x < z, \\ x \leq y, y < z &\implies x < z, \\ x < y, y < z &\implies x < z, \\ x < y &\implies y \not\leq x. \end{aligned}$$

*Dimostrazione.* Esercizio. □

Se  $S$  è un insieme ordinato e  $X \subseteq S$ , si può considerare la relazione indotta da  $\leq$  in  $X$ : tale relazione è ancora d'ordine (vedi 2.1.3) e di solito viene indicata ancora con il simbolo  $\leq$ . Ha quindi senso considerare l'insieme ordinato  $(X, \leq)$ .

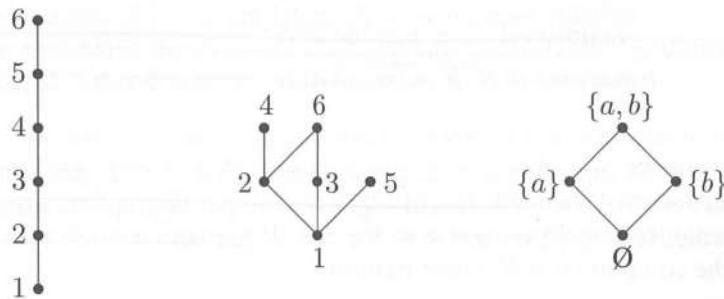
Se  $(S, \leq)$  e  $(S^*, \leq^*)$  sono insiemi ordinati, un'applicazione  $f : S \rightarrow S^*$  è detta **crescente** o un **omomorfismo di insiemi ordinati** se da  $x \leq y$  con  $x, y \in S$  segue  $f(x) \leq^* f(y)$ :

$$f \text{ crescente} : \iff (x, y \in S, x \leq y \implies f(x) \leq^* f(y)).$$

**2.4.3. Esempio.** L'applicazione identica  $\text{id}_{\mathbb{N}_0} : x \in \mathbb{N}_0 \mapsto x \in \mathbb{N}_0$  è un omomorfismo di  $(\mathbb{N}_0, \text{divide})$  in  $(\mathbb{N}_0, \text{usuale})$ , non lo è di  $(\mathbb{N}_0, \text{usuale})$  in  $(\mathbb{N}_0, \text{divide})$ . Infatti, con  $x, y \in \mathbb{N}_0$ , da  $x$  divide  $y$  segue  $x \leq y$ , cioè  $\text{id}_{\mathbb{N}_0}(x) \leq \text{id}_{\mathbb{N}_0}(y)$ , dove  $\leq$  indica l'ordine usuale. Ma, per esempio,  $2 \leq 3$  nell'ordine usuale mentre  $\text{id}_{\mathbb{N}_0}(2) = 2$  non divide  $\text{id}_{\mathbb{N}_0}(3) = 3$ .

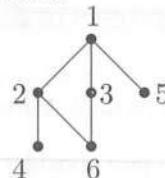
Un insieme ordinato finito non vuoto  $(S, \leq)$  può essere rappresentato efficacemente con un diagramma, detto **diagramma di Hasse**, in cui gli elementi sono indicati da punti e questi, se confrontabili, sono legati da segmenti secondo il seguente criterio. Sia, per esempio  $x < y$ , si disegna allora  $x$  più in basso rispetto a  $y$ ; si collegano poi i due punti con un tratto continuo se non esiste alcun elemento  $z \in S$  tale che  $x < z < y$  e si dice che  $y$  **copre**  $x$  o  $x$  è **coperto** da  $y$ ; così continuando si ragiona in maniera analoga con  $x$  e  $z$  e con  $z$  e  $y$ . La finitezza di  $S$  dà senso a questa costruzione.

**2.4.4. Esempio.** Siano  $A = \{1, 2, 3, 4, 5, 6\}$  e  $B = \{a, b\}$ . Gli insiemi ordinati  $(A, \text{usuale})$ ,  $(A, \text{divide})$  e  $(\mathcal{P}(B), \subseteq)$  si rappresentano nel seguente modo:



Come sarà ancora più chiaro nel seguito, i diagrammi di Hasse permettono di visualizzare efficacemente proprietà dell'insieme ordinato finito.

Si noti che la relazione opposta  $\mathcal{R}^{\text{op}}$  di una relazione d'ordine  $\mathcal{R}$  è anch'essa d'ordine, ha senso cioè considerare  $\leq^{\text{op}}$  di una relazione d'ordine  $\leq$ . Se  $(S, \leq)$  è un insieme finito, il diagramma di Hasse di  $(S, \leq^{\text{op}})$  si ottiene "capovolgendo" quello di  $(S, \leq)$ . Così, per esempio, il diagramma di Hasse di  $(A, \text{divide}^{\text{op}})$ , con  $A = \{1, 2, 3, 4, 5, 6\}$ , è il seguente:



Nel seguito del paragrafo si supporrà sempre  $S$  insieme *non vuoto*.

Sia  $(S, \leq)$  un insieme ordinato. Un elemento  $a \in S$  è detto **minimo** di  $S$  se è confrontabile con ogni elemento di  $S$  e risulta  $a \leq x$ , per ogni  $x \in S$ :

$$a \text{ minimo di } S : \iff a \leq x, \quad \forall x \in S.$$

Analogamente,  $b \in S$  è detto **massimo** di  $S$  se è confrontabile con ogni elemento di  $S$  e risulta  $x \leq b$ , per ogni  $x \in S$ :

$$b \text{ massimo di } S : \iff x \leq b, \quad \forall x \in S.$$

In  $(\mathbb{N}_0, \text{usuale})$  0 è minimo (vedi (1.2.26)) e non esiste massimo (vedi (1.2.27)); in  $(\mathbb{N}_0, \text{divide})$  1 è minimo e 0 è massimo; in  $(\mathbb{Z}, \text{usuale})$  non esiste né minimo né massimo (vedi (1.2.46)); in  $(\mathcal{P}(T), \subseteq)$  l'insieme vuoto è minimo,  $T$  è massimo.

Gli esempi precedenti mostrano che un insieme ordinato può essere privo di minimo (di massimo). Ma si prova facilmente che l'esistenza di un tale elemento comporta sempre la sua unicità sicché ha senso parlare *del* minimo di  $S$  e denotarlo con  $\min S$ , se esiste, e analogamente *del* massimo di  $S$ , denotato con  $\max S$ , se esiste:

$$a = \min S : \iff a \leq x, \quad \forall x \in S,$$

$$b = \max S : \iff x \leq b, \quad \forall x \in S.$$

Si ha infatti:

**2.4.5.** Sia  $(S, \leq)$  un insieme ordinato, e siano  $a, a', b, b' \in S$ . Si ha:

$$a \text{ minimo di } S, a' \text{ minimo di } S \implies a = a',$$

$$b \text{ massimo di } S, b' \text{ massimo di } S \implies b = b'.$$

*Dimostrazione.* Si supponga  $a \leq x$ , per ogni  $x \in S$ , e  $a' \leq x$ , per ogni  $x \in S$ . Allora si ha:  $a \leq a'$  e  $a' \leq a$ , da cui segue  $a = a'$  per la proprietà asimmetrica. Analogamente, se  $x \leq b$  per ogni  $x \in S$  e  $x \leq b'$  per ogni  $x \in S$ , si ha  $b \leq b'$  e  $b' \leq b$ , il che comporta  $b = b'$ , come richiesto.  $\square$

Ovviamente:

$$\begin{aligned} a = \min(S, \leq) &\iff a = \max(S, \leq^{\text{op}}), \\ b = \max(S, \leq) &\iff b = \min(S, \leq^{\text{op}}). \end{aligned}$$

Un elemento  $c$  di un insieme ordinato  $(S, \leq)$  è detto **minimale** se non esistono in  $S$  elementi strettamente minori di  $c$ :

$$c \text{ minimale in } S : \iff \nexists x \in S : x < c.$$

Ovviamente si ha:

$$c \text{ minimale in } S \iff (s \in S, s \leq c \implies s = c). \quad (2.4.1)$$

Infatti, se  $c$  è minimale e si ha  $s \leq c$  con  $s \in S$ , non può avversi  $s < c$  e dunque  $s = c$ . Viceversa, supposto  $c$  tale che da  $x \leq c$ , con  $x \in S$ , segue che  $x = c$ , si ha  $c$  minimale in  $S$  altrimenti esisterebbe  $s \in S$  con  $s < c$  e dunque esisterebbe  $s \in S$  tale che  $s \leq c$  e  $s \neq c$ , contro le ipotesi.

“Dualmente”, un elemento  $d$  di un insieme ordinato  $(S, \leq)$  è detto **massimale** in  $S$  se non esistono in  $S$  elementi strettamente maggiori di  $d$ :

$$d \text{ massimale in } S : \iff (\nexists x \in S : d < x).$$

Ragionando in analogia a quanto fatto in precedenza si ottiene:

$$d \text{ massimale in } S \iff (s \in S, d \leq s \implies d = s). \quad (2.4.2)$$

**2.4.6.** *Sia  $(S, \leq)$  un insieme ordinato e siano  $a, b, c, d \in S$ . Si ha:*

$$\begin{aligned} a = \min S &\implies a \text{ minimale in } S, \\ a = \min S, c \text{ minimale in } S &\implies a = c, \\ b = \max S &\implies b \text{ massimale in } S, \\ b = \max S, d \text{ massimale in } S &\implies b = d. \end{aligned}$$

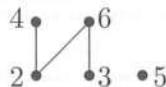
*Dimostrazione.* Si supponga  $a = \min S$  e sia  $s \leq a$ . L’essere  $a$  minimo assicura che  $a \leq s$ , e quindi dalla proprietà asimmetrica segue subito  $a = s$ .

Sia ancora  $a = \min S$  e si supponga  $c$  minimale in  $S$ . Da  $a$  minimo segue  $a \leq c$ , la minimalità di  $c$  assicura allora che  $a = c$ , come volevasi.

Le due successive implicazioni si ottengono “dualizzando” le dimostrazioni precedenti, cioè “sostituendo” il  $\geq$  al  $\leq$ .  $\square$

Pertanto, se un insieme ordinato ha minimo, questo è l’unico elemento minimale e, se ha massimo, questo è l’unico elemento massimale. Un insieme ordinato può però avere uno o più elementi minimi (rispettivamente massimi) senza ammettere minimo (risp. massimo). Può anche non avere elementi minimi (risp. massimi).

**2.4.7. Esempio.** L'insieme  $C = \{2, 3, 4, 5, 6\}$  ordinato con il “divide” ha 2, 3 e 5 come elementi minimali (e quindi non ha minimo), 4, 5 e 6 come elementi massimali (e quindi non ha massimo). Rappresentato  $(C, \text{divide})$  con un diagramma di Hasse, tali proprietà sono evidenti:



L'insieme  $D = \{2^n : n \in \mathbb{N}\} \cup \{3\}$  ordinato ponendo  $x \leq y : \iff y|x$  (cioè con la relazione indotta dalla opposta del “divide” in  $\mathbb{N}_0$ ) è tale che 3 è l'unico elemento minimale, ma  $D$  è privo di minimo. Infatti, con  $s \in D$ ,  $s \leq 3$  implica  $3|s$  e dunque  $s = 3$ . Pertanto 3 è minimale, ma non minimo in quanto, per esempio,  $3 \not\leq 2$  poiché 2 non divide 3. Ogni altro elemento  $2^n$  di  $D$  non è minimale poiché esiste  $2^{n+1} \in D$  tale che  $2^{n+1} \neq 2^n$  e  $2^n|2^{n+1}$ , cioè tale che  $2^{n+1} < 2^n$ .

L'insieme ordinato  $(D, \text{divide})$  ha come unico elemento massimale 3 ed è privo di massimo.

L'insieme  $(\mathbb{Z}, \text{usuale})$  è privo sia di elementi minimali che di elementi massimali.

È opportuno però osservare che:

**2.4.8.** Se  $(S, \leq)$  è un insieme totalmente ordinato e  $c \in S$  è minimale in  $S$ , allora  $c = \min S$ . Analogamente, se  $d \in S$  è massimale in  $S$ , è  $d = \max S$ .

*Dimostrazione.* Si supponga  $c$  minimale in  $S$  e sia  $x \in S$ . Allora  $x \not\leq c$  per la minimalità di  $c$  e  $x$  è confrontabile con  $c$  per le ipotesi su  $S$ . Pertanto  $c \leq x$ , come volevasi. L'altra proprietà è analoga.  $\square$

Anche gli insiemi ordinati finiti hanno proprietà particolari.

**2.4.9.** Sia  $(S, \leq)$  un insieme ordinato finito e non vuoto. Allora  $S$  ha elementi minimali e elementi massimali.

*Dimostrazione.* Sia  $x_1$  un elemento di  $S$ . Se  $x_1$  non è minimale, esiste  $x_2 \in S$  tale che  $x_2 < x_1$ ; se  $x_2$  non è minimale, esiste  $x_3 \in S$  tale che  $x_3 < x_2 < x_1$ . La finitezza di  $S$  garantisce che esiste  $x_t \in S$  ( $t \geq 1$ ) tale che  $x_t$  è minimale in  $S$ . Una dimostrazione analoga vale per i massimali.  $\square$

Le due proposizioni precedenti assicurano che:

**2.4.10.** Sia  $(S, \leq)$  un insieme totalmente ordinato finito e non vuoto. Allora  $S$  ha minimo e massimo.

*Dimostrazione.* Per la 2.4.9  $(S, \leq)$  ha elementi minimali e massimali sicché si può applicare la 2.4.8.  $\square$

Quindi un insieme totalmente ordinato finito non vuoto ha diagramma di Hasse del tipo



il che giustifica il termine “catena” utilizzato per gli insiemi totalmente ordinati.

Se  $(S, \leq)$  è un insieme ordinato e  $X \subseteq S$ , ha senso parlare di minimo di  $X$ , massimo di  $X$ , elementi minimali di  $X$ , elementi massimali di  $X$ . Precisamente:

$$\begin{aligned} v := \min X &\iff v \in X \text{ e } v \leq x, \forall x \in X, \\ v := \max X &\iff v \in X \text{ e } x \leq v, \forall x \in X, \\ v \text{ minimale in } X &:\iff v \in X \text{ e } \nexists x \in X : x < v, \\ v \text{ minimale in } X &\iff v \in X \text{ e } (y \leq v, y \in X \implies y = v), \\ v \text{ massimale in } X &:\iff v \in X \text{ e } \nexists x \in X : v < x, \\ v \text{ massimale in } X &\iff v \in X \text{ e } (v \leq y, y \in X \implies v = y). \end{aligned}$$

Di notevole importanza è la seguente definizione. Un insieme ordinato  $(S, \leq)$  è detto **ben ordinato** (e si dice anche che  $\leq$  è un **buon ordine**), se ogni parte non vuota di  $S$ , con l’ordinamento indotto, ammette minimo:

$$S \text{ ben ordinato} :\iff (\forall X \subseteq S, X \neq \emptyset, \exists \min X).$$

Quindi un insieme ben ordinato è un insieme dotato di minimo, in cui ogni parte non vuota ha minimo.

**2.4.11. Esempio.** L’insieme ordinato  $(\mathbb{N}_0, \text{usuale})$  è ben ordinato. L’insieme ordinato  $(\mathbb{N}_0, \text{divide})$  non è ben ordinato: infatti, pur ammettendo minimo, ha parti non vuote, per esempio  $\{2, 3\}$ , prive di minimo. L’insieme ordinato  $(\mathbb{Z}, \text{usuale})$  non ha minimo, dunque non è ben ordinato. L’insieme ordinato  $(\mathcal{P}(T), \subseteq)$ , con  $T$  insieme, è ben ordinato se e solo se  $|T| \leq 1$ : infatti, se  $a, b$  sono elementi distinti di  $T$ , l’insieme  $\{\{a\}, \{b\}\}$  non ha minimo.

Come si intuisce dagli esempi precedenti, si ha:

**2.4.12. Ogni insieme ben ordinato è totalmente ordinato.**

*Dimostrazione.* Sia  $(S, \leq)$  un insieme ben ordinato. Siano  $x$  e  $y$  elementi di  $S$  e si consideri l'insieme  $\{x, y\}$ . Ovviamente tale insieme è non vuoto, dunque dotato di minimo in quanto  $S$  è ben ordinato. Tale minimo è  $x$  oppure  $y$  sicché, nel primo caso, si ha  $x \leq y$  e, analogamente, nel secondo si ha  $y \leq x$ . In ogni caso  $x$  e  $y$  sono confrontabili.  $\square$

L'insieme  $(\mathbb{Z}, \text{usuale})$  mostra che esistono insiemi totalmente ordinati ma non ben ordinati.

Se  $(S, \leq)$  è un insieme ordinato e  $X$  è un sottoinsieme non vuoto di  $S$ , ha ovviamente senso cercare di “correlare” gli elementi di  $X$  con quelli di  $S$ . Ciò porta alla seguente definizione.

Sia  $(S, \leq)$  un insieme ordinato e sia  $X$  un sottoinsieme non vuoto di  $S$ . Un elemento  $w$  di  $S$  è detto un **minorante** di  $X$  in  $S$  se è confrontabile con ogni elemento di  $X$  e risulta minore o uguale di ogni  $x \in X$ :

$$w \text{ minorante di } X \text{ in } S : \iff (w \leq x, \forall x \in X).$$

È detto un **maggiorante** di  $X$  in  $S$  se è confrontabile con ogni elemento di  $X$  e risulta maggiore o uguale di ogni  $x \in X$ :

$$w \text{ maggiorante di } X \text{ in } S : \iff (x \leq w, \forall x \in X).$$

Ovviamente se  $S$  ha minimo (rispettivamente massimo) tale elemento risulta minorante (rispettivamente maggiorante) di un qualunque sottoinsieme non vuoto di  $S$ . Così, se  $X$ , ordinato con la relazione indotta, ha minimo (risp. massimo) questo è minorante (risp. maggiorante) di  $X$ . Più precisamente:

$$\begin{aligned} w \text{ minorante di } X, w \in X &\iff w = \min X, \\ w \text{ maggiorante di } X, w \in X &\iff w = \max X. \end{aligned}$$

**2.4.13. Esempio.** Il sottoinsieme  $2\mathbb{N}_0$  di  $(\mathbb{N}_0, \text{usuale})$  ha in  $\mathbb{N}_0$  un unico minorante, 0, che è il suo minimo; non ha maggioranti in  $\mathbb{N}_0$ . Il sottoinsieme  $2\mathbb{N}_0$  di  $(\mathbb{Z}, \text{usuale})$  ha infiniti minoranti in  $\mathbb{Z}$ , tutti gli elementi di  $\mathbb{Z} \setminus \mathbb{N}$ ; non ha maggioranti in  $\mathbb{Z}$ . In  $(\mathbb{N}_0, \text{divide})$  il sottoinsieme  $\{12, 18\}$  ha come minoranti 1, 2, 3, 6; ha infiniti maggioranti, tutti i multipli di 36 in  $\mathbb{N}_0$ . In  $(\mathcal{P}(A), \subseteq)$  con  $A = \{a, b, c\}$ , il sottoinsieme  $\{\{a\}, \{b\}\}$  ha come minoranti solo  $\emptyset$ , come maggioranti  $\{a, b\}$  e  $A$ .

Come evidenziano gli esempi precedenti, poi anche gli esercizi, un sottoinsieme non vuoto di un insieme ordinato può non avere minoranti (rispettivamente maggioranti), può averne uno solo, o un numero finito o infinito.

Se il sottoinsieme  $X$  ha minoranti, è non vuoto l'insieme

$$M = \{w \in S : w \text{ minorante di } X\}.$$

Ordinato questo insieme con la relazione indotta, questo può avere o meno massimo. Se tale massimo esiste, esso è ovviamente unico per 2.4.5 e viene detto

l'**estremo inferiore** di  $X$  in  $S$ , denotato con  $\inf_S X$  (o semplicemente con  $\inf X$  qualora non ci sia possibilità che ciò generi equivoci). Pertanto, con  $k \in S$ , si ha:

$$k = \inf X : \iff \begin{cases} (i) & k \leq x, \forall x \in X \\ (ii) & (s \leq x, \forall x \in X) \implies s \leq k. \end{cases} \quad (2.4.3)$$

Infatti la (i) esprime l'appartenenza di  $k$  all'insieme  $M$ , dopodiché la (ii) esprime il fatto che  $k = \max M$ .

“Dualmente”, supposto non vuoto l'insieme

$$N = \{w \in S : w \text{ maggiorante di } X\},$$

se tale insieme ha minimo, tale minimo è detto l'**estremo superiore** di  $X$  in  $S$ , e denotato con  $\sup_S X$  (o semplicemente con  $\sup X$ ). Pertanto, con  $h \in S$ , si ha:

$$h = \sup X : \iff \begin{cases} (i) & x \leq h, \forall x \in X \\ (ii) & (x \leq s, \forall x \in X) \implies h \leq s. \end{cases} \quad (2.4.4)$$

**2.4.14. Esempio.** Per ogni  $x \in \mathbb{N}$ , si indichi con  $\gamma(x)$  il numero delle cifre di  $x$ : se  $x = a_t a_{t-1} \dots a_0$ , con  $t \geq 0$ ,  $a_0, \dots, a_t \in \{0, 1, \dots, 9\}$  e  $a_t \neq 0$  è l'usuale scrittura decimale di  $x$ , si pone  $\gamma(x) = t + 1$ . Per esempio  $\gamma(30) = 2$ ,  $\gamma(5) = 1$ . Se in  $\mathbb{N}$  si pone:

$$x \mathcal{R} y : \iff (x = y) \text{ o } (\gamma(x) < \gamma(y)),$$

dove il  $\leq$  è l'ordine usuale in  $\mathbb{N}$ , si ottiene una relazione d'ordine. È facile allora osservare che il sottoinsieme  $\{10, 14, 47\}$  ha come minoranti  $1, 2, \dots, 9$ , ma non ammette estremo inferiore; così tutti i numeri naturali di tre o più cifre sono maggioranti, ma non esiste estremo superiore.

Può risultare utile la seguente osservazione:

**2.4.15.** Siano  $(S, \leq)$  un insieme ordinato e  $X \subseteq S$ . Se  $(X, \leq)$  ha minimo  $a$ , risulta  $a = \inf X$ . Analogamente, se  $(X, \leq)$  ha massimo  $b$ , risulta  $b = \sup X$ .

*Dimostrazione.* Si è già osservato che il minimo di  $X$  è un minorante di  $X$ . Se  $w \in S$  è un qualsiasi minorante di  $X$ , si ha  $w \leq x$  per ogni  $x \in X$ , e quindi in particolare  $w \leq a$ , sicché  $a$  è il massimo dei minoranti di  $X$ , ossia  $a = \inf X$ .

L'altra proprietà è la “duale”. □

In  $(\mathcal{P}(T), \subseteq)$ , con  $T$  insieme, ogni sottoinsieme non vuoto  $\mathcal{X}$  ha estremo inferiore e estremo superiore. Precisamente:

$$\inf \mathcal{X} = \bigcap_{Y \in \mathcal{X}} Y, \quad \sup \mathcal{X} = \bigcup_{Y \in \mathcal{X}} Y,$$

in quanto valgono le proprietà (i) e (ii) di (2.4.3) e (2.4.4) che definiscono tali elementi.

In  $(\mathbb{N}_0, \text{divide})$  ogni sottoinsieme finito e non vuoto  $X$  ha estremo inferiore e estremo superiore. Precisamente, se  $X = \{x_1, \dots, x_n\}$ , si ha:

$$\inf X = \text{MCD}(x_1, \dots, x_n), \\ \sup X = \text{mcm}(x_1, \dots, x_n),$$

dove i simboli “MCD” e “mcm” indicano rispettivamente il massimo comune divisore e il minimo comune multiplo. Il significato e l’esistenza di questi elementi sarà discusso nel Capitolo 5. Per il momento ci si appella alle conoscenze elementari del Lettore.

Un insieme ordinato  $(S, \leq)$  tale che, per ogni  $x, y \in S$  esiste  $\inf\{x, y\}$  e  $\sup\{x, y\}$  è detto un **reticolo**. Esempi di reticolo sono  $(\mathcal{P}(T), \subseteq)$  e  $(\mathbb{N}_0, \text{divide})$ , come illustrato in precedenza. Ai reticolati è dedicato parte del Capitolo 10, cui si rimanda.

## Esercizi

**Esercizio 2.4.1.** Si provi 2.4.2.

**Esercizio 2.4.2.** Si consideri l’insieme  $W$  costituito dai numeri naturali della forma  $2^n 3^m$ , con  $n, m \in \mathbb{N}_0$ :

$$W = \{2^n 3^m : n, m \in \mathbb{N}_0\}.$$

(i) Si verifichi che è d’ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n \leq s) \text{ e } (m \leq t),$$

dove il  $\leq$  indica la relazione d’ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si studi l’insieme ordinato  $(W, \mathcal{R})$ , precisando se l’ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimali, elementi massimali.
- (iii) Si provi che  $(W, \mathcal{R})$  è un reticolo.
- (iv) Si studi l’applicazione:

$$f : 2^n 3^m \in W \longrightarrow n + m \in \mathbb{N}_0,$$

e si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ .

- (v) Considerati i seguenti sottoinsiemi di  $W$ :

$$F = \{2, 4, 12, 16\}, \quad G = \{1, 3, 9, 81\}, \\ H = \{2, 8, 18, 72\}, \quad K = \{3, 16, 27, 32\},$$

si studino gli insiemi ordinati  $(F, \mathcal{R})$ ,  $(G, \mathcal{R})$ ,  $(H, \mathcal{R})$ ,  $(K, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

*Svolgimento.* (i) Da  $n \leq n$  e  $m \leq m$  segue subito che  $2^n 3^m \mathcal{R} 2^n 3^m$ , per ogni  $2^n 3^m \in W$ . Pertanto  $\mathcal{R}$  è riflessiva. Si supponga ora  $2^n 3^m \mathcal{R} 2^s 3^t$  e  $2^s 3^t \mathcal{R} 2^n 3^m$ , sia cioè  $n \leq s$  e  $m \leq t$  e anche  $s \leq n$  e  $t \leq m$ ; per l'asimmetria dell'ordine usuale in  $\mathbb{N}_0$  si ha  $n = s$  e  $m = t$ , sicché  $2^n 3^m = 2^s 3^t$ . Quindi  $\mathcal{R}$  è asimmetrica. Si supponga infine  $2^n 3^m \mathcal{R} 2^s 3^t$  e  $2^s 3^t \mathcal{R} 2^h 3^k$ , si abbia cioè  $n \leq s$  e  $m \leq t$ ,  $s \leq h$  e  $t \leq k$ . La transitività dell'ordine usuale in  $\mathbb{N}_0$  comporta  $n \leq h$  e  $m \leq k$  da cui  $2^n 3^m \mathcal{R} 2^h 3^k$ . Ciò assicura che  $\mathcal{R}$  è anche transitiva e quindi è una relazione d'ordine in  $W$ .

(ii) La relazione d'ordine  $\mathcal{R}$  non è totale perché, per esempio,  $2 \not\mathcal{R} 3$  e  $3 \not\mathcal{R} 2$  in quanto  $2 = 2^1 3^0$  e  $3 = 2^0 3^1$ . Pertanto  $\mathcal{R}$  non è un buon ordine (vedi 2.4.12). Risulta  $1 = \min W$  essendo  $0 \leq s, 0 \leq t$  per ogni  $s, t \in \mathbb{N}_0$  da cui  $1 = 2^0 3^0 \mathcal{R} 2^s 3^t$ , per ogni  $2^s 3^t \in W$ . Quindi 1 è l'unico elemento minima di  $W$ . Non esistono elementi massimali, e quindi non esiste il massimo di  $W$ : infatti, per esempio, per ogni  $2^n 3^m \in W$  esiste  $2^{n+1} 3^{m+1} \in W$  tale che  $2^n 3^m \mathcal{R} 2^{n+1} 3^{m+1}$  con  $2^n 3^m \neq 2^{n+1} 3^{m+1}$ .

(iii) Considerati  $2^n 3^m, 2^s 3^t \in W$ , si ha

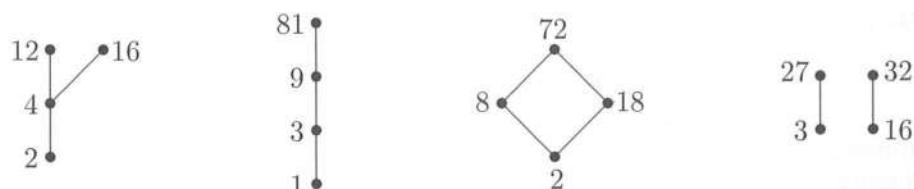
$$\inf\{2^n 3^m, 2^s 3^t\} = 2^h 3^k,$$

$$\sup\{2^n 3^m, 2^s 3^t\} = 2^v 3^w,$$

con  $h = \min\{n, s\}$ ,  $k = \min\{m, t\}$ ,  $v = \max\{n, s\}$  e  $w = \max\{m, t\}$ , dove tali minimi e massimi vanno intesi rispetto alla relazione d'ordine usuale in  $\mathbb{N}_0$ . Infatti, da  $h \leq n, h \leq s, k \leq m$  e  $k \leq t$  segue  $2^h 3^k \mathcal{R} 2^n 3^m$  e  $2^h 3^k \mathcal{R} 2^s 3^t$ , sicché  $2^h 3^k$  è minorante di  $\{2^n 3^m, 2^s 3^t\}$ ; supposto poi  $2^i 3^j$  minorante di  $\{2^n 3^m, 2^s 3^t\}$ , si ha  $i \leq n, j \leq m, i \leq s$  e  $j \leq t$ , sicché  $i \leq h$  e  $j \leq k$  essendo  $h = \min\{n, s\}$  e  $k = \min\{m, t\}$ . Pertanto  $2^h 3^k$  è il massimo dei minoranti di  $\{2^n 3^m, 2^s 3^t\}$ . “Dualizzando” si prova l'altra proprietà. Pertanto  $(W, \mathcal{R})$  è un reticolo.

(iv) L'applicazione  $f$  è ovviamente suriettiva e non iniettiva: infatti ogni  $y \in \mathbb{N}_0$  è immagine per esempio sia di  $2^y 3^0$  che di  $2^0 3^y$  e questi sono distinti se  $y \neq 0$ . È poi un omomorfismo di insiemi ordinati, perché, supposto  $2^n 3^m \mathcal{R} 2^s 3^t$ , ciò comporta  $n \leq s$  e  $m \leq t$ , sicché  $f(2^n 3^m) = n + m \leq s + t = f(2^s 3^t)$ .

(v) Da  $2 = 2^1 3^0$ ,  $4 = 2^2 3^0$ ,  $12 = 2^2 3^1$ ,  $16 = 2^4 3^0$ ,  $1 = 2^0 3^0$ ,  $3 = 2^0 3^1$ ,  $9 = 2^0 3^2$ ,  $8 = 2^3 3^0$ ,  $18 = 2^1 3^2$ ,  $72 = 2^3 3^2$ ,  $27 = 2^0 3^3$ ,  $32 = 2^5 3^0$  e  $81 = 2^0 3^4$  segue subito che i diagrammi di Hasse di  $F$ ,  $G$ ,  $H$  e  $K$  sono rispettivamente:



È evidente che  $F$  ha minimo 2 e elementi massimali 12 e 16,  $G$  è una catena di minimo 1 e massimo 81,  $H$  ha minimo 2 e massimo 72,  $K$  ha elementi minimi 3 e 16 e elementi massimali 27 e 32.

**Esercizio 2.4.3.** Posto  $M = \{n \in \mathbb{N} : n \geq 2\}$ , per ogni  $n \in M$  si dica  $\beta(n)$  il numero dei divisori primi positivi distinti di  $n$ , sia cioè

$$\beta(n) := |\{p \in \mathbb{N} : p \text{ primo, } p \text{ divide } n\}|.$$

Si consideri in  $M$  la seguente relazione:

$$n \mathcal{R} m : \iff (n = m) \text{ o } (\beta(n) < \beta(m)),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (i) Si dimostri che  $\mathcal{R}$  è una relazione d'ordine e la si studi, precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min M$ ,  $\max M$ , elementi minimi, elementi massimali.
- (ii) Posto  $V = \{6, 10, 11, 25, 27, 30\}$  e  $Z = \{26, 33, 34, 46, 70, 121\}$ , si precisi se  $V$  e  $Z$  hanno minoranti in  $M$ , se hanno maggioranti, estremo inferiore, estremo superiore. Ordinati poi  $V$  e  $Z$  con la relazione indotta da  $\mathcal{R}$ , si studino tali insiemi ordinati e se ne disegni il diagramma di Hasse.
- (iii) Si faccia uno studio analogo a quello del punto (ii) per gli insiemi:

$$\begin{aligned} W &= \{14, 32, 42, 66, 81, 125\}, \\ T &= \{24, 50, 135, 210, 220, 242\}, \\ D &= \{55, 154, 169, 210, 30030, 36960\}. \end{aligned}$$

*Svolgimento.* (i) La relazione  $\mathcal{R}$  è riflessiva in quanto da  $n = n$  segue  $n \mathcal{R} n$ , per ogni  $n \in M$ . È poi asimmetrica in quanto, supposto  $n \mathcal{R} m$  e  $n \neq m$ , si ha  $\beta(n) < \beta(m)$  e dunque  $\beta(m) \not< \beta(n)$  e così  $m \not\mathcal{R} n$ , come volevasi (o anche, supposto  $n \mathcal{R} m$  e  $m \mathcal{R} n$  si ha necessariamente  $n = m$ , non potendo avversi contemporaneamente  $\beta(n) < \beta(m)$  e  $\beta(m) < \beta(n)$  per l'asimmetria dell'ordine usuale in  $\mathbb{N}$ ). Infine  $\mathcal{R}$  è transitiva: supposto infatti  $n \mathcal{R} m$  e  $m \mathcal{R} t$ , si ha ovviamente  $n \mathcal{R} t$  se  $n = m$  o  $m = t$ ; se poi è  $n \neq m$  e  $m \neq t$ , le ipotesi assicurano che  $\beta(n) < \beta(m)$  e  $\beta(m) < \beta(t)$  sicché la transitività dell'ordine usuale in  $\mathbb{N}$  garantisce che  $\beta(n) < \beta(t)$  e ancora  $n \mathcal{R} t$ . La relazione  $\mathcal{R}$  non è totale perché, per esempio,  $\beta(3) = 1 = \beta(5)$  e dunque  $3 \not\mathcal{R} 5$  e  $5 \not\mathcal{R} 3$ . Di conseguenza  $\mathcal{R}$  non è un buon ordine (vedi 2.4.12). Esistono infiniti elementi minimi: tutti gli elementi  $n$  di  $M$  con  $\beta(n) = 1$ . Questi sono tutte e sole le potenze dei numeri naturali primi:

$$\{n \in M : n \text{ minimale}\} = \{p^i : p \text{ primo, } i \in \mathbb{N}\}.$$

Infatti non esistono elementi  $m$  di  $M$  tali che  $\beta(m) < 1$  e quindi se  $p$  è primo e  $i \in \mathbb{N}$  non esistono elementi  $m$  di  $M$  tali che  $m \neq p^i$  e  $m \mathcal{R} p^i$ . Esistendo infiniti elementi minimi non esiste minimo di  $M$ . Non esistono elementi massimali in  $M$  e dunque non esiste massimo di  $M$ . Infatti, considerato un qualunque  $n \in M$  esiste un numero naturale primo  $q$  che non divide  $n$ . Posto allora  $k = nq$ , si ha che  $k \in M$ ,  $k \neq n$  e  $\beta(k) = \beta(n) + 1$  sicché  $n \mathcal{R} k$  con  $k \neq n$ . Pertanto  $n$  non è

massimale in  $M$ .

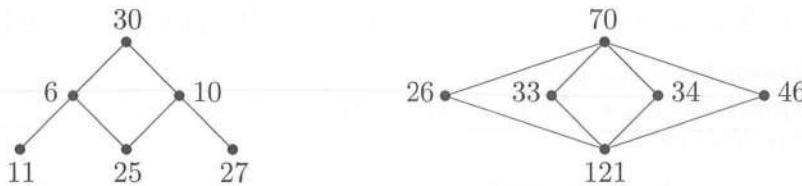
(ii) Si ha ovviamente:

$$\beta(6) = 2 = \beta(10), \quad \beta(11) = 1 = \beta(25) = \beta(27), \quad \beta(30) = 3,$$

e

$$\beta(26) = 2 = \beta(33) = \beta(34) = \beta(46), \quad \beta(121) = 1, \quad \beta(70) = 3,$$

sicché i diagrammi di Hasse di  $V$  e di  $Z$  sono i seguenti:



Come evidente, l'insieme ordinato  $(V, \mathcal{R})$  ha massimo 30 e elementi minimali 11, 25, 27 e dunque non ha minimo. L'insieme ordinato  $(Z, \mathcal{R})$  ha massimo 70, minimo 121 ed è un reticolo. Come sottoinsieme di  $M$ ,  $V$  non ha minoranti e quindi non esiste estremo inferiore. Ha come maggiorante 30 e tutti gli elementi  $n$  di  $M$  con  $\beta(n) > 3$ . Ovviamente (vedi 2.4.15) il massimo di  $V$  è anche il suo estremo superiore. I maggioranti di  $Z$  in  $M$  sono 70 e tutti i naturali  $n$  tali che  $\beta(n) > 3$ , ovviamente 70 è l'estremo superiore di  $Z$ . L'unico minorante è 121 che è anche l'estremo inferiore di  $Z$ .

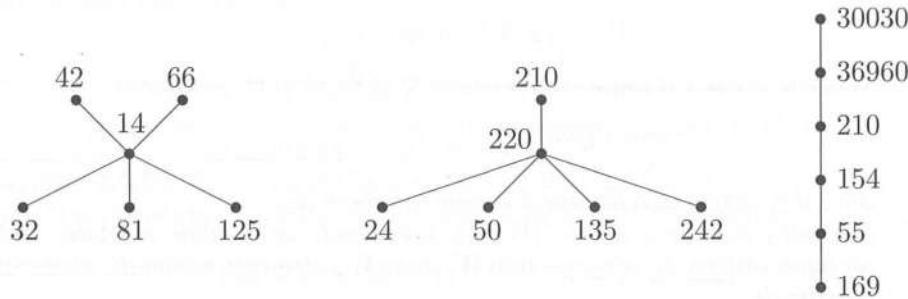
(iii) Si ha:

$$\beta(14) = 2, \quad \beta(32) = 1 = \beta(81) = \beta(125), \quad \beta(42) = 3 = \beta(66),$$

$$\beta(24) = 2 = \beta(50) = \beta(242) = \beta(135), \quad \beta(210) = 4, \quad \beta(220) = 3,$$

$$\beta(55) = 2, \quad \beta(154) = 3, \quad \beta(169) = 1, \quad \beta(30030) = 6, \quad \beta(36960) = 5,$$

(infatti:  $242 = 2 \cdot 11^2$ ,  $135 = 3^3 \cdot 5$ ,  $154 = 2 \cdot 7 \cdot 11$ ,  $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ ,  $36960 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ ), sicché si ottengono i seguenti diagrammi di Hasse:



È allora immediato riscontrare che  $W$  ha 42 e 66 come elementi massimali e 81, 32, 125 minimali;  $T$  ha massimo 210 e minimi 24, 50, 242, 135;  $D$  è una catena di massimo 30030 e minimo 169. Riguardati come sottoinsiemi di  $M$ , si

ha che  $W$  non ha minoranti e ha come maggioranti tutti gli elementi  $n \in M$  con  $\beta(n) > 3$ , sicché non esiste né  $\inf W$  né  $\sup W$ . Invece  $T$  ha come maggioranti 210 e tutti i naturali  $n \in M$  con  $\beta(n) > 4$ , e si ha  $\sup T = 210$ . Ha infiniti minoranti, tutti i naturali  $n \in M$  con  $\beta(n) = 1$ , e non esiste  $\inf T$ . Infine  $D$  ha maggioranti 30030 e i naturali  $n \in M$  tali che  $\beta(n) > 6$ , e ovviamente risulta  $30030 = \sup D$ . L'unico minorante è 169 che è quindi anche l'estremo inferiore.

**Esercizio 2.4.4.** Siano  $(S, \leq)$  e  $(S^*, \leq^*)$  insiemi ordinati. Si definisce **ordinamento lexicografico** in  $S \times S^*$  la relazione  $\mathcal{R}$  definita ponendo:

$$(x, y) \mathcal{R} (x', y') : \iff (x, y) = (x', y') \text{ o } (x < x') \text{ o } (x = x' \text{ e } y < y').$$

- (i) Si verifichi che  $\mathcal{R}$  è d'ordine.
- (ii) Si provi che se  $\leq$  e  $\leq^*$  sono totali, tale risulta  $\mathcal{R}$ .
- (iii) Si verifichi che:

$$\begin{aligned} (a, a') = \min(S \times S^*) &\iff a = \min S \text{ e } a' = \min S^*, \\ (b, b') = \max(S \times S^*) &\iff b = \max S \text{ e } b' = \max S^*. \end{aligned}$$

Si noti che tale ordine è analogo a quello di un qualunque vocabolario.

**Esercizio 2.4.5.** Sia  $(S, \leq)$  un insieme ordinato. Si verifichi che la relazione  $<$  definita in  $S$ , come al solito, dalla posizione:

$$x < y : \iff (x \leq y) \text{ e } (x \neq y)$$

gode della proprietà antiriflessiva e della proprietà transitiva.

**Esercizio 2.4.6.** Sia  $S$  un insieme e sia definita in  $S$  una relazione  $\mathcal{R}^*$  antiriflessiva e transitiva. Si provi che, ponendo:

$$x \mathcal{R} y : \iff (x \mathcal{R}^* y) \text{ o } (x = y)$$

si ottiene una relazione d'ordine in  $S$ .

**Esercizio 2.4.7.** Si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $2^n 3^m$ , con  $n, m \in \mathbb{N}_0$ :

$$W = \{2^n 3^m : n, m \in \mathbb{N}_0\}.$$

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n = s) \text{ e } (m \leq t),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.
- (iii) Considerati i sottoinsiemi  $F = \{1, 3, 9\}$  e  $G = \{2, 4, 12\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.8.** Si consideri l'insieme  $W = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n = s) \text{ e } (m|t),$$

dove il simbolo  $|$  indica la relazione del "divide" in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.

- (iii) Si consideri l'applicazione:

$$f : W \longrightarrow \mathcal{P}(\mathbb{N}_0)$$

definita ponendo:

$$\begin{cases} f(2^n 3^m) = \{x \in \mathbb{N}_0 : x > n\} & \text{se } m = 0, \\ f(2^n 3^m) = \{n+1, \dots, n+m\} & \text{se } m \neq 0. \end{cases}$$

Si studi l'applicazione  $f$ , e si provi che essa è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathcal{P}(\mathbb{N}_0), \subseteq)$ .

- (iv) Considerati i sottoinsiemi  $F = \{1, 3, 9\}$  e  $G = \{2, 18, 54\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.9.** Si consideri l'insieme  $V = \{4h + 1 : h \in \mathbb{Z}\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $V$  ponendo:

$$(4h + 1) \mathcal{R} (4k + 1) : \iff (h = k) \text{ o } (|h| < |k|),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(V, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min V$ ,  $\max V$ , elementi minimi, elementi massimi.

- (iii) Si studi l'applicazione

$$f : 4h + 1 \in V \longmapsto h^2 \in \mathbb{N}_0,$$

e si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(V, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ .

**Esercizio 2.4.10.** Si consideri l'insieme  $W = \{3h + 1 : h \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$(3h + 1) \mathcal{R} (3k + 1) : \iff (h = k) \text{ o } (h|k),$$

dove  $|$  indica la relazione del "divide" in  $\mathbb{N}_0$ .

- (ii) Si precisi se le seguenti affermazioni sono esatte:  $7 \mathcal{R} 16$ ,  $1 \mathcal{R} 4$ ,  $7 \mathcal{R} 1$ ,  $4 \mathcal{R} 13$ ,  $7 \mathcal{R} 31$ ,  $19 \mathcal{R} 10$ .

- (iii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.
- (iv) Considerati i sottoinsiemi  $F = \{1, 4, 7, 13\}$  e  $G = \{10, 22, 31, 34\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.11.** Si consideri l'insieme  $W = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n = s \text{ e } m = t) \text{ o } (|n - 2m| < |s - 2t|),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.
- (iii) Si studi l'applicazione

$$f : 2^n 3^m \in W \longmapsto n^2 - 4nm + 4m^2 \in \mathbb{N}_0,$$

e si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ .

- (iv) Considerati i sottoinsiemi  $F = \{8, 27, 162, 288\}$  e  $G = \{3, 4, 48, 72\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.12.** Si consideri l'insieme  $W = \{2^n 7^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 7^m \mathcal{R} 2^s 7^t : \iff (n = s \text{ e } m = t) \text{ o } (n + 2m < s + 2t),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.
- (iii) Si studino le applicazioni

$$\begin{aligned} f : 2^n 7^m \in W &\longmapsto n + 2m \in \mathbb{N}_0, \\ g : 2^n 7^m \in W &\longmapsto n + m \in \mathbb{N}_0. \end{aligned}$$

- (iv) Si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ , e che  $g$  non lo è.
- (v) Considerati i sottoinsiemi  $F = \{4, 7, 8, 14\}$  e  $G = \{32, 56, 64, 98\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.13.** Sia  $\mathbb{P}$  l'insieme dei numeri primi in  $\mathbb{N}_0$ , e si consideri l'insieme

$$W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}.$$

(i) Si verifichi che non è d'ordine la relazione  $\mathcal{R}^*$  definita in  $W$  da:

$$p_1 p_2 \mathcal{R}^* q_1 q_2 : \iff p_1 = q_1.$$

(ii) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$p_1 p_2 \mathcal{R} q_1 q_2 : \iff (p_1 = q_1) \text{ e } (p_2 \leq q_2),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (iii) Si precisi se le seguenti affermazioni sono esatte:  $25 \mathcal{R} 26$ ,  $26 \mathcal{R} 25$ ,  $9 \mathcal{R} 46$ ,  $65 \mathcal{R} 65$ ,  $21 \mathcal{R} 33$ ,  $49 \mathcal{R} 91$ ,  $34 \mathcal{R} 38$ ,  $38 \mathcal{R} 34$ .
- (iv) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimi.
- (v) Si studi l'applicazione

$$f : p_1 p_2 \in W \longmapsto p_1 p_2 \in \mathbb{N}_0,$$

e si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ , non lo è tra  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \text{divide})$ .

- (vi) Considerati i sottoinsiemi  $F = \{39, 49, 77, 187\}$  e  $G = \{35, 38, 55, 62\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.4.14.** Si ponga:

$$\begin{aligned} A &= \{n \in \mathbb{N}_0 : n \text{ divide } 36\}, \\ B &= \{n \in \mathbb{N}_0 : n \text{ divide } 30\}, \\ C &= \{n \in \mathbb{N}_0 : n \text{ divide } 18\}, \\ D &= \{n \in \mathbb{N}_0 : n \text{ divide } 32\}, \\ E &= \{n \in \mathbb{N}_0 : n \text{ divide } 35\}, \\ F &= \{n \in \mathbb{N}_0 : n \text{ divide } 24\}. \end{aligned}$$

Si disegnino i diagrammi di Hasse degli insiemi ordinati:  $(A, \text{divide})$ ,  $(B, \text{divide})$ ,  $(C, \text{divide})$ ,  $(D, \text{divide})$ ,  $(E, \text{divide})$ ,  $(F, \text{divide})$ .

## 2.5 Esercizi di riepilogo

**Esercizio 2.5.1.** Si considerino le applicazioni:

$$f : x \in \mathbb{Z} \longmapsto x^4 + 2 \in \mathbb{Z}, \quad g : x \in \mathbb{Z} \longmapsto \frac{15}{2} \in \mathbb{Q}.$$

- (i) Si calcolino:  $f(-3), f(0), f(2), f(-1), g(-3), g(-4), g(91), g(0), g(\mathbb{Z}), f(\{1, 2, 3\}), f(\{1, -1\}), g(\{1, 2, 3\}), g(\{1, -1, -4\}), f^{-1}(\{2, -2, 9, 18\}), g^{-1}(\{8, -8, \frac{1}{9}, \frac{15}{2}\}), g^{-1}(\{8\})$ .
- (ii) Si stabilisca se  $f$  e  $g$  sono iniettive o suriettive.

**Esercizio 2.5.2.** Si considerino le applicazioni:

$$h : x \in \mathbb{Z} \longmapsto 6|x| \in 6\mathbb{N}_0, \quad k : t \in 6\mathbb{N}_0 \longmapsto t + 7 \in \mathbb{N}_0.$$

- (i) Si calcolino:  $h(\{-2, -1, 0, 1, 2\}), h(2\mathbb{Z}), h^{-1}(\{0, 12, 18, 36\}), k(12\mathbb{N}), k(\{0, 12, 18, 36\}), k^{-1}(\mathbb{N}_0 \setminus \{7, 13\}), k^{-1}(\{12, 18, 36\})$ .
- (ii) Si stabilisca se  $h$  e  $k$  sono iniettive o suriettive.
- (iii) Si determini la composta  $k \circ h$  e la si studi.

**Esercizio 2.5.3.** Si considerino le applicazioni:

$$h : x \in 5\mathbb{N}_0 \longmapsto \frac{x}{5} + 1 \in \mathbb{N}_0, \quad k : t \in \mathbb{N}_0 \longmapsto 4|t - 1| \in 4\mathbb{N}_0.$$

- (i) Si calcolino:  $h(\{0, 5, 15\}), h(10\mathbb{N}), h^{-1}(\{0, 2, 8, 11\}), k(\{0, 1, 2, 3, 4, 5\}), k^{-1}(\{0, 4, 8, 16\}), k^{-1}(4\mathbb{N}_0 \setminus \{0, 4, 12\})$ .
- (ii) Si stabilisca se  $h$  e  $k$  sono iniettive o suriettive.
- (iii) Si determini la composta  $k \circ h$ , si verifichi che è biettiva e se ne individui l'inversa.

**Esercizio 2.5.4.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff |x - 6| = |y - 6|,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{llll} -3 \mathcal{R} 19, & 0 \mathcal{R} 6, & -5 \mathcal{R} -5, & 0 \mathcal{R} -6, \\ 11 \mathcal{R} 1, & -2 \mathcal{R} 14, & 9 \mathcal{R} 9, & 14 \mathcal{R} -2. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva.

**Esercizio 2.5.5.** Considerata in  $\mathbb{Z}$  la relazione binaria definita ponendo:

$$x \mathcal{R} y : \iff x^2 + 5x - 6 = y^2 - y - 12,$$

si precisi se le seguenti affermazioni sono esatte:

$$\begin{array}{llllll} -2 \mathcal{R} 1, & -1 \mathcal{R} -1, & 2 \mathcal{R} -5, & 0 \mathcal{R} 0, & 0 \mathcal{R} 3, & 4 \mathcal{R} 1, \\ -2 \mathcal{R} 0, & 1 \mathcal{R} 4, & -6 \mathcal{R} 4, & 1 \mathcal{R} 0, & 2 \mathcal{R} 4, & 0 \mathcal{R} -3, \\ 0 \mathcal{R} -2, & -6 \mathcal{R} -3, & 2 \mathcal{R} 2, & -3 \mathcal{R} 0, & 1 \mathcal{R} -3, & -3 \mathcal{R} -6. \end{array}$$

Si stabilisca poi se  $\mathcal{R}$  è riflessiva, simmetrica, asimmetrica, transitiva.

**Esercizio 2.5.6.** Considerate le seguenti relazioni tra  $\mathbb{N}$  e  $\mathbb{Q}$ , si precisi, motivando la risposta, se sono applicazioni e, in tal caso, se sono iniettive, suriettive, biettive:

$$\begin{aligned}x \mathcal{R}_1 y & : \iff 5x^2 = 4y; \\x \mathcal{R}_2 y & : \iff 5x = 4|y|; \\x \mathcal{R}_3 y & : \iff 5x = 4y; \\x \mathcal{R}_4 y & : \iff 5x = 4y^2.\end{aligned}$$

**Esercizio 2.5.7.** Con  $H = \{a, b, c, d\}$  e  $K = \{0, 1, 2\}$  si considerino le seguenti relazioni:

$$\begin{aligned}\mathcal{R}_1 &= \{(a, 2), (c, 1), (b, 0)\}, \quad \mathcal{R}_2 = \{(a, 2), (d, 1), (b, 1), (c, 0)\} \text{ tra } H \text{ e } K; \\ \mathcal{R}_3 &= \{(1, c), (0, b), (2, a)\}, \quad \mathcal{R}_4 = \{(2, c), (0, c), (1, c)\} \text{ tra } K \text{ e } H; \\ \mathcal{R}_5 &= \{(a, b), (c, d)\}, \quad \mathcal{R}_6 = \{(a, a), (b, b), (c, c), (d, d)\} \text{ tra } H \text{ e } H; \\ \mathcal{R}_7 &= \{(1, 1), (2, 2), (1, 0)\}, \quad \mathcal{R}_8 = \{(0, 1), (1, 2), (2, 0), (1, 0)\} \text{ tra } K \text{ e } K.\end{aligned}$$

Di ciascuna si precisi se è un'applicazione, e in tal caso se è iniettiva, suriettiva, biettiva.

**Esercizio 2.5.8.** Con  $V = \{s, t, w\}$  si precisi quali delle seguenti relazioni binarie in  $V$  sono riflessive, simmetriche, asimmetriche, transitive:

$$\begin{aligned}\mathcal{R}_1 &= \{(s, s), (t, t), (w, w), (t, w)\}, \\ \mathcal{R}_2 &= \{(t, w), (w, t)\}, \\ \mathcal{R}_3 &= \{(s, t), (t, s), (s, s), (t, t)\}.\end{aligned}$$

**Esercizio 2.5.9.** Considerate le seguenti relazioni tra  $\mathbb{N}$  e  $\mathbb{Z}$ , si precisi, motivando la risposta, se sono applicazioni:

$$\begin{aligned}n \mathcal{R}_1 z & : \iff n + z = 3; \\n \mathcal{R}_2 z & : \iff n + 4 = z; \\n \mathcal{R}_3 z & : \iff n = z^3; \\n \mathcal{R}_4 z & : \iff z = -n^2; \\n \mathcal{R}_5 z & : \iff n = |z|; \\n \mathcal{R}_6 z & : \iff z + 11 = n; \\n \mathcal{R}_7 z & : \iff n + 4 > z.\end{aligned}$$

**Esercizio 2.5.10.** Con  $n$  numero naturale positivo, si dica  $h(n)$  il massimo numero naturale  $h$  tale che  $3^h$  divide  $n$ , sia cioè  $n = 3^{h(n)}k$ , con  $k \in \mathbb{N}_0$  tale che  $3$  non divide  $k$ . Si dimostri che non è d'equivalenza né d'ordine la relazione  $\mathcal{R}$  definita in  $\mathbb{N}$  da:

$$n \mathcal{R} m : \iff h(n) \leq h(m),$$

dove  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

**Esercizio 2.5.11.** Si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $3h + 1$ , con  $h \in \mathbb{N}_0$ :

$$W = \{3h + 1 : h \in \mathbb{N}_0\}.$$

Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$(3h + 1) \mathcal{R} (3k + 1) : \iff h + k \in 2\mathbb{N}_0$$

è d'equivalenza. Si determinino poi:  $[1]_{\mathcal{R}}, [4]_{\mathcal{R}}, [7]_{\mathcal{R}}$ . Si provi che ha senso definire l'applicazione:

$$\psi : [3h + 1]_{\mathcal{R}} \in W / \mathcal{R} \longmapsto (-1)^h \in \mathbb{Z}$$

e si studi tale applicazione.

**Esercizio 2.5.12.** Si consideri l'insieme  $W = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ . Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff |n - 3m| = |s - 3t|$$

è d'equivalenza. Si descriva poi la generica classe d'equivalenza  $[2^n 3^m]_{\mathcal{R}}$  e in particolare:  $[1]_{\mathcal{R}}, [2]_{\mathcal{R}}, [3]_{\mathcal{R}}$  e  $[24]_{\mathcal{R}}$ .

**Esercizio 2.5.13.** Si consideri l'insieme  $W = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ .

(i) Si dimostri che la relazione  $\mathcal{R}^*$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R}^* 2^s 3^t : \iff n - m = t - s,$$

non è né d'equivalenza né d'ordine.

(ii) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n = s \text{ e } m = t) \text{ o } (|n - m| < |s - t|),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (iii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimali, elementi massimali.
- (iv) Considerati i sottoinsiemi  $F = \{8, 27, 162, 288\}$  e  $G = \{48, 72, 216, 648\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.
- (v) Posto  $A = \{n \in W : n \text{ divide } 484\}$ , si disegni il diagramma di Hasse dell'insieme ordinato  $(A, \mathcal{R})$ .

**Esercizio 2.5.14.** Si consideri l'insieme  $W = \{2^n 7^m : n, m \in \mathbb{N}_0\}$ .

(i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 7^m \mathcal{R} 2^s 7^t : \iff (n = s \text{ e } m = t) \text{ o } (m < t),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si precisi se le seguenti affermazioni sono esatte:  $7 \mathcal{R} 14, 32 \mathcal{R} 7, 28 \mathcal{R} 28, 512 \mathcal{R} 343, 7 \mathcal{R} 32, 14 \mathcal{R} 7, 56 \mathcal{R} 64, 16 \mathcal{R} 14$ .
- (iii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W, \max W$ , elementi minimi, elementi massimi.
- (iv) Si studino le applicazioni:

$$f : 2^n 7^m \in W \longmapsto n \in \mathbb{N}_0, \quad g : 2^n 7^m \in W \longmapsto m \in \mathbb{N}_0,$$

e si provi che  $f$  non è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ ,  $g$  invece lo è.

- (v) Considerati i sottoinsiemi  $F = \{7, 14, 28, 56\}$  e  $G = \{32, 49, 64, 98\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.5.15.** Sia  $\mathbb{P}$  l'insieme dei numeri primi in  $\mathbb{N}_0$ , e si consideri l'insieme

$$W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}.$$

- (i) Si verifichi che non è d'ordine la relazione  $\mathcal{R}^*$  definita in  $W$  da:

$$p_1 p_2 \mathcal{R}^* q_1 q_2 : \iff p_2 = q_2.$$

- (ii) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$p_1 p_2 \mathcal{R} q_1 q_2 : \iff (p_1 \leq q_1) \text{ e } (p_2 = q_2),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (iii) Si precisi se le seguenti affermazioni sono esatte:  $49 \mathcal{R} 49, 26 \mathcal{R} 4, 4 \mathcal{R} 26, 14 \mathcal{R} 35, 26 \mathcal{R} 39, 10 \mathcal{R} 14, 77 \mathcal{R} 121, 4 \mathcal{R} 10$ .
- (iv) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W, \max W$ , elementi minimi, elementi massimi.
- (v) Considerati i sottoinsiemi  $F = \{21, 26, 55, 121\}$  e  $G = \{15, 21, 35, 49\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.5.16.** Si consideri l'insieme  $W = \{2^n 3^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 3^m \mathcal{R} 2^s 3^t : \iff (n \leq s) \text{ e } (m|t),$$

dove il simbolo  $|$  indica la relazione del "divide" in  $\mathbb{N}_0$ .

- (ii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W, \max W$ , elementi minimi, elementi massimi.

(iii) Considerata l'applicazione  $f : W \rightarrow \mathcal{P}(\mathbb{N}_0)$  definita ponendo:

$$\begin{cases} f(2^n 3^m) = \{x \in \mathbb{N}_0 : x > n\} \text{ se } m = 0, \\ f(2^n 3^m) = \{n+1, \dots, n+m\} \text{ se } m \neq 0, \end{cases}$$

la si studi e si stabilisca poi se essa è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathcal{P}(\mathbb{N}_0), \subseteq)$ .

- (iv) Considerati i sottoinsiemi  $F = \{2, 4, 12, 16\}$  e  $G = \{1, 3, 9, 81\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.5.17.** Si consideri l'insieme  $W = \{3^n 5^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si verifichi che è d'ordine la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$3^n 5^m \mathcal{R} 3^s 5^t : \iff (n = s \text{ e } m = t) \text{ o } (3n + m < 3s + t),$$

dove il  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (ii) Si precisi se le seguenti affermazioni sono esatte:  $75 \mathcal{R} 75$ ,  $9 \mathcal{R} 75$ ,  $25 \mathcal{R} 3$ ,  $3 \mathcal{R} 125$ ,  $15 \mathcal{R} 625$ ,  $625 \mathcal{R} 15$ ,  $25 \mathcal{R} 15$ ,  $15 \mathcal{R} 9$ .  
 (iii) Si studi l'insieme ordinato  $(W, \mathcal{R})$ , precisando se l'ordine è totale, se è un buon ordine, se esistono  $\min W$ ,  $\max W$ , elementi minimi, elementi massimali.  
 (iv) Si studino le applicazioni:

$$f : 3^n 5^m \in W \mapsto 3n + m \in \mathbb{N}_0, \quad g : 3^n 5^m \in W \mapsto n + m \in \mathbb{N}_0,$$

e si provi che  $f$  è un omomorfismo tra gli insiemi ordinati  $(W, \mathcal{R})$  e  $(\mathbb{N}_0, \leq)$ ,  $g$  non lo è.

- (v) Considerati i sottoinsiemi  $F = \{27, 45, 75, 225\}$  e  $G = \{9, 27, 375, 15625\}$  di  $W$ , si studino gli insiemi ordinati  $(F, \mathcal{R})$  e  $(G, \mathcal{R})$ , disegnandone anche il relativo diagramma di Hasse.

**Esercizio 2.5.18.** Nell'insieme  $A = \{0, 1, 2, \dots, 11\}$  dei numeri naturali minori di 12 si consideri la relazione  $\mathcal{R}$  definita ponendo

$$a \mathcal{R} b : \iff a = b \text{ oppure } 5a < 2b,$$

dove  $\leq$  indica la relazione d'ordine usuale in  $\mathbb{N}$ .

- (i) Si verifichi che  $\mathcal{R}$  è una relazione d'ordine in  $A$ .  
 (ii) Si disegni il diagramma di Hasse di  $(A, \mathcal{R})$ .  
 (iii) Si stabilisca se  $(A, \mathcal{R})$  è ben ordinato.  
 (iv) Si determinino gli eventuali elementi minimi, elementi massimali, minimo e massimo di  $(A, \mathcal{R})$ .  
 (v) Si determinino tutti i maggioranti in  $A$  del sottoinsieme  $\{1, 2\}$ .  
 (vi) Si determini l'estremo superiore in  $A$  del sottoinsieme  $\{1, 2\}$ .

# 3

## Elementi di calcolo combinatorio

In questo capitolo verranno illustrati elementi del cosiddetto “calcolo combinatorio”, che fornisce tecniche utili nel conto in situazioni che frequentemente si verificano anche nella vita quotidiana. La presentazione che si farà è volutamente informale, fondandosi più sull’intuito che sul rigore; si è preferito privilegiare le idee di base, lasciando eventualmente al Lettore una formalizzazione rigorosa. Anche gli esercizi proposti richiamano spesso a momenti della vita di tutti i giorni, nell’intento di mostrare come i principi enunciati possano avere applicazioni in contesti probabilmente molto familiari al Lettore.

### 3.1 I principi di addizione e di inclusione-esclusione

Del tutto immediate sono le seguenti:

**3.1.1. Principio di addizione.** Siano  $A$  e  $B$  insiemi finiti disgiunti. Allora:

$$|A \cup B| = |A| + |B|.$$

*Dimostrazione.* Siano  $A = \{x_1, \dots, x_n\}$ ,  $B = \{y_1, \dots, y_m\}$  con  $|A| = n$  e  $|B| = m$ . Allora  $A \cup B = \{x_1, \dots, x_n, y_1, \dots, y_m\}$  e  $|A \cup B| = |A| + |B|$ , in quanto l’essere  $A$  e  $B$  disgiunti assicura che gli elementi  $x_1, \dots, x_n, y_1, \dots, y_m$  sono a due a due distinti.  $\square$

**3.1.2.** Sia  $A$  un insieme finito. Allora:

- (i) da  $C \subseteq A$  segue  $|A \setminus C| = |A| - |C|$ ;
- (ii) se  $B$  un insieme qualunque, si ha  $|A \setminus B| = |A| - |A \cap B|$ .

*Dimostrazione.* La (i) è ovvia. La (ii) discende dall’essere  $A \setminus B = A \setminus (A \cap B)$  (vedi 1.4.10), da (1.4.6) e dalla (i).  $\square$

Si è ora in grado di provare il seguente:

**3.1.3. Principio di inclusione-esclusione.** *Siano  $A$  e  $B$  insiemi finiti. Si ha:*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

*Dimostrazione.* Ovviamente risulta  $A \cup B = (A \setminus B) \cup B$  con  $(A \setminus B) \cap B = \emptyset$ . Pertanto, per la 3.1.1, si ha  $|A \cup B| = |A \setminus B| + |B|$  e dalla 3.1.2 si ottiene  $|A \cup B| = |A| - |A \cap B| + |B|$ , come volevasi.  $\square$

Più in generale si ha:

**3.1.4. Principio di inclusione-esclusione (forma generale).** *Sia  $k \geq 2$  e siano  $A_1, \dots, A_k$  insiemi finiti. Allora si ha:*

$$\begin{aligned} |\bigcup_{i=1}^k A_i| &= \sum_{i=1}^k |A_i| - \sum_{1 \leq i < j \leq k} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < h \leq k} |A_i \cap A_j \cap A_h| + \cdots + (-1)^{k-1} \left| \bigcap_{i=1}^k A_i \right|. \end{aligned}$$

*Dimostrazione.* Esercizio.  $\square$

**3.1.5. Esempio.** I numeri naturali positivi minori di 31 e divisibili per 2 o per 3 sono 20. Infatti, posto

$$\begin{aligned} S &:= \{x \in \mathbb{N} : x \leq 30\}, \\ A &:= \{x \in S : 2 \text{ divide } x\}, \\ B &:= \{x \in S : 3 \text{ divide } x\}, \end{aligned}$$

si ha  $A \cup B = \{x \in S : 2 \text{ divide } x \text{ o } 3 \text{ divide } x\}$  e  $A \cap B = \{x \in S : 6 \text{ divide } x\}$ . Risulta poi  $|A| = \frac{30}{2} = 15$ ,  $|B| = \frac{30}{3} = 10$  e  $|A \cap B| = \frac{30}{6} = 5$ ; dalla 3.1.3 segue allora

$$|A \cup B| = 15 + 10 - 5 = 20.$$

**3.1.6. Esempio.** I numeri naturali positivi minori di 31 e divisibili per almeno uno tra 2, 3 e 5 sono 22. Infatti, con  $S$ ,  $A$  e  $B$  come nell'esempio precedente e con

$$C := \{x \in S : 5 \text{ divide } x\},$$

si ha  $|C| = \frac{30}{5} = 6$ ,  $|A \cap C| = \frac{30}{10} = 3$ ,  $|B \cap C| = \frac{30}{15} = 2$ ,  $|A \cap B \cap C| = \frac{30}{30} = 1$ ; dalla 3.1.4 segue allora

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 15 + 10 + 6 - 5 - 3 - 2 + 1 = 22. \end{aligned}$$

## Esercizi

**Esercizio 3.1.1.** Con  $k \geq 2$  siano  $A_1, A_2, \dots, A_k$  insiemi finiti a due a due disgiunti. Si provi che:

$$\left| \bigcup_{i=1}^k A_i \right| = \sum_{i=1}^k |A_i|.$$

**Esercizio 3.1.2.** Siano  $A, B$  e  $C$  insiemi finiti. Si provi che  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ .

**Esercizio 3.1.3.** Quanti sono i numeri naturali tra 1 e 1250 divisibili per almeno uno tra 17 e 31?

**Esercizio 3.1.4.** Si provi 3.1.4.

**Esercizio 3.1.5.** Alla discoteca “Furore” la consumazione è obbligatoria e ogni bibita costa 5 euro. All’interno ci sono 21 giovani, ognuno dei quali consuma al più due bibite e comunque di tipo diverso, e sono state servite 12 aranciate e 15 chinotti. Quanti scontrini da 10 euro deve preparare il cassiere?

**Esercizio 3.1.6.** Quanti sono i numeri tra 1 e 101 divisibili per almeno uno tra 2 e 5? E quanti quelli divisibili per almeno uno tra 2, 5 e 7?

**Esercizio 3.1.7.** Quanti sono i numeri tra 1 e 1000 che non sono divisibili né per 5, né per 6 né per 8?

**Esercizio 3.1.8.** Un parallelepipedo di legno misura  $5 \times 7 \times 7$  centimetri ed è dipinto di blu sulla superficie esterna. Se viene suddiviso in 245 cubetti di 1 centimetro di lato ciascuno, quanti di questi avranno almeno una faccia dipinta di blu?

## 3.2 Il principio di moltiplicazione

Il principio che ora viene illustrato è di uso molto frequente ed è già stato anticipato nel Capitolo 1.

**3.2.1. Principio di moltiplicazione.** Siano  $S$  e  $T$  insiemi finiti. Allora:

$$|S \times T| = |S| \cdot |T|.$$

*Dimostrazione.* Siano  $S = \{x_1, \dots, x_n\}$  e  $T = \{y_1, \dots, y_m\}$ , con  $|S| = n$  e  $|T| = m$ . Risulta

$$\begin{aligned} S \times T &= \{(x_1, y_1), \dots, (x_1, y_m), (x_2, y_1), \dots \\ &\quad \dots, (x_2, y_m), \dots, (x_n, y_1), \dots, (x_n, y_m)\}, \end{aligned}$$

dove gli elementi descritti sono a due a due distinti (vedi (1.5.1)). Pertanto

$$|S \times T| = \underbrace{m + \cdots + m}_{n \text{ volte}} = n \cdot m = |S| \cdot |T|.$$

Ciò prova l'asserto.  $\square$

**3.2.2. Principio di moltiplicazione (forma generale).** Siano  $S_1, \dots, S_k$  insiemi finiti, con  $k \geq 2$ . Si ha:

$$|S_1 \times \cdots \times S_k| = |S_1| \cdot \cdots \cdot |S_k|.$$

*Dimostrazione.* Esercizio.  $\square$

**Osservazione.** Il principio di moltiplicazione ha la seguente efficace interpretazione: siano  $E_1, \dots, E_k$  eventi indipendenti tali che per  $E_1$  ci siano  $n_1$  possibilità, per  $E_2$  ci siano  $n_2$  possibilità, ..., per  $E_k$  ci siano  $n_k$  possibilità. Allora il numero di possibilità per la sequenza  $E_1 E_2 \dots E_k$  è dato da  $n_1 n_2 \dots n_k$ .

Tra le numerose applicazioni del principio di moltiplicazione notevoli sono le seguenti.

**3.2.3.** Sia  $S$  un insieme finito. L'insieme  $\mathcal{P}(S)$  delle parti di  $S$  ha ordine  $2^{|S|}$ .

*Dimostrazione.* Sia  $S = \{x_1, \dots, x_n\}$ , con  $|S| = n$ . Per individuare tutti i sottinsiemi  $X$  di  $S$  vanno considerati gli  $n$  eventi  $E_i$ ,  $i \in \{1, \dots, n\}$ , ciascuno determinato dall'appartenere o non appartenere  $x_i$  a  $X$ . Per ciascun evento  $E_i$  ci sono 2 possibilità, sicché  $|\mathcal{P}(S)| = \underbrace{2 \cdot \cdots \cdot 2}_{n \text{ volte}} = 2^n = 2^{|S|}$ .  $\square$

**3.2.4.** Siano  $S$  e  $T$  insiemi finiti. Allora l'insieme  $T^S$  delle applicazioni di  $S$  in  $T$  ha ordine  $|T|^{|S|}$ .

*Dimostrazione.* Siano  $S = \{x_1, \dots, x_n\}$  e  $T = \{y_1, \dots, y_m\}$ , con  $|S| = n$  e  $|T| = m$ . Per descrivere la generica applicazione  $f : S \rightarrow T$  è necessario determinare  $f(x_1), \dots, f(x_n)$ ; ogni  $f(x_i)$  può essere uno qualunque degli elementi di  $T$ , sicché per  $f(x_i)$  ci sono  $m$  possibilità. Pertanto

$$|T^S| = \underbrace{|T| \cdot \cdots \cdot |T|}_{n \text{ volte}} = |T|^n = |T|^{|S|}.$$

Ciò prova l'asserto.  $\square$

## Esercizi

**Esercizio 3.2.1.** Si dimostri 3.2.2.

**Esercizio 3.2.2.** Quante parole di 3 lettere, non necessariamente di senso compiuto, si possono scrivere con le lettere dell’alfabeto italiano?

**Esercizio 3.2.3.** Quanti numeri naturali (in forma decimale) sono composti da 3 cifre, tutte distinte da 0, 1, 3 e 5?

**Esercizio 3.2.4.** Avendo a disposizione 7 colori distinti, e volendo dipingere una stellina e un fiorellino, il piccolo Marco quante possibilità ha?

**Esercizio 3.2.5.** Matilde vuole abbinare i suoi nuovi pantaloni con uno dei suoi maglioni e con una delle sue camicette. Ha maglioni uno nero, uno turchese, uno viola, uno verde, uno giallo, uno bianco, e camicette una bianca, una gialla, una azzurra, una lilla. In quanti modi può fare l’abbinamento?

**Esercizio 3.2.6.** Nel ristorante di Betty viene proposto un menu turistico composto di primo, secondo e contorno, con 4 scelte per il primo, 2 per il secondo e 5 per il contorno. I componenti un gruppo di giapponesi sono riusciti a ordinare ciascuno un pranzo diverso. Da quante persone al più è composto il gruppo?

## 3.3 Il principio dei cassetti

Il principio dei cassetti, enunciato per la prima volta da Dirichlet nel 1834, e noto anche come “pigeonhole principle” (principio delle casette dei piccioni), o come “principio delle scatole di Dirichlet”, formalizza una proprietà molto evidente:

**3.3.1. Principio dei cassetti.** Siano  $m$  e  $n$  numeri naturali positivi, con  $m > n$ . Se si vogliono riporre  $m$  oggetti in  $n$  scatole, almeno una scatola deve contenere più di un oggetto.

*Dimostrazione.* Se ogni scatola contenesse al più un oggetto, il numero totale degli oggetti riposti sarebbe al più  $n$ , contro l’essere  $m > n$  il numero degli oggetti considerati. □

Il principio dei cassetti, così intuitivo, ha molte applicazioni, come mostrano gli esempi che seguono.

**3.3.2. Esempio.** In una classe composta da  $m = 27$  studenti, almeno due hanno il cognome che inizia con la stessa lettera dell’alfabeto inglese. Infatti le lettere dell’alfabeto inglese sono  $n = 26$ ; se si considerano  $n$  scatole, contrassegnate ciascuna con una delle lettere dell’alfabeto, e in ogni scatola si pone un bigliettino con il cognome di ciascuno studente iniziante con la lettera che contrassegna la scatola, per il principio dei cassetti almeno una scatola dovrà contenere 2 bigliettini.

**3.3.3. Esempio.** Se a una festa partecipano  $n$  persone che si stringono eventualmente la mano, con l'abitudine di non stringere più volte la stessa mano né stringere la propria, allora almeno due di queste persone stringeranno lo stesso numero di mani. Infatti, considerate  $n$  scatole, contrassegnate con  $0, 1, \dots, n-1$ , all'interno della scatola contrassegnata con il numero  $i$  si ponga un bigliettino con il nome di chi ha stretto  $i$  mani ( $0 \leq i \leq n-1$ ). Non può succedere che ciascuna scatola contenga un sol biglietto, altrimenti esisterebbe un signor  $x$  che ha stretto 0 mani e un signor  $y$  che ne ha strette  $n-1$ , dunque tutte le possibili, e quindi anche quella del signor  $x$ . Pertanto in una delle scatole ci sono i nomi di due diverse persone, come volevasi.

**3.3.4. Esempio.** Considerati 101 numeri naturali positivi distinti  $a_1, \dots, a_{101}$  tra 1 e 200, esistono tra questi  $b$  e  $c$  distinti tali che  $b$  divide  $c$  o  $c$  divide  $b$ . Infatti, se  $x$  è un numero naturale qualsiasi, si può scrivere, e in unico modo,  $x$  come  $2^k h$ , con  $k \geq 0$  e  $h$  dispari. Se  $1 \leq x \leq 200$ , ovviamente  $h$  appartiene all'insieme  $T = \{1, 3, 5, \dots, 199\}$ , e  $|T| = 100$ . Considerato allora l'insieme  $V$  costituito dai 101 elementi  $a_1, \dots, a_{101}$ , si ha che esistono  $b, c \in V$ ,  $b \neq c$ , con  $b = 2^i w$ ,  $c = 2^j w$ , con  $i, j \geq 0$  e  $w$  opportuno elemento di  $T$ . Se  $i \leq j$ , allora  $b$  divide  $c$ ; supposto invece  $i \geq j$ , si ha che  $c$  divide  $b$ .

**3.3.5. Esempio.** Siano  $a_1, a_2, \dots, a_{10}$  numeri naturali positivi a due a due distinti, tutti strettamente minori di 107. Esistono allora insiemi disgiunti

$$\{b_1, \dots, b_t\}, \{c_1, \dots, c_s\} \subseteq \{a_1, \dots, a_{10}\}$$

tali che  $b_1 + \dots + b_t = c_1 + \dots + c_s$ , ( $t, s \geq 1$ ). Infatti, ovviamente si ha  $a_1 + \dots + a_{10} \leq 1015$ , in quanto il massimo valore che possono assumere  $a_1, \dots, a_{10}$  è 97, 98, ..., 106, la cui somma è appunto 1015. I sottoinsiemi  $X$  di  $S = \{a_1, \dots, a_{10}\}$  sono  $2^{10} = 1024$  (vedi 3.2.3), e, se  $X = \{d_1, \dots, d_l\}$ , si ha  $1 \leq d_1 + \dots + d_l \leq 1015$ . Pertanto esistono  $Y, V \subseteq S$ ,  $Y \neq V$ , con  $Y = \{b_1, \dots, b_t\}$ ,  $V = \{c_1, \dots, c_s\}$ , tali che  $b_1 + \dots + b_t = c_1 + \dots + c_s$ . Se  $w \in Y \cap V$ , si verifica facilmente che le proprietà prima enunciate sono soddisfatte anche dagli insiemi  $Y \setminus \{w\}$  e  $V \setminus \{w\}$ . Così procedendo si ottengono insiemi soddisfacenti le proprietà richieste.

Volendo essere un po' più formali, il principio dei cassetti afferma che se  $A$  e  $B$  sono insiemi finiti con  $|A| > |B|$ , allora non esistono applicazioni iniettive di  $A$  in  $B$ . Più in generale sussiste:

**3.3.6. Principio dei cassetti (forma forte).** *Sia  $n$  un numero naturale positivo e si considerino numeri naturali  $q_1, \dots, q_n \geq 2$ . Si ponga  $k := q_1 + \dots + q_n - n + 1$ . Se  $k$  oggetti sono ripartiti in  $n$  scatole, allora o la prima contiene almeno  $q_1$  oggetti, o la seconda almeno  $q_2$  oggetti, ..., o la  $n$ -ma almeno  $q_n$  oggetti.*

*Dimostrazione.* Si dicono  $a_1$  il numero degli oggetti riposti nella prima scatola,  $a_2$  il numero degli oggetti riposti nella seconda scatola, ...,  $a_n$  il numero degli

oggetti riposti nella  $n$ -ma scatola. Per assurdo si abbia  $a_1 < q_1, a_2 < q_2, \dots, a_n < q_n$ , cioè  $a_1 \leq q_1 - 1, a_2 \leq q_2 - 1, \dots, a_n \leq q_n - 1$ . Allora si ottiene  $k = a_1 + \dots + a_n \leq (q_1 - 1) + (q_2 - 1) + \dots + (q_n - 1) = q_1 + q_2 + \dots + q_n - n$ , assurdo.  $\square$

**3.3.7. Corollario.** *Siano  $n$  e  $r$  numeri naturali con  $n \geq 1$  e  $r \geq 2$ . Se  $n(r-1)+1$  oggetti sono ripartiti in  $n$  scatole, allora almeno una delle scatole contiene  $r$  o più oggetti.*

*Dimostrazione.* Basta porre, in 3.3.6,  $q_1 = q_2 = \dots = q_n = r$ .  $\square$

**3.3.8. Esempio.** Si abbiano a disposizione mele, banane e arance, e si voglia riempire un cesto in modo che in esso ci siano sicuramente almeno 8 mele o 6 banane o 9 arance. Allora il numero minimo dei frutti da riporre nel cesto è 21. Infatti, con le notazioni di 3.3.6 si ha ora  $n = 3, q_1 = 8, q_2 = 6, q_3 = 9$ , sicché il numero cercato è dato da  $q_1 + q_2 + q_3 - n + 1 = 8 + 6 + 9 - 3 + 1 = 21$ .

## Esercizi

**Esercizio 3.3.1.** *In una foresta ci sono un milione di alberi, ogni albero ha al più 600000 foglie. Si provi che in ogni istante ci sono due alberi che hanno esattamente lo stesso numero di foglie.*

**Esercizio 3.3.2.** *In una classe vi sono 25 studenti. Ad una esercitazione ciascuno prende 30 o 28 o 27. Si provi che esistono almeno 9 studenti che prendono lo stesso voto.*

**Esercizio 3.3.3.** *Siano  $S$  e  $T$  insiemi finiti non vuoti. Si utilizzi il principio dei cassetti per provare la proposizione seguente, già enunciata nel Capitolo 2 (vedi 2.2.8):*

$$\exists f : S \longrightarrow T \text{ iniettiva} \implies |S| \leq |T|.$$

**Esercizio 3.3.4.** *Si provi che in un gruppo di 13 persone, ve ne sono due che hanno il compleanno nello stesso mese.*

**Esercizio 3.3.5.** *Sia  $n$  un numero naturale positivo e si fissino  $a_1, a_2, \dots, a_n \in \mathbb{N}$ , a due a due distinti. Si provi che esiste un sottoinsieme di  $\{a_1, \dots, a_n\}$  in cui la somma degli elementi è divisibile per  $n$ .*

*Svolgimento.* Si denoti innanzitutto con  $\text{rest}(a, n)$  il resto della divisione di  $a$  per  $n$ : si ha  $0 \leq \text{rest}(a, n) < n$ , e ovviamente  $a$  è divisibile per  $n$  se e solo se  $\text{rest}(a, n) = 0$ . Si considerino gli  $n$  numeri:

$$a_1, a_1 + a_2, \dots, a_1 + a_2 + \dots + a_n,$$

e i resti della divisione di ciascuno di essi per  $n$ :

$$\text{rest}(a_1, n), \text{rest}(a_1 + a_2, n), \dots, \text{rest}(a_1 + a_2 + \dots + a_n, n).$$

Se uno di questi resti è 0, l'asserto è provato. In caso contrario, esistono  $s$  e  $t$  distinti,  $s < t$ , tali che  $\text{rest}(a_1 + \dots + a_s, n) = h = \text{rest}(a_1 + \dots + a_t, n)$ . Si ha allora  $a_1 + \dots + a_s = nq + h$  e  $a_1 + \dots + a_t = nq' + h$ , per opportuni  $q, q' \geq 0$ . Pertanto  $a_{s+1} + \dots + a_t = (a_1 + \dots + a_t) - (a_1 + \dots + a_s) = (nq + h) - (nq' + h) = n(q - q')$ , e l'insieme  $\{a_{s+1}, \dots, a_t\}$  soddisfa le proprietà richieste.

**Esercizio 3.3.6.** Considerati 30 numeri naturali, si provi che almeno due di essi hanno la differenza multiplo di 12.

### 3.4 Permutazioni semplici e con ripetizioni

Sia  $n$  un numero naturale positivo. Il prodotto  $1 \cdot 2 \cdot \dots \cdot n$  viene anche detto il **fattoriale** di  $n$  e denotato col simbolo  $n!$ . Si ha cioè:

$$n! := 1 \cdot 2 \cdot \dots \cdot n.$$

Si pone inoltre  $0! := 1$ .

Si noti che ciò equivale a porre, con  $n \in \mathbb{N}_0$ ,  $0! = 1$  e, induttivamente,  $(n+1)! = n!(n+1)$ .

**3.4.1. Esempio.** Si ha:  $1! = 1, 2! = 2, 3! = 6, 4! = 24, 5! = 120$ .

Sia ora  $X$  un insieme. Un'applicazione biettiva di  $X$  in  $X$  è detta una **permutazione** (o **sostituzione**) di  $X$ . L'insieme delle permutazioni di  $X$  è di solito denotato con il simbolo  $\mathbb{S}_X$ :

$$\mathbb{S}_X := \{f : f \text{ permutazione di } X\}.$$

**3.4.2. Sia  $X$  un insieme finito. Se  $|X| = n$ , si ha  $|\mathbb{S}_X| = n!$**

*Dimostrazione.* L'asserto è ovvio quando  $n = 0$  o  $n = 1$ . Sia ora  $n > 1$  e si ponga  $X = \{x_1, \dots, x_n\}$ . Definire un'applicazione iniettiva e quindi biettiva (vedi 2.2.10) di  $X$  in  $X$  equivale a precisare gli elementi  $f(x_1), \dots, f(x_n)$  a due a due distinti. L'immagine  $f(x_1)$  può essere un qualunque elemento di  $X$ , l'immagine  $f(x_2)$  un qualunque elemento di  $X \setminus \{f(x_1)\}$ , l'immagine  $f(x_3)$  un qualunque elemento di  $X \setminus \{f(x_1), f(x_2)\}$ , e così via, l'immagine  $f(x_n)$  è allora necessariamente l'unico elemento di  $X \setminus \{f(x_1), \dots, f(x_{n-1})\}$ . Pertanto  $f$  può essere definita in  $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1$  modi, sicché  $|\mathbb{S}_X| = n!$ , come volevasi.  $\square$

**3.4.3. Esempio.** Le permutazioni di un qualunque insieme di ordine 2 sono 2, di ordine 3 sono 6, di ordine 4 sono 24.

**3.4.4. Esempio.** Volendo contare in quanti modi si possono allineare 3 dischetti di diverso colore, basta determinare il numero delle permutazioni di un insieme di ordine 3; pertanto ci sono 6 possibilità.

**3.4.5. Siano  $X$  e  $Y$  insiemi e sia  $\varphi : X \rightarrow Y$  un'applicazione biettiva. Allora esiste un'applicazione biettiva di  $\mathbb{S}_X$  in  $\mathbb{S}_Y$ .**

*Dimostrazione.* Esercizio. □

La proprietà precedente giustifica il simbolo  $\mathbb{S}_n$  che a volte è usato per denotare l'insieme delle permutazioni di un qualunque insieme finito di ordine  $n$ .

Si considerino ora  $k$  oggetti  $a_1, a_2, \dots, a_k$  a due a due distinti ( $k \geq 1$ ), sia  $n = n_1 + n_2 + \dots + n_k$ , con ogni  $n_i \geq 1$ , e siano  $b_1, \dots, b_n$  tali che  $n_1$  di essi coincidono con  $a_1$ ,  $n_2$  coincidono con  $a_2, \dots, n_k$  coincidono con  $a_k$ . Una  $n$ -upla  $(b_1, \dots, b_n)$  in cui  $a_1$  compare  $n_1$  volte,  $a_2$  compare  $n_2$  volte,  $\dots$ ,  $a_k$  compare  $n_k$  volte, è denotata anche col simbolo  $b_1 \dots b_n$  e detta una **permutazione con ripetizioni** dei  $k$  oggetti  $a_1, \dots, a_k$ , in cui  $a_1$  si ripete  $n_1$  volte,  $\dots$ ,  $a_k$  si ripete  $n_k$  volte.

**3.4.6. Esempio.** 1131733739 è una permutazione con ripetizioni dei 4 numeri 1, 3, 7, 9, in cui 1 si ripete 3 volte, 3 si ripete 4 volte, 7 si ripete 2 volte, 9 si ripete 1 volta.

**3.4.7. Siano  $k, n_1, \dots, n_k$  naturali positivi e si ponga  $n = n_1 + \dots + n_k$ . Il numero delle permutazioni con ripetizioni dei  $k$  oggetti  $a_1, \dots, a_k$ , in cui  $a_1$  si ripete  $n_1$  volte,  $\dots$ ,  $a_k$  si ripete  $n_k$  volte è dato da:**

$$\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}.$$

*Dimostrazione.* Le  $n$ -uple costituite da  $n$  elementi distinti sono  $n!$ . Se invece  $n_1$  delle coordinate sono tutte uguali a uno stesso  $a_1$ , le  $n$ -uple distinte sono  $\frac{n!}{n_1!}$ , in quanto una qualunque permutazione delle coordinate uguali ad  $a_1$  determina la stessa  $n$ -upla. Così continuando si ottiene l'asserto. □

**3.4.8. Esempio.** Con riferimento all'Esempio 3.4.6, le permutazioni con ripetizioni dei 4 numeri 1, 3, 7, 9, in cui 1 si ripete 3 volte, 3 si ripete 4 volte, 7 si ripete 2 volte, 9 si ripete 1 volta sono in numero di  $\frac{10!}{3!4!2!1!} = 12600$ .

**3.4.9. Esempio.** Il numero delle parole distinte (non necessariamente di senso compiuto) di 7 lettere ottenute utilizzando le lettere della parola NONNINO è data da  $\frac{7!}{4!2!} = \frac{7 \cdot 6 \cdot 5}{2 \cdot 1} = 105$ .

**3.4.10. Esempio.** Si vogliano disporre dal basso verso l'alto 13 dischi di cui 5 rossi, 6 azzurri e 2 bianchi. Il numero dei possibili modi distinti in cui farlo è:  $\frac{13!}{5!6!2!} = 36.036$ .

## Esercizi

**Esercizio 3.4.1.** *Si dimostri 3.4.5.*

*Suggerimento.* Si consideri l'applicazione

$$\psi : f \in \mathbb{S}_X \longmapsto \varphi \circ f \circ \varphi^{-1} \in \mathbb{S}_Y$$

e si provi che  $\psi$  è biettiva.

**Esercizio 3.4.2.** *La porta di una cassaforte si apre azionando 4 dispositivi, in un ordine particolare. Dopo quanti distinti tentativi si è sicuri di aprire la cassaforte?*

**Esercizio 3.4.3.** *Quanti numeri naturali sono scritti (in forma decimale) con le cifre 2, 3, 5, 6, 7 che compaiono tutte e una volta sola?*

**Esercizio 3.4.4.** *Un tenore, in un recital, ha deciso di cantare “Nessun dorma”, “La donna è mobile”, “Una furtiva lacrima”, “E lucevan le stelle”, “Recondita armonia”. In quanti modi può approntare la “scaletta” della sua esibizione?*

**Esercizio 3.4.5.** *Rosaria vuole collocare sul suo ampio divano, da sinistra verso destra, gli 8 cuscini colorati che le sono stati regalati. Di questi 3 sono a fiori, 2 in tinta unita, 2 a righe e 1 a pois. In quanti modi diversi può disporli?*

**Esercizio 3.4.6.** *Fiammetta sta disponendo nel suo zaino, dal basso verso l'alto, i suoi quaderni: ne ha 4 a righe, 3 a quadretti, 2 per stenografare. In quanti modi diversi può disporli?*

**Esercizio 3.4.7.** *Si calcolino il numero  $a$  e  $b$ , rispettivamente, delle parole, non necessariamente di senso compiuto, che si possono formare con le lettere della parola “ZANZARA” e della parola “NINNANANNA”.*

**Esercizio 3.4.8.** *Mario vuole disporre i suoi barattoli di vernice sulla mensola, da sinistra verso destra: ne ha 3 identici di vernice verde, 4 identici di vernice rossa, 2 di gialla e 1 di nera. Quante diverse alternanze di colori può ottenere?*

**Esercizio 3.4.9.** *Mariangela sa che domani ha lezione di matematica, italiano, scienze, inglese e disegno, ma non ricorda in che ordine. Allora prova a indovinare: ha una probabilità su quante di individuare l'esatta successione delle lezioni?*

**Esercizio 3.4.10.** *Lucio, Rodolfo, Andrea e Giacomo si sfidano a un torneo di carte. Ogni partita finisce con un risultato diverso; qual è al più il numero di partite giocate?*

### 3.5 Disposizioni semplici e con ripetizioni

Siano  $n$  e  $h$  numeri naturali positivi. Il simbolo  $d_{n,h}$  definito con la seguente posizione:

$$d_{n,h} := \begin{cases} 0 & \text{se } h > n \\ n(n-1)\dots(n-(h-1)) & \text{se } h \leq n \end{cases}$$

è detto il numero delle **disposizioni** di  $n$  elementi su  $h$  posti.

Quindi, per  $h \leq n$ , il numero

$$d_{n,h} = n(n-1)\dots(n-h+1)$$

è ottenuto moltiplicando tra loro i primi  $h$  numeri, presi in ordine decrescente, a partire da  $n$ . Si noti che, se  $h \leq n$ , si ha:

$$d_{n,h} = \frac{n!}{(n-h)!}.$$

Il principio di moltiplicazione assicura che:

**3.5.1. Il numero delle applicazioni iniettive di un insieme di ordine  $h$  in un insieme di ordine  $n$ , con  $h, n > 0$ , è  $d_{n,h}$ .**

**Dimostrazione.** Siano  $S$  e  $T$  insiemi,  $S = \{x_1, \dots, x_h\}$ ,  $T = \{y_1, \dots, y_n\}$ , con  $|S| = h$  e  $|T| = n$ . Se si ha  $h > n$ , non esistono (vedi 2.2.8) applicazioni iniettive di  $S$  in  $T$ , e dunque il loro numero è  $0 = d_{n,h}$ . Si supponga allora  $h \leq n$ . Per assegnare un'applicazione iniettiva  $f$  di  $S$  in  $T$ , occorre precisare le immagini  $f(x_1), \dots, f(x_h)$  e queste devono essere elementi a due a due distinti di  $T$ . Per  $f(x_1)$  ci sono allora  $n$  possibilità, per  $f(x_2)$  ci sono  $n - 1$  possibilità, ..., per  $f(x_h)$  ci sono  $n - (h - 1) = n - h + 1$  possibilità e quindi il numero complessivo è dato da  $n(n-1)\dots(n-h+1) = d_{n,h}$ .  $\square$

La proposizione precedente giustifica la nomenclatura usata per  $d_{n,h}$  in quanto assegnare un'applicazione iniettiva di  $S$  in  $T$ , con le notazioni precedenti, vuol dire disporre  $h$  degli  $n$  elementi di  $T$  (che corrispondono a  $f(x_1), \dots, f(x_h)$ ) negli  $h$  "posti"  $1, 2, \dots, h$ .

Si noti che in tali considerazioni l'ordine è essenziale e che gli  $h$  elementi di  $T$  presi in esame sono ovviamente a due a due distinti.

**3.5.2. Esempio.** Il numero delle applicazioni iniettive dell'insieme  $\{a, b, c, d, e\}$  nell'insieme  $\{41, 42, 43, 44, 45, 46, 47, 48\}$  è  $d_{8,5} = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6720$ .

**3.5.3. Esempio.** Le parole, non necessariamente di senso compiuto, che si possono scrivere con 4 lettere distinte scelte nell'insieme  $\{A, C, D, E, I, S, O\}$  sono  $7 \cdot 6 \cdot 5 \cdot 4 = 840$ .

**3.5.4. Esempio.** Al cinodromo Valeria vuole puntare sui primi 4 classificati della prossima corsa, cui partecipano 8 levrieri. Ha una possibilità su 1680 di indovinare l'esatto ordine di arrivo. Infatti si ha  $d_{8,4} = 8 \cdot 7 \cdot 6 \cdot 5 = 1680$ .

Si noti che per  $n = h$  si ha

$$d_{n,n} = n \cdot (n-1) \cdot \dots \cdot (n-n+1) = n \cdot (n-1) \cdot \dots \cdot 1 = n!,$$

e infatti ogni applicazione iniettiva tra insiemi finiti dello stesso ordine è biettiva.

Si noti anche che, come è logico che sia,

$$d_{n,n-1} = n \cdot (n-1) \cdot \dots \cdot (n-(n-1)+1) = n \cdot (n-1) \cdot \dots \cdot 2 = n! = d_{n,n}.$$

Se si vogliono disporre su  $h$  posti oggetti scelti tra  $n$ , permettendo ripetizioni, ciò equivale a definire un'applicazione di un insieme di ordine  $h$  nell'insieme costituito dagli  $n$  oggetti. Il numero di tali applicazioni è  $n^h$ , come osservato nel Paragrafo 3.2. Si ha cioè:

**3.5.5. Il numero delle disposizioni con ripetizioni di  $n$  oggetti su  $h$  posti è  $n^h$ .**

**3.5.6. Esempio.** Il numero dei naturali positivi costituiti da 4 cifre dispari non necessariamente distinte è dato da  $5^4 = 625$ .

## Esercizi

**Esercizio 3.5.1.** Lora ha 5 palline colorate; una rossa, una bianca, una verde, una azzurra, una gialla, e vuole darne una ciascuna a Bianca, Clorinda, Silvana e Claudia. In quanti modi può farlo?

**Esercizio 3.5.2.** Il giovane cameriere Salvo è alle prese con i bicchieri: ha davanti a sé 6 bicchieri diversi e sa solo che ne deve porre 4 sul tavolo, ma non ricorda quali, e in che posizione. Procedendo a caso, ha una probabilità su quante di apparecchiare bene la tavola?

**Esercizio 3.5.3.** Nella borsa di Giovanna ci sono 3 tasche, una sul davanti, una interna e una sul retro, e in ciascuna c'è spazio solo per un oggetto. Giovanna vorrebbe riporre il rossetto, le chiavi, l'agendina, il cellulare, il portafoglio, il portamonete e la penna. In quanti modi distinti può riporre 3 di questi oggetti?

**Esercizio 3.5.4.** Quanti numeri naturali (in forma decimale) sono composti da 3 cifre, tutte distinte da 0, 1, 3 e 5?

**Esercizio 3.5.5.** Stefano ricorda solo che il suo numero di Bancomat è formato da 5 cifre, e che tra esse non compaiono né 0 né 5 né 9. Digitando a caso, ha una probabilità su quante di indovinare il numero giusto?

### 3.6 Combinazioni semplici e con ripetizioni

Siano  $n$  e  $h$  numeri naturali, con  $0 < h \leq n$ . Il numero

$$c_{n,h} := \frac{d_{n,h}}{h!} = \frac{n(n-1)\dots(n-h+1)}{h!}$$

è detto il numero delle **combinazioni semplici** di  $n$  elementi ad  $h$  ad  $h$ .

Si pone inoltre, per ogni  $n \in \mathbb{N}_0$ :

$$c_{n,0} := 1.$$

Per esempio:

$$\begin{aligned} c_{7,0} &= 1 = c_{7,7}, \\ c_{7,1} &= \frac{7}{1!} = 7 = c_{7,6}, \\ c_{7,2} &= \frac{7 \cdot 6}{2!} = 21 = c_{7,5}, \\ c_{7,3} &= \frac{7 \cdot 6 \cdot 5}{3!} = 35 = c_{7,4}. \end{aligned}$$

Si noti che

$$c_{n,n} = \frac{n!}{n!} = 1 = c_{n,0},$$

e che, con  $0 < h \leq n$ ,

$$c_{n,h} = \frac{d_{n,h}}{h!} = \frac{\frac{n!}{(n-h)!}}{h!} = \frac{n!}{h!(n-h)!},$$

e dunque

$$c_{n,h} = c_{n,n-h}.$$

Il numero  $c_{n,h}$  è sempre un intero come per esempio segue da:

**3.6.1.** Se  $n$  e  $h$  sono numeri interi, con  $0 \leq h \leq n$ , il numero dei sottoinsiemi di ordine  $h$  di un insieme di ordine  $n$  è  $c_{n,h}$ .

*Dimostrazione.* L'asserto è ovvio se  $n = 0$  o  $h = 0$ . Siano dunque  $0 < h \leq n$  e  $S = \{x_1, \dots, x_n\}$  un insieme di ordine  $n$ . Per individuare un sottoinsieme  $\{y_1, \dots, y_h\}$  di ordine  $h$  di  $S$  si può procedere come segue: fissare  $y_1$ , scegliere poi  $y_2$  in  $S \setminus \{y_1\}$ , ..., scegliere  $y_h$  in  $S \setminus \{y_1, \dots, y_{h-1}\}$ ; l'elemento  $y_1$  può essere scelto in  $n$  modi,  $y_2$  in  $n - 1$  modi, ...,  $y_h$  in  $n - (h - 1)$  modi. Così procedendo però ogni sottoinsieme  $\{y_1, \dots, y_h\}$  si ripresenta tante volte quanto è il numero delle permutazioni di  $h$  elementi, cioè  $h!$  volte. Pertanto il numero cercato è  $\frac{d_{n,h}}{h!}$ .  $\square$

La proposizione precedente giustifica il termine utilizzato per il simbolo  $c_{n,h}$ : individuare un sottoinsieme di ordine  $h$  di un insieme di ordine  $n$  equivale infatti a scegliere  $h$  elementi tra  $n$ , indipendentemente dal loro ordine.

Si ritrova così che  $c_{n,h} = c_{n,n-h}$ : individuare un sottoinsieme di ordine  $h$  di un insieme di ordine  $n$  equivale a determinare il suo complementare che è un insieme di ordine  $n - h$ .

**3.6.2. Esempio.** I terni che si possono giocare al Lotto sono quanti le combinazioni di 90 elementi a 3 a 3, ossia  $c_{90,3} = \frac{90 \cdot 89 \cdot 88}{3!} = 117480$ .

**3.6.3. Esempio.** Considerati una rosa, una margherita, un'orchidea, una violetta, una gardenia, un garofano e un iris, il numero dei distinti bouquet che si possono fare con 5 di questi fiori è  $c_{7,5} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3}{5!} = 21 = c_{7,2}$ .

A volte, invece di utilizzare il simbolo  $c_{n,h}$ , si usa il simbolo  $\binom{n}{h}$  detto *coefficiente binomiale*  $n$  su  $h$ . Pertanto:

$$\binom{n}{h} = \frac{n(n-1)\dots(n-h+1)}{h!} = \frac{n!}{h!(n-h)!}.$$

Per esempio:

$$\binom{n}{n} = 1 = \binom{n}{0}, \quad \binom{n}{1} = n = \binom{n}{n-1},$$

e, più in generale,

$$\binom{n}{h} = \binom{n}{n-h}, \text{ per ogni } 0 \leq h \leq n.$$

Si ha inoltre:

**3.6.4.** Per ogni  $0 < h \leq n$ , risulta:

$$\binom{n}{h-1} + \binom{n}{h} = \binom{n+1}{h}.$$

*Dimostrazione.* Esercizio. □

La precedente nomenclatura è giustificata dal seguente risultato:

**3.6.5. Formula del binomio (o di Newton).** Siano  $a$  e  $b$  numeri reali, e sia  $n$  un numero naturale. Si ha:

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

*Dimostrazione.* L'asserto è banale se  $n = 0$  e evidente se  $n = 1$ , infatti

$$(a+b)^1 = a+b = \binom{1}{0}ab^0 + \binom{1}{1}a^0b.$$

Per induzione su  $n$  si assuma

$$\begin{aligned}(a+b)^m &= \sum_{i=0}^m \binom{m}{i} a^{m-i} b^i \\ &= a^m + \binom{m}{1} a^{m-1} b + \cdots + \binom{m}{m-1} a b^{m-1} + b^m.\end{aligned}$$

Si ha allora:

$$\begin{aligned}(a+b)^{m+1} &= (a+b)^m(a+b) \\ &= \left[ a^m + \binom{m}{1} a^{m-1} b + \cdots + \binom{m}{m-1} a b^{m-1} + b^m \right] (a+b) \\ &= a^{m+1} + \binom{m}{1} a^m b + \cdots + \binom{m}{m-1} a^2 b^{m-1} + a b^m + \\ &\quad + a^m b + \binom{m}{1} a^{m-1} b^2 + \cdots + \binom{m}{m-1} a b^m + b^{m+1} \\ &= a^{m+1} + \left[ \binom{m}{1} + \binom{m}{0} \right] a^m b + \left[ \binom{m}{2} + \binom{m}{1} \right] a^{m-1} b^2 + \\ &\quad + \cdots + \left[ \binom{m}{m-1} + \binom{m}{m-2} \right] a^2 b^{m-1} + \\ &\quad + \left[ \binom{m}{m} + \binom{m}{m-1} \right] a b^m + b^{m+1} \\ &= a^{m+1} + \binom{m+1}{1} a^m b + \cdots + \binom{m+1}{m} a b^m + b^{m+1} \\ &= \sum_{i=0}^{m+1} \binom{m+1}{i} a^{(m+1)-i} b^i,\end{aligned}$$

come richiesto.  $\square$

### 3.6.6. Esempio.

$$\begin{aligned}(a+b)^2 &= \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2 = a^2 + 2ab + b^2, \\ (a+b)^3 &= \binom{3}{0} a^3 b^0 + \binom{3}{1} a^2 b^1 + \binom{3}{2} a^1 b^2 + \binom{3}{3} a^0 b^3 \\ &= a^3 + 3a^2 b + 3ab^2 + b^3.\end{aligned}$$

Si osservi che i coefficienti binomiali che compaiono nello sviluppo di  $(a + b)^n$  costituiscono l' $n$ -esima riga del ben noto *Triangolo di Tartaglia*, le cui prime righe sono:

$$\begin{array}{ccccc} & 1 & & 1 & \\ & 1 & 2 & 1 & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array}$$

che ovviamente coincidono con

$$\begin{array}{ccccc} \binom{1}{0} & & \binom{1}{1} & & \\ \binom{2}{0} & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & & \binom{3}{3} \\ \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \end{array}$$

ottenute utilizzando 3.6.4.

**3.6.7.** *Sia  $n$  un intero non negativo. Allora*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n,$$

*ossia la somma degli elementi sulla  $n$ -esima riga del triangolo di Tartaglia è  $2^n$ .*

*Dimostrazione.* Basta porre  $a = b = 1$  nella formula del binomio 3.6.5. □

Tra l'altro, 3.6.1 e 3.6.7 permettono di ritrovare 3.2.3. È poi interessante evidenziare che:

**3.6.8.** *Sia  $p$  un numero primo. Allora  $p$  divide  $\binom{p}{i}$ , per ogni  $i$  tale che  $0 < i < p$ .*

*Dimostrazione.* Basta osservare che  $p$  divide  $p(p - 1) \dots (p - i + 1)$  e non divide  $i!$ . □

Si vuole ora contare in quanti modi è possibile scegliere  $n$  oggetti, non necessariamente distinti, tra  $k$  possibilità.

A tal fine può essere utile rappresentare tali oggetti con stelline e suddividere le possibilità in settori, utilizzando  $k - 1$  sbarrette:

prima possibilità | seconda possibilità | ... |  $k$ -ma possibilità .

Allora ogni scelta determina una sequenza di stelline e sbarrette e, viceversa, ogni siffatta sequenza individua una scelta.

Per esempio, volendo comprare 3 frutti non necessariamente di tipo diverso, e potendo scegliere tra mele, pere, banane, arance e kiwi, si devono collocare 3 stelline nei 5 settori

| | | |

individuati da 4 sbarrette, che corrispondono ordinatamente ai tipi di frutta elencati. Per esempio, la scelta di due mele e un'arancia determina la sequenza

★★| | |★|,

le sequenze

|★|★★| |,  
| | | |★★★|,

individuano, rispettivamente, la scelta di una pera e due banane, e la scelta di tre kiwi.

Vanno quindi contate le permutazioni con ripetizioni degli  $n + k - 1$  oggetti,  $n$  dei quali sono uguali a una stellina, mentre i restanti  $k - 1$  sono sbarrette. Come osservato in 3.4.7 tale numero è

$$\frac{(n+k-1)!}{n!(k-1)!}$$

ed è detto il numero delle *combinazioni con ripetizioni* di  $n$  oggetti tra  $k$ .

Si è così provato che:

### 3.6.9. Il numero delle combinazioni con ripetizioni di $n$ oggetti tra $k$ è

$$\frac{(n+k-1)!}{n!(k-1)!} = c_{n+k-1,n} = c_{n+k-1,k-1}.$$

**3.6.10. Esempio.** Al mercato sono disponibili mele, pere, banane, arance e kiwi. Volendo acquistare 2 frutti, non necessariamente di diverso tipo, si hanno tante possibili scelte quante sono le combinazioni con ripetizioni di 2 oggetti tra 5, ossia

$$\frac{(2+5-1)!}{2!4!} = 15$$

(o anche  $c_{2+5-1,2} = c_{6,2} = \frac{6 \cdot 5}{2} = 15$ ).

Se invece si vogliono comprare 3 frutti, non necessariamente di diverso tipo, la scelta può essere effettuata in tanti modi diversi quante sono le combinazioni con ripetizioni di 3 oggetti tra 5, cioè

$$\frac{(3+5-1)!}{3!4!} = 35$$

(o anche  $c_{3+5-1,3} = c_{7,3} = \frac{7 \cdot 6 \cdot 5}{3!} = 35$ ).

**3.6.11. Esempio.** Al termine di un'esibizione ginnica, ognuno dei 5 componenti la giuria valuta la prova di ciascun atleta con uno dei seguenti giudizi: eccellente, ottimo, buono, discreto, sufficiente, insufficiente. Quanti erano al più gli atleti partecipanti, se non ci sono due di essi che hanno ottenuto lo stesso numero di giudizi di ciascun tipo? Qui ovviamente bisogna contare le combinazioni con ripetizioni di 5 oggetti tra 6, cioè

$$\frac{(5+6-1)!}{5!5!} = 252$$

(o anche  $c_{5+6-1,5} = c_{10,5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5!} = 252$ ).

## Esercizi

**Esercizio 3.6.1.** Si provi 3.6.4.

**Esercizio 3.6.2.** Sia  $p \in \mathbb{P}$ . Si provi che  $p$  divide  $a^p - a$ , per ogni  $a \in \mathbb{N}_0$ .

*Suggerimento.* Si ragioni per induzione su  $a$ , utilizzando la formula del binomio (vedi 3.6.5) e la 3.6.8.

**Esercizio 3.6.3.** Giovanni vuole giocare al Lotto 2 numeri dispari; quante scelte possibili ha?

**Esercizio 3.6.4.** Renato vuole portare in gita con la sua auto Carlo, Franco, Gigi, Enzo, Antonio e Giovanni. In auto c'è posto solo per 4 persone, oltre ovviamente il conducente. In quanti modi può scegliere i suoi amici?

**Esercizio 3.6.5.** Qual è il numero delle combinazioni con ripetizioni di 7 oggetti scelti tra 3?

**Esercizio 3.6.6.** Tony vuole regalare all'amico Paolo 4 dei suoi giornaletti: ne ha uno di Paperino, uno di Topolino, uno di Tex, uno di Diabolik, uno di Mandrake, uno di Nembo Kid. In quanti modi diversi può scegliere i 4 giornaletti da regalare?

**Esercizio 3.6.7.** Rosa sta preparando la borsa per il mare: vuole portare con sé 3 costumi, e può sceglierli tra i 9 che ha nel cassetto. In quanti modi può effettuare la sua scelta?

**Esercizio 3.6.8.** Gloria può cogliere 4 fiori, eventualmente dello stesso tipo, nel giardino del vicino, che è ricco di gardenie, rose, lilium, margherite, garofani e ortensie. Quante scelte diverse può fare?

**Esercizio 3.6.9.** Lola sta preparando delle coppe di gelato per i suoi amici. In ciascuna colloca 4 palline di gelato. Avendo a disposizione solo i gusti cioccolato, caffè e nocciola, quante coppe distinte può preparare?

**Esercizio 3.6.10.** Roberto deve acquistare 12 piastrelle per rivestire un angolo della cucina. Ne ha viste sia alcune di una bella gradazione di grigio sia altre con un simpatico disegno, e non sa se sceglierle tutte uguali, o di tipo diverso. In quanti modi può fare la sua scelta?

**Esercizio 3.6.11.** In un bar sono in vendita paste al cioccolato, alla crema, al caffè, alla panna, alla fragola, alla nocciola, allo zabaione. Dovendo acquistare 3 paste distinte, quante sono le possibili scelte?

**Esercizio 3.6.12.** La giuria di una gara canora è composta da 7 persone. Ognuna di queste valuta la prova di ciascun cantante assegnando uno dei seguenti punteggi: 1000 (eccellente), 100 (ottimo), 10 (buono), 1 (sufficiente), 0 (insufficiente). Se i cantanti ottengono punteggi complessivi a due a due distinti e tutti minori di 7000, quanti sono al massimo i partecipanti alla gara?

## 3.7 I numeri di Stirling di seconda specie

Nel Capitolo 2 si è parlato di partizioni di un insieme. Se  $A$  è un insieme di ordine  $n > 0$  e  $\mathcal{F}$  è una sua partizione, ovviamente si ha  $|\mathcal{F}| = k$ , con  $1 \leq k \leq n$ . Il numero delle partizioni di ordine  $k$  di un insieme di ordine  $n$  è denotato con il simbolo  $S(n, k)$  e detto **numero di Stirling di seconda specie** relativo a  $n$  e  $k$ . Il numero complessivo delle partizioni di un insieme di ordine  $n$  è detto **numero di Bell** relativo a  $n$  e indicato con  $\mathcal{B}_n$ . Ovviamente si ha:

**3.7.1.** Per ogni  $n \geq 1$  risulta:

$$\mathcal{B}_n = \sum_{i=1}^n S(n, i).$$

Dal teorema fondamentale sulle relazioni d'equivalenza (vedi 2.3.6) segue quindi che il numero delle relazioni d'equivalenza di un insieme di ordine  $n$  è  $\mathcal{B}_n$ .

È immediato riscontrare che, per ogni  $n \geq 1$ , si ha:

$$S(n, 1) = 1 = S(n, n),$$

in quanto, se  $|A| = n$ , la partizione  $\{A\}$  è l'unica costituita da un sol elemento e  $\{\{x\} : x \in A\}$  è l'unica avente ordine  $n$ . In particolare:

$$S(1, 1) = 1, \quad S(2, 1) = 1 = S(2, 2).$$

Di facile dimostrazione, ma di notevole interesse è il seguente risultato:

**3.7.2.** Per ogni  $1 < k \leq n$  si ha:

$$S(n+1, k) = S(n, k-1) + kS(n, k).$$

*Dimostrazione.* Sia  $A$  un insieme di ordine  $n+1$ , si vogliono contare le partizioni di  $A$  di ordine  $k$ . Si fissi  $\bar{a} \in A$ , ovviamente l'insieme  $A \setminus \{\bar{a}\}$  ha ordine  $n$ . Se  $\mathcal{F}$  è una partizione di  $A \setminus \{\bar{a}\}$  di ordine  $k-1$ , l'insieme  $\mathcal{F} \cup \{\{\bar{a}\}\}$  è allora una partizione di  $A$  di ordine  $k$ . Si ottengono così  $S(n, k-1)$  partizioni distinte di  $A$  di ordine  $k$ . Sia ora  $\mathcal{G}$  una partizione di  $A \setminus \{\bar{a}\}$  di ordine  $k$  costituita dai sottoinsiemi  $X_1, \dots, X_k$  di  $A \setminus \{\bar{a}\}$ . Da  $\mathcal{G}$  si ottengono  $k$  partizioni distinte di  $A$  di ordine  $k$  sostituendo uno a uno solo degli  $X_i$  ( $i \in \{1, \dots, k\}$ ) con  $X_i \cup \{\bar{a}\}$ :

$$\mathcal{G}_1 = \{X_1 \cup \{\bar{a}\}, X_2, \dots, X_k\}, \dots, \mathcal{G}_k = \{X_1, X_2, \dots, X_k \cup \{\bar{a}\}\}.$$

Al variare di  $\mathcal{G}$  nell'insieme delle partizioni di ordine  $k$  di  $A \setminus \{\bar{a}\}$  si ottengono così  $kS(n, k)$  partizioni distinte di ordine  $k$  di  $A$ . Tali partizioni sono anche ovviamente distinte da quelle ottenute in precedenza a partire da partizioni di ordine  $k-1$  di  $A \setminus \{\bar{a}\}$ .

Restano così individuate  $S(n, k-1) + kS(n, k)$  partizioni di ordine  $k$  di  $A$ . È poi facile riscontrare che sono tutte, in quanto, se  $\mathcal{H}$  è una partizione di  $A$  di ordine  $k$ , si ha  $\{\bar{a}\} \in \mathcal{H}$  o  $\bar{a} \in X$ , con  $X$  elemento di  $\mathcal{H}$  di ordine  $> 1$ .  $\square$

Il risultato precedente permette di costruire facilmente il cosiddetto *triangolo di Stirling* che elenca i valori dei numeri  $S(n, k)$  al crescere di  $n$  e di  $k$ :

$n \setminus k$	1	2	3	4	...
1	$S(1, 1)$				
2	$S(2, 1)$	$S(2, 2)$			
3	$S(3, 1)$	$S(3, 2)$	$S(3, 3)$		
4	$S(4, 1)$	$S(4, 2)$	$S(4, 3)$	$S(4, 4)$	
...	...	...	...	...	...

Infatti, ricordando che  $S(n, 1) = 1 = S(n, n)$ , per ogni  $n$  e utilizzando la 3.7.2, si ottiene

$n \setminus k$	1	2	3	4	...
1	1				
2	1	1			
3	1	3	1		
4	1	7	6	1	
...	...	...	...	...	...

La prima colonna e la diagonale principale della tabella sono costituite da tutti 1, gli altri valori si ottengono sommando il termine a sinistra della riga precedente con il prodotto del termine in alto della riga precedente per il numero della colonna:

$$S(3, 2) = S(2, 1) + 2S(2, 2) = 1 + 2 = 3,$$

$$S(4, 2) = S(3, 1) + 2S(3, 2) = 1 + 2 \cdot 3 = 7,$$

$$S(4, 3) = S(3, 2) + 3S(3, 3) = 3 + 3 \cdot 1 = 6,$$

così la quinta riga del triangolo è:

$$1 \quad 15 \quad 25 \quad 10 \quad 1.$$

**3.7.3. Esempio.** Marianna ha ricevuto per posta i 6 utensili comprati per corrispondenza: un frullatore, uno spremiagrumi, un ferro da stiro, una macchina per caffè, una bistecchiera e un tostapane. Il tutto è contenuto in 4 pacchi identici. In quanti modi diversi possono essere stati ripartiti gli oggetti? I pacchi sono identici e non vuoti, quindi il numero che va calcolato è  $S(6, 4)$ . Si ha

$$S(6, 4) = S(5, 3) + 4 \cdot S(5, 4) = 25 + 4 \cdot 10 = 65.$$

**3.7.4. Esempio.** Alberto ha 2 borse identiche in cui vuole collocare gli 8 fascicoli relativi alle cause a cui sta lavorando. Ogni borsa contiene al più 7 di essi. In quanti modi può ripartirli? Alberto deve utilizzare entrambe le borse, sicché va calcolato

$$S(7, 2) = S(6, 1) + 2S(6, 2) = 1 + 2(S(5, 1) + 2S(5, 2)) = 1 + 2(1 + 2 \cdot 15) = 63.$$

Per determinare una formula che esprima il valore di ogni  $S(n, k)$  è utile e interessante la seguente osservazione:

**3.7.5. Siano  $S$  e  $T$  insiemi finiti, con  $|S| = n$ ,  $|T| = k$  e  $1 \leq k \leq n$ . Il numero delle applicazioni suriettive di  $S$  in  $T$  è**

$$k!S(n, k).$$

*Dimostrazione.* Siano  $S = \{x_1, \dots, x_n\}$  e  $T = \{y_1, \dots, y_k\}$ . Essendo  $k \leq n$ , esistono applicazioni suriettive di  $S$  in  $T$  (vedi 2.2.8). Se  $\mathcal{F} = \{X_1, \dots, X_k\}$  è una partizione di  $S$  di ordine  $k$ , restano individuate  $k!$  distinte applicazioni suriettive di  $S$  in  $T$ : infatti, per ogni permutazione  $\sigma$  di  $\{1, \dots, k\}$ , si può definire l'applicazione

$$f_\sigma : S \longrightarrow T$$

ponendo, se  $x \in X_i$ ,

$$f_\sigma(x) = y_{\sigma(i)}.$$

Tale applicazione ha senso perché ogni  $x \in S$  appartiene a uno e un solo degli  $X_i$ , ed è suriettiva poiché ogni  $X_i$  è non vuoto e  $\{y_{\sigma(i)} : i \in \{1, \dots, k\}\} = T$ . A partire da  $\mathcal{F}$  restano così determinate  $k!$  applicazioni suriettive di  $S$  in  $T$ . Al variare di  $\mathcal{F}$  si ottengono ovviamente applicazioni a due a due distinte. Si individuano pertanto  $k!S(n, k)$  applicazioni suriettive di  $S$  in  $T$ . Sono poi tutte, perché, considerata un'applicazione suriettiva  $g$  di  $S$  in  $T$ , si ha che, per ogni  $i \in \{1, \dots, k\}$ , l'insieme  $g^{-1}(\{y_i\})$  è non vuoto e  $\{X_1 = g^{-1}(\{y_1\}), \dots, X_k = g^{-1}(\{y_k\})\}$  è una partizione  $\mathcal{G}$  di  $S$ , tale che l'applicazione  $f_{\text{id}}$  relativa a  $\mathcal{G}$  coincide con  $g$  (dove  $\text{id}$  denota la permutazione identità di  $\{1, \dots, k\}$ ). È infatti immediato riscontrare che, se  $x$  è un elemento di  $S$  tale che  $x \in X_i = g^{-1}(\{y_i\})$ , si ha  $g(x) = y_i = f_{\text{id}}(x)$ .  $\square$

**3.7.6. Esempio.** Al parco giochi ci sono uno scivolo, una giostra, una costruzione da scalare e un tiro a segno. Luca, Andrea, Marco, Piero, Michele e Gaetano si distribuiscono tra i vari giochi, e nessuno di questi resta deserto. In quanti modi possono essersi distribuiti? I 6 bimbi possono scegliere tra 4 giochi diversi. Visto che nessuno di questi resta deserto, bisogna contare le applicazioni suriettive di un insieme di ordine 6 in un insieme di ordine 4. Il numero cercato è quindi  $4!S(6, 4) = 24 \cdot 65 = 1560$ .

**3.7.7. Esempio.** Monica ha promesso di prestare a ciascuna delle sue amiche Viola, Rosalba e Antonella almeno uno dei suoi CD. A malincuore ha deciso di privarsi per un po' dell'ultimo CD di Baglioni, di Vasco Rossi, di Max Gazzè, di Fiorella Mannoia, di Biagio Antonacci e di Piero Pelù. In quanti modo diversi può distribuire i 6 CD alle 3 amiche? Il numero cercato è  $3!S(6, 3) = 6 \cdot 90 = 540$ .

Si conteranno ora le applicazioni suriettive tra insiemi finiti, determinando così anche i relativi numeri di Stirling di seconda specie.

**3.7.8. Siano  $S$  e  $T$  insiemi finiti,  $|S| = n$ ,  $|T| = k$ , con  $1 \leq k \leq n$ . Il numero delle applicazioni suriettive di  $S$  in  $T$  è dato da:**

$$\sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n.$$

*Dimostrazione.* Sia  $T = \{y_1, \dots, y_k\}$ . Posto

$$V := \{f \in T^S : f \text{ suriettiva}\}, \quad W := \{f \in T^S : f \text{ non suriettiva}\},$$

si ha ovviamente  $V = T^S \setminus W$ , da cui  $|V| = |T^S| - |W|$  (vedi (i) di 3.1.2). Si determinerà ora  $|W|$  utilizzando il principio di inclusione-esclusione. Si considerino gli insiemi:

$$\begin{aligned} C_1 &:= \{f \in T^S : y_1 \notin f(S)\}, \\ C_2 &:= \{f \in T^S : y_2 \notin f(S)\}, \\ &\vdots \\ C_k &:= \{f \in T^S : y_k \notin f(S)\}. \end{aligned}$$

Ovviamente risulta

$$W = C_1 \cup C_2 \cup \dots \cup C_k,$$

e, per ogni  $i \in \{1, \dots, k\}$ , si ha che gli elementi di  $C_i$  sono tanti quante sono le applicazioni di  $S$  in  $T \setminus \{y_i\}$ , sicché (vedi 3.2.4)

$$|C_i| = |(T \setminus \{y_i\})^S| = (k-1)^n.$$

Analogamente, se  $i, j \in \{1, \dots, k\}$ , con  $i \neq j$ , da

$$C_i \cap C_j = \{f \in T^S : y_i, y_j \notin f(S)\}$$

segue che

$$|C_i \cap C_j| = |(T \setminus \{y_i, y_j\})^S| = (k-2)^n,$$

e così

$$|C_i \cap C_j \cap C_s| = (k-3)^n,$$

per ogni  $i, j, s \in \{1, \dots, k\}$  con  $i < j < s$ , e così via fino a

$$|C_1 \cap C_2 \cap \dots \cap C_k| = |(T \setminus \{y_1, \dots, y_k\})^S| = |\emptyset^S| = 0.$$

Applicando il principio di inclusione-esclusione si ottiene:

$$\begin{aligned} |W| &= |C_1 \cup \dots \cup C_k| = \sum_{i=1}^k |C_i| - \sum_{1 \leq i < j \leq k} |C_i \cap C_j| + \\ &\quad + \sum_{1 \leq i < j < s \leq k} |C_i \cap C_j \cap C_s| - \dots + (-1)^{k-1} |C_1 \cap \dots \cap C_k|. \end{aligned}$$

I sottoinsiemi  $C_i$  sono  $k = \binom{k}{1}$ , le intersezioni  $C_i \cap C_j$  con  $1 \leq i < j \leq k$  sono tante quante sono i sottoinsiemi di ordine 2 di  $\{1, \dots, k\}$ , cioè  $\binom{k}{2}$ , così le intersezioni  $C_i \cap C_j \cap C_s$  con  $1 \leq i < j < s \leq k$  sono tante quanti sono i sottoinsiemi di ordine 3 di  $\{1, \dots, k\}$  e dunque sono  $\binom{k}{3}$ , e così via. Pertanto

$$|W| = \binom{k}{1}(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n - \dots + (-1)^{k-1} \binom{k}{k}(k-k)^n.$$

Da  $|T^S| = k^n = \binom{k}{0}(k-0)^n$  segue dunque che

$$\begin{aligned} |V| &= \binom{k}{0}(k-0)^n - \left[ \sum_{i=1}^k (-1)^{i-1} \binom{k}{i} (k-i)^n \right] \\ &= \binom{k}{0}(k-0)^n + \sum_{i=1}^k (-1)^i \binom{k}{i} (k-i)^n \\ &= \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n, \end{aligned}$$

come volevasi. □

Dalle proposizioni precedenti segue dunque:

**3.7.9.** *Sia  $n$  un numero naturale positivo. Allora*

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n$$

per ogni  $1 \leq k \leq n$ , e

$$B_n = \sum_{k=1}^n \left[ \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n \right].$$

**3.7.10. Esempio.** Le applicazioni suriettive di un insieme di ordine 8 in un insieme di ordine 5 sono 126000. Infatti risulta:

$$\begin{aligned} \sum_{i=0}^5 (-1)^i \binom{5}{i} (5-i)^8 &= 5^8 - \binom{5}{1} 4^8 + \binom{5}{2} 3^8 - \binom{5}{3} 2^8 + \binom{5}{4} 1^8 \\ &= 5^8 - 5 \cdot 4^8 + 10 \cdot 3^8 - 10 \cdot 2^8 + 5 \cdot 1 \\ &= 390625 - 5 \cdot 65536 + 10 \cdot 6561 - 10 \cdot 256 + 5 \\ &= 390625 - 327680 + 65610 - 2560 + 5 \\ &= 126000. \end{aligned}$$

Le partizioni di ordine 3 di un insieme di ordine 9 sono 3025. Infatti si ha:

$$\begin{aligned} S(9, 3) &= \frac{1}{3!} \sum_{i=0}^3 (-1)^i \binom{3}{i} (3-i)^9 = \frac{1}{6} (3^9 - 3 \cdot 2^9 + 3 \cdot 1) \\ &= \frac{1}{6} (19683 - 1536 + 3) = \frac{18150}{6} = 3025. \end{aligned}$$

## Esercizi

**Esercizio 3.7.1.** Si verifichi che la sesta e la settima riga del triangolo di Stirling sono, rispettivamente,

$$1 \quad 31 \quad 90 \quad 65 \quad 15 \quad 1,$$

$$1 \quad 63 \quad 301 \quad 350 \quad 140 \quad 21 \quad 1.$$

**Esercizio 3.7.2.** Vanna sta riponendo la biancheria da cucina nei due ripiani identici a sua disposizione. Deve collocare i grembiuli, gli asciugamani, gli strofinacci, le presine, il guanto da forno, le tovaglie, i tovaglioli. In quanti modi può ripartirli, utilizzando entrambi i ripiani?

**Esercizio 3.7.3.** Manuela la scorsa Pasqua ha fabbricato da sé le uova di cioccolato da regalare, con una forma donatale dalla mamma. Aveva comprato anche le sorprese: un portachiavi, uno spillo, un braccialetto, una collanina e un anellino. Con la cioccolata a disposizione è riuscita però a confezionare solo 4 uova; in quanti modi poteva ripartire le 5 sorprese nelle uova, volendo utilizzare tutti i regali acquistati e volendo ovviamente che ogni uovo fosse dotato di sorpresa?

**Esercizio 3.7.4.** La piccola Susy vuole utilizzare tutti e tre i suoi astucci identici per riporre i suoi pastelli: ne ha uno rosso, uno giallo, uno azzurro, uno arancione, uno verde, uno marrone e uno lilla. In quanti modi può ripartirli?

**Esercizio 3.7.5.** Giovanni sta riordinando la sua scrivania: ha 4 contenitori identici che vuole utilizzare, e in essi vuole riporre i suoi appunti di storia, quelli di filosofia, quelli di italiano, quelli di matematica e quelli di inglese. In quanti modi può ripartirli?

**Esercizio 3.7.6.** Romeo ha due scatoloni, uno di base quadrata e uno di base triangolare. Utilizzandoli entrambi, vuole conservare in essi i suoi modellini di auto: ha una Ferrari, una Porsche, una Jaguar, una Mercedes, una Maserati, un'Alfa e una Ford. In quanti modi può ripartirli?

**Esercizio 3.7.7.** Rosaria ha 3 guardaroba, uno in camera da letto, uno nel corridoio, uno nella camera dei bambini. Volendo utilizzarli tutti per riporre il plaid, la coperta matrimoniale, il piumone, le lenzuola di flanella e il copertino estivo, in quanti modi può ripartirli?

**Esercizio 3.7.8.** Rodolfo ha 2 piccoli amici, Goffredo e Vittorio, cui vuole regalare i suoi oggetti per il mare: la paletta, il secchiello, il rastrello, l'innaffiatoio, la formetta a forma di pesce, quella a forma di sole, quella a forma di stella e quella a forma di barca. Donando a ciascuno almeno un oggetto, in quanti modi può distribuirli?

**Esercizio 3.7.9.** Silvana ha comprato delle statuette raffiguranti i 7 nani di Biancaneve, e vuole collocarle in giardino, divise in due gruppi. In quanti modi può ripartirle?

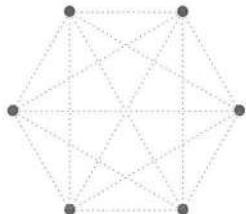
**Esercizio 3.7.10.** Zaira ha 4 astucci identici, che vuole tutti utilizzare per riporre i suoi 5 anelli preziosi: uno ha una pietra di zaffiro, uno un rubino, uno un topazio, uno un opale e uno un diamante. In quanti modi diversi può ripartire gli anelli?

## 3.8 Cenni sulla teoria di Ramsey

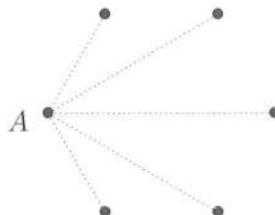
La teoria di Ramsey deve il suo nome a Frank Ramsey (1903-1930) che ne fu il fondatore. Si comincerà con il presentarne un aspetto particolare.

**3.8.1. Esempio.** Si considerino 6 (o più) persone. Allora tra queste esistono 3 che a 2 a 2 si conoscono o esistono 3 che a 2 a 2 non si conoscono. Infatti

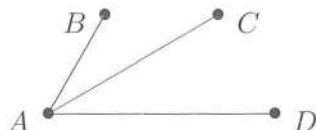
si rappresentino le 6 persone con 6 punti e si uniscano due di essi con una linea continua se le relative persone si conoscono, con una linea tratteggiata nel caso contrario.



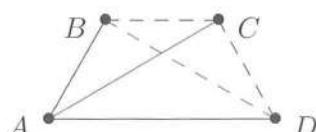
Se  $A$  è uno dei punti, rappresentante la persona  $a$ , questo è l'estremo di 5 segmenti,



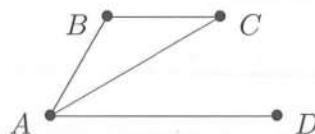
almeno 3 dei quali dello stesso tipo (come si ottiene anche applicando la forma forte del principio dei cassetti (vedi 3.3.6) con  $n = 2$ : “conosce  $A$ ” o “non conosce  $A$ ” e con  $q_1 = 3 = q_2$ ,  $q_1 + q_2 - n + 1 = 5$ ). Si supponga, per esempio, che i segmenti  $AB, AC, AD$  siano tutti continui:



cioè  $a$  conosce sia  $b$  che  $c$  che  $d$ , persone rappresentate dai punti  $B, C, D$  rispettivamente. Si considerino ora i punti  $B, C$  e  $D$ . Se i 3 segmenti  $BC, BD$  e  $CD$  sono tutti tratteggiati:



ciò significa che  $b, c$  e  $d$  a due a due non si conoscono e l'asserto è provato. Se invece almeno uno di questi segmenti, per esempio  $BC$ , è continuo:



si ottiene che  $AB, AC$  e  $BC$  sono dello stesso tipo e dunque  $a, b$  e  $c$  si conoscono a due a due, come volevasi.

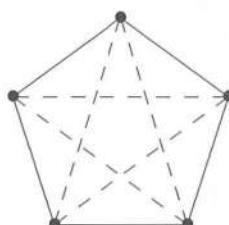
Quanto provato si può anche esprimere efficacemente nel seguente modo:

**3.8.2.** *Se ogni sottoinsieme di ordine 2 di un insieme  $S$  di ordine 6 è colorato in rosso o in azzurro, esiste un sottoinsieme  $V$  di  $S$  di ordine 3 tale che ogni suo sottoinsieme di ordine 2 ha lo stesso colore.*

Si introduca ora la notazione seguente: sia  $k$  un numero naturale positivo, e sia  $S$  un insieme di ordine  $n \geq k$ ; si indichi con  $[S]^k$  il sottoinsieme di  $\mathcal{P}(S)$  costituito dai sottoinsiemi di ordine  $k$  di  $S$ . Allora 3.8.2 può esprimersi più sinteticamente nel seguente modo:

**3.8.3.** *Sia  $S$  un insieme di ordine 6. Se  $[S]^2 = \Delta_1 \cup \Delta_2$ , allora esiste un sottoinsieme  $T$  di  $S$  di ordine 3 tale che  $[T]^2 \subseteq \Delta_1$  o  $[T]^2 \subseteq \Delta_2$ .*

Si noti che 6 è minimo per tale proprietà, come illustrato dalla figura che segue:



Siano ora  $k$  e  $h$  interi positivi, con  $k < h$ . Il minimo intero positivo  $r > h$  tale che, se  $S$  è un insieme di ordine  $r$  e  $[S]^k = \Delta_1 \cup \Delta_2$ , esiste un sottoinsieme proprio  $T$  di  $S$ , di ordine  $h$ , tale che  $[T]^k \subseteq \Delta_1$  o  $[T]^k \subseteq \Delta_2$ , è detto il **numero di Ramsey** relativo a  $k$  e  $h$ . Il fatto rimarchevole, e per nulla evidente, è che per ogni scelta dei parametri  $k$  e  $h$  esiste il numero di Ramsey relativo a  $k$  e  $h$ . Questo risultato è noto come **teorema di Ramsey**; il Lettore interessato potrà trovarne la dimostrazione su un qualunque testo di Combinatoria. Sebbene il teorema di Ramsey ne assicuri l'esistenza, è incredibilmente arduo calcolare il valore esplicito dei numeri di Ramsey. Nella maggior parte dei casi ci si deve accontentare di limitazioni inferiori e superiori, spesso notevolmente larghe.

**3.8.4. Esempio.** Se  $k = 2$  e  $h = 3$ , si ha  $r = 6$ . Si può provare che per  $k = 3$  e  $h = 4$ , si ha  $r = 21$ .

Esistono svariate versioni del teorema di Ramsey. Per esempio, è possibile sostituire il numero 2 con un numero arbitrario  $m$  di colori utilizzabili per la colorazione. La teoria di Ramsey riguarda anche insiemi infiniti.

**3.8.5. Siano  $m > 1$  un intero, ed  $S$  un insieme infinito. Se  $[S]^2 = \Delta_1 \cup \dots \cup \Delta_m$ , esiste un sottoinsieme infinito  $T$  di  $S$  tale che  $[T]^2 \subseteq \Delta_j$ , per un opportuno  $j \in \{1, \dots, m\}$ . Più in generale, con  $k > 1$  intero, se  $[S]^k = \Delta_1 \cup \dots \cup \Delta_m$ , esiste un sottoinsieme infinito  $T$  di  $S$  tale che  $[T]^k \subseteq \Delta_j$ , per un opportuno  $j \in \{1, \dots, m\}$ .**

*Dimostrazione.* Per semplicità, si considererà solo il caso  $k = 2 = m$ . Si supponga cioè  $[S]^2 = \Delta_1 \cup \Delta_2$ ; si vuole provare che, per un opportuno sottoinsieme infinito  $T$  di  $S$ , risulta  $[T]^2 \subseteq \Delta_1$  o  $[T]^2 \subseteq \Delta_2$ . Si fissi  $a_1 \in S$  e si consideri l'insieme  $\{\{a_1, s\} : s \in S \setminus \{a_1\}\}$ . Tale insieme ovviamente è infinito e contenuto in  $\Delta_1 \cup \Delta_2$ . Pertanto esiste un insieme infinito  $S_1 \subseteq S \setminus \{a_1\}$  tale che  $\{\{a_1, s\} : s \in S_1\}$  è contenuto in  $\Delta_{t_1}$ , con  $t_1 \in \{1, 2\}$ . Si fissi allora  $a_2 \in S_1$ . Ovviamente  $a_2 \neq a_1$  e  $\{a_1, a_2\} \subseteq \Delta_{t_1}$ . Ancora è infinito l'insieme  $\{\{a_2, s\} : s \in S_1 \setminus \{a_2\}\}$  ed è contenuto in  $\Delta_1 \cup \Delta_2$ . Ragionando come in precedenza, esiste un insieme infinito  $S_2 \subseteq S_1 \setminus \{a_2\}$  tale che  $\{\{a_2, s\} : s \in S_2\} \subseteq \Delta_{t_2}$ , per un opportuno  $t_2 \in \{1, 2\}$ . Così continuando si individuano la sequenza  $a_1, a_2, \dots, a_n, \dots$  di elementi di  $S$  a due a due distinti e la sequenza  $t_1, t_2, \dots, t_n, \dots$  di numeri appartenenti a  $\{1, 2\}$  tali che, se  $i$  e  $j$  sono entrambi positivi, con  $i < j$ , si ha  $\{a_i, a_j\} \in \Delta_{t_i}$ . Ovviamente esiste un sottoinsieme infinito  $M$  di  $\mathbb{N}$  tale che  $t_i = t_j = t$ , per ogni  $i, j \in M$ . Si ponga  $T := \{a_i : i \in M\}$ . Questo insieme è un sottoinsieme infinito di  $S$  ed è tale che, per ogni  $i, j \in M$ , con  $i \neq j$ , si ha  $\{a_i, a_j\} \in \Delta_t$ , cioè tale che  $[T]^2 \subseteq \Delta_t$ , come volevasi.  $\square$

## 3.9 Esercizi di riepilogo

**Esercizio 3.9.1.** Si individui in quante e quali delle proposizioni del Capitolo 3 si è usato il principio di moltiplicazione (vedi 3.2.1).

**Esercizio 3.9.2.** Quanti sono i numeri tra 1 e 101 divisibili per almeno uno tra 5 e 7? E quanti quelli divisibili per almeno uno tra 5, 7 e 11?

**Esercizio 3.9.3.** Si calcoli il numero dei naturali tra 1 e 10.000 che non sono divisibili né per 4, né per 5, né per 6.

**Esercizio 3.9.4.** Si provi che in ogni gruppo di persone ve ne sono due che hanno lo stesso numero di amici nel gruppo.

**Esercizio 3.9.5.** Sia  $n$  un numero naturale positivo e si considerino  $n + 1$  numeri naturali positivi. Si provi che due di questi differiscono per un multiplo di  $n$ .

**Esercizio 3.9.6.** Si provi che esistono due potenze di 2 che differiscono per un multiplo di 2001.

**Esercizio 3.9.7.** Vittorio sta riponendo a caso nello zaino i libri di francese, letteratura italiana, geometria e latino, che gli serviranno per le lezioni del giorno dopo. Ha una probabilità su quante di riportli nello stesso ordine in cui gli serviranno?

**Esercizio 3.9.8.** Si calcoli il numero delle parole, non necessariamente di senso compiuto, che si possono formare con le lettere della parola "PAGNOTTA".

**Esercizio 3.9.9.** Lorenzo vuol far visitare all'amico milanese Ischia, Capri, Procida, Sorrento e Positano; quanti distinti itinerari può proporgli?

**Esercizio 3.9.10.** Si calcoli il numero delle parole, non necessariamente di senso compiuto, che si possono formare con le lettere della parola "ZIZZANIA".

**Esercizio 3.9.11.** Si calcoli il numero delle parole, non necessariamente di senso compiuto, che si possono formare con le lettere della parola "ASSASSINI".

**Esercizio 3.9.12.** Olimpia sta disponendo sul suo balcone, da sinistra verso destra, le 7 piante che ha preparato: 2 sono di rose, 3 di margherite e 2 di azalee. In quanti modi diversi può disporle?

**Esercizio 3.9.13.** La piccola Luciana sta costruendo una torre con tutti i suoi mattoni colorati, ponendoli uno sull'altro. Ha 5 mattoni rossi, 4 gialli, 3 verdi e 3 marroni. In quanti modi può costruirla?

**Esercizio 3.9.14.** Roberto vuole giocare al Lotto 5 numeri tra i primi 20; quante scelte possibili ha?

**Esercizio 3.9.15.** Uno scommettitore decide di giocare tutte le colonne del Totocalcio con la "formula" 7-5-2, ossia tutte le colonne in cui compaiono 7 vittorie in casa, 5 pareggi e 2 vittorie in trasferta. Quante colonne dovrà giocare?

**Esercizio 3.9.16.** Quante rette di un piano sono individuate da 25 punti a tre a tre non allineati? E quanti triangoli?

**Esercizio 3.9.17.** Il Presidente del Consiglio deve inserire 4 nuovi ministri nel suo governo. Sono candidati 10 uomini e 12 donne, ma il presidente vuole inserire almeno 2 donne. Quante sono le possibili scelte?

**Esercizio 3.9.18.** Quanti sono i numeri tra 1 e 600 divisibili per almeno uno tra 11 e 19?

**Esercizio 3.9.19.** Per preparare un affettato misto, Rosanna vuole acquistare 4 tipi diversi di salumi. Il negoziante ha prosciutto crudo, prosciutto cotto, salame napoletano, salame milanese, salame ungherese, mortadella, pancetta. Quante scelte diverse può fare Rosanna?

**Esercizio 3.9.20.** L'anziano Valerio sta facendo testamento: ora deve decidere a chi lasciare la sua villa al mare, la casa di campagna, l'attico di Parigi, il negozio di New York e l'appartamento di Roma. Ha 5 figli, Romano, Ruggero, Romualdo, Renato e Carlo, e a ciascuno andrà qualcosa. In quanti modi diversi può fare il lascito?

**Esercizio 3.9.21.** Volendo giocare al Lotto 5 numeri multipli di 11, quante scelte ci sono? Volendo giocare al Lotto 4 numeri maggiori di 75, quante scelte ci sono?

**Esercizio 3.9.22.** Susanna, Titty, Doriana, Valentina e Giovanna si sono sfidate a una corsa, e ora propongono a Walter di indovinare l'ordine di arrivo. Walter ha una probabilità su quante di non fare alcun errore?

**Esercizio 3.9.23.** Catello ha bisogno di un giardiniere, un manovale, un cameriere e un autista. Si presentano Simone, Vincenzo, Corrado, Diego, Pino e Pierino, e ciascuno afferma di saper far tutto. In quanti modi distinti può Catello assumere?

**Esercizio 3.9.24.** Rosa è stata invitata a una festa, ma non conosce nessuno. Le vengono presentati Antonio, Bruno, Cesare, Dario, Emilio e Federico, e poi, in ordine casuale, le loro mogli Assunta, Barbara, Caterina, Donatella, Enza e Floriana. Viene poi sfidata a indovinare le giuste coppie marito-moglie. Ha una probabilità su quante di non commettere errori?

**Esercizio 3.9.25.** Quanti sottoinsiemi di ordine 4 ha l'insieme  $\{a, c, f, k, z, w\}$ ?

**Esercizio 3.9.26.** Stefania ha una scatola tonda, una quadrata, una triangolare, una rettangolare e una ovale, e deve riporre un anellino, un braccialetto, un orologio, una collanina e una medaglia. In quanti modi diversi può collocare gli oggetti, uno in ogni scatola?

**Esercizio 3.9.27.** Stefano sta giocando alla guerra con i suoi amici Renato, Marcello, Marco, Giovanni, Roberto e Andrea, e deve nominare tra loro "il comandante", il "capitano" e il "tenente". In quanti modi diversi può farlo?

**Esercizio 3.9.28.** Simona ha deciso di chiamare Pupo, Billy, Zorro e Bobby i suoi pupazzi: sono un cane, un orso, un coniglio e un gatto. In quanti modi diversi potrà farlo?

**Esercizio 3.9.29.** Vittorio ha 6 fratelli: Rosario, Maurizio, Aldo, Luca, Sossio e Aristide. La sua cagna Stella ha avuto 4 cagnolini: Roby, Placida, Saetta e Pisolo, e Vittorio vuole farne dono a 4 dei suoi fratelli. In quanti modi diversi può farlo?

**Esercizio 3.9.30.** La piccola Lori vuole colorare i disegni appena fatti: una barchetta, una casetta, una stellina, un fiorellino, ognuno con un colore diverso. Ha a disposizione il verde, il giallo, il rosso e il viola. In quanti modi diversi può farlo?

**Esercizio 3.9.31.** Vanni ha 3 posti-macchina per le sue 3 auto: una Seicento, una Panda e una Clio. In quanti modi diverse può parcheggiarle?

**Esercizio 3.9.32.** Giovanna ha 5 figli: Giacomo, Luca, Marco, Matteo e Antonio, e vuole che facciano dello sport. Sono aperte le iscrizioni per corsi di nuoto, di ginnastica, di calcio e di pallanuoto. Volendo iscrivere ciascun figlio a un solo corso, quante scelte diverse può fare?

**Esercizio 3.9.33.** Valerio deve comprare un disco, un libro, una penna e un orologio. Non ha ancora deciso se acquistare un disco di musica classica, lirica o moderna, se un libro di avventura, di narrativa, di satira o poliziesco, se una penna stilografica o biro, se un orologio da polso, da tavolo o da taschino. Quante scelte diverse può fare?

**Esercizio 3.9.34.** Volendo giocare al Lotto 4 numeri multipli di 10, quante scelte ci sono?

**Esercizio 3.9.35.** Quante parole, non necessariamente di senso compiuto, si possono formare con 5 lettere distinte della parola “ARGOMENTI”?

**Esercizio 3.9.36.** Vanni ha ordinato una coppa gelato gigante: sarà formata da 5 dosi di gelato. È incerto perché non sa di che gusti ordinarla, se uguali o differenti. Può scegliere tra cioccolato, caffè, nocciola, fragola, vaniglia, crema e pistacchio. Quante scelte diverse può fare?

**Esercizio 3.9.37.** Giovanna ha 5 biglietti per la rappresentazione teatrale di domenica, e vuole regalarli ai suoi vicini, ma è incerta se donarli tutti a una stessa famiglia o distribuirli in modo diverso. Le famiglie in questione sono: Rossi, Romano, Lombardo, Esposito, Carli e Bianchi. Quante scelte diverse può fare?

**Esercizio 3.9.38.** Volendo guarnire il gelato con 6 frutti di bosco, e avendo a disposizione delle more, dei mirtilli e delle fragole, quante scelte ci sono? E volendo guarnire il gelato con 3 frutti di bosco distinti, e avendo a disposizione delle more, dei mirtilli, delle fragole, delle gelse e dei fragoloni, quante scelte ci sono?

**Esercizio 3.9.39.** Nel portafoglio il nonno ha 4 banconote. Il piccolo Ezio vuole indovinare di che tipo sono: da 5, 10, 20, 50 o 100 euro. Quante probabilità ha di indovinarle tutte e 4? E se Ezio sa che nel portafoglio del nonno le banconote sono di importo diverso, quante probabilità ha Ezio di indovinarle tutte e 4?

**Esercizio 3.9.40.** Quanti sono i numeri naturali di 4 cifre, con la prima uguale a 3, 4, 5 o 6, e la seconda uguale a 0, 2, 4, 6 o 8?

**Esercizio 3.9.41.** Quante sono le parole, non necessariamente di senso compiuto, che si ottengono utilizzando le lettere della parola “PULLULA”? E della parola “PALERMO”?

**Esercizio 3.9.42.** Quante sono le parole, non necessariamente di senso compiuto, che si ottengono utilizzando 3 lettere, non necessariamente diverse tra loro, della parola “NONNA”?

**Esercizio 3.9.43.** Volendo comprare 3 pacchi di biscotti (eventualmente dello stesso tipo), e avendo a disposizione dei wafer, dei Pavesini, delle lingue di gatto e dei brigidini, quante scelte ci sono? E volendoli comprare di tipo diverso, quante scelte ci sono?

**Esercizio 3.9.44.** Quante sono le parole di 4 lettere (non necessariamente di senso compiuto) con 2 vocali distinte, una al II posto, l'altra al IV, e 2 consonanti distinte dell'insieme  $\{B, D, L, V, G, N\}$ ?

**Esercizio 3.9.45.** Volendo comprare 3 tramezzini (eventualmente dello stesso tipo), e avendone a disposizione al prosciutto, al salmone, al tonno, al salame, al formaggio, quante scelte ci sono? E volendone comprare 3 di diverso tipo, quante scelte ci sono?

**Esercizio 3.9.46.** Pina vuole fare una bella insalata mista, e può scegliere tra lattuga, radicchio bianco, radicchio rosso, indivia, finocchi. Volendo comprare 3 varietà diverse, quante scelte può fare?

**Esercizio 3.9.47.** Il professore di geografia dovrà parlare di alcune città italiane, e la sua scelta ricadrà su 5 delle seguenti città: Roma, Firenze, Napoli, Venezia, Palermo, Bari, Milano, Torino, Genova. Quante sono le sue possibili scelte? Parlerà, poi, di Piemonte, Veneto, Lombardia, Emilia e Liguria, ma non ha ancora deciso in che ordine farlo. Quante scelte diverse può effettuare?

**Esercizio 3.9.48.** Stefano deve telefonare all'amico Rino, alla mamma, alla nonna e al cugino Vanni, ma non sa in che ordine farlo. In quanti modi diversi può effettuare le chiamate?

**Esercizio 3.9.49.** Renata ha 7 bambole Barbie, 5 vestitini e 4 cappottini. Volendo ricoprire un po' ciascuna bambola, quante avranno sia l'abito che il soprabito?

**Esercizio 3.9.50.** Maria ha preparato per il buffet della sua festa 30 coppe di gelato, 25 fette di torta e 20 tramezzini. I suoi amici prendono tutti qualcosa ma nessuno di loro mangia sia la torta che il tramezzino, 15 scelgono torta e gelato, 12 gelato e tramezzino. Quando Maria si avvicina al buffet, è tutto finito. Quanti amici erano presenti?

# 4

## Strutture algebriche

In questo capitolo verrà introdotto il concetto di operazione in un insieme, concetto che generalizza le familiari nozioni di somma e prodotto di numeri, e verranno presentate definizioni che prendono spunto da ben note proprietà delle suddette somma e prodotto. Si perverrà così al concetto di struttura algebrica e saranno descritte alcune delle principali strutture.

### 4.1 Generalità

Sia  $S$  un insieme. Un'applicazione

$$\perp: S \times S \longrightarrow S$$

è detta un'**operazione interna** di  $S$  o **legge interna** in  $S$ . L'immagine mediante  $\perp$  della coppia  $(x, y)$  è di solito denotata col simbolo  $x \perp y$  e detta **composto** di  $x$  e  $y$  in  $\perp$ . Si userà il simbolo  $(S, \perp)$  per indicare l'insieme  $S$  dotato dell'operazione interna  $\perp$ .

**4.1.1. Esempi.** L'addizione e la moltiplicazione usuali in  $\mathbb{N}_0$ , in  $\mathbb{N}$ , in  $\mathbb{Z}$ , in  $\mathbb{Q}$ , in  $\mathbb{R}$  sono operazioni interne nei rispettivi insiemi.

Con  $V$  insieme, le applicazioni:

$$\begin{aligned}\cup : (X, Y) \in \mathcal{P}(V) \times \mathcal{P}(V) &\longmapsto X \cup Y \in \mathcal{P}(V), \\ \cap : (X, Y) \in \mathcal{P}(V) \times \mathcal{P}(V) &\longmapsto X \cap Y \in \mathcal{P}(V), \\ \setminus : (X, Y) \in \mathcal{P}(V) \times \mathcal{P}(V) &\longmapsto X \setminus Y \in \mathcal{P}(V), \\ \dot{\cup} : (X, Y) \in \mathcal{P}(V) \times \mathcal{P}(V) &\longmapsto X \dot{\cup} Y \in \mathcal{P}(V)\end{aligned}$$

sono operazioni interne in  $\mathcal{P}(V)$ .

Con  $V$  insieme, l'applicazione

$$\cdot : (f, g) \in V^V \longmapsto g \circ f \in V^V$$

è un'operazione interna in  $V^V$ .

Altri esempi di operazioni in  $\mathbb{Z}$  sono la sottrazione, e anche:

$$\begin{aligned}\perp_1 : (x, y) \in \mathbb{Z} \times \mathbb{Z} &\longmapsto x^2 + y^2 \in \mathbb{Z}, \\ \perp_2 : (x, y) \in \mathbb{Z} \times \mathbb{Z} &\longmapsto x^2 + y - 1 \in \mathbb{Z}, \\ \perp_3 : (x, y) \in \mathbb{Z} \times \mathbb{Z} &\longmapsto xy + y \in \mathbb{Z}, \\ \perp_4 : (x, y) \in \mathbb{Z} \times \mathbb{Z} &\longmapsto x + y + xy \in \mathbb{Z}.\end{aligned}$$

Si consideri l'operazione  $\perp$  nell'insieme  $S$ . Elementi  $x, y \in S$  sono detti **permutabili** in  $(S, \perp)$  se si ha  $x \perp y = y \perp x$ . Ovviamente ogni elemento  $x \in S$  è permutabile con se stesso. L'operazione  $\perp$  è detta **commutativa** se  $x$  e  $y$  sono permutabili, per ogni  $x, y \in S$ ; cioè se si ha  $x \perp y = y \perp x$ , per ogni  $(x, y) \in S \times S$ . L'operazione  $\perp$  è detta **associativa** se si ha  $(x \perp y) \perp z = x \perp (y \perp z)$ , per ogni  $x, y, z \in S$ .

**4.1.2. Esempi.** Le usuali operazioni di somma e prodotto in  $\mathbb{N}_0$ , in  $\mathbb{N}$ , in  $\mathbb{Z}$ , in  $\mathbb{Q}$ , in  $\mathbb{R}$  sono sia commutative che associative.

Come osservato in 1.4, lo sono anche l'unione, l'intersezione e l'unione disgiunta in  $\mathcal{P}(V)$ , per ogni insieme  $V$ . Il complemento non è commutativo né associativo per ogni insieme  $V$  non vuoto.

La sottrazione in  $\mathbb{Z}$  è tale che ogni elemento è permutabile solo con se stesso, in quanto  $x - 0 \neq 0 - x$ , per ogni  $x \in \mathbb{Z} \setminus \{0\}$ . Non è dunque commutativa, e non è associativa in quanto, per esempio,  $(1 - 2) - 3 = -4 \neq 2 = 1 - (2 - 3)$ .

L'operazione  $\cdot$  in  $V^V$  definita negli Esempi 4.1.1 è associativa (vedi 2.2.12) e non commutativa se  $V$  ha almeno due elementi (vedi Esempio 2.2.11).

Le operazioni in  $\mathbb{Z}$  definite in 4.1.1 sono tali che:  $\perp_1$  è commutativa e non associativa,  $\perp_2$  non è commutativa né associativa,  $\perp_3$  non è commutativa e non è associativa,  $\perp_4$  è commutativa e associativa. Si ha infatti, per ogni  $x, y \in \mathbb{Z}$ ,  $x \perp_1 y = x^2 + y^2 = y^2 + x^2 = y \perp_1 x$  e, per esempio,  $(1 \perp_1 2) \perp_1 3 = (1^2 + 2^2) \perp_1 3 = 5 \perp_1 3 = 34 \neq 170 = 1 \perp_1 13 = 1 \perp_1 (2^2 + 3^2) = 1 \perp_1 (2 \perp_1 3)$ . Si ha poi, per esempio,  $2 \perp_2 3 = 6 \neq 10 = 3 \perp_2 2$  e  $(2 \perp_2 3) \perp_2 0 = 6 \perp_2 0 = 35 \neq 11 = 2 \perp_2 8 = 2 \perp_2 (3 \perp_2 0)$ . Ancora, si ha, per esempio,  $2 \perp_3 0 = 0 \neq 2 = 0 \perp_3 2$  e  $(1 \perp_3 2) \perp_3 3 = 4 \perp_3 3 = 15 \neq 18 = 1 \perp_3 9 = 1 \perp_3 (2 \perp_3 3)$ . Si ha poi, qualunque siano  $x, y \in \mathbb{Z}$ ,  $x \perp_4 y = x + y + xy = y + x + yx = y \perp_4 x$ . L'associatività di  $\perp_4$  sarà provata nell'Esercizio 4.1.1.

Come osservato negli esempi precedenti, un'operazione può essere associativa e non commutativa, o commutativa e non associativa, o godere di entrambe le proprietà o di nessuna delle due.

Se l'operazione  $\perp$  in  $S$  è associativa, è lecito utilizzare la scrittura  $x \perp y \perp z$  per denotare l'elemento  $(x \perp y) \perp z = x \perp (y \perp z)$ . Più in generale, se  $S$  è un insieme dotato di un'operazione associativa  $\perp$  e  $s_1, s_2, \dots, s_n$  sono elementi di  $S$ , con  $n \geq 3$ , si pone induttivamente:

$$s_1 \perp s_2 \perp \cdots \perp s_n = (s_1 \perp s_2 \perp \cdots \perp s_{n-1}) \perp s_n.$$

Pertanto, per  $n = 4$ , si ha  $s_1 \perp s_2 \perp s_3 \perp s_4 = ((s_1 \perp s_2) \perp s_3) \perp s_4$ , ma tale elemento coincide anche con  $((s_1 \perp s_2) \perp (s_3 \perp s_4))$  o anche, per esempio, con  $s_1 \perp (s_2 \perp (s_3 \perp s_4))$ , per l'associatività di  $\perp$ . Più in generale l'associatività di  $\perp$  permette analoghe arbitrarietà nel calcolo del composto di più elementi, che verranno utilizzate senza ulteriori precisazioni.

Se  $S$  è un insieme finito,  $S = \{x_1, \dots, x_n\}$ , dotato di un'operazione interna  $\perp$ , è possibile rappresentare tale operazione mediante una tabella, la cosiddetta *tavola di moltiplicazione* di  $(S, \perp)$ :

$\perp$	$x_1$	$x_2$	$\dots$	$x_n$
$x_1$	$x_1 \perp x_1$	$x_1 \perp x_2$	$\dots$	$x_1 \perp x_n$
$x_2$	$x_2 \perp x_1$	$x_2 \perp x_2$	$\dots$	$x_2 \perp x_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$x_n$	$x_n \perp x_1$	$x_n \perp x_2$	$\dots$	$x_n \perp x_n$

dove si riportano tutti i composti degli elementi di  $S$ .

**4.1.3. Esempi.** Considerato l'insieme degli interi  $\{-1, 1\}$  con l'usuale prodotto, si ha:

.	1	-1
1	1	-1
-1	-1	1

Con  $V = \{a, b\}$ , le tavole di moltiplicazione di  $(\mathcal{P}(V), \cup)$ ,  $(\mathcal{P}(V), \cap)$ ,  $(\mathcal{P}(V), \setminus)$ ,  $(\mathcal{P}(V), \dot{\cup})$ , sono rispettivamente:

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\{a\}$	$\{a\}$	$\{a\}$	$V$	$V$
$\{b\}$	$\{b\}$	$V$	$\{b\}$	$V$
$V$	$V$	$V$	$V$	$V$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$V$	$\emptyset$	$\{a\}$	$\{b\}$	$V$

$\setminus$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$
$\{b\}$	$\{b\}$	$\{b\}$	$\emptyset$	$\emptyset$
$V$	$V$	$\{b\}$	$\{a\}$	$\emptyset$

$\dot{\cup}$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$V$
$\{a\}$	$\{a\}$	$\emptyset$	$V$	$\{b\}$
$\{b\}$	$\{b\}$	$V$	$\emptyset$	$\{a\}$
$V$	$V$	$\{b\}$	$\{a\}$	$\emptyset$

Si noti che, considerato un insieme finito  $S$ , è possibile definire in esso un'opera-

zione assegnando una tabella. Per esempio, con  $S = \{a, b, c\}$ , la tabella

$\perp$	$a$	$b$	$c$
$a$	$b$	$c$	$a$
$b$	$b$	$b$	$c$
$c$	$b$	$a$	$c$

individua un'operazione, in cui, tra l'altro,  $a \perp b = c$ ,  $c \perp b = a$ ,  $c \perp a = b$ .

Sia  $S$  un insieme dotato di un'operazione interna  $\perp$ . Un elemento  $e \in S$  è detto **neutro** rispetto a  $\perp$  se si ha  $e \perp x = x = x \perp e$ , per ogni  $x \in S$ . Si noti che in particolare un elemento neutro è permutabile con ogni elemento di  $S$ .

**4.1.4. Esempi.** In  $(\mathbb{N}_0, +)$  il numero 0 è elemento neutro. In  $(\mathbb{N}_0, \cdot)$  il numero 1 è elemento neutro. In  $(\mathbb{N}, +)$  non esiste elemento neutro.

Se  $V$  è un insieme, l'insieme vuoto è elemento neutro in  $(\mathcal{P}(V), \cup)$  e in  $(\mathcal{P}(V), \dot{\cup})$ , l'insieme  $V$  è elemento neutro in  $(\mathcal{P}(V), \cap)$ . Se  $V$  è non vuoto, non esistono elementi neutri in  $(\mathcal{P}(V), \setminus)$ : infatti risulta  $X \setminus V = \emptyset \neq V$ , per ogni  $X \in \mathcal{P}(V)$ .

L'applicazione identica  $\text{id}_V$  è elemento neutro in  $(V^V, \cdot)$ , dove  $\cdot$  è l'operazione interna in  $V^V$  definita in 4.1.1 (vedi 2.2.13).

Le operazioni in  $\mathbb{Z}$  definite in 4.1.1 sono tali che: 0 è elemento neutro rispetto a  $\perp_4$  e non esiste elemento neutro rispetto a  $\perp_1, \perp_2, \perp_3$ .

Come evidenziato dagli esempi precedenti, può esistere o meno elemento neutro rispetto a un'operazione. Si noti però che, qualora esista, l'elemento neutro è unico. Vale infatti:

**4.1.5.** *Sia  $S$  un insieme dotato dell'operazione interna  $\perp$  e siano  $e, e'$  neutri rispetto a  $\perp$ . Allora si ha:  $e = e'$ .*

*Dimostrazione.* Risulta  $e \perp e' = e'$ , essendo  $e$  neutro, e  $e \perp e' = e$ , essendo  $e'$  neutro. Pertanto  $e = e'$ , come volevasi.  $\square$

Più in generale, un elemento  $e \in S$  è detto **neutro a sinistra** (rispettivamente **neutro a destra**) rispetto a  $\perp$  se si ha:  $e \perp x = x$  (risp.  $x \perp e = x$ ), per ogni  $x \in S$ . Ovviamente richiedere che  $e \in S$  sia neutro rispetto a  $\perp$  equivale a richiedere che  $e$  sia neutro a destra e a sinistra rispetto a  $\perp$ . Naturalmente se l'operazione  $\perp$  in  $S$  è commutativa, si ha che  $e \in S$  è neutro se lo è da un lato.

**4.1.6. Esempi.** Il numero 0 è (l'unico) elemento neutro a destra rispetto alla sottrazione in  $\mathbb{Z}$ , non è neutro a sinistra, in quanto per esempio  $0 - 1 \neq 1$ .

Se  $V$  è un insieme non vuoto, l'insieme vuoto è elemento neutro a destra rispetto al complemento in  $\mathcal{P}(V)$  (vedi (1.4.13)), ma non è neutro a sinistra, essendo  $\emptyset \setminus V = \emptyset \neq V$  (vedi (1.4.14)).

Considerati gli Esempi 4.1.1, si ha che non esistono elementi neutri né a destra né a sinistra rispetto a  $\perp_1$ , 1 e  $-1$  sono entrambi elementi neutri a sinistra rispetto a  $\perp_2$ , 0 è elemento neutro solo a sinistra rispetto a  $\perp_3$ .

Gli esempi precedenti evidenziano che possono esistere più elementi neutri solo da un lato. Si ha però:

**4.1.7.** *Sia  $S$  un insieme dotato dell'operazione interna  $\perp$  e siano  $e_1, e_2 \in S$  con  $e_1$  neutro a sinistra,  $e_2$  neutro a destra rispetto a  $\perp$ . Allora si ha:  $e_1 = e_2$ .*

*Dimostrazione.* Segue subito da  $e_2 = e_1 \perp e_2 = e_1$  (vedi anche 4.1.5).  $\square$

Da 4.1.7 segue che se esistono più elementi neutri da un lato allora non esiste elemento neutro. Si ritrova così, per esempio, che non esiste elemento neutro in  $(\mathbb{Z}, \perp_2)$ . Sempre da 4.1.7 segue che, individuato un elemento neutro da un lato, esiste elemento neutro se e solo se tale elemento lo è anche dall'altro lato. Per esempio non esiste elemento neutro in  $(\mathbb{Z}, -)$  né in  $(\mathbb{Z}, \perp_3)$ , come già osservato.

Sia  $(S, \perp)$  dotato di elemento neutro  $e$  e sia  $x \in S$ . Un elemento  $x' \in S$  è detto **simmetrico** di  $x$  se si ha:  $x \perp x' = e = x' \perp x$ . L'elemento  $x$  è detto **simmetrizzabile** se è dotato di simmetrico.

Ovviamente se  $x$  è simmetrizzabile e ha simmetrico  $x'$ , allora  $x'$  è anch'esso simmetrizzabile avendo come simmetrico  $x$ . L'elemento neutro è sempre simmetrizzabile, avendo come unico simmetrico se stesso.

**4.1.8. Esempi.** In  $(\mathbb{N}_0, +)$  il numero 0 è l'unico elemento simmetrizzabile, così in  $(\mathbb{N}_0, \cdot)$  il numero 1 è l'unico elemento simmetrizzabile.

In  $(\mathbb{Z}, +)$  ogni  $x \in \mathbb{Z}$  ha come simmetrico il numero  $-x$ .

In  $(\mathbb{Z}, \cdot)$  gli unici elementi simmetrizzabili sono 1 e  $-1$  e ciascuno ha per simmetrico se stesso (vedi (1.2.44)).

In  $(\mathbb{Q}, +)$  ogni elemento  $x$  ha simmetrico  $-x$ , in  $(\mathbb{Q}, \cdot)$  ogni elemento  $\frac{m}{n} \neq 0$  ha come simmetrico il numero  $\frac{n}{m}$ .

In  $(\mathcal{P}(V), \cup)$  e  $(\mathcal{P}(V), \cap)$  solo gli elementi neutri sono simmetrizzabili.

In  $(\mathcal{P}(V), \dot{\cup})$  ogni elemento  $X$  ha per simmetrico se stesso (vedi (1.4.24)).

In  $(V^V, \cdot)$ , con  $\cdot$  definita in 4.1.1, le uniche applicazioni  $f$  simmetrizzabili sono quelle biettive, di simmetrico  $f^{-1}$  (vedi 2.2.16).

**4.1.9. Esempio.** Considerata nell'insieme  $\mathbb{Q}$  l'operazione:

$$\perp: (x, y) \in \mathbb{Q} \times \mathbb{Q} \mapsto x + y + |xy| \in \mathbb{Q},$$

si ha che tale operazione è commutativa, 0 è elemento neutro e, per esempio, il numero 1 non è simmetrizzabile, mentre  $-2$  ha come simmetrici  $-2$  e  $\frac{2}{3}$  (vedi anche Esercizio 4.1.11). Infatti, da  $1 + y + |y| = 0$  segue  $1 + y + y = 0$  se  $y \geq 0$ , da cui  $2y = -1$  e  $y = -\frac{1}{2}$ , assurdo, oppure  $1 + y - y = 0$  se  $y < 0$ , cioè  $1 = 0$ , ancora un assurdo. Si ha invece  $(-2) \perp (-2) = (-2) + (-2) + 4 = 0$  e  $(-2) \perp \frac{2}{3} = (-2) + \frac{2}{3} + \frac{4}{3} = 0$ .

L'operazione  $\perp$  non è associativa in quanto, per esempio,  $(1 \perp 2) \perp (-1) = 9 \neq 7 = 1 \perp (2 \perp (-1))$ .

Infatti sussiste il seguente notevole risultato:

**4.1.10.** *Sia  $S$  un insieme dotato dell'operazione interna associativa  $\perp$  con elemento neutro  $e$ . Siano  $x, x', x'' \in S$  con  $x'$  e  $x''$  simmetrici di  $x$ . Allora si ha  $x' = x''$ .*

*Dimostrazione.* Per l'associatività di  $\perp$  riesce:  $x' = x' \perp e = x' \perp (x \perp x'') = (x' \perp x) \perp x'' = e \perp x'' = x''$ .  $\square$

Può accadere che il composto di elementi simmetrizzabili non sia simmetrizzabile, come si ottiene considerando in  $(\mathbb{Q}, \perp)$ , come definito in 4.1.9, i numeri  $-3$  e  $-2$  (vedi anche Esercizio 4.1.11). Si noti però che:

**4.1.11.** *Sia  $S$  un insieme dotato dell'operazione interna associativa  $\perp$  con elemento neutro  $e$ , e siano  $x, y \in S$  simmetrizzabili. Allora  $x \perp y$  è simmetrizzabile, di simmetrico  $y' \perp x'$ , con  $x'$  simmetrico di  $x$  e  $y'$  simmetrico di  $y$ .*

*Dimostrazione.* Risulta infatti:

$$(x \perp y) \perp (y' \perp x') = x \perp (y \perp y') \perp x' = x \perp e \perp x' = x \perp x' = e$$

e, analogamente,

$$(y' \perp x') \perp (x \perp y) = y' \perp (x' \perp x) \perp y = y' \perp e \perp y = y' \perp y = e,$$

da cui l'asserto.  $\square$

Sia  $S$  un insieme dotato dell'operazione interna  $\perp$  con elemento neutro  $e$ . L'elemento  $x'$  è detto *simmetrico a sinistra* (rispettivamente *simmetrico a destra*) di  $x$  se si ha  $x' \perp x = e$  (risp.  $x \perp x' = e$ ). L'elemento  $x$  è detto *simmetrizzabile a sinistra* (risp. *simmetrizzabile a destra*) se è dotato di simmetrico a sinistra (risp. a destra).

**4.1.12. Esempio.** In  $(V^V, \cdot)$ , con  $V$  insieme non vuoto, un'applicazione è simmetrizzabile a sinistra (a destra) se e solo se è suriettiva (rispettivamente iniettiva) (vedi Esercizio 2.2.20).

Ovviamente  $x'$  è simmetrico di  $x$  se e solo se lo è sia a destra che a sinistra. Può succedere che un elemento abbia uno o più simmetrici da un lato, ma che non sia simmetrizzabile. Per esempio, con  $V$  insieme, un'applicazione  $f$  di  $V$  in  $V$  suriettiva e non iniettiva (iniettiva non suriettiva) ha più inverse a sinistra (rispettivamente a destra) in  $(V^V, \cdot)$ , pur non ammettendo simmetrico (vedi 4.1.8). O anche può accadere che un elemento abbia un simmetrico a sinistra e uno a destra (distinti) ma sia privo di simmetrico, come accade all'elemento  $b$  nell'esempio seguente:

$\perp$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	$d$
$b$	$b$	$c$	$a$	$d$
$c$	$c$	$b$	$b$	$c$
$d$	$d$	$a$	$c$	$d$

Qui  $a$  è elemento neutro,  $b$  ha simmetrici a destra e a sinistra rispettivamente  $c$  e  $d$ , ma non ha simmetrico.

Ancora una volta, l'associatività dell'operazione determina un interessante risultato:

**4.1.13.** *Sia  $S$  un insieme dotato dell'operazione interna associativa  $\perp$  con elemento neutro  $e$ , e siano  $x, x_1, x_2 \in S$ . Se  $x_1$  è simmetrico a sinistra di  $x$  e  $x_2$  è simmetrico a destra di  $x$ , si ha  $x_1 = x_2$ .*

*Dimostrazione.* Con lo stesso procedimento già utilizzato in 4.1.10, si ha infatti:  $x_1 = x_1 \perp e = x_1 \perp (x \perp x_2) = (x_1 \perp x) \perp x_2 = e \perp x_2 = x_2$ .  $\square$

Sia sempre  $S$  un insieme con un'operazione interna  $\perp$ . Un elemento  $a \in S$  è detto **cancellabile** (o **regolare**) a sinistra rispetto a  $\perp$  se da  $a \perp x = a \perp y$  segue  $x = y$  (equivalentemente, se da  $x \neq y$  segue  $a \perp x \neq a \perp y$ ); è detto **cancellabile** (o **regolare**) a destra rispetto a  $\perp$  se da  $x \perp a = y \perp a$  segue  $x = y$  (cioè se  $x \neq y$  implica  $x \perp a \neq y \perp a$ ). Un elemento regolare a destra e a sinistra è detto **cancellabile** (o **regolare**) rispetto a  $\perp$ .

L'elemento neutro, se esiste, è ovviamente sempre regolare.

**4.1.14. Esempi.** In  $(\mathbb{N}, +)$ ,  $(\mathbb{N}_0, +)$ ,  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  ogni elemento è regolare, così in  $(\mathbb{N}, \cdot)$ .

In  $(\mathbb{N}_0, \cdot)$ ,  $(\mathbb{Z}, \cdot)$ ,  $(\mathbb{Q}, \cdot)$ ,  $(\mathbb{R}, \cdot)$  ogni elemento diverso da zero è regolare, lo 0 non lo è, avendosi, per esempio,  $0 \cdot 1 = 0 \cdot 2$  con  $1 \neq 2$ .

Considerate le operazioni in  $\mathbb{Z}$  introdotte in 4.1.1, si ha che nessun elemento è regolare rispetto a  $\perp_1$ ; ogni elemento è cancellabile a sinistra, nessuno a destra rispetto a  $\perp_2$ ; rispetto a  $\perp_3$  ogni elemento diverso da 0 è cancellabile a destra, mentre ogni elemento diverso da  $-1$  è cancellabile a sinistra, il che assicura che è regolare ogni elemento diverso da 0 e da  $-1$ . Quanto detto si ottiene osservando che, per esempio, per ogni  $x, y, z \in \mathbb{Z}$  risulta  $x \perp_1 1 = x \perp_1 (-1)$ , e che da  $x \perp_2 y = x \perp_2 z$  segue  $x^2 + y - 1 = x^2 + z - 1$ , da cui  $y = z$ . Si ha poi  $1 \perp_2 y = (-1) \perp_2 y$ ,  $1 \perp_3 0 = 2 \perp_3 0$ ,  $(-1) \perp_3 2 = (-1) \perp_3 3$ . Per ogni  $x, y, z \in \mathbb{Z}$ , se  $y \neq 0$  da  $xy + y = zy + y$  segue  $(x - z)y = 0$ , da cui  $x = z$ ; se invece  $x \neq -1$  da  $xy + y = xz + z$  segue  $(x + 1)y = (x + 1)z$ , da cui  $y = z$ . In  $\perp_4$  ogni elemento diverso da  $-1$  è regolare.

Si noti che, se l'operazione  $\perp$  è associativa, sussiste ancora un'interessante proprietà:

**4.1.15.** Sia  $S$  un insieme con un'operazione interna associativa  $\perp$  dotata di elemento neutro  $e$  e sia  $a \in S$ . Se  $a$  è simmetrizzabile, allora  $a$  è regolare.

*Dimostrazione.* Sia  $a'$  il simmetrico di  $a$ . Allora da  $a \perp x = a \perp y$  segue  $a' \perp (a \perp x) = a' \perp (a \perp y)$ , cioè  $(a' \perp a) \perp x = (a' \perp a) \perp y$ , il che equivale a  $e \perp x = e \perp y$ , ossia  $x = y$ . Analogamente da  $x \perp a = y \perp a$  segue  $x = y$ .  $\square$

L'ipotesi di associatività dell'operazione nella 4.1.15 è essenziale, come si può vedere dall'esempio che segue:

$\perp$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	$d$
$b$	$b$	$a$	$a$	$d$
$c$	$c$	$a$	$b$	$a$
$d$	$d$	$b$	$b$	$b$

Qui l'elemento  $a$  è neutro, l'elemento  $b$  ha per simmetrici  $b$  e  $c$ , l'elemento  $c$  ha simmetrico  $b$  e simmetrico a destra  $d$  (che non è simmetrico a sinistra), l'elemento  $d$  ha simmetrico a sinistra  $c$ , ma non ha simmetrico a destra. In particolare,  $b$  è simmetrizzabile ma non regolare, in quanto per esempio  $b \perp b = a = b \perp c$ .

In  $(\mathbb{N}_0, +)$  ogni numero diverso da 0 è regolare ma non simmetrizzabile, pertanto la proprietà enunciata nella 4.1.15 non si inverte, neppure se l'operazione è associativa. Se l'insieme  $S$  è finito e l'operazione  $\perp$  è associativa si ha però che un elemento è regolare se e solo se è simmetrizzabile (vedi Esercizio 4.1.15).

Spesso l'operazione  $\perp$  viene denotata col simbolo  $+$  o col simbolo  $\cdot$ , adottando rispettivamente la cosiddetta **notazione additiva** o **moltiplicativa**. Nel primo caso l'elemento neutro, se esiste, è indicato col simbolo 0, nel secondo col simbolo 1. Così, se l'operazione in  $S$  è associativa e l'elemento  $x$  è simmetrizzabile, il suo unico simmetrico è indicato col simbolo  $-x$ , detto l'**opposto** di  $x$ , in notazione additiva, col simbolo  $x^{-1}$ , detto l'**inverso** di  $x$ , in notazione moltiplicativa. Pertanto, in tali casi, con  $x, y \in S$  si ha:

$$\begin{aligned} -(x+y) &= (-y) + (-x), \\ -(-x) &= x, \\ (x^{-1})^{-1} &= x, \\ (xy)^{-1} &= y^{-1}x^{-1}. \end{aligned}$$

Se l'operazione  $+$  in  $S$  è associativa e  $x \in S$ , ha senso definire il **multiplo**  $nx$ , con  $n \in \mathbb{N}$ , ponendo:

$$nx := \begin{cases} x, & \text{se } n = 1, \\ (n-1)x + x, & \text{se } n > 1. \end{cases}$$

Dall'associatività segue subito che, per ogni  $x \in S$  e  $n, m \in \mathbb{N}$ , risulta:

$$(n+m)x = nx + mx, \quad (4.1.1)$$

$$(nm)x = n(mx). \quad (4.1.2)$$

Se in  $(S, +)$  c'è elemento neutro si pone inoltre  $0x := 0$ . Infine se in  $(S, +)$  esiste l'opposto  $-x$  di  $x$ , si pone, per ogni intero  $n < 0$ :

$$nx := (-n)(-x),$$

e così resta definito il multiplo  $nx$  per ogni  $n \in \mathbb{Z}$ , e continuano a valere le proprietà (4.1.1) e (4.1.2).

Analogamente, se l'operazione  $\cdot$  in  $S$  è associativa e  $x \in S$ , si definisce la *potenza*  $n$ -esima di  $x$ , con  $n \in \mathbb{N}$ , ponendo:

$$x^n := \begin{cases} x, & \text{se } n = 1, \\ x^{n-1} \cdot x, & \text{se } n > 1. \end{cases}$$

Se in  $(S, \cdot)$  esiste l'elemento neutro si pone inoltre  $x^0 := 1$  e, se esiste  $x^{-1}$ , si pone, per ogni intero  $n < 0$ :

$$x^n = (x^{-1})^{-n},$$

definendo così  $x^n$  per ogni  $n \in \mathbb{Z}$ . Per ogni  $x \in S$  e  $n, m \in \mathbb{N}$  valgono le proprietà:

$$x^{n+m} = x^n x^m, \quad (4.1.3)$$

$$x^{nm} = (x^n)^m. \quad (4.1.4)$$

Le (4.1.3) e (4.1.4) valgono per ogni  $n, m \in \mathbb{Z}$  se  $x$  è invertibile, quindi se esiste  $x^{-1}$ . Se in più l'operazione  $+$  (rispettivamente  $\cdot$ ) è commutativa, si ha, per ogni  $x, y \in S$  e per ogni  $n \in \mathbb{N}$  (per ogni  $n \in \mathbb{Z}$  se esistono i simmetrici di  $x$  e  $y$ ),

$$n(x+y) = nx + ny, \quad (\text{rispettivamente } (xy)^n = x^n y^n). \quad (4.1.5)$$

Si supponga che nell'insieme  $S$  siano definite operazioni interne  $\perp$  e  $\top$ . Si dice che l'operazione  $\top$  è **distributiva a sinistra** (rispettivamente **distributiva a destra**) rispetto a  $\perp$  se  $x \top (y \perp z) = (x \top y) \perp (x \top z)$  per ogni  $x, y, z \in S$  (risp.  $(x \perp y) \top z = (x \top z) \perp (y \top z)$ ). L'operazione  $\top$  è detta **distributiva** rispetto a  $\perp$  se lo è a destra e a sinistra.

**4.1.16. Esempi.** Il prodotto in  $\mathbb{N}$  (o in  $\mathbb{N}_0$ , o in  $\mathbb{Z}$ , o in  $\mathbb{Q}$ , o in  $\mathbb{R}$ ) è distributivo rispetto alla somma (vedi anche 1.2), la somma non lo è rispetto al prodotto in quanto, per esempio,  $1 + (2 \cdot 3) \neq (1 + 2) \cdot (1 + 3)$ .

Se  $V$  è un insieme, in  $\mathcal{P}(V)$  l'unione è distributiva rispetto all'intersezione (vedi (1.4.10)), e così l'intersezione rispetto all'unione (vedi (1.4.11)). L'intersezione è distributiva rispetto all'unione disgiunta (vedi 1.4.15), e, se  $V$  è non vuoto, il complemento è distributivo solo a destra rispetto all'unione e all'intersezione (vedi Esercizi 1.4.38 e 1.4.12).

Siano ora  $S$  e  $\Omega$  insiemi. Un'applicazione

$$\star : \Omega \times S \longrightarrow S$$

è detta un'*operazione esterna* di  $S$  con *dominio di operatori* in  $\Omega$  (o anche con *operatori* in  $\Omega$ ). Gli elementi di  $\Omega$  vengono di solito indicati con lettere greche e detti anche *scalari*; l'immagine mediante  $\star$  della coppia  $(\alpha, x)$  è di solito denotata col simbolo  $\alpha \star x$  e detta il *composto* di  $\alpha$  e  $x$  in  $\star$ .

#### 4.1.17. Esempi.

L'applicazione:

$$\star_1 : (\alpha, x) \in \mathbb{Q} \times \mathbb{R} \longmapsto \alpha \cdot x \in \mathbb{R}$$

è un'operazione esterna di  $\mathbb{R}$  con operatori in  $\mathbb{Q}$ . Così l'applicazione:

$$\star_2 : (\alpha, x) \in \mathbb{R} \times \mathbb{R} \longmapsto \alpha \cdot x \in \mathbb{R}$$

è un'operazione esterna di  $\mathbb{R}$  con operatori in  $\mathbb{R}$ , e l'applicazione:

$$\star_3 : (\alpha, (x, y)) \in \mathbb{R} \times \mathbb{R}^2 \longmapsto (\alpha \cdot x, \alpha \cdot y) \in \mathbb{R}^2$$

è un'operazione esterna di  $\mathbb{R}^2$  con operatori in  $\mathbb{R}$ . Con  $V$  insieme, l'applicazione:

$$\star_4 : (f, x) \in V^V \times V \longmapsto f(x) \in V$$

è un'operazione esterna di  $V$  con operatori in  $V^V$  e l'applicazione:

$$\star_5 : (v, X) \in V \times \mathcal{P}(V) \longmapsto X \cup \{v\} \in \mathcal{P}(V)$$

è un'operazione esterna di  $\mathcal{P}(V)$  con operatori in  $V$ .

Per un'operazione esterna  $\star$  di  $S$  con operatori in  $\Omega$  si preferisce di solito utilizzare il simbolo  $\cdot$ , e quindi denotare con  $\alpha \cdot x$  o più semplicemente con  $\alpha x$  il composto di  $\alpha$  e  $x$  in  $\star$ .

Un insieme  $S$  munito di una o più operazioni interne o esterne è detto una *struttura algebrica, semplice* se l'operazione è unica.

Per esempio  $(\mathbb{N}_0, +)$ ,  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot, \star_1)$ ,  $(\mathcal{P}(V), \cup, \cap, \setminus, \star_5)$  sono strutture algebriche, solo la prima di queste è semplice.

Si introdurranno ora alcune tra le principali strutture algebriche, che saranno poi considerate in capitoli seguenti.

La struttura  $(S, \perp)$ , con  $\perp$  operazione interna, è detta un *semigruppo* se  $\perp$  è associativa, un *monoide* se  $\perp$  è associativa e dotata di elemento neutro, un *gruppo* se  $\perp$  è associativa, esiste elemento neutro e ogni elemento è simmetrizzabile, un *gruppo abeliano* se l'operazione è anche commutativa.

La struttura  $(S, \perp, \top)$  con  $\perp$  e  $\top$  operazioni interne è detta un *anello* se  $(S, \perp)$  è un gruppo abeliano,  $\top$  è associativa ed è distributiva rispetto a  $\perp$ . Se in più esiste elemento neutro rispetto a  $\top$  l'anello è detto *unitario*; l'anello è detto *commutativo* se  $\top$  è commutativa. Un anello unitario  $(S, \perp, \top)$  è detto un

**corpo** se ha più di un elemento e ogni elemento distinto dall'elemento neutro di  $\perp$  è simmetrizzabile rispetto a  $\top$ ; se poi  $\top$  è commutativa,  $(S, \perp, \top)$  è detto un **campo**.

Sia  $(\Omega, +, \cdot)$  un corpo. La struttura  $(S, \perp, \star)$ , con  $\perp$  operazione interna e  $\star$  operazione esterna con operatori in  $\Omega$ , è detta un  **$\Omega$ -spazio vettoriale sinistro** (rispettivamente **destro**) se  $(S, \perp)$  è un gruppo abeliano e valgono le seguenti proprietà:

- 1)  $(\alpha + \beta) \star x = (\alpha \star x) \perp (\beta \star x)$ ,
- 2)  $\alpha \star (x \perp y) = (\alpha \star x) \perp (\alpha \star y)$ ,
- 3)  $(\alpha \cdot \beta) \star x = \alpha \star (\beta \star x)$ , (rispettivamente  $(\alpha \cdot \beta) \star x = \beta \star (\alpha \star x)$ ),
- 4)  $1 \star x = x$ ,

per ogni  $x, y \in S$  e  $\alpha, \beta \in \Omega$ , con 1 elemento neutro di  $(\Omega, \cdot)$ .

**4.1.18. Esempi.**  $(\mathbb{N}, +)$  è un semigruppo, non è un monoide;  $(\mathbb{N}_0, +)$  è un monoide, non è un gruppo;  $(\mathbb{Z}, +)$  è un gruppo abeliano;  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo unitario, non è un corpo;  $(\mathbb{Q}, +, \cdot)$  è un campo, e così  $(\mathbb{R}, +, \cdot)$ .

Con  $V$  insieme,  $(V^V, \cdot)$  è un monoide, ed è un gruppo se e solo se  $|V| = 1$ ;  $(\mathcal{P}(V), \cup, \cap)$  è un anello commutativo unitario, che risulta un campo se e solo se  $|V| = 1$ ;  $(\mathbb{R}, +, \star_1)$  è un  $\mathbb{Q}$ -spazio vettoriale.

**4.1.19. Esempio.** Una tabella del tipo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con  $a, b, c, d \in \mathbb{R}$ , è detta una **matrice**  $2 \times 2$  su  $\mathbb{R}$ , e si pone

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} : \iff a = a', b = b', c = c', d = d'.$$

Nell'insieme delle matrici  $2 \times 2$  su  $\mathbb{R}$ , indicato col simbolo  $M_2(\mathbb{R})$ , si introducono le seguenti operazioni interne:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & t \end{pmatrix} := \begin{pmatrix} a+x & b+y \\ c+z & d+t \end{pmatrix},$$

e

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} := \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}.$$

Si prova facilmente che  $(M_2(\mathbb{R}), +, \cdot)$  è un anello unitario, di unità  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , ma non commutativo. In modo analogo si costruiscono gli anelli  $M_2(\mathbb{Z})$ ,  $M_2(\mathbb{Q})$ ,  $M_2(\mathbb{C})$ . Si rimanda al Capitolo 7 per uno studio più dettagliato dell'anello delle matrici su un qualunque anello commutativo unitario.

Siano  $(S, \perp_1)$  e  $(T, \perp_2)$  strutture semplici con operazioni interne e si consideri, nel prodotto cartesiano  $S \times T$ , la seguente operazione:

$$(x, y) \perp (x', y') := (x \perp_1 x', y \perp_2 y').$$

La struttura  $(S \times T, \perp)$  viene detta il **prodotto** di  $(S, \perp_1)$  e  $(T, \perp_2)$ .

**4.1.20.** Con le notazioni precedenti si ha:

- (i)  $\perp$  è commutativa (rispettivamente associativa) se e solo se  $\perp_1$  e  $\perp_2$  sono entrambe commutative (risp. associative);
- (ii) esiste elemento neutro  $e$  in  $(S \times T, \perp)$  se e solo se le strutture  $(S, \perp_1)$  e  $(T, \perp_2)$  sono entrambe dotate di elemento neutro, rispettivamente  $e_1$  ed  $e_2$ , e si ha  $e = (e_1, e_2)$ ;
- (iii) l'elemento  $(x, y)$  di  $S \times T$  è simmetrizzabile in  $(S \times T, \perp)$ , di simmetrico  $(x, y)'$ , se e solo se  $x$  è simmetrizzabile in  $(S, \perp_1)$ , di simmetrico  $x'$ , e  $y$  è simmetrizzabile in  $(T, \perp_2)$ , di simmetrico  $y'$ , e si ha  $(x, y)' = (x', y')$ .

*Dimostrazione.* Esercizio. □

La proposizione precedente assicura che  $(S \times T, \perp)$  è un semigruppo (monoide, gruppo) se  $(S, \perp_1)$  e  $(T, \perp_2)$  sono entrambi semigruppi (rispettivamente monoidi, gruppi).

## Esercizi

**Esercizio 4.1.1.** Si provi l'associatività dell'operazione  $\perp_4$  in  $\mathbb{Z}$  definita in 4.1.1.

**Svolgimento.** Per ogni  $x, y, z \in \mathbb{Z}$  si ha:  $(x \perp_4 y) \perp_4 z = (x + y + xy) \perp_4 z = x + y + xy + z + xz + yz + xyz$ , e  $x \perp_4 (y \perp_4 z) = x \perp_4 (y + z + yz) = x + y + z + yz + xy + xz + xyz$ , pertanto  $(x \perp_4 y) \perp_4 z = x \perp_4 (y \perp_4 z)$ .

**Esercizio 4.1.2.** Si consideri, nell'insieme  $\mathbb{Z}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = n + m - 1$  per ogni  $n, m \in \mathbb{Z}$ . Si studi la struttura  $(\mathbb{Z}, \perp)$ .

**Esercizio 4.1.3.** Si consideri, nell'insieme  $\mathbb{Z}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = nm - 5n - 5m + 30$  per ogni  $n, m \in \mathbb{Z}$ . Si studi la struttura  $(\mathbb{Z}, \perp)$ .

**Esercizio 4.1.4.** Si consideri, nell'insieme  $\mathbb{Q}$ , l'operazione  $\perp$  definita ponendo  $x \perp y = \frac{3xy}{2}$  per ogni  $x, y \in \mathbb{Q}$ . Si studi la struttura  $(\mathbb{Q}, \perp)$ .

**Esercizio 4.1.5.** Si consideri, nell'insieme  $5\mathbb{N}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = \frac{nm}{5}$  per ogni  $n, m \in 5\mathbb{N}$ . Si studi la struttura  $(5\mathbb{N}, \perp)$ .

**Esercizio 4.1.6.** Si consideri, nell'insieme  $\mathbb{Q}$ , l'operazione  $\perp$  definita ponendo  $x \perp y = x + y - \frac{1}{3}$  per ogni  $x, y \in \mathbb{Q}$ . Si studi la struttura  $(\mathbb{Q}, \perp)$ .

**Esercizio 4.1.7.** Si consideri, nell'insieme  $2\mathbb{N}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = 8 + n + m$  per ogni  $n, m \in 2\mathbb{N}$ . Si studi la struttura  $(2\mathbb{N}, \perp)$ .

**Esercizio 4.1.8.** Si consideri, nell'insieme  $2\mathbb{Z}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = 6 + n + m$  per ogni  $n, m \in 2\mathbb{Z}$ . Si studi la struttura  $(2\mathbb{Z}, \perp)$ .

**Esercizio 4.1.9.** Si consideri, nell'insieme  $2\mathbb{Z}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = 4n + 4m - \frac{mn}{2} - 40$  per ogni  $n, m \in 2\mathbb{Z}$ . Si studi la struttura  $(2\mathbb{Z}, \perp)$ .

**Esercizio 4.1.10.** Si consideri, nell'insieme  $3\mathbb{Z}$ , l'operazione  $\perp$  definita ponendo  $n \perp m = n + m - 18$  per ogni  $n, m \in 3\mathbb{Z}$ . Si studi la struttura  $(3\mathbb{Z}, \perp)$ .

**Esercizio 4.1.11.** Si consideri in  $\mathbb{Q}$  l'operazione  $\perp$  introdotta nell'Esempio 4.1.9. Si provi che  $x$  è simmetrizzabile se e solo se  $x < 1$  e ha come unico simmetrico  $-\frac{x}{1-x}$  se  $x \geq -1$ , ha come simmetrici  $-\frac{x}{1-x}$  e  $-\frac{x}{1+x}$  se  $x < -1$ .

**Esercizio 4.1.12.** Si consideri nell'insieme  $\mathbb{Z}$  l'operazione interna definita ponendo  $x \perp y = x + y - xy$  per ogni  $x, y \in \mathbb{Z}$ . Si provi che 0 è elemento neutro, che 0 e 2 sono i soli elementi simmetrizzabili e che ogni elemento di  $\mathbb{Z} \setminus \{1\}$  è regolare.

**Esercizio 4.1.13.** Il concetto di regolarità può essere espresso utilizzando le seguenti applicazioni:

$$\begin{aligned} T_a^s : x \in S &\longmapsto a \perp x \in S, \\ T_a^d : x \in S &\longmapsto x \perp a \in S, \end{aligned}$$

dette, rispettivamente, la **traslazione sinistra** e la **traslazione destra** individuata da  $a$  in  $(S, \perp)$ . Si provi che infatti:

- (i)  $a$  è cancellabile a sinistra se e solo se  $T_a^s$  è iniettiva,
- (ii)  $a$  è cancellabile a destra se e solo se  $T_a^d$  è iniettiva.

**Esercizio 4.1.14.** Sia  $(S, \perp)$  un insieme con un'operazione interna  $\perp$  associativa e sia  $a \in S$ . Si provi che le seguenti affermazioni sono equivalenti:

- (i)  $a$  è simmetrizzabile;
- (ii)  $T_a^s$  e  $T_a^d$  biettive;
- (iii)  $T_a^s$  e  $T_a^d$  suriettive.

**Suggerimento.** Per provare che (iii) implica (i) si osservi innanzitutto che esiste un elemento  $u \in S$  tale che  $u \perp a = a$ . Scritto ogni elemento  $s \in S$  come  $a \perp s'$ , si verifichi che  $u$  è elemento neutro a sinistra per  $\perp$ . Ragionando in modo analogo si provi l'esistenza di un elemento neutro a destra. Si deduca che esiste elemento neutro. Si individuino poi elementi  $a'$  e  $a''$  tali che  $u = a \perp a' = a'' \perp a$  e si concluda che  $a$  è simmetrizzabile.

**Esercizio 4.1.15.** Sia  $(S, \perp)$  una struttura algebrica, con  $S$  finito e  $\perp$  associativa. Si provi che un elemento  $a \in S$  è simmetrizzabile se e solo se è regolare.

**Suggerimento.** Si utilizzi l'esercizio precedente.

**Esercizio 4.1.16.** Si considerino, nell'insieme  $\mathbb{N}_0$ , le operazioni binarie  $\perp$  e  $\top$  definite ponendo

$$\begin{aligned} n \perp m &= n + 2m, \\ n \top m &= 2nm, \end{aligned}$$

per ogni  $n, m \in \mathbb{N}_0$ . Si studi la struttura  $(\mathbb{N}_0, \perp, \top)$ , e in particolare si provi che  $\top$  è distributiva rispetto a  $\perp$ .

**Esercizio 4.1.17.** Siano  $S = \{x_1, \dots, x_n\}$  un insieme finito e  $\perp$  un'operazione interna in  $S$ , e si rappresenti  $\perp$  mediante una tabella.

- (i) Si mostri che  $\perp$  è commutativa se, e solo se, la tabella che la rappresenta è simmetrica rispetto alla diagonale principale.
- (ii) Si dimostri che l'elemento  $e \in S$  è neutro a sinistra (destra) se, e solo se, nella riga (nella colonna) corrispondente a  $e$  ricompaiono, nell'ordine, gli elementi  $x_1, \dots, x_n$ .
- (iii) Si dimostri che l'elemento  $x_i$  ha simmetrico a sinistra (a destra) se, e solo se, nella colonna (nella riga) corrispondente a  $x_i$  compare l'elemento neutro  $e$ .
- (iv) Si dimostri che l'elemento  $x_i$  è cancellabile a sinistra (a destra) se, e solo se, nella riga (nella colonna) corrispondente a  $x_i$  non compaiono ripetizioni.

**Esercizio 4.1.18.** Si dimostri 4.1.20.

**Esercizio 4.1.19.** Siano  $(S, \star_1)$  e  $(T, \star_2)$  strutture semplici con operazioni esterne entrambe con operatori in  $\Omega$ . In  $S \times T$  si può definire un'operazione esterna con operatori in  $\Omega$  ponendo  $\alpha \star (x, y) := (\alpha \star_1 x, \alpha \star_2 y)$ . Si provi che se  $(S, \perp_1, \star_1)$  e  $(T, \perp_2, \star_2)$  sono spazi vettoriali sinistri (destrici) sul corpo  $(\Omega, +, \cdot)$ , la struttura prodotto  $(S \times T, \perp, \star)$  è uno spazio vettoriale sinistro (destro) su  $\Omega$ .

## 4.2 Sottostrutture e strutture quoziante

Si consideri la struttura  $(S, \perp)$ , con  $\perp$  operazione interna in  $S$ . Una parte  $X$  di  $S$  è detta **stabile** (o **chiusa**) rispetto a  $\perp$  (o di  $(S, \perp)$ ) se da  $x, y \in X$  segue  $x \perp y \in X$ . In tal caso è possibile definire in  $X$  la cosiddetta **operazione indotta**  $\perp'$  da  $\perp$  su  $X$  nel seguente modo:

$$\perp': (x, y) \in X \times X \longmapsto x \perp y \in X.$$

Si pone cioè  $x \perp' y := x \perp y$ , per ogni  $x, y \in X$ .

**4.2.1. Esempi.** Il sottoinsieme vuoto di  $S$  è sempre una parte stabile di  $(S, \perp)$ , e così  $S$  stesso.

L'insieme  $\mathbb{N}_0$  è stabile in  $(\mathbb{Z}, +)$  e in  $(\mathbb{Z}, \cdot)$  e le operazioni indotte coincidono con le usuali somma e prodotto di  $\mathbb{N}_0$ . Così  $\mathbb{N}$  è parte stabile in  $(\mathbb{N}_0, +)$  e  $(\mathbb{N}_0, \cdot)$  (vedi (1.2.4) e (1.2.11)).

Il sottoinsieme  $\mathbb{N}_p$  di  $\mathbb{N}_0$  è una parte stabile sia in  $(\mathbb{N}_0, +)$  che in  $(\mathbb{N}_0, \cdot)$ ; il sottoinsieme  $\mathbb{N}_d$  di  $\mathbb{N}_0$  è stabile in  $(\mathbb{N}_0, \cdot)$ , non lo è in  $(\mathbb{N}_0, +)$ , avendosi, per esempio,  $1 + 1 = 2 \notin \mathbb{N}_d$ .

**4.2.2.** Sia  $S$  un insieme dotato di un'operazione interna  $\perp$  e sia  $X \subseteq S$  stabile rispetto a  $\perp$ . Sia  $\perp'$  l'operazione indotta da  $\perp$  su  $X$ . Si ha che:

- (i) se  $\perp$  è associativa, lo è anche  $\perp'$ ;
- (ii) se  $\perp$  è commutativa, tale è anche  $\perp'$ ;
- (iii) se in  $S$  esiste elemento neutro  $e$  ed  $e \in X$ , allora  $e$  è neutro in  $(X, \perp')$ ; se inoltre l'elemento  $x \in S$  ha simmetrico  $x'$  in  $S$ , con  $x, x' \in X$ , allora  $x'$  è simmetrico di  $x$  in  $(X, \perp')$ .

*Dimostrazione.* Esercizio. □

Spesso nel seguito l'operazione indotta su una parte stabile  $X$  da un'operazione interna  $\perp$  di  $S$  sarà denotata ancora con il simbolo  $\perp$ .

Di notevole interesse è la seguente:

**4.2.3.** Sia  $(S, \perp)$  un monoide e si consideri l'insieme

$$U(S) = \{x \in S : x \text{ simmetrizzabile}\}.$$

Allora  $U(S)$  è una parte stabile di  $(S, \perp)$  e, con la legge indotta, è un gruppo, detto il **gruppo degli elementi simmetrizzabili** del monoide  $(S, \perp)$ .

*Dimostrazione.* La stabilità di  $U(S)$  segue subito da 4.1.11, e l'operazione indotta è associativa per la (i) di 4.2.2. Inoltre, come già osservato, l'elemento neutro  $e$  di  $S$  appartiene a  $U(S)$  e, se  $x \in U(S)$ , anche il suo simmetrico  $x' \in U(S)$ . Pertanto da (iii) di 4.2.2 segue che  $(U(S), \perp)$  è un gruppo. □

Ovviamente, se  $(S, \perp)$  è un gruppo, esso coincide con  $(U(S), \perp)$ .

**4.2.4. Esempi.** Il gruppo degli elementi simmetrizzabili di  $(\mathbb{N}_0, +)$  è  $(\{0\}, +)$ , di  $(\mathbb{N}_0, \cdot)$  è  $(\{1\}, \cdot)$ , di  $(\mathbb{Z}, \cdot)$  è  $(\{1, -1\}, \cdot)$ , di  $(\mathbb{Q}, \cdot)$  è  $(\mathbb{Q} \setminus \{0\}, \cdot)$ , di  $(V^V, \cdot)$  è  $(S_V, \cdot)$ , dove  $S_V$  è l'insieme delle permutazioni su  $V$ .

Un analogo concetto di parte stabile viene introdotto per un insieme  $S$  dotato di un'operazione esterna  $\star$  con operatori in  $\Omega$ .

Un sottoinsieme  $X$  di  $S$  è detto **stabile** rispetto a  $\star$  se da  $\alpha \in \Omega, x \in X$  segue  $\alpha \star x \in X$ . È allora possibile definire l'operazione esterna  $\star'$  di  $X$  con operatori in  $\Omega$  ponendo:

$$\star' : (\alpha, x) \in \Omega \times X \longmapsto \alpha \star x \in X.$$

Ancora si userà spesso il simbolo  $\star$  per denotare anche l'operazione indotta.

**4.2.5. Esempio.** La diagonale  $\Delta_{\mathbb{R}}$  di  $\mathbb{R}^2$  è stabile rispetto all'operazione esterna  $\star_3$  definita in 4.1.17, in quanto risulta  $\alpha \star_3 (x, x) = (\alpha x, \alpha x) \in \Delta_{\mathbb{R}}$ , per ogni  $\alpha \in \mathbb{R}, (x, x) \in \Delta_{\mathbb{R}}$ .

L'unione di parti stabili non è di solito una parte stabile: si considerino per esempio  $3\mathbb{N}$  e  $4\mathbb{N}$  in  $(\mathbb{N}, +)$ . Vale però la notevole:

**4.2.6.** *Sia  $(S, \perp)$  una struttura algebrica semplice e sia  $(T_i)_{i \in I}$  una famiglia di parti stabili di  $S$ . Allora  $\bigcap_{i \in I} T_i$  è stabile.*

*Dimostrazione.* Si supponga  $\perp$  interna e siano  $x, y \in \bigcap_{i \in I} T_i$ . Allora  $x, y \in T_i$  per ogni  $i \in I$  e dunque, per la stabilità di  $T_i$ , si ha  $x \perp y \in T_i$ , per ogni  $i \in I$ , da cui  $x \perp y \in \bigcap_{i \in I} T_i$ .

Sia ora  $\perp$  esterna con dominio di operatori  $\Omega$ , e siano  $x \in \bigcap_{i \in I} T_i$  e  $\alpha \in \Omega$ . Da  $x \in T_i$  per ogni  $i \in I$  e da  $T_i$  stabile, per ogni  $i \in I$ , segue  $\alpha \perp x \in T_i$  per ogni  $i \in I$ , da cui  $\alpha \perp x \in \bigcap_{i \in I} T_i$ .  $\square$

La proprietà precedente suggerisce la seguente importante definizione. Sia  $(S, \perp)$  una struttura algebrica semplice e sia  $X$  una sua parte. Si definisce **parte stabile generata da  $X$** , e si indica con il simbolo  $\overline{X}$ , l'intersezione delle parti stabili di  $S$  contenenti  $X$ :

$$\overline{X} := \bigcap_{\substack{X \subseteq T \subseteq S \\ T \text{ stabile}}} T.$$

Ovviamente si ha  $\overline{X} = X$  se e solo se  $X$  è una parte stabile. Si noti poi che  $\overline{X}$  è una parte stabile, ovviamente contiene  $X$ , ed è contenuta in ogni parte stabile di  $S$  contenente  $X$ . Tali proprietà caratterizzano la parte  $\overline{X}$ , infatti si ha:

**4.2.7.** *Sia  $(S, \perp)$  una struttura algebrica semplice e sia  $X$  una parte di  $S$ . La parte  $W$  di  $S$  coincide con  $\overline{X}$  se e solo se valgono le seguenti proprietà:*

- (i)  $W$  è stabile;
- (ii)  $W \supseteq X$ ;
- (iii)  $T \subseteq S$ ,  $T$  stabile,  $T \supseteq X \implies T \supseteq W$ .

*Dimostrazione.* Esercizio.  $\square$

Se la struttura  $(S, \perp)$  è tale che l'operazione  $\perp$  è interna e associativa, e  $X \subseteq S$ , sussiste un'efficace descrizione di  $\overline{X}$ .

**4.2.8.** *Sia  $(S, \perp)$  una struttura algebrica semplice, con  $\perp$  interna e associativa, e sia  $X$  una parte non vuota di  $S$ . Allora:*

$$\overline{X} = \{x_1 \perp \cdots \perp x_n : n \in \mathbb{N}, x_1, \dots, x_n \in X\}.$$

*Dimostrazione.* Si ponga  $W = \{x_1 \perp \cdots \perp x_n : n \in \mathbb{N}, x_1, \dots, x_n \in X\}$ . È facile allora provare che  $W$  gode delle proprietà (i), (ii) e (iii) della 4.2.7, sicché  $W = \overline{X}$ .  $\square$

Sia  $\perp$  un'operazione interna in un insieme  $S$  e sia  $\mathcal{R}$  una relazione d'equivalenza in  $S$ . La relazione  $\mathcal{R}$  è detta **compatibile** con  $\perp$ , o una **congruenza** in  $(S, \perp)$ , se, con  $x, x_1, y, y_1 \in S$ , da  $x \mathcal{R} x_1, y \mathcal{R} y_1$  segue  $(x \perp y) \mathcal{R} (x_1 \perp y_1)$ .

Se  $\mathcal{R}$  è una congruenza in  $(S, \perp)$ , è possibile definire la cosiddetta **operazione quoziante**  $\tilde{\perp}$  di  $\perp$  in  $S/\mathcal{R}$  ponendo:

$$\tilde{\perp} : ([x]_{\mathcal{R}}, [y]_{\mathcal{R}}) \in S/\mathcal{R} \times S/\mathcal{R} \mapsto [x \perp y]_{\mathcal{R}} \in S/\mathcal{R},$$

cioè

$$[x]_{\mathcal{R}} \tilde{\perp} [y]_{\mathcal{R}} := [x \perp y]_{\mathcal{R}}.$$

Infatti, se  $([x]_{\mathcal{R}}, [y]_{\mathcal{R}}) = ([x_1]_{\mathcal{R}}, [y_1]_{\mathcal{R}})$ , cioè se  $[x]_{\mathcal{R}} = [x_1]_{\mathcal{R}}$  e  $[y]_{\mathcal{R}} = [y_1]_{\mathcal{R}}$ , si ha  $x \mathcal{R} x_1$  e  $y \mathcal{R} y_1$ , sicché, per la compatibilità di  $\mathcal{R}$ , riesce  $(x \perp y) \mathcal{R} (x_1 \perp y_1)$ , da cui  $[x \perp y]_{\mathcal{R}} = [x_1 \perp y_1]_{\mathcal{R}}$ .

**Osservazione.** Si noti che la compatibilità di  $\mathcal{R}$  è anche condizione necessaria perché abbia senso l'applicazione  $\tilde{\perp}$ .

**4.2.9. Esempio.** Nel monoide  $(\mathbb{N}_0, +)$  è una congruenza la relazione  $\mathcal{R}$  definita ponendo  $a \mathcal{R} b : \iff a + b \in 2\mathbb{N}_0$ , in quanto  $x \mathcal{R} x_1, y \mathcal{R} y_1$  comporta  $x + x_1, y + y_1 \in 2\mathbb{N}_0$ , sicché  $x + x_1 + y + y_1 \in 2\mathbb{N}_0$ , da cui  $(x + y) \mathcal{R} (x_1 + y_1)$ . Ha quindi senso la struttura  $(\mathbb{N}_0/\mathcal{R}, \tilde{+})$ , dove  $[x]_{\mathcal{R}} \tilde{+} [y]_{\mathcal{R}} = [x + y]_{\mathcal{R}}$ . Risulta (vedi Esempi 2.3.4)  $\mathbb{N}_0/\mathcal{R} = \{[0]_{\mathcal{R}}, [1]_{\mathcal{R}}\}$  e

$\tilde{+}$	$[0]_{\mathcal{R}}$	$[1]_{\mathcal{R}}$
$[0]_{\mathcal{R}}$	$[0]_{\mathcal{R}}$	$[1]_{\mathcal{R}}$
$[1]_{\mathcal{R}}$	$[1]_{\mathcal{R}}$	$[0]_{\mathcal{R}}$

Sussiste la seguente:

**4.2.10.** Sia  $S$  un insieme dotato di un'operazione interna  $\perp$  e sia  $\mathcal{R}$  una congruenza in  $(S, \perp)$ . Sia  $\tilde{\perp}$  l'operazione quoziante. Si ha che:

- (i) se  $\perp$  è associativa, lo è anche  $\tilde{\perp}$ ;
- (ii) se  $\perp$  è commutativa, tale è anche  $\tilde{\perp}$ ;
- (iii) se in  $S$  esiste elemento neutro  $e$ , allora  $[e]_{\mathcal{R}}$  è neutro in  $(S/\mathcal{R}, \tilde{\perp})$ ; se inoltre l'elemento  $x \in S$  ha simmetrico  $x'$  in  $S$ , allora  $[x']_{\mathcal{R}}$  è simmetrico di  $[x]_{\mathcal{R}}$  in  $(S/\mathcal{R}, \tilde{\perp})$ .

Se in  $S$  è definita anche l'operazione  $\top$  e  $\mathcal{R}$  è compatibile anche con  $\top$ , si ha che:

- (iv) se  $\top$  è distributiva rispetto a  $\perp$ , allora l'operazione quoziante  $\tilde{\top}$  è distributiva rispetto a  $\tilde{\perp}$ .

*Dimostrazione.* Esercizio. □

Spesso nel seguito l'operazione quoziante individuata da una congruenza  $\mathcal{R}$  in  $(S, \perp)$  sarà denotata ancora con il simbolo  $\perp$ .

Dalla 4.2.10 segue subito che se  $(S, \perp)$  è un semigruppo, anche  $(S/\mathcal{R}, \perp)$  è un semigruppo, se  $(S, \perp)$  è un monoide, anche  $(S/\mathcal{R}, \perp)$  è un monoide, e se  $(S, \perp)$  è un gruppo, anche  $(S/\mathcal{R}, \perp)$  è un gruppo.

Se in  $S$  è definita l'operazione esterna  $*$  con operatori in  $\Omega$ , una relazione d'equivalenza  $\mathcal{R}$  in  $S$  è detta **compatibile** con  $*$ , o una **congruenza** in  $(S, *)$ , se, con  $\alpha \in \Omega$  e  $x, y \in S$ , da  $x \mathcal{R} y$  segue  $(\alpha * x) \mathcal{R} (\alpha * y)$ .

In tal caso si definisce l'operazione quoziante  $\tilde{*}$  di  $S/\mathcal{R}$  con dominio di operatori  $\Omega$  ponendo:

$$\tilde{*} : (\alpha, [x]_{\mathcal{R}}) \in \Omega \times S/\mathcal{R} \longmapsto [\alpha * x]_{\mathcal{R}} \in S/\mathcal{R}.$$

Ciò è lecito in quanto da  $(\alpha, [x]_{\mathcal{R}}) = (\alpha, [y]_{\mathcal{R}})$ , cioè da  $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$  segue  $x \mathcal{R} y$  e  $(\alpha * x) \mathcal{R} (\alpha * y)$ , da cui  $[\alpha * x]_{\mathcal{R}} = [\alpha * y]_{\mathcal{R}}$ .

Ancora si userà spesso il simbolo  $*$  per denotare anche l'operazione quoziante individuata da una congruenza  $\mathcal{R}$  in  $(S, *)$ .

**4.2.11. Esempio.** Considerato  $\mathbb{R}^2$  con l'operazione esterna  $*_3$  con operatori in  $\mathbb{R}$  definita in 4.1.17, si ha che è una congruenza la relazione  $\mathcal{R}$  definita da  $(a, b) \mathcal{R} (c, d) : \iff a = c$ . Infatti  $(a, b) \mathcal{R} (c, d)$  implica  $\alpha *_3 (a, b) \mathcal{R} \alpha *_3 (c, d)$ , poiché da  $a = c$  segue  $\alpha a = \alpha c$  e dunque  $(\alpha a, \alpha b) \mathcal{R} (\alpha c, \alpha d)$ . Si ottiene così la struttura  $(\mathbb{R}^2/\mathcal{R}, \tilde{*}_3)$ , dove  $\alpha \tilde{*}_3 [(x, y)]_{\mathcal{R}} = [(\alpha x, \alpha y)]_{\mathcal{R}}$ , per ogni  $\alpha \in \mathbb{R}$ ,  $(x, y) \in \mathbb{R}^2$ .

Se in  $S$  sono definite più operazioni, una parte  $X$  è detta stabile (o chiusa) nella struttura  $S$  se è stabile rispetto a ogni operazione di  $S$ . Una relazione d'equivalenza  $\mathcal{R}$  è poi una congruenza nella struttura  $S$  se è una congruenza rispetto a ogni operazione di  $S$ . Da 4.2.10 segue allora che se  $\mathcal{R}$  è una congruenza nell'anello  $(S, \perp, \top)$ , anche la struttura quoziante  $(S/\mathcal{R}, \tilde{\perp}, \tilde{\top})$  è un anello, commutativo se lo è  $(S, \perp, \top)$ , unitario se lo è  $(S, \perp, \top)$ .

## Esercizi

**Esercizio 4.2.1.** Si dimostri 4.2.2.

**Esercizio 4.2.2.** Si dimostri 4.2.7.

**Esercizio 4.2.3.** Si dimostri 4.2.10.

**Esercizio 4.2.4.** Si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $3h + 1$ , con  $h \in \mathbb{N}_0$ :

$$W = \{3h + 1 : h \in \mathbb{N}_0\}.$$

(i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ , non di  $(\mathbb{N}_0, +)$ .

(ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$(3h + 1) \mathcal{R} (3k + 1) : \iff h + k \in 2\mathbb{N}_0$$

è d'equivalenza.

(iii) Si verifichi che  $\mathcal{R}$  è una congruenza in  $(W, \cdot)$  e si studi la struttura quoziante  $(W/\mathcal{R}, \cdot)$ .

**Esercizio 4.2.5.** Si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $2^n 3^m$ , con  $n, m \in \mathbb{N}_0$ :

$$W = \{2^n 3^m : n, m \in \mathbb{N}_0\}.$$

(i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ .

(ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$(2^n 3^m) \mathcal{R} (2^s 3^t) : \iff n + t = m + s$$

è d'equivalenza.

(iii) Si verifichi che  $\mathcal{R}$  è una congruenza in  $(W, \cdot)$  e che quindi ha senso definire in  $W/\mathcal{R}$  l'operazione quoziante ponendo

$$[2^n 3^m]_{\mathcal{R}} \cdot [2^i 3^j]_{\mathcal{R}} = [2^{n+i} 3^{m+j}]_{\mathcal{R}}.$$

(iv) Si studi la struttura  $(W/\mathcal{R}, \cdot)$ .

**Esercizio 4.2.6.** Si consideri l'insieme  $W$  costituito dai numeri naturali della forma  $3^n 7^m$ , con  $n, m \in \mathbb{N}_0$ :

$$W = \{3^n 7^m : n, m \in \mathbb{N}_0\}.$$

(i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ , non di  $(\mathbb{N}_0, +)$ .

(ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$3^n 7^m \mathcal{R} 3^s 7^t : \iff |n - m| = |s - t|$$

è d'equivalenza e non è una congruenza in  $(W, \cdot)$ .

**Esercizio 4.2.7.** Si consideri l'insieme

$$W = \{2^n 5^m : n, m \in \mathbb{N}_0\}.$$

(i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ , non di  $(\mathbb{N}_0, +)$ .

(ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 5^m \mathcal{R} 2^s 5^t : \iff |n - s| \in 2\mathbb{N}_0$$

è d'equivalenza e che è una congruenza in  $(W, \cdot)$ .

(iii) Si studi la struttura  $(W/\mathcal{R}, \cdot)$ .

**Esercizio 4.2.8.** Sia  $\perp$  un'operazione interna in un insieme  $S$  e sia  $\mathcal{R}$  una relazione d'equivalenza in  $S$ . La relazione  $\mathcal{R}$  è detta **compatibile a sinistra** (rispettivamente **a destra**) con  $\perp$  se da  $a \mathcal{R} b$ ,  $c \in S$  segue  $(c \perp a) \mathcal{R} (c \perp b)$  (risp.  $(a \perp c) \mathcal{R} (b \perp c)$ ). Si provi che  $\mathcal{R}$  è una congruenza in  $(S, \perp)$  se e solo se è compatibile a destra e a sinistra. In particolare, se  $\perp$  è commutativa,  $\mathcal{R}$  è una congruenza in  $(S, \perp)$  se, e solo se, è compatibile a sinistra (o a destra).

### 4.3 Omomorfismi tra strutture

Siano  $(S, \perp)$  e  $(T, \top)$  strutture algebriche con un'operazione interna. Un'applicazione  $f : S \rightarrow T$  è detta un **omomorfismo** di  $(S, \perp)$  in  $(T, \top)$  se si ha  $f(x \perp y) = f(x) \top f(y)$ , per ogni  $x, y \in S$ . Un omomorfismo iniettivo è detto un **monomorfismo**, un omomorfismo suriettivo è detto un **epimorfismo**, un omomorfismo biettivo è detto un **isomorfismo**. Un omomorfismo di una struttura  $(S, \perp)$  in se stessa è detto un **endomorfismo**, **automorfismo** se è anche biettivo.

**4.3.1. Esempi.** L'applicazione  $g : n \in \mathbb{N}_0 \mapsto 2^n \in \mathbb{N}$  è un monomorfismo di  $(\mathbb{N}_0, +)$  in  $(\mathbb{N}, \cdot)$ , infatti si ha  $g(n+m) = 2^{n+m} = 2^n \cdot 2^m = g(n) \cdot g(m)$ , per ogni  $n, m \in \mathbb{N}_0$ . Inoltre  $g$  è ovviamente iniettiva. Tale applicazione  $g$  non è un omomorfismo di  $(\mathbb{N}_0, \cdot)$  in  $(\mathbb{N}, \cdot)$ , in quanto, per esempio,  $g(2 \cdot 3) = g(6) = 2^6 \neq 2^5 = 2^2 \cdot 2^3 = g(2) \cdot g(3)$ .

Con  $V$  insieme d'ordine 1, l'applicazione  $h : \mathcal{P}(V) \rightarrow \{1, -1\}$  definita ponendo  $h(\emptyset) = 1, h(V) = -1$  è un isomorfismo di  $(\mathcal{P}(V), \dot{\cup})$  in  $(\{-1, 1\}, \cdot)$ .

Si consideri la struttura  $(S, \perp)$ ; l'applicazione identica  $\text{id}_S : S \rightarrow S$  è un isomorfismo di  $(S, \perp)$ . Più in generale, se  $X$  è una parte stabile di  $S$ , l'immersione  $\text{imm}_X : X \rightarrow S$  è un monomorfismo di  $(X, \perp')$  in  $(S, \perp)$ , dove  $\perp'$  indica, come al solito, l'operazione indotta da  $\perp$  su  $X$ .

Se  $\mathcal{R}$  è una congruenza in  $(S, \perp)$ , l'applicazione

$$\pi : x \in S \mapsto [x]_{\mathcal{R}} \in S/\mathcal{R}$$

è un epimorfismo di  $(S, \perp)$  in  $(S/\mathcal{R}, \tilde{\perp})$ , dove  $\tilde{\perp}$  indica l'operazione quoziante di  $\perp$  in  $(S/\mathcal{R})$ . Infatti ovviamente  $\pi$  è suriettiva; inoltre, per come è definita l'operazione quoziante  $\tilde{\perp}$ , si ha  $\pi(x \perp y) = [x \perp y]_{\mathcal{R}} = [x]_{\mathcal{R}} \tilde{\perp} [y]_{\mathcal{R}} = \pi(x) \tilde{\perp} \pi(y)$ , per ogni  $x, y \in S$ , come volevasi. L'epimorfismo  $\pi$  è detto l'**epimorfismo canonico** di  $(S, \perp)$  in  $(S/\mathcal{R}, \tilde{\perp})$ .

Si ha:

**4.3.2.** Siano  $(S, \perp), (T, \top)$  e  $(V, \odot)$  strutture semplici, con  $\perp, \top, \odot$  operazioni interne. Siano  $f : S \rightarrow T$  e  $g : T \rightarrow V$  omomorfismi. Allora  $g \circ f$  è un omomorfismo di  $(S, \perp)$  in  $(V, \odot)$ .

*Dimostrazione.* Esercizio. □

**4.3.3.** Siano  $(S, \perp)$  e  $(T, \top)$  strutture semplici, con  $\perp$  e  $\top$  operazioni interne. Se  $f : S \rightarrow T$  è un isomorfismo di  $(S, \perp)$  in  $(T, \top)$ , allora l'inversa  $f^{-1}$  di  $f$  è un isomorfismo di  $(T, \top)$  in  $(S, \perp)$ .

*Dimostrazione.* Esercizio. □

Strutture  $(S, \perp)$  e  $(T, \top)$  tali che esiste un isomorfismo  $f : S \rightarrow T$  sono dette **isomorfe**, e si scrive  $S \xrightarrow{f} T$  o, semplicemente  $S \simeq T$ . Da 4.3.2 e 4.3.3 segue subito che:

a. Un'applicazione se si ha iniettivo è **rifismo**, una struttura biettivo.

orfismo di  $g(m)$ , per non è un  $\exists) = 2^6 \neq$

} definita  $1, 1\}, \cdot)$ .

$\rightarrow S$  è un'immersione ica, come

viente di  $\tau(y)$ , per un'anonico

erazioni  $\circ f$  è un

erne. Se  $f$  è un

□

4.3.4. Qualunque siano le strutture semplici  $(S, \perp), (T, \top)$  e  $(V, \odot)$  si ha:

- (i)  $S \simeq S$ ;
- (ii)  $S \simeq T \implies T \simeq S$ ;
- (iii)  $S \simeq T, T \simeq V \implies S \simeq V$ .

*Dimostrazione.* Esercizio. □

4.3.5. **Esempio.** Con  $V$  insieme d'ordine 1 si ha  $(\mathcal{P}(V), \dot{\cup}) \simeq (\{-1, 1\}, \cdot)$ .

4.3.6. Sia  $f : S \rightarrow T$  un omomorfismo tra le strutture  $(S, \perp)$  e  $(T, \top)$ . Allora:

- (i) se  $x$  e  $y$  sono elementi di  $S$  permutabili rispetto a  $\perp$ , allora  $f(x)$  e  $f(y)$  sono elementi di  $T$  permutabili rispetto a  $\top$ ;
- (ii) se  $X$  è una parte stabile di  $(S, \perp)$ ,  $f(X)$  è una parte stabile di  $(T, \top)$ ; in particolare  $\text{Im } f = f(S)$  è una parte stabile di  $(T, \top)$ ;
- (iii) se  $\perp$  è commutativa (associativa), tale risulta l'operazione  $\top'$  indotta da  $\top$  su  $f(S)$ ;
- (iv) se esiste elemento neutro  $e$  in  $(S, \perp)$ , l'elemento  $f(e)$  è neutro in  $(f(S), \top')$ ;
- (v) se  $x \in S$  ha simmetrico  $x'$  in  $(S, \perp)$ , l'elemento  $f(x) \in T$  ha simmetrico  $f(x')$  in  $(f(S), \top')$ .

*Dimostrazione.* Esercizio. □

Da 4.3.6 segue che strutture isomorfe godono delle stesse proprietà algebriche e, in tale ottica, possono essere identificate. Ciò giustifica anche la terminologia usata, infatti il termine "isomorfismo" deriva dalle parole greche " $\muορφή$ ", che si legge "morfè" e significa "forma", e " $\ισος$ ", che si legge "íisos" e significa "uguale". Quanto detto si evidenzia ulteriormente nell'osservare che le tavole di moltiplicazione di strutture finite isomorfe sono in qualche modo sovrapponibili.

Fondamentale è il seguente risultato:

□

4.3.7. **Teorema di omomorfismo.** Sia  $f : S \rightarrow T$  un omomorfismo tra le strutture  $(S, \perp)$  e  $(T, \top)$ . Allora si ha che:

- (i)  $\text{Im } f = f(S)$  è una parte stabile di  $(T, \top)$ ;
- (ii) la relazione  $\mathcal{R}_f$  determinata da  $f$  è una congruenza in  $(S, \perp)$ ;
- (iii) ponendo  $g([x]_{\mathcal{R}_f}) := f(x)$  si definisce un'applicazione  $g : S / \mathcal{R}_f \rightarrow f(S)$  che è un isomorfismo di  $(S / \mathcal{R}_f, \tilde{\perp})$  in  $(f(S), \top')$ ;
- (iv) le strutture  $(S / \mathcal{R}_f, \tilde{\perp})$  e  $(f(S), \top')$  sono isomorfe.

□

*Dimostrazione.* La (i) segue subito dalla (ii) di 4.3.6.

Da  $x \mathcal{R}_f x_1$  e  $y \mathcal{R}_f y_1$  segue  $f(x) = f(x_1)$  e  $f(y) = f(y_1)$ , e quindi, essendo  $f$  un omomorfismo,  $f(x \perp y) = f(x) \top f(y) = f(x_1) \top f(y_1) = f(x_1 \perp y_1)$ , sicché  $f(x \perp y) = f(x_1 \perp y_1)$ , cioè  $(x \perp y) \mathcal{R}_f (x_1 \perp y_1)$ . Pertanto  $\mathcal{R}_f$  è una congruenza in  $(S, \perp)$  e vale (ii).

Da  $[x]_{\mathcal{R}_f} = [y]_{\mathcal{R}_f}$  segue  $x \mathcal{R}_f y$ , da cui  $f(x) = f(y)$  e  $g([x]_{\mathcal{R}_f}) = g([y]_{\mathcal{R}_f})$ , sicché  $g$  è ben posta. Da  $g([x]_{\mathcal{R}_f}) = g([y]_{\mathcal{R}_f})$  segue  $f(x) = f(y)$ , cioè  $x \mathcal{R}_f y$  e  $[x]_{\mathcal{R}_f} = [y]_{\mathcal{R}_f}$ , sicché  $g$  è iniettiva. Ovviamente  $g$  è suriettiva. Infine, per ogni  $[x]_{\mathcal{R}_f}, [y]_{\mathcal{R}_f} \in S/\mathcal{R}_f$ , si ha  $g([x]_{\mathcal{R}_f} \tilde{\perp} [y]_{\mathcal{R}_f}) = g([x \perp y]_{\mathcal{R}_f}) = f(x \perp y) = f(x) \top f(y) = g([x]_{\mathcal{R}_f}) \top g([y]_{\mathcal{R}_f})$ , pertanto  $g$  è un isomorfismo e vale la (iii).

La (iv) segue subito da (iii).  $\square$

Sia  $\Omega$  un insieme e siano  $\star$  e  $\triangledown$  operazioni esterne rispettivamente di  $S$  e  $T$  con dominio di operatori  $\Omega$ . Un'applicazione  $f : S \longrightarrow T$  è detta un **omomorfismo** di  $(S, \star)$  in  $(T, \triangledown)$  se si ha  $f(\alpha \star x) = \alpha \triangledown f(x)$ , per ogni  $\alpha \in \Omega, x \in S$ . Come in precedenza restano definiti i concetti di **monomorfismo**, **epimorfismo**, **isomorfismo**, **endomorfismo**, **automorfismo**.

**4.3.8. Esempi.** Se  $S$  è dotato dell'operazione esterna  $\star$  con operatori in  $\Omega$  l'applicazione identica  $\text{id}_S$  è un automorfismo di  $(S, \star)$ .

L'applicazione  $g : (x, y) \in \mathbb{R}^2 \longmapsto x + y \in \mathbb{R}$  è un epimorfismo di  $(\mathbb{R}^2, \star_3)$  su  $(\mathbb{R}, \star_2)$ , con  $\star_2$  e  $\star_3$  operazioni esterne con operatori in  $\mathbb{R}$  definite in 4.1.17.

Se  $\star$  è un'operazione esterna di  $S$  con operatori in  $\Omega$  e  $\mathcal{R}$  è una congruenza in  $(S, \star)$ , l'applicazione  $\pi : x \in S \longmapsto [x]_{\mathcal{R}} \in S/\mathcal{R}$  è un epimorfismo di  $(S, \star)$  in  $(S/\mathcal{R}, \widetilde{\star})$ , dove  $\widetilde{\star}$  indica l'operazione quoziante di  $\star$  in  $(S/\mathcal{R})$ ; si ha infatti  $\pi(\alpha \star x) = [\alpha \star x]_{\mathcal{R}} = \alpha \widetilde{\star} [x]_{\mathcal{R}} = \alpha \widetilde{\star} \pi(x)$ , per ogni  $\alpha \in \Omega, x \in S$ . L'epimorfismo  $\pi$  è detto l'**epimorfismo canonico** di  $(S, \star)$  in  $(S/\mathcal{R}, \widetilde{\star})$ .

**4.3.9.** Siano  $(S, \star)$  e  $(T, \triangledown)$  strutture con un'operazione esterna con operatori in  $\Omega$  e sia  $f : S \longrightarrow T$  un omomorfismo. Se  $X$  è una parte stabile di  $S$  allora  $f(X)$  è una parte stabile di  $T$ .

*Dimostrazione.* Esercizio.  $\square$

In analogia a quanto accade per le operazioni interne (vedi 4.3.7), si ha:

**4.3.10. Teorema di omomorfismo.** Siano  $(S, \star)$  e  $(T, \triangledown)$  strutture con un'operazione esterna con operatori in  $\Omega$  e sia  $f : S \longrightarrow T$  un omomorfismo. Allora si ha:

- (i)  $\text{Im } f = f(S)$  è una parte stabile di  $(T, \triangledown)$ ;
- (ii) la relazione  $\mathcal{R}_f$  determinata da  $f$  è una congruenza in  $(S, \star)$ ;
- (iii) ponendo  $g([x]_{\mathcal{R}_f}) := f(x)$  si definisce un'applicazione  $g : S/\mathcal{R}_f \longrightarrow f(S)$  che è un isomorfismo di  $(S/\mathcal{R}_f, \widetilde{\star})$  in  $(f(S), \triangledown')$ ;
- (iv) le strutture  $(S/\mathcal{R}_f, \widetilde{\star})$  e  $(f(S), \triangledown')$  sono isomorfe.

*Dimostrazione.* Esercizio. □

Si parla di omomorfismo anche tra strutture non semplici; è necessario però che tali strutture siano omologhe, cioè abbiano lo stesso numero di operazioni interne e/o esterne, quest'ultime con corrispondenti domini di operatori. Siano pertanto  $(S, \perp_1, \dots, \perp_n, \star_1, \dots, \star_m)$  e  $(T, \top_1, \dots, \top_n, \triangleright_1, \dots, \triangleright_m)$  strutture algebriche con  $\perp_1, \dots, \perp_n, \top_1, \dots, \top_n$  operazioni interne,  $\star_1$  e  $\triangleright_1$  operazioni esterne con operatori in  $\Omega_1, \dots, \star_m$  e  $\triangleright_m$  operazioni esterne con operatori in  $\Omega_m$ . Un'applicazione  $f : S \rightarrow T$  è detta un **omomorfismo** di  $(S, \perp_1, \dots, \perp_n, \star_1, \dots, \star_m)$  in  $(T, \top_1, \dots, \top_n, \triangleright_1, \dots, \triangleright_m)$  se è un omomorfismo di  $(S, \perp_i)$  in  $(T, \top_i)$  e di  $(S, \star_j)$  in  $(T, \triangleright_j)$ , per ogni  $i \in \{1, \dots, n\}$ ,  $j \in \{1, \dots, m\}$ .

Continua a valere la nomenclatura usata in precedenza per strutture semplici, e sussistono risultati analoghi a quelli precedentemente illustrati.

**4.3.11. Esempio.** L'applicazione  $g : (x, y) \in \mathbb{R}^2 \mapsto x+y \in \mathbb{R}$  è un epimorfismo di  $(\mathbb{R}^2, +, \star_3)$  su  $(\mathbb{R}, +, \star_2)$ , con  $\star_2$  e  $\star_3$  operazioni esterne con operatori in  $\mathbb{R}$  definite in 4.1.17.

## Esercizi

**Esercizio 4.3.1.** Si dimostri 4.3.2.

*Svolgimento.* Per ogni  $x, y \in S$  si ha  $(g \circ f)(x \perp y) = g(f(x \perp y)) = g(f(x) \top f(y)) = g(f(x)) \odot g(f(y)) = (g \circ f)(x) \odot (g \circ f)(y)$ .

**Esercizio 4.3.2.** Si dimostri 4.3.3.

*Svolgimento.* Siccome  $f$  è biettiva, per ogni  $a, b \in T$  esistono elementi  $x, y \in S$  tali che  $a = f(x)$ ,  $b = f(y)$ , da cui  $x = f^{-1}(a)$ ,  $y = f^{-1}(b)$ , e  $f^{-1}(a \top b) = f^{-1}(f(x) \top f(y)) = f^{-1}(f(x \perp y)) = x \perp y = f^{-1}(a) \perp f^{-1}(b)$ .

**Esercizio 4.3.3.** Si dimostri 4.3.4.

**Esercizio 4.3.4.** Si dimostrino 4.3.6 e 4.3.9.

**Esercizio 4.3.5.** Si dimostri 4.3.10.

**Esercizio 4.3.6.** Con  $V$  insieme, si provi che l'applicazione

$$g : X \in \mathcal{P}(V) \longmapsto V \setminus X \in \mathcal{P}(V)$$

è un isomorfismo di  $(\mathcal{P}(V), \cup)$  in  $(\mathcal{P}(V), \cap)$ .

**Esercizio 4.3.7.** Si enunci e si dimostri un teorema di omomorfismo analogo a 4.3.7 e a 4.3.10 per strutture  $(S, \perp, \star)$  e  $(T, \top, \triangleright)$ , con  $\perp$  e  $\top$  operazioni interne e  $\star$  e  $\triangleright$  operazioni esterne con operatori in  $\Omega$ .

**Esercizio 4.3.8.** Si consideri, nell'insieme  $\mathbb{Z}$ , l'operazione interna  $\perp$  definita ponendo  $n \perp m = n + m - 5$ , per ogni  $n, m \in \mathbb{Z}$ . Si studi la struttura  $(\mathbb{Z}, \perp)$ . Si dimostri poi che l'applicazione  $f : x \in \mathbb{Z} \mapsto 5 - x \in \mathbb{Z}$  è un isomorfismo di  $(\mathbb{Z}, +)$  in  $(\mathbb{Z}, \perp)$ .

**Esercizio 4.3.9.** Si consideri, nell'insieme  $\mathbb{Z}$ , l'operazione interna  $\perp$  definita ponendo  $n \perp m = nm - 2n - 2m + 6$ , per ogni  $n, m \in \mathbb{Z}$ . Si studi la struttura  $(\mathbb{Z}, \perp)$ . Si dimostri poi che l'applicazione  $f : x \in \mathbb{Z} \mapsto x + 2 \in \mathbb{Z}$  è un isomorfismo di  $(\mathbb{Z}, \cdot)$  in  $(\mathbb{Z}, \perp)$ .

**Esercizio 4.3.10.** Si consideri, nell'insieme  $\mathbb{Q}$ , l'operazione interna  $\perp$  definita ponendo  $x \perp y = \frac{3xy}{2}$ , per ogni  $x, y \in \mathbb{Q}$ . Si studi la struttura  $(\mathbb{Q}, \perp)$ . Si dimostri poi che l'applicazione  $f : x \in \mathbb{Q} \mapsto \frac{2}{3}x \in \mathbb{Q}$  è un isomorfismo di  $(\mathbb{Q}, \cdot)$  in  $(\mathbb{Q}, \perp)$ .

**Esercizio 4.3.11.** Si consideri, nell'insieme  $2\mathbb{N}_0$ , l'operazione interna  $\perp$  definita ponendo  $n \perp m = \frac{nm}{2}$ , per ogni  $n, m \in 2\mathbb{N}_0$ . Si studi la struttura  $(2\mathbb{N}_0, \perp)$ . Si dimostri poi che l'applicazione  $f : x \in \mathbb{N}_0 \mapsto 2x \in 2\mathbb{N}_0$  è un isomorfismo di  $(\mathbb{N}_0, \cdot)$  in  $(2\mathbb{N}_0, \perp)$ .

**Esercizio 4.3.12.** Si consideri l'insieme  $W = \{2^n 7^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ , non di  $(\mathbb{N}_0, +)$ .
- (ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$2^n 7^m \mathcal{R} 2^s 7^t : \iff m + t \in 2\mathbb{N}_0$$

è una congruenza in  $(W, \cdot)$ .

- (iii) Si provi che ha senso definire l'applicazione

$$\varphi : [2^n 7^m]_{\mathcal{R}} \in W / \mathcal{R} \mapsto (-1)^m \in \mathbb{Z},$$

si studi tale applicazione e si provi che è un omomorfismo di  $(W / \mathcal{R}, \cdot)$  in  $(\mathbb{Z}, \cdot)$ .

**Esercizio 4.3.13.** Con  $n$  numero naturale positivo, si dica  $h(n)$  il massimo naturale  $h$  tale che  $2^h$  divide  $n$ , sia cioè  $n = 2^{h(n)}k$ , con  $k \in \mathbb{N}$  tale che 2 non divide  $k$ . Si dimostri che è d'equivalenza la relazione  $\mathcal{R}$  definita in  $\mathbb{N}$  da:

$$n \mathcal{R} m : \iff h(n) = h(m).$$

Si provi che  $\mathcal{R}$  è una congruenza in  $(\mathbb{N}, \cdot)$ , non lo è in  $(\mathbb{N}, +)$ , che ha senso l'applicazione

$$\varphi : [n]_{\mathcal{R}} \in \mathbb{N} / \mathcal{R} \mapsto h(n) \in \mathbb{N}_0.$$

Infine si verifichi che  $\varphi$  è un omomorfismo di  $(\mathbb{N} / \mathcal{R}, \cdot)$  in  $(\mathbb{N}_0, +)$ , non in  $(\mathbb{N}_0, \cdot)$ .

## 4.4 Esercizi di riepilogo

**Esercizio 4.4.1.** Si consideri l'insieme  $W = \{9h + 1 : h \in \mathbb{N}_0\}$ .

- (i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ , non di  $(\mathbb{N}_0, +)$ .
- (ii) Si dimostri che è d'equivalenza la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$(9h+1) \mathcal{R} (9k+1) : \iff h + k \in 2\mathbb{N}_0.$$

- (iii) Si provi che  $\mathcal{R}$  è una congruenza in  $(W, \cdot)$  e si studi la struttura  $(W/\mathcal{R}, \cdot)$ .  
 (iv) Si verifichi che ha senso definire l'applicazione

$$\varphi : [9h+1]_{\mathcal{R}} \in W/\mathcal{R} \longmapsto (-1)^h \in \mathbb{Z},$$

la si studi, e si provi che essa non è un omomorfismo di  $(W/\mathcal{R}, \cdot)$  in  $(\mathbb{Z}, \cdot)$ .

**Esercizio 4.4.2.** Con  $S = \{v, w\}$ , si scrivano le tabelle moltiplicative delle strutture  $(\mathcal{P}(S), \cup)$ ,  $(\mathcal{P}(S), \cap)$ ,  $(\mathcal{P}(S), \setminus)$  e  $(\mathcal{P}(S), \dot{\cup})$ .

**Esercizio 4.4.3.** Si studi la struttura  $(2\mathbb{Z}, \perp)$  dove  $\perp$  è l'operazione interna nell'insieme  $2\mathbb{Z}$  definita ponendo, con  $n, m \in 2\mathbb{Z}$ :

$$n \perp m = 4n + 4m - \frac{mn}{2} - 24.$$

Si dimostri che l'applicazione  $f : x \in \mathbb{Z} \longmapsto 8 - 2x \in 2\mathbb{Z}$  è biettiva, se ne determini l'inversa, e si provi che  $f$  è un omomorfismo di  $(\mathbb{Z}, \cdot)$  in  $(2\mathbb{Z}, \perp)$ .

**Esercizio 4.4.4.** Si consideri l'insieme  $X = \{2^n 7^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si dimostri che  $X$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ .  
 (ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $X$  ponendo:

$$2^n 7^m \mathcal{R} 2^s 7^t : \iff n = s \text{ e } m + t \in 2\mathbb{N}_0$$

è d'equivalenza. Si provi che  $\mathcal{R}$  è una congruenza in  $(X, \cdot)$  e si studi la struttura quoziante  $(X/\mathcal{R}, \cdot)$ .

- (iii) Si provi che ha senso definire l'applicazione

$$\varphi : [2^n 7^m]_{\mathcal{R}} \in X/\mathcal{R} \longmapsto (-1)^{mn} \in \mathbb{Z},$$

si studi tale applicazione e si dimostri che  $\varphi$  non è un omomorfismo di  $(X/\mathcal{R}, \cdot)$  in  $(\mathbb{Z}, +)$ .

**Esercizio 4.4.5.** Si consideri l'insieme  $W = \{3^n 5^m : n, m \in \mathbb{N}_0\}$ .

- (i) Si dimostri che  $W$  è una parte stabile di  $(\mathbb{N}_0, \cdot)$ .  
 (ii) Si verifichi che la relazione  $\mathcal{R}$  definita in  $W$  ponendo:

$$3^n 5^m \mathcal{R} 3^s 5^t : \iff 2n + m = 2s + t$$

è una congruenza in  $(W, \cdot)$  e si studi la struttura quoziante  $(W/\mathcal{R}, \cdot)$ .

- (iii) Si provi che ha senso definire l'applicazione

$$\varphi : [3^n 5^m]_{\mathcal{R}} \in W/\mathcal{R} \longmapsto (-1)^m \in \mathbb{Z},$$

si studi tale applicazione e si provi che  $\varphi$  è un omomorfismo di  $(W/\mathcal{R}, \cdot)$  in  $(\mathbb{Z}, \cdot)$ .

**Esercizio 4.4.6.** Sia  $S$  un insieme e si fissi un suo sottoinsieme  $B$ .

- Si studi la struttura  $(\mathcal{P}(S), \star)$  dove  $\star$  è l'operazione nell'insieme  $\mathcal{P}(S)$ , definita da  $X \star Y = (X \cap Y) \setminus B$ , per ogni  $X, Y \in \mathcal{P}(S)$ .
- Si studi l'applicazione  $f : X \in \mathcal{P}(S) \mapsto X \setminus B \in \mathcal{P}(S)$ , e si provi che  $f$  è un omomorfismo di  $(\mathcal{P}(S), \cap)$  in  $(\mathcal{P}(S), \star)$ .
- Si scriva la tavola di moltiplicazione di  $(\mathcal{P}(S), \star)$  con  $S = \{a, b\}$  e  $B = \{b\}$ .

**Esercizio 4.4.7.** Sia  $S$  un insieme e si fissi un suo sottoinsieme  $B$ .

- Si studi la struttura  $(\mathcal{P}(S), \star)$  dove  $\star$  è l'operazione nell'insieme  $\mathcal{P}(S)$ , definita ponendo  $X \star Y = (X \setminus B) \cup Y$ , per ogni  $X, Y \in \mathcal{P}(S)$ .
- Si studi l'applicazione  $f : X \in \mathcal{P}(S) \mapsto X \setminus B \in \mathcal{P}(S)$ , e si provi che  $f$  è un omomorfismo di  $(\mathcal{P}(S), \cup)$  in  $(\mathcal{P}(S), \star)$ .
- Si scriva la tavola di moltiplicazione di  $(\mathcal{P}(S), \star)$ , con  $S = \{a, b\}$  e  $B = \{b\}$ .

**Esercizio 4.4.8.** Nell'insieme  $W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}$ , dove  $\mathbb{P}$  denota l'insieme dei primi di  $\mathbb{N}_0$ , si considerino le operazioni  $\star_1, \star_2, \star_3$  e  $\star_4$ , definite ponendo, per ogni  $p_1 p_2, q_1 q_2 \in W$ :

$$p_1 p_2 \star_i q_1 q_2 = \begin{cases} 2p_1 & \text{se } i = 1, \\ 2p_2 & \text{se } i = 2, \\ 2q_1 & \text{se } i = 3, \\ 2q_2 & \text{se } i = 4. \end{cases}$$

Per  $i = 1, 2, 3, 4$ :

- si studi la struttura  $(W, \star_i)$ ;
- si provi che le parti  $T = \{2q : q \in \mathbb{P}\}$  e  $K = \{4, 6, 10\}$  sono stabili rispetto a  $\star_i$ , e si studino le strutture  $(T, \star_i)$  e  $(K, \star_i)$ , scrivendo di quest'ultima anche una tavola di moltiplicazione;
- si studino le applicazioni

$$f : 2q \in T \mapsto q \in \mathbb{Z}, \quad g : 2q \in T \mapsto (-1)^q \in \mathbb{Z},$$

e si stabilisca se esse sono omomorfismi di  $(T, \star_i)$  in  $(\mathbb{Z}, \cdot)$ .

**Esercizio 4.4.9.** Nell'insieme  $W = \{p_1 p_2 : p_1, p_2 \in \mathbb{P}, p_1 \leq p_2\}$ , dove  $\mathbb{P}$  denota l'insieme dei primi di  $\mathbb{N}_0$ , si consideri l'operazione  $\star$  definita mediante la posizione  $p_1 p_2 \star q_1 q_2 = kp_2$ , con  $k = \min\{p_1, q_1\}$ .

- Si studi la struttura  $(W, \star)$ .
- Si provi che la parte  $H = \{35, 34\}$  non è stabile in  $(W, \star)$ , che le parti  $T = \{3q : 3 \leq q\}$  e  $K = \{15, 21, 33\}$  sono stabili, e si studino le strutture  $(T, \star)$  e  $(K, \star)$ , scrivendo di quest'ultima anche una tavola di moltiplicazione.
- Infine si studino le applicazioni

$$f : 3q \in T \mapsto q \in \mathbb{Z}, \quad g : 3q \in T \mapsto (-1)^q \in \mathbb{Z},$$

e si stabilisca se esse sono omomorfismi di  $(T, \star)$  in  $(\mathbb{Z}, \cdot)$ .

# 5

## Elementi di aritmetica

In questo capitolo verranno ripresi insiemi numerici notevoli, illustrandone ulteriori proprietà. Tra l'altro, viene descritto l'ormai celebre codice RSA.

### 5.1 I numeri naturali e la seconda forma del principio d'induzione

Si ricorda che si sta denotando con  $\mathbb{N}_0$  l'insieme dei numeri naturali  $\{0, 1, 2, \dots\}$  e con  $\mathbb{N}$  l'insieme dei numeri naturali non nulli; nel Capitolo 1 se ne sono già evidenziate alcune proprietà, quale per esempio il principio d'induzione nella prima forma. L'esistenza di tali insiemi è stata data come intuitiva. In realtà essa è assiomatizzata mediante i cosiddetti **assiomi di Peano**. Non si intende qui presentare la teoria nella sua completezza e nel suo rigore, ma solo farne dei cenni.

Si accetta per assioma l'esistenza di una terna  $(\mathbb{N}_0, 0, f)$ , dove  $\mathbb{N}_0$  è un insieme, 0 un suo elemento e  $f$  un'applicazione di  $\mathbb{N}_0$  in  $\mathbb{N}_0$  tale che:

- (1)  $0 \notin f(\mathbb{N}_0)$ ;
- (2)  $f$  è iniettiva;
- (3) se  $X \subseteq \mathbb{N}_0$  è tale che
  - (i)  $0 \in X$ ,
  - (ii) da  $s \in X$  segue  $f(s) \in X$ ,allora è  $X = \mathbb{N}_0$ .

Dall'iniettività di  $f$  segue che ha senso introdurre le seguenti notazioni:

$$1 := f(0), 2 := f(1), \dots,$$

e chiamare, per ogni  $s \in \mathbb{N}_0$ ,  $f(s)$  il **successivo** di  $s$ .

Si può poi provare che, a partire da  $f$ , è possibile definire in  $\mathbb{N}_0$  un'operazione di somma che gode delle proprietà elencate nel Capitolo 1 (vedi (1.2.1) – (1.2.6)). Rispetto a tale operazione si ha poi, per ogni  $n \in \mathbb{N}_0$ :

$$f(n) = n + 1.$$

La proprietà (3) coincide così con la prima forma del principio d'induzione, enunciata nel Capitolo 1 (vedi (1.3.1)).

Inoltre è possibile definire un'operazione di prodotto che verifica le proprietà elencate nel Capitolo 1 (vedi (1.2.7) – (1.2.16)). Si ottiene così la nota struttura  $(\mathbb{N}_0, +, \cdot)$ .

Come fatto sempre nel Capitolo 1, si può introdurre in  $\mathbb{N}_0$  la cosiddetta “relazione d’ordine usuale” ponendo:

$$x \leq y : \iff \exists t \in \mathbb{N}_0 : y = x + t,$$

e si può provare che questo è un buon ordine in  $\mathbb{N}_0$ .

Così si definisce in  $\mathbb{N}_0$  la relazione d’ordine del “divide”, ponendo, con  $x, y \in \mathbb{N}_0$ ,

$$x|y : \iff \exists k \in \mathbb{N}_0 : y = xk.$$

Sussiste la seguente proprietà che, come si potrebbe provare, è equivalente alla prima forma del principio d’induzione. Sia  $X \subseteq \mathbb{N}_0$  tale che:

$$(j) \quad 0 \in X,$$

$$(jj) \quad \text{da } t > 0 \text{ e } k \in X \text{ per ogni } k \in \mathbb{N}_0, k < t, \text{ segue che } t \in X.$$

Allora si ha  $X = \mathbb{N}_0$ .

Più in generale, sia  $\bar{n} \in \mathbb{N}_0$  e sia  $Y \subseteq \mathbb{N}_0$  tale che:

$$(j) \quad \bar{n} \in Y,$$

$$(jj) \quad \text{con } t > \bar{n}, \text{ si ha } t \in Y \text{ se si ha } k \in Y, \text{ per ogni } k \text{ soddisfacente } \bar{n} \leq k < t.$$

Allora  $n \in Y$ , per ogni  $n \geq \bar{n}$ .

Tale proprietà viene detta la *seconda forma del principio d’induzione* e, come la prima forma, si applica nella dimostrazione di enunciati relativi ai numeri naturali. Precisamente:

**5.1.1. Seconda forma del principio d’induzione.** *Sia  $\bar{n}$  un numero naturale e sia P una proprietà relativa ai numeri naturali  $n \geq \bar{n}$ . Se P è vera per  $\bar{n}$  e, con  $t > \bar{n}$ , P è vera per t ogni qualvolta P è vera per ogni numero naturale k soddisfacente  $\bar{n} \leq k < t$ , allora la proprietà P è vera per ogni naturale  $n \geq \bar{n}$ .*

Come prima applicazione della seconda forma del principio d’induzione si può fornire un’altra dimostrazione della seguente proposizione, già parzialmente provata nel Capitolo 1 (vedi 1.3.4):

**5.1.2. Algoritmo della divisione in  $\mathbb{N}_0$ .** *Sia b un numero naturale non nullo. Allora, per ogni  $n \in \mathbb{N}_0$ , esistono, e sono univocamente individuati, numeri naturali q e r tali che:*

$$n = bq + r, \text{ con } r < b.$$

*Tali numeri sono detti, rispettivamente, il quoziente e il resto della divisione di n per b.*

*Dimostrazione.* Per l’esistenza di q ed r si proceda per induzione su n utilizzando la seconda forma. Se  $n = 0$ , allora  $n = b0 + 0$ , con  $0 < b$ , e dunque la proprietà è soddisfatta con  $q = 0 = r$ . Sia  $n > 0$  e si supponga la proprietà vera per ogni

naturale  $k < n$ . Se  $n < b$ , allora da  $n = b0 + n$  segue la proprietà richiesta ponendo  $q = 0$  e  $r = n$ . Si supponga dunque  $n \geq b$ , ha allora senso considerare  $n - b \geq 0$ . Da  $b \neq 0$  segue  $n - b < n$ , sicché, per l'ipotesi induttiva, esistono  $q', r' \in \mathbb{N}_0$  tali che  $n - b = bq' + r'$ , con  $r' < b$ . Pertanto  $n = b + bq' + r' = b(q' + 1) + r'$ , e si ha l'asserto con  $q = q' + 1$  e  $r = r'$ .

Si supponga ora  $n = bq_1 + r_1 = bq_2 + r_2$ , con  $r_1, r_2 < b$ . Sia per esempio  $r_1 \geq r_2$ , sicché  $0 \leq r_1 - r_2 = bq_2 - bq_1 = b(q_2 - q_1)$ , con  $r_1 - r_2 \leq r_1 < b$ . Quindi è  $q_2 - q_1 = 0$ , altrimenti da  $q_2 - q_1 \geq 1$  seguirebbe  $r_1 - r_2 = b(q_2 - q_1) \geq b$ . Si ha dunque  $q_1 = q_2$  e poi anche  $r_1 = r_2$ .  $\square$

Si noti che, con  $a, b$  numeri naturali diversi da 0, si ha che  $b$  divide  $a$  se e solo se è 0 il resto della divisione di  $a$  per  $b$ .

Come ulteriore applicazione della seconda forma del principio d'induzione è possibile provare la prima parte del teorema fondamentale dell'aritmetica, già enunciato nel Capitolo 1 (vedi 1.2.5).

**5.1.3. Teorema fondamentale dell'aritmetica (in  $\mathbb{N}$ ).** *Sia  $n$  un numero naturale,  $n \geq 2$ . Allora esistono  $t \geq 1$  e  $p_1, \dots, p_t \in \mathbb{P}$  tali che  $n = p_1 \dots p_t$ . Inoltre tale scrittura è unica a meno dell'ordine dei fattori.*

*Dimostrazione.* Si procederà per induzione su  $n$  utilizzando la seconda forma. Se  $n = 2$ , l'asserto è ovvio essendo 2 un numero primo. Sia  $n > 2$ . Se  $n$  è un numero primo, si ottiene l'asserto con  $t = 1$  e  $p_1 = n$ . Sia  $n$  composto, esistano quindi  $a, b \in \mathbb{N}$  tali che  $n = ab$ , con  $1 < a < n$  e  $1 < b < n$ . Agli interi  $a$  e  $b$  si può applicare l'ipotesi d'induzione sicché esistono  $h, k \geq 1$  e  $p_1, \dots, p_h, q_1, \dots, q_k$  primi tali che  $a = p_1 \dots p_h$ ,  $b = q_1 \dots q_k$ , e quindi  $n = p_1 \dots p_h q_1 \dots q_k$ , come volevasi.

Per l'unicità della fattorizzazione si veda l'Esercizio 1.3.4.  $\square$

Il teorema fondamentale dell'aritmetica evidenzia il ruolo chiave dei numeri primi nello studio dei numeri naturali. Un celeberrimo, antichissimo risultato dovuto a Euclide (e quindi risalente al III – II secolo avanti Cristo) assicura che:

**5.1.4. Teorema di Euclide.** *Esistono infiniti numeri primi.*

*Dimostrazione.* Si indichi con  $\mathbb{P}$  l'insieme dei numeri primi e si supponga per assurdo  $\mathbb{P}$  finito,  $|\mathbb{P}| = l \geq 1$ ,  $\mathbb{P} = \{p_1, \dots, p_l\}$ . Ha senso considerare il numero naturale

$$n = p_1 p_2 \dots p_l,$$

e il suo successivo

$$n + 1 = p_1 p_2 \dots p_l + 1 > 2.$$

Per la 5.1.3 esiste almeno un primo  $q$  che divide  $n + 1$ . Da  $q \in \mathbb{P}$  segue allora che  $q$  divide anche  $n$ , pertanto  $q$  divide 1 (vedi (1.2.42)), il che è assurdo perché  $q$  è primo.  $\square$

Esistono ancora molti problemi aperti relativi ai numeri primi, alla loro individuazione e alla loro distribuzione. Metodi per “setacciare” i primi tra i numeri naturali vengono detti “crivelli”. Ovviamente un numero naturale  $n \geq 2$  è primo se non ha alcun divisore  $d$  tale che  $1 < d < n$ . In più si ha il famoso e antichissimo:

**5.1.5. Crivello di Eratostene.** *Sia  $n$  un numero naturale,  $n \geq 2$ . Allora  $n$  è primo se non ammette alcun divisore primo  $p$  con  $p^2 \leq n$ .*

*Dimostrazione.* Per assurdo si assuma  $n$  non primo. Esistono quindi naturali  $a, b$  con  $a, b > 1$  tali che  $n = ab$ . Da  $a, b \geq 2$  segue per la 5.1.3 che esistono primi  $q$  e  $q'$  tali che  $q$  divide  $a$  e  $q'$  divide  $b$ , da cui  $n = qq'l$  per un opportuno naturale  $l \geq 1$ . Pertanto  $q$  e  $q'$  sono divisorii primi di  $n$  e quindi per le ipotesi sono tali che  $q^2 > n$  e  $(q')^2 > n$ , da cui  $(qq')^2 = q^2(q')^2 > n^2$  (vedi Esercizio 1.2.1), il che comporta  $qq' > n$ , un assurdo.  $\square$

## Esercizi

**Esercizio 5.1.1.** *Si determinino tutti i numeri primi  $\leq 100$ .*

*Svolgimento.* Si elenchino tutti i numeri naturali  $n$ , con  $2 \leq n \leq 100$ . Il numero 2 ovviamente è primo, mentre non lo sono tutti i numeri da 3 a 100 divisibili per 2: 4, 6, 8, 10, .... Si cancellino dunque tali numeri. Il primo numero non cancellato, cioè 3, è allora privo di divisori  $k$ , con  $1 < k < 3$ . Pertanto è primo, mentre non lo sono i numeri  $h$  non ancora cancellati, con  $3 < h \leq 100$ , che sono divisibili per 3. Cancellando tali numeri: 9, 15, 21, ..., il primo a non essere stato cancellato è 5 che è quindi primo. Si cancellino allora tutti i numeri sulla destra che ancora compaiono e che sono divisibili per 5: 25, 35, 55, .... Il primo numero non cancellato è 7, che è quindi primo. Si cancellino allora tutti i numeri che ancora compaiono sulla destra e che sono multipli di 7: 49, 77, 91. I restanti numeri sono tutti primi in quanto il primo numero non ancora cancellato è 11 e tutti i suoi multipli  $\leq 100$  sono già stati cancellati perché divisibili per un primo  $< 11$ , e un discorso analogo vale per i restanti numeri.

Ciò esprime l’idea che è alla base del crivello di Eratostene.

**Esercizio 5.1.2.** *Si verifichi, utilizzando il crivello di Eratostene, se il numero 151 è primo.*

**Esercizio 5.1.3.** *Si verifichi, utilizzando il crivello di Eratostene, se il numero 149 è primo.*

**Esercizio 5.1.4.** *Si verifichi, utilizzando il crivello di Eratostene, se il numero 191 è primo.*

**Esercizio 5.1.5.** *Utilizzando il ragionamento dell’Esercizio 5.1.1 si scrivano tutti i numeri primi  $\leq 250$ .*

## 5.2 Rappresentazione dei numeri naturali in base fissata

Per i numeri naturali si usa di solito la cosiddetta rappresentazione decimale o in base 10: per opportuni  $k \geq 0$ ,  $a_0, \dots, a_k \in \{0, 1, \dots, 9\}$ ,  $a_k \neq 0$ , si ha

$$n = a_k a_{k-1} \dots a_1 a_0 = a_0 + 10a_1 + \dots + 10^k a_k,$$

e ovviamente tale scrittura è unica. Più in generale si ha:

**5.2.1.** *Fissato un numero naturale  $b \geq 2$ , ogni numero naturale  $n$  ha una e una sola scrittura del tipo*

$$n = c_0 + c_1 b + \dots + c_s b^s,$$

*per opportuni numeri naturali  $s \geq 0$ ,  $c_0, \dots, c_s \in \{0, 1, \dots, b-1\}$ ,  $c_s \neq 0$ . Si scrive allora anche:*

$$n = (c_s c_{s-1} \dots c_1 c_0)_b$$

*e questa scrittura viene detta la rappresentazione di  $n$  in base  $b$ .*

*Dimostrazione.* Per l'algoritmo della divisione (vedi 5.1.2) risulta:

$$\begin{array}{ll} n = bq_0 + c_0 & \text{con } q_0, c_0 \in \mathbb{N}_0 \text{ e } c_0 < b \\ q_0 = bq_1 + c_1 & \text{con } q_1, c_1 \in \mathbb{N}_0 \text{ e } c_1 < b \\ \vdots & \vdots \\ q_{s-1} = bq_s + c_s & \text{con } q_s, c_s \in \mathbb{N}_0 \text{ e } c_s < b. \end{array}$$

Si osservi che si ha  $q_0 = 0$ , oppure riesce  $q_0 > q_1 > \dots$ , sicché esiste uno e un solo  $s > 0$  tale che  $q_s = 0$  e  $q_{s-1} \neq 0$ . Restano così univocamente individuati i numeri  $s \geq 0$ ,  $c_0, \dots, c_s \in \{0, \dots, b-1\}$  e si ha:

$$\begin{aligned} n &= c_0 + bq_0 \\ &= c_0 + b(bq_1 + c_1) \\ &= c_0 + bc_1 + b^2 q_1 \\ &= c_0 + bc_1 + b^2(bq_2 + c_2) \\ &= c_0 + bc_1 + b^2 c_2 + b^3 q_2 \\ &\quad \vdots \\ &= c_0 + bc_1 + b^2 c_2 + \dots + b^{s-1}(bq_{s-1} + c_{s-1}) \\ &= c_0 + bc_1 + b^2 c_2 + \dots + b^{s-1} c_{s-1} + b^s q_{s-1} \\ &= c_0 + bc_1 + b^2 c_2 + \dots + b^{s-1} c_{s-1} + b^s(bq_s + c_s) \\ &= c_0 + bc_1 + b^2 c_2 + \dots + b^{s-1} c_{s-1} + b^s c_s, \end{aligned}$$

e ciò prova l'esistenza di una scrittura del tipo richiesto. Sia ora

$$n = c_0 + c_1 b + \cdots + c_s b^s = c'_0 + c'_1 b + \cdots + c'_t b^t,$$

con  $s, t \in \mathbb{N}_0$ ,  $c_0, \dots, c_s, c'_0, \dots, c'_t \in \{0, 1, \dots, b-1\}$ ,  $c_s \neq 0$ ,  $c'_t \neq 0$ , e si assuma  $s \leq t$ . Allora risulta

$$n = c_0 + bq = c'_0 + bq', \text{ con } 0 \leq c_0, c'_0 < b,$$

dove  $q = c_1 + c_2 b + \cdots + c_s b^{s-1}$ ,  $q' = c'_1 + c'_2 b + \cdots + c'_t b^{t-1}$ . Per l'unicità del quoziente e del resto della divisione euclidea di  $n$  per  $b$  (vedi 5.1.2) si ottiene  $c_0 = c'_0$  e  $q = q'$ . Procedendo in modo analogo si ottiene anche  $c_i = c'_i$  per ogni  $i = 1, \dots, s$ . Se per assurdo fosse  $s < t$  si avrebbe poi  $0 = c'_{s+1} b^{s+1} + \cdots + c'_t b^t$ , il che non è possibile in quanto  $c'_t > 0$  e  $c'_{s+1}, \dots, c'_{t-1} \geq 0$ . Dunque  $s = t$ , e le due espressioni coincidono. Ciò prova l'asserto.  $\square$

**5.2.2. Esempi.** Il numero naturale che, in base 10, è 133, in base 2 si scrive  $(10000101)_2$ , in quanto:

$$\begin{aligned} 133 &= 2 \cdot 66 + 1 \\ 66 &= 2 \cdot 33 + 0 \\ 33 &= 2 \cdot 16 + 1 \\ 16 &= 2 \cdot 8 + 0 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

Il numero naturale che, in base 3, si scrive  $(21012)_3$ , in base 10 è 194, poiché:  $2 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 = 2 + 3 + 0 + 27 + 162 = 194$ .

La rappresentazione in base 2, particolarmente utile in Informatica, è detta anche *binaria*.

## Esercizi

**Esercizio 5.2.1.** Si determini la rappresentazione decimale dei seguenti numeri:  $(11011011)_2$ ,  $(12210)_3$ ,  $(12310)_4$ ,  $(34024)_5$ ,  $(25401)_6$ ,  $(3456)_7$ ,  $(277)_8$ ,  $(881)_9$ .

**Esercizio 5.2.2.** Si determinino le rappresentazioni in base 3, 6, 8 e 9 dei seguenti numeri, dati in rappresentazione decimale: 324, 14, 662, 201, 55, 1200.

**Esercizio 5.2.3.** Si determini prima la rappresentazione binaria, poi quella in base 7, dei numeri seguenti:  $(245)_8$ ,  $(54)_9$ ,  $(2001)_4$ ,  $(22222)_3$ ,  $(2020)_5$ .

**Esercizio 5.2.4.** Si fornisca la rappresentazione decimale del più grande numero naturale che si rappresenta in base 6 con 4 cifre tutte distinte.

**Esercizio 5.2.5.** Si fornisca la rappresentazione decimale del più piccolo numero naturale che si rappresenta in base 7 con 5 cifre tutte distinte.

### 5.3 I numeri interi

Come più volte ricordato nel Capitolo 1, i numeri interi sono gli elementi dell'insieme  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ , e tra essi sono definite le usuali operazioni di somma e prodotto. È possibile costruire la struttura  $(\mathbb{Z}, +, \cdot)$  a partire da  $(\mathbb{N}_0, +, \cdot)$ , procedendo nel seguente modo.

Nell'insieme  $\mathbb{N}_0 \times \mathbb{N}_0$  si introduce la seguente relazione:

$$(a, b) \sim (c, d) : \iff a + d = b + c. \quad (5.3.1)$$

Utilizzando le proprietà di  $(\mathbb{N}_0, +)$  si ottiene facilmente che tale relazione è d'equivalenza e che è una congruenza nella struttura prodotto  $(\mathbb{N}_0 \times \mathbb{N}_0, +)$  (vedi Esercizio 5.3.1). Si noti, in particolare, che la classe  $[(0, 0)]_\sim$  coincide con la diagonale  $\Delta_{\mathbb{N}_0}$  (vedi Esercizio 5.3.2). L'insieme quoziante  $(\mathbb{N}_0 \times \mathbb{N}_0)/_\sim$  viene denotato con il simbolo  $\mathbb{Z}$ . La struttura quoziante  $(\mathbb{Z}, +)$ , dove ovviamente per ogni  $[(x, y)]_\sim, [(z, t)]_\sim \in \mathbb{Z}$  si pone

$$[(x, y)]_\sim + [(z, t)]_\sim := [(x + z, y + t)]_\sim,$$

è un monoide commutativo, con  $[(0, 0)]_\sim$  elemento neutro. In più ogni elemento è dotato di opposto, in quanto, per ogni  $[(x, y)]_\sim \in \mathbb{Z}$ , esiste  $[(y, x)]_\sim \in \mathbb{Z}$  tale che:

$$[(x, y)]_\sim + [(y, x)]_\sim = [(x + y, y + x)]_\sim = [(0, 0)]_\sim.$$

Pertanto  $(\mathbb{Z}, +)$  è un gruppo abeliano. Ponendo poi, con  $[(x, y)]_\sim, [(z, t)]_\sim \in \mathbb{Z}$ ,

$$[(x, y)]_\sim \cdot [(z, t)]_\sim := [(xz + yt, xt + yz)]_\sim,$$

si definisce un'operazione in  $\mathbb{Z}$  in quanto si verifica facilmente, utilizzando le proprietà di  $(\mathbb{N}_0, +, \cdot)$ , che da  $(x, y) \sim (x', y')$ ,  $(z, t) \sim (z', t')$  segue che  $(xz + yt, xt + yz) \sim (x'z' + y't', x't' + y'z')$  (vedi Esercizio 5.3.3). Si può poi provare che tale prodotto è associativo, commutativo, distributivo rispetto alla somma prima introdotta, e ha elemento neutro  $[(1, 0)]_\sim$  (vedi Esercizio 5.3.4). Pertanto  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo unitario.

Sia  $[(x, y)]_\sim \in \mathbb{Z}$ . In  $\mathbb{N}_0$  si verifica una e una sola delle seguenti:  $x \geq y$  o  $x < y$ ; nel primo caso  $x - y \in \mathbb{N}_0$ , nel secondo  $y - x \in \mathbb{N}$  e si verifica subito che, rispettivamente,  $[(x, y)]_\sim = [(x - y, 0)]_\sim$  o  $[(x, y)]_\sim = [(0, y - x)]_\sim$ . Pertanto:

$$\mathbb{Z} = \{[(n, 0)]_\sim : n \in \mathbb{N}_0\} \cup \{[(0, m)]_\sim : m \in \mathbb{N}\},$$

e si ha  $[(n, 0)]_\sim \neq [(0, m)]_\sim$ , per ogni  $n \in \mathbb{N}_0$ ,  $m \in \mathbb{N}$ . Inoltre  $[(n, 0)]_\sim = [(t, 0)]_\sim$  con  $n, t \in \mathbb{N}_0$  implica  $n = t$ , e così  $[(0, m)]_\sim = [(0, s)]_\sim$  con  $m, s \in \mathbb{N}$  implica  $m = s$ . L'applicazione  $\varphi : n \in \mathbb{N}_0 \mapsto [(n, 0)]_\sim \in \mathbb{Z}$  è dunque iniettiva e si verifica (vedi Esercizio 5.3.5) che è un omomorfismo di  $(\mathbb{N}_0, +, \cdot)$  in  $(\mathbb{Z}, +, \cdot)$ . Identificato ogni  $n \in \mathbb{N}_0$  con l'elemento  $[(n, 0)]_\sim \in \mathbb{Z}$  si ha  $\mathbb{N}_0 \subseteq \mathbb{Z}$  e le operazioni di  $\mathbb{N}_0$  coincidono con quelle indotte dalle operazioni di  $\mathbb{Z}$ .

Da  $[(0, m)]_{\sim} = -[(m, 0)]_{\sim}$ , per ogni  $m \in \mathbb{N}$  segue, per l'identificazione fatta,  $[(0, m)]_{\sim} = -m$ . Si ritrova così l'usuale descrizione di  $\mathbb{Z}$ :

$$\mathbb{Z} = \{n : n \in \mathbb{N}_0\} \cup \{-m : m \in \mathbb{N}\}.$$

È possibile verificare che si ritrovano tutte le proprietà degli interi descritte nel Capitolo 1. In particolare, il fatto che  $(\mathbb{Z}, +, \cdot)$  è un dominio d'integrità (vedi Esercizio 5.3.6).

Come già ricordato nel Capitolo 1 e nel Capitolo 2, in  $\mathbb{Z}$  è definita la relazione d'ordine “usuale” ponendo, con  $a, b \in \mathbb{Z}$ ,

$$a \leq b : \iff \exists t \in \mathbb{N}_0 : b = a + t.$$

Tale relazione è un ordine totale e gode delle proprietà elencate nel Capitolo 1.

Si ricorda inoltre che il simbolo  $|a|$ , con  $a \in \mathbb{Z}$ , denota il valore assoluto di  $a$ , definito uguale ad  $a$ , se  $a \geq 0$ , uguale a  $-a$ , se  $a < 0$ .

Anche in  $\mathbb{Z}$  vale:

**5.3.1. Algoritmo della divisione.** Siano  $a, b \in \mathbb{Z}$  con  $b \neq 0$ . Allora esistono, e sono univocamente individuati, interi  $q$  e  $r$  tali che:

$$a = bq + r, \text{ con } 0 \leq r < |b|.$$

L'intero  $q$  è detto il **quoziente** della divisione di  $a$  per  $b$ , l'intero  $r$  ne è detto il **resto** e denotato col simbolo  $\text{rest}(a, b)$ .

*Dimostrazione.* Si proverà l'esistenza di  $q$  ed  $r$ . Si supponga dapprima  $b > 0$ , e quindi  $|b| = b$ . Se  $a \geq 0$ , l'asserto segue da 5.1.2. Sia  $a < 0$ . Da  $-a > 0$  segue, sempre per 5.1.2, che esistono  $q^*, r^* \in \mathbb{N}_0$  tali che  $-a = bq^* + r^*$ , con  $0 \leq r^* < b$ , sicché  $a = -(bq^* + r^*) = b(-q^*) - r^*$ . Se  $r^* = 0$ , basta porre  $q = -q^*$  e  $r = r^* = 0$ . Se  $r^* > 0$ , allora da  $r^* < b$  segue  $0 < b - r^* < b$  e da  $a = b(-q^*) - b + b - r^* = b(-q^* - 1) + (b - r^*)$  segue l'asserto con  $q = -q^* - 1$  e  $r = b - r^*$ . Si supponga ora  $b < 0$  e quindi  $-b > 0$  e  $|b| = |-b| = -b$ . Per quanto appena provato esistono  $\bar{q}, \bar{r} \in \mathbb{Z}$  tali che  $a = (-b)\bar{q} + \bar{r}$ , con  $0 \leq \bar{r} < -b$ . Si ottiene allora  $a = bq + r$ , con  $0 \leq r < |b|$ , ponendo  $q = -\bar{q}$  e  $r = \bar{r}$ .

Si supponga ora  $a = bq + r = bq' + r'$ , con  $0 \leq r, r' < |b|$ . Sia per esempio  $r \geq r'$ . Si ha allora:  $r - r' = bq' - bq = b(q' - q)$ , con  $0 \leq r - r' \leq r < |b|$ . Da  $r - r' = |r - r'| = |b(q - q')| = |b||q - q'|$  (vedi (1.2.47)) segue  $0 \leq |b||q' - q| < |b|$ , sicché risulta  $|q' - q| = 0$ , altrimenti  $|q' - q| \geq 1$  comporterebbe  $|b||q' - q| \geq |b|$ . Pertanto  $q' - q = 0$ , da cui  $q = q'$  e ancora  $r - r' = b(q' - q) = 0$  e dunque  $r = r'$ .  $\square$

**Osservazione.** Si noti che dalla precedente dimostrazione segue subito che, con

$a, b \in \mathbb{Z}, a, b > 0$ , si ha:

$$\begin{aligned}\text{rest}(-a, b) &= \begin{cases} 0 & \text{se } \text{rest}(a, b) = 0 \\ b - \text{rest}(a, b) & \text{se } \text{rest}(a, b) \neq 0, \end{cases} \\ \text{rest}(a, -b) &= \text{rest}(a, b), \\ \text{rest}(-a, -b) &= \text{rest}(-a, b).\end{aligned}$$

**5.3.2. Esempio.** Da  $15 = 4 \cdot 3 + 3$  segue che  $\text{rest}(15, 4) = 3$ ,  $\text{rest}(-15, 4) = 1$ ,  $\text{rest}(15, -4) = 3$ ,  $\text{rest}(-15, -4) = 1$ .

## Esercizi

**Esercizio 5.3.1.** Si provi che la relazione  $\sim$  definita in (5.3.1) è d'equivalenza in  $\mathbb{N}_0 \times \mathbb{N}_0$ , e che essa è una congruenza nella struttura prodotto  $(\mathbb{N}_0 \times \mathbb{N}_0, +)$ .

**Esercizio 5.3.2.** Con le notazioni dell'esercizio precedente, si dimostri che risulta  $[(0, 0)]_\sim = \Delta_{\mathbb{N}_0}$ .

**Esercizio 5.3.3.** Con le notazioni dell'Esercizio 5.3.1 si provi che  $(x, y) \sim (x', y')$  e  $(z, t) \sim (z', t')$  implicano  $(xz + yt, xt + yz) \sim (x'z' + y't', x't' + y'z')$ .

**Esercizio 5.3.4.** Con le notazioni dell'Esercizio 5.3.1 si provi che il prodotto definito in  $\mathbb{Z} = \mathbb{N}_0 \times \mathbb{N}_0 / \sim$  ponendo  $[(x, y)]_\sim \cdot [(z, t)]_\sim := [(xz + yt, xt + yz)]_\sim$  è associativo, commutativo e distributivo rispetto alla somma quoziente della somma di  $\mathbb{N}_0 \times \mathbb{N}_0$ , e che  $[(1, 0)]_\sim$  ne è elemento neutro.

**Esercizio 5.3.5.** Con le notazioni degli Esercizi 5.3.1 e 5.3.4 si provi che l'applicazione

$$\varphi : n \in \mathbb{N}_0 \longmapsto [(n, 0)]_\sim \in \mathbb{Z}$$

è un omomorfismo di  $(\mathbb{N}_0, +, \cdot)$  in  $(\mathbb{Z}, +, \cdot)$ .

**Esercizio 5.3.6.** Sia  $\mathbb{Z} = \{[(n, 0)]_\sim : n \in \mathbb{N}_0\} \cup \{[(0, m)]_\sim : m \in \mathbb{N}\}$ . Si provi che in  $(\mathbb{Z}, \cdot)$  vale la legge di annullamento del prodotto.

**Esercizio 5.3.7.** Si calcolino i seguenti resti:

$$\begin{aligned}\text{rest}(17, -4), \quad \text{rest}(-17, 3), \quad \text{rest}(17, 3), \quad \text{rest}(-21, -6), \\ \text{rest}(-30, -5), \quad \text{rest}(19, -3), \quad \text{rest}(-21, -4), \quad \text{rest}(-24, 6).\end{aligned}$$

**Esercizio 5.3.8.** Si calcolino i seguenti resti:

$$\begin{aligned}\text{rest}(19, 3), \quad \text{rest}(-19, 3), \quad \text{rest}(21, -4), \quad \text{rest}(24, 6), \\ \text{rest}(15, 4), \quad \text{rest}(4, -6), \quad \text{rest}(-7, -5), \quad \text{rest}(-11, 3).\end{aligned}$$

## 5.4 Divisibilità tra interi

Come già detto nel Capitolo 1, con  $x, y \in \mathbb{Z}$ , si dice che  $x$  divide  $y$  e si scrive  $x|y$  se esiste  $k \in \mathbb{Z}$  tale che  $y = xk$ . In tal caso si dice anche che  $x$  è un divisore di  $y$  o che  $y$  è un multiplo di  $x$ . Si noti che, con  $x \neq 0$ ,  $x|y$  se e solo se  $\text{rest}(y, x) = 0$ , che  $0|y$  se e solo se  $y = 0$  e che  $z|0$  per ogni  $z \in \mathbb{Z}$ . Con  $a \in \mathbb{Z}$ , si pone:

$$D(a) := \{z \in \mathbb{Z} : z|a\}.$$

Si ha  $1, -1, a, -a \in D(a)$  (vedi 1.2.10); inoltre ovviamente:

$$\begin{aligned} D(a) &= D(-a), \\ D(1) &= D(-1) = \{1, -1\}, \\ D(0) &= \mathbb{Z}. \end{aligned}$$

In particolare, se  $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ , da 1.2.10 e dal teorema fondamentale dell'aritmetica segue che  $D(a)$  è un insieme finito e che  $|D(a)| \geq 4$ .

Si ha:

**5.4.1.** Siano  $x, y, z, k \in \mathbb{Z}$ , con  $x = yk + z$ . Allora  $D(x) \cap D(y) = D(y) \cap D(z)$ .

*Dimostrazione.* Esercizio. □

Un intero  $p \in \mathbb{Z}$  è detto **primo** se  $p \neq \pm 1$  e  $D(p) = \{1, -1, p, -p\}$ , cioè le uniche fattorizzazioni in  $\mathbb{Z}$  di  $p$  sono, a meno dell'ordine,  $p = 1 \cdot p = (-1) \cdot (-p)$ . Ovviamente  $p$  è primo se e solo se tale risulta  $-p$ .

Siano  $a, b \in \mathbb{Z}$ . Un intero  $d \in \mathbb{Z}$  è detto un **massimo comune divisore** di  $a$  e  $b$ , se risulta:

- (1)  $d|a, d|b,$
- (2)  $t|a, t|b \implies t|d.$

Ovviamente se  $a = 0 = b$ , 0 è l'unico massimo comune divisore di  $a$  e  $b$ . Se  $a|b$ , allora dalla definizione segue subito che  $a$  è un massimo comune divisore di  $a$  e  $b$ . In particolare  $a$  è un massimo comune divisore di  $a$  e 0, per ogni  $a \in \mathbb{Z}$ .

Si osservi inoltre che:

**5.4.2.** Siano  $a, b \in \mathbb{Z}$  non entrambi nulli. Si ha:

- (i)  $d$  è un massimo comune divisore di  $a$  e  $b$  se e solo se  $-d$  lo è;
- (ii) se  $d$  è un massimo comune divisore di  $a$  e  $b$ , allora  $k$  lo è se e solo se  $k = \pm d$ .

*Dimostrazione.* (i) Se  $d$  è un massimo comune divisore di  $a$  e  $b$ , si ha, per la 1.2.10, che  $-d|a$  e  $-d|b$ . Supposto poi  $v|a, v|b$ , dalla (2) segue che  $v|d$  e quindi anche  $v|-d$ , sempre per la 1.2.10. Quindi  $-d$  è un massimo comune divisore di  $a$  e  $b$ . Il viceversa è ovvio.

(ii) Siano ora  $d$  e  $k$  entrambi massimo comune divisore di  $a$  e  $b$ . Applicando le proprietà (1) e (2) si ha che  $d|k$  e  $k|d$ , da cui segue l'asserto per la 1.2.11. □

Si può dunque affermare che, se  $a, b \in \mathbb{Z}$  sono non entrambi nulli, e se esiste un massimo comune divisore di  $a$  e  $b$ , allora ne esistono esattamente due, l'uno l'opposto dell'altro. Di solito quello positivo viene denotato col simbolo  $\text{MCD}(a, b)$ , o più semplicemente con  $(a, b)$ . Si pone anche  $\text{MCD}(0, 0) = 0$ .

**Osservazione.** Con  $a, b, d \in \mathbb{Z}$  e  $d \geq 0$  si ha:

$$\begin{aligned} d = \text{MCD}(a, b) &\iff d = \text{MCD}(-a, b) \\ &\iff d = \text{MCD}(a, -b) \\ &\iff d = \text{MCD}(-a, -b). \end{aligned}$$

L'osservazione precedente e la (i) della 5.4.2 si ritrovano immediatamente osservando che:

**5.4.3.** *Siano  $a, b, d \in \mathbb{Z}$ , con  $d \geq 0$ . Si ha:*

$$d = \text{MCD}(a, b) \iff D(d) = D(a) \cap D(b).$$

*Dimostrazione.* Segue subito dalla definizione di massimo comune divisore.  $\square$

**5.4.4.** *Per ogni  $a, b \in \mathbb{Z}$  esiste  $\text{MCD}(a, b)$ .*

*Dimostrazione.* Siano  $a, b \in \mathbb{Z}$ . Siccome  $\text{MCD}(0, 0) = 0$ , si può supporre che  $a$  e  $b$  non siano entrambi nulli, per esempio  $b \neq 0$ . Per l'osservazione precedente è lecito supporre  $b > 0$ . Esistono allora  $q_1, r_1 \in \mathbb{Z}$  tali che:

$$a = bq_1 + r_1, \text{ con } 0 \leq r_1 < b.$$

Se  $r_1 \neq 0$ , esistono  $q_2, r_2 \in \mathbb{Z}$  tali che:

$$b = r_1 q_2 + r_2, \text{ con } 0 \leq r_2 < r_1.$$

Se  $r_2 \neq 0$ , esistono  $q_3, r_3 \in \mathbb{Z}$  tali che:

$$r_1 = r_2 q_3 + r_3, \text{ con } 0 \leq r_3 < r_2.$$

Così continuando, poiché  $r_1 > r_2 > \dots \geq 0$ , si ha che, posto  $b = r_0$ , per qualche  $t > 0$  risulta  $r_t \neq 0$  e:

$$r_{t-1} = r_t q_{t+1} + r_{t+1}, \text{ con } r_{t+1} = 0.$$

Pertanto per 5.4.1 risulta:

$$\begin{aligned} D(a) \cap D(b) &= D(b) \cap D(r_1) = \dots = \\ &= D(r_{t-1}) \cap D(r_t) = D(r_t) \cap D(r_{t+1}) = D(r_t) \cap \mathbb{Z} = D(r_t), \end{aligned}$$

quindi per 5.4.3 si ha  $r_t = \text{MCD}(a, b)$ .  $\square$

Il procedimento utilizzato nella dimostrazione di 5.4.4, noto come *algoritmo euclideo delle divisioni successive*, non solo garantisce l'esistenza di  $\text{MCD}(a, b)$  per ogni  $a, b \in \mathbb{Z}$ , ma fornisce anche una maniera per determinarlo.

Interi  $a$  e  $b$  sono detti *coprimi* se  $\text{MCD}(a, b) = 1$ . Si noti, per esempio, che:

**5.4.5.** *Siano  $a, p \in \mathbb{Z}$ , con  $p$  primo. Se  $p$  non divide  $a$ , allora  $a$  e  $p$  sono coprimi.*

*Dimostrazione.* Si ha  $D(p) = \{1, -1, p, -p\}$  e  $p, -p \notin D(a)$ . Pertanto risulta  $D(p) \cap D(a) = \{1, -1\} = D(1)$ , e l'asserto segue da 5.4.3.  $\square$

Si osservi che:

**5.4.6.** *Siano  $a$  e  $b$  interi non nulli, e sia  $d = \text{MCD}(a, b)$ . Allora si ha  $a = da'$  e  $b = db'$ , con  $\text{MCD}(a', b') = 1$ .*

*Dimostrazione.* Esercizio.  $\square$

L'algoritmo euclideo fornisce anche una dimostrazione del celebre:

**5.4.7. Teorema di Bézout.** *Siano  $a, b \in \mathbb{Z}$ , e sia  $d = \text{MCD}(a, b)$ . Allora esistono  $v, w \in \mathbb{Z}$  tali che  $d = av + bw$ . In particolare, se  $a$  e  $b$  sono coprimi, esistono  $v, w \in \mathbb{Z}$  tali che  $1 = av + bw$ .*

*Dimostrazione.* Ovviamente si può assumere che  $a$  e  $b$  non siano entrambi nulli. Con le notazioni utilizzate nella dimostrazione di 5.4.4 si ha allora:

$$r_1 = a + b(-q_1),$$

$$r_2 = b + r_1(-q_2) = b + (a + b(-q_1))(-q_2) = a(-q_2) + b(1 + q_1q_2),$$

e, così, per ogni  $i$ , continuando,  $r_i = as_i + bl_i$  per opportuni interi  $s_i, l_i$ . In particolare  $d = r_t = av + bw$  per opportuni  $v, w \in \mathbb{Z}$ .  $\square$

**5.4.8. Esempio.** Si ha  $\text{MCD}(1218, 132) = 6$  e  $6 = 1218 \cdot 9 + 132 \cdot (-83)$ . Infatti:

$$1218 = 132 \cdot 9 + 30,$$

$$132 = 30 \cdot 4 + 12,$$

$$30 = 12 \cdot 2 + 6,$$

$$12 = 6 \cdot 2 + 0,$$

da cui si ottiene

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 \\ &= 30 - (132 - 30 \cdot 4) \cdot 2 = 30 \cdot 9 + 132 \cdot (-2) \\ &= (1218 - 132 \cdot 9) \cdot 9 + 132 \cdot (-2) = 1218 \cdot 9 + 132 \cdot (-83). \end{aligned}$$

Dal teorema di Bézout (vedi 5.4.7) segue l'interessante proprietà:

**5.4.9.** *Siano  $a, b, c \in \mathbb{Z}$ , con  $a$  che divide il prodotto  $bc$ . Se  $a$  e  $b$  sono coprimi, allora  $a$  divide  $c$ .*

*Dimostrazione.* Sia  $bc = ak$ , per qualche  $k \in \mathbb{Z}$ , e si supponga  $\text{MCD}(a, b) = 1$ . Allora per 5.4.7 esistono  $v, w \in \mathbb{Z}$  tali che  $1 = av + bw$  e si ha  $c = 1 \cdot c = (av + bw) \cdot c = avc + bwc = avc + akw = a(vc + kw)$ . Quindi  $a|c$ , come volevasi.  $\square$

Come caso particolare si ottiene la seguente proprietà dei numeri primi, già enunciata nel Capitolo 1, relativamente ai numeri naturali primi:

**5.4.10.** *Siano  $a, b, p \in \mathbb{Z}$ , con  $p$  primo. Se  $p$  divide il prodotto  $ab$  allora  $p$  divide  $a$  o  $p$  divide  $b$ .*

*Dimostrazione.* Segue subito da 5.4.5 e 5.4.9.  $\square$

Estendendo quanto valido in  $\mathbb{N}$  (vedi 5.1.3), si può provare che:

**5.4.11. Teorema fondamentale dell'aritmetica (in  $\mathbb{Z}$ ).** *Sia  $z \in \mathbb{Z} \setminus \{0, 1, -1\}$ . Allora esistono  $k \geq 1$  e  $p_1, \dots, p_k \in \mathbb{Z}$ ,  $p_1, \dots, p_k$  primi, tali che*

$$z = p_1 \dots p_k.$$

*Supposto poi  $z = q_1 \dots q_s$ , con  $s \geq 1$  e  $q_1, \dots, q_s$  interi primi, si ha  $k = s$  e si possono riordinare i fattori  $q_1, \dots, q_s$  in modo che sia  $|p_1| = |q_1|, \dots, |p_k| = |q_k|$ .*

*Dimostrazione.* Esercizio.  $\square$

Siano  $a, b$  interi. Un intero  $m$  è detto un **minimo comune multiplo** di  $a$  e  $b$  se risulta:

- (1)  $a|m, b|m$ ,
- (2)  $a|t, b|t \implies m|t$ .

Ovviamente 0 è l'unico minimo comune multiplo di 0 e 0, e, con  $a, b \in \mathbb{Z}$ , da  $a|b$  segue subito che  $b$  è un minimo comune multiplo di  $a$  e  $b$ .

Esiste sempre un minimo comune multiplo, infatti si ha:

**5.4.12.** *Siano  $a$  e  $b$  interi non nulli e sia  $d = \text{MCD}(a, b)$ . Allora posto  $a = da'$ ,  $b = db'$  si ha:*

- (i)  $m = da'b'$  è un minimo comune multiplo di  $a$  e  $b$ ;
- (ii)  $m'$  è un minimo comune multiplo di  $a$  e  $b$  se e solo se  $m' = \pm m$ .

*Dimostrazione.* Sia  $m = da'b'$ . Ovviamente  $a|m$  e  $b|m$ . Supposto poi  $t \in \mathbb{Z}$  tale che  $a|t$  e  $b|t$ , si ha  $t = ah = da'h$  e  $t = bs = db's$ , per opportuni  $h, s \in \mathbb{Z}$ , da cui  $a'h = b's$ , con  $\text{MCD}(a', b') = 1$  (vedi 5.4.6). Pertanto  $b'|h$  (vedi 5.4.9) e dunque  $m|t$ , e la (i) è provata.

La dimostrazione della (ii) è analoga a quella fatta in 5.4.2.  $\square$

La 5.4.12 assicura che per ogni  $a, b \in \mathbb{Z}$  esiste sempre un minimo comune multiplo di  $a$  e  $b$ ; in più, se  $a$  e  $b$  sono non nulli, allora ne esistono precisamente due, l'uno l'opposto dell'altro. In tal caso, quello positivo viene denotato col simbolo  $\text{mcm}(a, b)$ . Ovviamente poi è  $\text{mcm}(a, b) = 0$  se almeno uno tra  $a$  e  $b$  è nullo. Da 5.4.12 segue subito che con  $a, b \in \mathbb{Z}$  non entrambi nulli vale

$$\text{mcm}(a, b) = \frac{|ab|}{\text{MCD}(a, b)}. \quad (5.4.1)$$

## Esercizi

**Esercizio 5.4.1.** Si dimostri 5.4.1.

**Esercizio 5.4.2.** Si dimostri 5.4.6.

**Esercizio 5.4.3.** Si determini, mediante l'algoritmo euclideo delle divisioni successive, il massimo comune divisore positivo dei numeri 824 e 376, e lo si esprima in funzione di essi.

**Esercizio 5.4.4.** Si determini, mediante l'algoritmo euclideo delle divisioni successive, il massimo comune divisore positivo dei numeri 494 e 214, e lo si esprima in funzione di essi.

**Esercizio 5.4.5.** Si determini, mediante l'algoritmo euclideo delle divisioni successive, il massimo comune divisore positivo dei numeri 689 e 534, e lo si esprima in funzione di essi.

**Esercizio 5.4.6.** Si dimostri 5.4.11.

**Esercizio 5.4.7.** Utilizzando la (5.4.1) e l'algoritmo euclideo delle divisioni successive, si determini il minimo comune multiplo positivo dei numeri 762 e 666.

**Esercizio 5.4.8.** Utilizzando la (5.4.1) e l'algoritmo euclideo delle divisioni successive, si determini il minimo comune multiplo positivo dei numeri 1221 e 165.

## 5.5 Congruenze tra interi

Si parlerà ora di una classe di notevoli relazioni d'equivalenza nell'insieme degli interi, dette congruenze modulo un intero  $m$ . Ciò porterà a considerare la cosiddetta “aritmetica modulo  $m$ ”, detta anche “aritmetica dell'orologio” per un motivo che risulterà chiaro nel seguito.

Sia  $m$  un intero, e si consideri in  $\mathbb{Z}$  la relazione  $m\mathbb{Z}$  definita ponendo, con  $a, b \in \mathbb{Z}$ :

$$a(m\mathbb{Z})b : \iff m|a - b.$$

Si ha dunque:

$$a(m\mathbb{Z})b \iff \exists k \in \mathbb{Z} : a - b = mk.$$

**5.5.1. La relazione  $m\mathbb{Z}$  è una relazione d'equivalenza, compatibile con le operazioni  $+ e \cdot$  in  $\mathbb{Z}$ .**

**Dimostrazione.** Per ogni  $a \in \mathbb{Z}$ , da  $m|0$  segue che  $m|a - a$ , sicché  $m\mathbb{Z}$  è riflessiva. Sia ora  $a(m\mathbb{Z})b$ , con  $a, b \in \mathbb{Z}$ , allora  $m|a - b$  e dunque, per la 1.2.10,  $m|b - a$  e quindi  $b(m\mathbb{Z})a$ . Pertanto  $m\mathbb{Z}$  è simmetrica. Supposto infine  $a(m\mathbb{Z})b$  e  $b(m\mathbb{Z})c$ , con  $a, b, c \in \mathbb{Z}$ , da  $m|a - b$  e  $m|b - c$  segue subito, ancora per la 1.2.10, che  $m|(a - b) + (b - c)$ , cioè  $m|a - c$ . Quindi  $m\mathbb{Z}$  è transitiva. Dunque la relazione  $m\mathbb{Z}$  è d'equivalenza.

Siano ora  $a, b, c, d \in \mathbb{Z}$  tali che  $a(m\mathbb{Z})c$  e  $b(m\mathbb{Z})d$ . Si ha allora:  $m|a - c$  e  $m|b - d$ , da cui  $m|(a - c) + (b - d)$ , cioè  $m|(a + b) - (c + d)$ , e ciò comporta  $(a + b)(m\mathbb{Z})(c + d)$ . Inoltre dalle ipotesi segue che:  $m|(a - c)b$  e  $m|c(b - d)$  e così  $m|ab - cb + cb - cd$ , cioè  $m|ab - cd$  e  $ab(m\mathbb{Z})cd$ , come volevasi.  $\square$

Quanto provato giustifica il termine **congruenza modulo  $m$**  usato per denotare la relazione  $m\mathbb{Z}$ . Se  $a(m\mathbb{Z})b$  si scrive anche  $a \equiv b \pmod{m}$  o talvolta, brevemente,  $a \equiv b \pmod{m}$  e si legge “ $a$  è congruo  $b$  modulo  $m$ ”. In caso contrario si scrive  $a \not\equiv b \pmod{m}$  o, in breve,  $a \not\equiv b \pmod{m}$  e si legge “ $a$  è incongruo  $b$  modulo  $m$ ”.

**5.5.2. Esempio.** Si ha:  $11 \equiv 2 \pmod{3}$ ,  $-8 \equiv 4 \pmod{3}$ ,  $-10 \equiv -2 \pmod{4}$ ,  $12 \not\equiv 3 \pmod{2}$ .

Se  $m = 0$  si ha  $a \equiv b \pmod{0}$  se e solo se  $a = b$ , sicché  $0\mathbb{Z}$  coincide con  $\text{id}_{\mathbb{Z}}$ . Supposto  $m \neq 0$  si ha ovviamente  $a \equiv b \pmod{m}$  se e solo se  $a \equiv b \pmod{-m}$ , sicché  $m\mathbb{Z} = (-m)\mathbb{Z}$ . Dunque non è riduttivo nel seguito supporre  $m > 0$ . Si osservi che da  $1|z$ , per ogni  $z \in \mathbb{Z}$ , segue che  $1\mathbb{Z}$  è la relazione totale in  $\mathbb{Z}$ . Perciò nel seguito si supporrà spesso  $m > 1$ .

La classe d'equivalenza modulo  $m\mathbb{Z}$  di un qualunque  $x \in \mathbb{Z}$  viene di solito denotata con  $[x]_m$ , o anche con  $\bar{x}$ , quando ciò non dà adito ad ambiguità. L'insieme quoziante  $\mathbb{Z}/m\mathbb{Z}$  è denotato anche col simbolo  $\mathbb{Z}_m$  ed è detto l'**insieme degli interi modulo  $m$** . In tale insieme è allora possibile introdurre le operazioni quoziante della somma e del prodotto di  $\mathbb{Z}$  (vedi Paragrafo 4.2 e 5.5.1). Si pone quindi, per ogni  $a, b \in \mathbb{Z}$ :

$$[a]_m + [b]_m := [a + b]_m,$$

$$[a]_m \cdot [b]_m := [a \cdot b]_m,$$

e si ha:

**5.5.3.** Per ogni intero  $m$ , la struttura  $(\mathbb{Z}_m, +, \cdot)$  è un anello commutativo unitario.

*Dimostrazione.* Da 4.2.10 segue subito che  $+$  e  $\cdot$  sono commutative e associative, che  $\cdot$  è distributiva rispetto a  $+$ , che  $[0]_m$  è elemento neutro in  $(\mathbb{Z}_m, +)$ , che  $[1]_m$  è elemento neutro in  $(\mathbb{Z}_m, \cdot)$  e che  $[-x]_m$  è l'opposto di  $[x]_m$  per ogni  $[x]_m \in \mathbb{Z}_m$ . Pertanto  $(\mathbb{Z}_m, +, \cdot)$  è un anello commutativo unitario.  $\square$

In particolare si ha quindi:  $-[x]_m = [-x]_m = [m - x]_m$ , per ogni  $x \in \mathbb{Z}$ . Si ha:

**5.5.4.** Sia  $m \in \mathbb{Z}$  e si consideri  $x \in \mathbb{Z}$ . Allora risulta:

$$[x]_m = \{x + mk : k \in \mathbb{Z}\}.$$

Supposto  $m \neq 0$ , si ha poi:

$$[x]_m = [\text{rest}(x, m)]_m.$$

*Dimostrazione.* Da  $y \in [x]_m$  segue che  $m|y - x$  e quindi esiste  $k \in \mathbb{Z}$  tale che  $y - x = mk$ , cioè  $y = x + mk$ . Viceversa ovviamente ogni  $x + mk$  è tale che  $m|x - (x + mk)$ .

Sia ora  $m \neq 0$ . Dall'algoritmo della divisione segue  $x = mq + \text{rest}(x, m)$ , sicché  $m|x - \text{rest}(x, m)$ , quindi ovviamente  $x \equiv \text{rest}(x, m) \pmod{m}$  e dunque  $[x]_m = [\text{rest}(x, m)]_m$ .  $\square$

Dalla 5.5.4 si ritrova che  $[x]_0 = \{x\}$  e si ottiene che  $[x]_m$  è infinita, per ogni  $m \neq 0$  e  $x \in \mathbb{Z}$ . Si noti che:

**5.5.5.** Sia  $m > 0$  e siano  $a, b \in \mathbb{Z}$  tali che  $0 \leq a, b < m$ . Allora:

$$a \equiv b \pmod{m} \iff a = b.$$

*Dimostrazione.* Si supponga  $a \equiv b \pmod{m}$  con  $a \geq b$ . Allora  $m|a - b$ , cioè  $a - b = mk$ , per qualche  $k \in \mathbb{Z}$  e si ha  $0 \leq a - b = mk \leq a < m$ . Pertanto  $k = 0$  e dunque  $a = b$ . Il viceversa segue subito dalla riflessività della congruenza modulo  $m$ .  $\square$

Le considerazioni precedenti portano al seguente notevole risultato:

**5.5.6.** Sia  $m > 0$ . Allora  $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$  e  $|\mathbb{Z}_m| = m$ .

*Dimostrazione.* Da 5.5.5 segue che  $[0]_m, [1]_m, \dots, [m-1]_m$  sono a due a due distinte, sicché  $\{[0]_m, [1]_m, \dots, [m-1]_m\}$  è un sottoinsieme di ordine  $m$  di  $\mathbb{Z}_m$ . Per ogni  $x \in \mathbb{Z}$  si ha poi  $[x]_m = [\text{rest}(x, m)]_m \in \{[0]_m, [1]_m, \dots, [m-1]_m\}$ . Ciò prova l'asserto.  $\square$

**5.5.7. Esempio.** Si ha ovviamente:  $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ ,  $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ ,  $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ ,  $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ .

La 5.5.6 giustifica il termine *insieme dei resti modulo  $m$*  che talvolta si usa per denotare  $\mathbb{Z}_m$ . Si parla a volte anche di *aritmetica modulo  $m$*  quando, considerati i numeri da 0 a  $m-1$ , li si somma e moltiplica in  $\mathbb{Z}$  considerando poi come risultato il relativo resto modulo  $m$ . Per esempio, nell'aritmetica modulo 7, si ha:  $3+4=0$ ,  $-5=2$ ,  $6\cdot 3=4$ ,  $2\cdot 3=6$ . Questa aritmetica è anche detta l'*aritmetica dell'orologio*, come chiarisce l'esempio seguente.

**5.5.8. Esempio.** Se in questo momento sono le 16 e si vuole sapere che ora sarà tra 60 ore, basta ragionare modulo 24. In tal modo da  $\text{rest}(60, 24) = 12$  e da  $\text{rest}(16+12, 24) = \text{rest}(28, 24) = 4$  segue che saranno le 4 di mattina.

**5.5.9. Esempio.** Se oggi è martedì, allora tra 40 giorni sarà domenica in quanto  $\text{rest}(40, 7) = 5$ .

Dall'essere la congruenza modulo  $m$  compatibile con la somma e col prodotto segue che:

**5.5.10. Siano  $a, b, m$  interi. Si ha:**

- (i)  $a \equiv b \pmod{m} \iff a+t \equiv b+t \pmod{m}, \forall t \in \mathbb{Z}$ ;
- (ii)  $a \equiv b \pmod{m} \implies at \equiv bt \pmod{m}, \forall t \in \mathbb{Z}$ ;
- (iii)  $at \equiv bt \pmod{m} \implies a \equiv b \pmod{m}, \forall t \in \mathbb{Z}$  con  $\text{MCD}(t, m) = 1$ .

*Dimostrazione.* La (i) segue subito dalla riflessività della congruenza modulo  $m$  e da 5.5.1, e così la (ii). Per la (iii) si osservi che da  $at \equiv bt \pmod{m}$  segue che  $m$  divide  $(a-b)t$  sicché  $m$  divide  $a-b$  per la 5.4.9.  $\square$

Si osservi che in (iii) la condizione  $\text{MCD}(t, m) = 1$  è necessaria. Infatti, supposto  $\text{MCD}(t, m) = d \neq 1$  e scritto  $m = dm'$ , si ha  $tm' \equiv t0 \pmod{m}$  con  $m' \not\equiv 0 \pmod{m}$ .

Da 5.5.6 e 5.5.10 segue subito che:

**5.5.11. Sia  $m$  un intero. Si ha  $\mathbb{Z}_m = \{[a]_m, [a+1]_m, \dots, [a+(m-1)]_m\}$ , per ogni  $a \in \mathbb{Z}$ , e  $\mathbb{Z}_m = \{[a \cdot 0]_m, [a \cdot 1]_m, \dots, [a \cdot (m-1)]_m\}$ , per ogni  $a \in \mathbb{Z}$  tale che  $\text{MCD}(a, m) = 1$ .**

Dalla precedente osservazione segue che:

**5.5.12. Sia  $m > 1$ . L'elemento  $[a]_m \in \mathbb{Z}_m$  è invertibile se e solo se  $(a, m) = 1$ .**

*Dimostrazione.* Sia  $(a, m) = 1$ . Da 5.5.11 si ha che esiste  $b \in \{0, 1, \dots, m - 1\}$  tale che  $[1]_m = [a \cdot b]_m$ , e da  $[a \cdot b]_m = [a]_m \cdot [b]_m$  segue l'asserto.

Viceversa, se esiste  $[b]_m \in \mathbb{Z}_m$  tale che  $[1]_m = [a]_m \cdot [b]_m = [a \cdot b]_m$ , allora  $a \cdot b \equiv 1 \pmod{m}$ , sicché  $ab - 1 = km$  per qualche  $k \in \mathbb{Z}$ . Da ciò segue  $\text{MCD}(a, m) = 1$ .  $\square$

In particolare risulta:

**5.5.13.** *Sia  $m > 1$ . La struttura  $(\mathbb{Z}_m, +, \cdot)$  è un campo se e solo se  $m$  è un numero primo.*

*Dimostrazione.* Supposto  $m$  primo, da 5.5.12 segue che  $[a]_m$  è invertibile, per ogni  $[a]_m \in \mathbb{Z}_m \setminus \{[0]_m\}$ .

Viceversa, se  $\mathbb{Z}_m$  è un campo, si ha, sempre per 5.5.12, che  $\text{MCD}(a, m) = 1$  per ogni  $0 < a < m$ , da cui segue che  $m$  è un numero primo.  $\square$

Da 4.1.15, da 5.5.12 e da quanto osservato subito dopo 5.5.10 segue anche che in  $(\mathbb{Z}_m, \cdot)$  l'elemento  $[a]_m \neq [0]_m$  è non regolare se e solo se  $\text{MCD}(a, m) \neq 1$ .

L'insieme  $U(\mathbb{Z}_m)$  degli elementi invertibili di  $(\mathbb{Z}_m, \cdot)$  è di solito denotato col simbolo  $\mathbb{Z}_m^*$ . Ovviamente  $(\mathbb{Z}_m^*, \cdot)$  è un gruppo abeliano e, per la 5.5.12, risulta:

$$\mathbb{Z}_m^* = \{[a]_m \in \mathbb{Z}_m : (a, m) = 1\} = \{[a]_m : 0 < a < m, (a, m) = 1\}.$$

Si ha quindi che l'ordine di  $\mathbb{Z}_m^*$  coincide col numero degli interi positivi minori di  $m$  e coprimi con  $m$ . Tale numero è di solito indicato con  $\varphi(m)$  e detto l'*indicatore di Gauss-Eulero*.

**5.5.14. Esempio.** Si ha:

$$\begin{aligned}\varphi(4) &= |\{1, 3\}| = 2, \\ \varphi(5) &= |\{1, 2, 3, 4\}| = 4, \\ \varphi(9) &= |\{1, 2, 4, 5, 7, 8\}| = 6, \\ \varphi(12) &= |\{1, 5, 7, 11\}| = 4.\end{aligned}$$

Se  $p$  è un qualsiasi numero naturale primo, allora

$$\begin{aligned}\varphi(p) &= p - 1, \\ \varphi(p^2) &= p^2 - p,\end{aligned}$$

e più in generale

$$\varphi(p^n) = p^n - p^{n-1},$$

per ogni  $n \geq 1$ , in quanto gli unici naturali positivi minori di  $p^n$  e non coprimi con  $p^n$  sono i multipli di  $p$ . Proprietà di  $\varphi(n)$ ,  $n \geq 1$ , saranno studiate nel paragrafo successivo.

## Esercizi

**Esercizio 5.5.1.** Si precisi se le seguenti affermazioni sono esatte:

$$\begin{aligned} -7 &\equiv -7 \pmod{11}, 22 \equiv 4 \pmod{11}, 23 \equiv 45 \pmod{11}, 5 \equiv 38 \pmod{11}, \\ -7 &\equiv 29 \pmod{12}, 22 \equiv 2 \pmod{12}, 21 \equiv 21 \pmod{12}, 5 \equiv 29 \pmod{12}. \end{aligned}$$

**Esercizio 5.5.2.** Siano  $x, y$  e  $m$  interi, con  $m > 1$ , e si supponga  $x \equiv y \pmod{m}$ . Si provi che  $m$  divide  $x$  se e solo se  $m$  divide  $y$ .

**Esercizio 5.5.3.** Si determini il valore delle seguenti espressioni modulo 9, esprimendo il risultato con un numero non negativo minore di 9:

$$\begin{array}{cccccccc} 6+3, & 4+8, & 6\cdot 3, & 4\cdot 8, & 4+6, & 2+2, & 2\cdot 6, & 2\cdot 2, \\ 6+6, & -4, & 6\cdot 6, & 5-1, & 3-4, & -2, & 1-2, & 2-1. \end{array}$$

**Esercizio 5.5.4.** Si verifichi se le seguenti assegnazioni definiscono applicazioni di  $\mathbb{Z}_4$  in  $\mathbb{Z}_6$  e, in caso affermativo, si precisi se l'applicazione è iniettiva, se suriettiva:

$$[z]_4 \longmapsto [z]_6, \quad [z]_4 \longmapsto [2z]_6, \quad [z]_4 \longmapsto [3z]_6, \quad [z]_4 \longmapsto [4z]_6.$$

**Esercizio 5.5.5.** Si scrivano le tabelle moltiplicative di  $(\mathbb{Z}_4, +)$ , di  $(\mathbb{Z}_5, +)$ , di  $(\mathbb{Z}_7, +)$ , di  $(\mathbb{Z}_4, \cdot)$ , di  $(\mathbb{Z}_5, \cdot)$ , di  $(\mathbb{Z}_7, \cdot)$ , di  $(\mathbb{Z}_6^*, \cdot)$ , di  $(\mathbb{Z}_8^*, \cdot)$ , di  $(\mathbb{Z}_{10}^*, \cdot)$ .

**Esercizio 5.5.6.** Siano  $m > 1, a, b \in \mathbb{Z}$ . Allora:

- (1) da  $a \equiv b \pmod{m}$  segue  $a \equiv b \pmod{s}$ , per ogni  $s$  divisore di  $m$ ;
- (2) da  $a \equiv b \pmod{m}$  segue  $at \equiv bt \pmod{mt}$ , per ogni  $t \in \mathbb{Z}$ ; e, viceversa, da  $at \equiv bt \pmod{mt}$  segue  $a \equiv b \pmod{m}$ , per ogni  $t \neq 0$ ;
- (3) da  $a \equiv b \pmod{m}$  e  $a \equiv b \pmod{l}$ , con  $(m, l) = 1$ , segue  $a \equiv b \pmod{ml}$ .

**Esercizio 5.5.7. Alcuni criteri di divisibilità.** Sia  $n \in \mathbb{N}$ , scritto in forma decimale come  $n = a_k a_{k-1} \dots a_1 a_0$ , con  $k \geq 0$ ,  $a_0, \dots, a_k \in \{0, \dots, 9\}$  e  $a_k \neq 0$ . Si verifichi che:

- (1) 2 divide  $n$  se e solo se 2 divide  $a_0$ ;
- (2) 5 divide  $n$  se e solo se 5 divide  $a_0$ ;
- (3) con  $i$  tale che  $1 \leq i \leq k$ , si ha che  $2^i$  (rispettivamente  $5^i$ ) divide  $n$  se e solo se  $2^i$  (risp.  $5^i$ ) divide  $a_{i-1} \dots a_1 a_0$ ;
- (4) 9 (risp. 3) divide  $n$  se e solo se 9 (risp. 3) divide  $a_0 + a_1 + \dots + a_k$ ;
- (5) 11 divide  $n$  se e solo se 11 divide  $a_0 - a_1 + \dots + (-1)^k a_k$ .

*Svolgimento.* Si osservi in primo luogo che, con  $m > 1$  e  $x, y \in \mathbb{Z}$  tali che  $x \equiv y \pmod{m}$ , si ha ovviamente che  $m$  divide  $x$  se e solo se  $m$  divide  $y$  (vedi Esercizio 5.5.2). Per ipotesi  $n = a_k \dots a_1 a_0 = a_0 + 10a_1 + \dots + 10^k a_k$ . Pertanto la (1) e la (2) seguono subito dall'essere  $n = a_0 + 10(a_1 + 10a_2 + \dots + 10^{k-1} a_k)$ . Più in generale, considerato  $i$  tale che  $1 \leq i \leq k$ , si ha

$$n = a_0 + \dots + a_{i-1} 10^{i-1} + 10^i (a_i + 10a_{i+1} + \dots + 10^{k-i} a_k),$$

da cui  $n \equiv a_0 + a_1 10 + \cdots + a_{i-1} 10^{i-1} \pmod{10^i}$ , cioè  $n \equiv a_{i-1} \dots a_1 a_0 \pmod{10^i}$ . Per provare la (4) si osservi che  $10^j \equiv 1 \pmod{9}$  per ogni  $j \geq 0$ , come segue subito da  $10 \equiv 1 \pmod{9}$  e dalla compatibilità rispetto al prodotto della congruenza modulo  $m$ . Pertanto  $10^j a_j \equiv a_j \pmod{9}$ , per ogni  $j \in \{0, \dots, k\}$ , da cui, per la compatibilità rispetto alla somma della congruenza modulo  $m$ , segue che  $a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + a_1 + \cdots + a_k \pmod{9}$ , cioè  $n \equiv a_0 + a_1 + \cdots + a_k \pmod{9}$ . L'osservazione iniziale assicura la (4). Infine, da  $10 \equiv -1 \pmod{11}$  segue  $10^j \equiv (-1)^j \pmod{11}$  per ogni  $j \in \{0, \dots, k\}$ . Ragionando come per la (4), si ottiene la (5).

**Esercizio 5.5.8.** Utilizzando le considerazioni fatte per la (4) dell'Esercizio 5.5.7, si dimostri la ben nota prova del nove per la somma e per il prodotto di interi.

## 5.6 La funzione di Eulero

L'applicazione  $\varphi : n \in \mathbb{N} \longmapsto \varphi(n) \in \mathbb{N}$ , dove

$$\begin{cases} \varphi(1) := 1, \\ \varphi(n) := |\{i \in \mathbb{N} : i < n, \text{MCD}(n, i) = 1\}| \quad \text{se } n > 1, \end{cases}$$

è detta la **funzione di Eulero**. Come già osservato, si ha

$$\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1),$$

per ogni numero naturale primo  $p$  e ogni  $s \geq 1$ . Tale risultato permette di calcolare  $\varphi(n)$  per ogni  $n > 1$  in quanto vale la seguente notevole proposizione:

**5.6.1.** Siano  $h$  e  $k$  numeri naturali positivi coprimi. Allora si ha:

$$\varphi(hk) = \varphi(h)\varphi(k).$$

*Dimostrazione.* È facile verificare che ha senso l'applicazione

$$\theta : [a]_{hk} \in \mathbb{Z}_{hk} \longmapsto ([a]_h, [a]_k) \in \mathbb{Z}_h \times \mathbb{Z}_k,$$

che tale applicazione è iniettiva e che è un omomorfismo tra l'anello  $(\mathbb{Z}_{hk}, +, \cdot)$  e l'anello prodotto  $(\mathbb{Z}_h \times \mathbb{Z}_k, +, \cdot)$ . Da  $|\mathbb{Z}_h \times \mathbb{Z}_k| = hk = |\mathbb{Z}_{hk}|$  segue allora che  $\theta$  è un isomorfismo di anelli (vedi 2.2.10). In particolare  $\theta(\mathbb{Z}_{hk}^*) = U(\mathbb{Z}_h \times \mathbb{Z}_k) = \mathbb{Z}_h^* \times \mathbb{Z}_k^*$ , sicché  $\varphi(h)\varphi(k) = |\mathbb{Z}_h^* \times \mathbb{Z}_k^*| = |\theta(\mathbb{Z}_{hk}^*)| = |\mathbb{Z}_{hk}^*| = \varphi(hk)$ .  $\square$

Ne segue che, considerato  $n \in \mathbb{N} \setminus \{1\}$ , se  $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ , con  $s \geq 1$ ,  $p_1, \dots, p_s$  primi a due a due distinti,  $\alpha_1, \dots, \alpha_s > 0$ , si ha:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} \dots p_s^{\alpha_s}) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_s^{\alpha_s}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_s^{\alpha_s} - p_s^{\alpha_s-1}) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right). \end{aligned}$$

Interessante è anche il seguente risultato, che generalizza quanto già evidenziato nell'Esercizio 3.6.2, fornendone una differente dimostrazione:

**5.6.2. Piccolo teorema di Fermat.** *Sia  $p$  un numero naturale primo. Allora per ogni  $a \in \mathbb{Z}$  si ha:  $a^p \equiv a \pmod{p}$ .*

*Dimostrazione.* Sia  $a \in \mathbb{Z}$ . Se  $p$  divide  $a$ , l'asserto è ovvio. Si supponga quindi  $p$  e  $a$  coprimi. Si ha allora  $\mathbb{Z}_p = \{[0 \cdot a]_p, [1 \cdot a]_p, \dots, [(p-1) \cdot a]_p\}$  (vedi 5.5.11), sicché  $[1]_p [2]_p \dots [p-1]_p = [1 \cdot a]_p [2 \cdot a]_p \dots [(p-1) \cdot a]_p$  e dunque  $(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$ . Ovviamente  $p$  è coprimo con  $(p-1)!$ , pertanto si ottiene (vedi 5.5.10)  $a^{p-1} \equiv 1 \pmod{p}$  e anche  $a^p \equiv a \pmod{p}$ .  $\square$

La precedente dimostrazione evidenzia che, se  $p$  non divide  $a$ , allora  $a^{p-1} \equiv 1 \pmod{p}$ . Più in generale:

**5.6.3. Teorema di Fermat-Eulero.** *Sia  $m > 1$  e sia  $a$  un intero coprimo con  $m$ . Allora:  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .*

*Dimostrazione.* Da 5.5.11 segue che  $\mathbb{Z}_m \setminus \{\bar{0}\} = \{\bar{1 \cdot a}, \bar{2 \cdot a}, \dots, \bar{(m-1) \cdot a}\}$ . Si ponga

$$I := \{h \in \mathbb{N} : h < m, \text{MCD}(h, m) = 1\}.$$

Ovviamente  $|I| = \varphi(m)$  e si ha  $\text{MCD}(ha, m) = 1$  se e solo se  $\text{MCD}(h, m) = 1$ , in quanto  $a$  e  $m$  sono coprimi. Pertanto risulta  $\mathbb{Z}_m^* = \{\bar{h \cdot a} : h \in I\}$ , da cui  $\prod_{h \in I} \bar{h \cdot a} = \prod_{h \in I} \bar{h}$  e quindi anche

$$\left( \prod_{h \in I} h \right) a^{\varphi(m)} \equiv \prod_{h \in I} h \pmod{m}.$$

Da ciò e da 5.5.10 segue l'asserto essendo  $\text{MCD} \left( \prod_{h \in I} h, m \right) = 1$ .  $\square$

Il seguente celebre risultato fornisce un criterio di primalità:

**5.6.4. Teorema di Wilson.** *Sia  $p \in \mathbb{N} \setminus \{1\}$ . Allora  $p$  è primo se e solo se  $(p-1)! \equiv -1 \pmod{p}$ .*

*Dimostrazione.* Da  $(p-1)! \equiv -1 \pmod{p}$  segue subito che l'unico divisore positivo  $d$  di  $p$  minore di  $p$  è 1, in quanto  $d$  divide  $(p-1)!$ . Pertanto  $p$  è primo.

Viceversa, sia  $p$  primo. L'asserto è ovvio se  $p = 2, 3$ . Si supponga dunque  $p \geq 5$ . Si ha  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ , cioè per ogni  $a \in \{1, \dots, p-1\}$  esiste uno e un solo  $b \in \{1, \dots, p-1\}$  tale che  $ab \equiv 1 \pmod{p}$ . Si osserva poi facilmente che si ha

$a^2 \equiv 1 \pmod{p}$  se e solo se  $a \equiv 1 \pmod{p}$  o  $a \equiv -1 \pmod{p}$ . Quindi gli unici  $a \in \{1, \dots, p-1\}$  tali che  $ab \equiv 1 \pmod{p}$  con  $b = a$  sono 1 e  $p-1$ . Considerati allora  $2, \dots, p-2$ , si ottiene che  $2 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$ , cioè  $(p-2)! \equiv 1 \pmod{p}$ , da cui  $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$ , come volevasi.  $\square$

Essenziali per la segretezza negli scambi di informazioni risultano i cosiddetti **codici a chiave pubblica** e, forse inaspettatamente, il teorema di Fermat-Eulero risulta fondamentale per quello più famoso ed efficace: il **codice RSA**, dal nome degli inventori Rivest, Shamir, Adleman.

Si parla di codice a chiave pubblica quando è resa nota la chiave del codice, senza che ciò danneggi la segretezza dello scambio. Si descriverà ora rapidamente e senza particolare precisione il codice RSA che, come si vedrà, sfrutta anche l'esistenza di numeri primi sufficientemente grandi (vedi 5.1.4).

Si supponga che le persone  $T_1, \dots, T_k$  ( $k \geq 2$ ) vogliano scambiarsi informazioni in modo tale che solo il previsto ricevente possa interpretarle. Allora ciascuno sceglie due primi  $p_i$  e  $q_i$  sufficientemente grandi, cioè di almeno 100 cifre ciascuno, effettua il prodotto  $n_i = p_i q_i$  e rende noto  $n_i$ . L'efficacia di tale codice è legata al fatto che, noto un numero naturale molto grande, è difficile, se non impossibile con i mezzi attuali, determinarne la decomposizione in primi. Poi ciascun  $T_i$  calcola  $\varphi(n_i) = (p_i - 1)(q_i - 1)$  e fissa un numero naturale  $e_i$  coprimo con  $\varphi(n_i)$ . Esiste allora un naturale  $f_i$  tale che  $e_i f_i \equiv 1 \pmod{\varphi(n_i)}$  (vedi 5.5.12);  $T_i$  rende noto  $e_i$ . Se  $T_i$  vuole mandare un messaggio a  $T_j$ , trasforma tale messaggio in un numero  $a$  (o in una sequenza di numeri), utilizzando un metodo stabilito in precedenza, per esempio sostituendo a ciascuna lettera dell'alfabeto il numero che rappresenta la sua posizione nell'alfabeto, e facendo sì che tale  $a$  risulti coprimo con  $n_j$ , calcola  $a^{e_j}$  modulo  $n_j$  e invia tale numero a  $T_j$ . Questi calcola  $a^{e_j f_j}$  modulo  $n_j$  e ritrova  $a$  in quanto  $a^{\varphi(n_j)} \equiv 1 \pmod{n_j}$ , per il teorema di Fermat-Eulero,  $e_j f_j \equiv 1 \pmod{\varphi(n_j)}$ , cioè  $e_j f_j = 1 + k\varphi(n_j)$  per qualche  $k$ , e dunque  $a^{e_j f_j} = a^{1+k\varphi(n_j)} \equiv a \pmod{n_j}$ .

Ovviamente se  $T_l$ , con  $l \neq i, j$ , intercetta il messaggio, non è in grado di decodificarlo in quanto non conosce, né può calcolare  $f_j$  vista l'impossibilità di determinare la fattorizzazione di  $n_j$  e dunque  $\varphi(n_j)$ .

C'è anche la possibilità che  $T_i$  "firmi" il suo messaggio in modo tale che  $T_j$ , ricevuto questo, possa individuarne il mittente. Per fare ciò  $T_i$  calcola prima  $b = a^{f_i}$  modulo  $n_i$  e poi  $b^{e_j}$  modulo  $n_j$ , inviando tale numero a  $T_j$ . Questi calcola prima  $b^{e_j f_j} \equiv b \pmod{n_j}$ , e solo dopo aver determinato il giusto indice  $i$  per cui  $b^{e_i}$  modulo  $n_i$  individua un messaggio sensato, può leggere tale messaggio e riconoscere anche da chi proviene.

## Esercizi

**Esercizio 5.6.1.** Si provi che, con  $n \in \mathbb{N}$ , si ha  $\varphi(n)$  dispari se e solo se  $n \leq 2$ .

**Esercizio 5.6.2.** Si verifichi che  $\varphi(n) = 4$  se e solo se  $n \in \{5, 8, 10, 12\}$ .

**Esercizio 5.6.3.** Con  $n, k \in \mathbb{N}$ , si provi che se  $k$  divide  $n$  allora  $\varphi(k)$  divide  $\varphi(n)$ .

## 5.7 Sistemi di equazioni congruenziali lineari

Come è ben noto, nell'aritmetica elementare risulta molto utile saper risolvere un'equazione di primo grado, del tipo cioè  $a_0 + a_1x = 0$ , con  $a_1 \neq 0$ . Un analogo studio viene ora affrontato relativamente all'aritmetica modulo un intero  $m$ . Più in generale sono presi in considerazione poi sistemi con più equazioni.

Sia  $m$  un intero positivo e siano  $a, b \in \mathbb{Z}$ . L'equazione

$$ax \equiv b \pmod{m}$$

con  $x$  indeterminata è detta un'**equazione congruenziale lineare** in  $x$  modulo  $m$ . Studiarla significa ovviamente individuare se esistono soluzioni, cioè interi  $s$  tali che  $as \equiv b \pmod{m}$ , quali sono e come sono tra loro legate. Si ha:

**5.7.1.** *Sia  $m$  un intero positivo e siano  $a, b \in \mathbb{Z}$ . Si consideri l'equazione*

$$ax \equiv b \pmod{m}.$$

*Se  $a$  e  $m$  sono coprimi, esiste  $s \in \mathbb{Z}$  tale che  $as \equiv b \pmod{m}$ . Inoltre risulta  $\{z \in \mathbb{Z} : az \equiv b \pmod{m}\} = [s]_m$ .*

*Dimostrazione.* Per il teorema di Bézout (vedi 5.4.7) esistono  $v, w \in \mathbb{Z}$  tali che  $1 = av + mw$ , da cui  $av \equiv 1 \pmod{m}$  e quindi  $avb \equiv 1b \pmod{m}$ . Pertanto  $s := vb$  è soluzione dell'equazione. Sia ora  $z \in \mathbb{Z}$  tale che  $az \equiv b \pmod{m}$ . Allora  $az \equiv as \pmod{m}$  da cui  $z \equiv s \pmod{m}$  essendo  $(a, m) = 1$  (vedi 5.5.10). Viceversa, ovviamente, da  $t \equiv s \pmod{m}$  segue  $at \equiv as \pmod{m}$  e dunque  $at \equiv b \pmod{m}$ .  $\square$

La dimostrazione precedente fornisce un metodo costruttivo per l'individuazione di una e quindi di tutte le soluzioni dell'equazione.

**5.7.2. Esempio.** L'equazione  $12x \equiv 8 \pmod{35}$  ha soluzioni in quanto risulta  $(12, 35) = 1$ . Da  $35 = 12 \cdot 2 + 11$ ,  $12 = 11 \cdot 1 + 1$ , segue che  $1 = 12 - 11 \cdot 1 = 12 - (35 - 12 \cdot 2) \cdot 1 = 12 \cdot 3 + 35 \cdot (-1)$ , da cui  $12 \cdot 3 \equiv 1 \pmod{35}$  e quindi  $12 \cdot 3 \cdot 8 \equiv 8 \cdot 1 \pmod{35}$ , cioè  $12 \cdot 24 \equiv 8 \pmod{35}$ . Le soluzioni sono dunque tutti e soli gli interi congrui 24 modulo 35.

Si osservi che:

**5.7.3.** *Sia  $m$  un intero positivo e siano  $a, b, t \in \mathbb{Z}$  tali che  $t$  divida  $m$ ,  $a$  e  $b$ . Allora l'equazione  $ax \equiv b \pmod{m}$  ha soluzione  $s \in \mathbb{Z}$  se e solo se l'equazione*

$$\frac{a}{t}x \equiv \frac{b}{t} \pmod{\frac{m}{t}}$$

*ha soluzione  $s$ .*

*Dimostrazione.* Se  $as \equiv b \pmod{m}$ , da 5.5.10 segue  $\frac{as}{t} = \frac{a}{t}s \equiv \frac{b}{t} \pmod{\frac{m}{t}}$ . Il viceversa è analogo.  $\square$

Si ha:

**5.7.4.** *Sia  $m$  un intero positivo e siano  $a, b \in \mathbb{Z}$ . L'equazione  $ax \equiv b \pmod{m}$  ha soluzioni se e solo se  $d$  divide  $b$ , con  $d = (a, m)$ .*

*Dimostrazione.* Sia  $d = \text{MCD}(a, m)$ . Se  $s$  è una soluzione di  $ax \equiv b \pmod{m}$ , allora  $as - b = lm$ , per qualche  $l \in \mathbb{Z}$ , sicché si ha che  $d$  divide  $as - lm = b$ . Il viceversa segue subito da 5.7.1 osservando che  $(\frac{a}{d}, \frac{m}{d}) = 1$ .  $\square$

Più precisamente si ha:

**5.7.5.** *Sia  $m$  un intero positivo, siano  $a, b \in \mathbb{Z}$  e si supponga  $d$  divisore di  $b$  con  $d = (a, m)$ . Si ponga:  $S = \{z \in \mathbb{Z} : az \equiv b \pmod{m}\}$ . Allora:*

- (i)  $S = \{u \in \mathbb{Z} : \frac{a}{d}u \equiv \frac{b}{d} \pmod{\frac{m}{d}}\}$ .
- (ii)  $S$  si ripartisce in  $d$  classi di congruenza modulo  $m$ .

*Dimostrazione.* La (i) segue da 5.7.3. Per la (ii) si osservi che, con  $s$  soluzione di  $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$  si ha:  $S = [s]_{\frac{m}{d}} = [s]_m \cup [s + \frac{m}{d}]_m \cup \dots \cup [s + (d-1)\frac{m}{d}]_m$ .  $\square$

**5.7.6. Esempio.** Si consideri l'equazione  $36x \equiv 24 \pmod{105}$ . Siccome risulta  $(36, 105) = 3$  e 3 divide 24, si può considerare l'equazione  $12x \equiv 8 \pmod{35}$ . Come osservato nell'Esempio 5.7.2, 24 ne è soluzione, sicché l'insieme delle soluzioni dell'equazione  $36x \equiv 24 \pmod{105}$  è :

$$[24]_{35} = [24]_{105} \cup [24 + 35]_{105} \cup [24 + 70]_{105}.$$

Si hanno informazioni anche su sistemi di equazioni congruenziali lineari. Sussiste il celebre, antichissimo:

**5.7.7. Teorema cinese del resto.** *Siano  $m_1, \dots, m_k$  interi positivi a due a due coprimi ( $k \geq 2$ ) e siano  $b_1, \dots, b_k$  interi. Allora il sistema*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

*ha una soluzione  $s$ , e l'insieme delle soluzioni del sistema coincide con la classe  $[s]_{m_1 \dots m_k}$ .*

*Dimostrazione.* Si procederà per induzione su  $k$ . Sia  $k = 2$  e, per comodità, si scriva il sistema come:

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv b' \pmod{m'} \end{cases}$$

con  $(m, m') = 1$ . La generica soluzione della prima equazione è del tipo  $b + my$ , con  $y \in \mathbb{Z}$ . Si imponga che un tal numero sia soluzione anche della seconda equazione e si interpreti  $y$  come indeterminata. Si ottiene in questo modo l'equazione  $b + my \equiv b' \pmod{m'}$ , cioè  $my \equiv b' - b \pmod{m'}$  nell'indeterminata  $y$ . Tale equazione ha soluzione  $t$  in quanto  $(m, m') = 1$  (vedi 5.7.1). Il numero intero

$$s := b + mt$$

è allora soluzione sia della prima che della seconda equazione, e dunque è soluzione del sistema. Se anche  $s'$  è soluzione del sistema, si ha  $s' \equiv b \pmod{m}$ ,  $s' \equiv b' \pmod{m'}$  e dunque  $s' \equiv s \pmod{m}$  e  $s' \equiv s \pmod{m'}$ , sicché  $m$  ed  $m'$  dividono  $s' - s$ . Da  $(m, m') = 1$  segue allora che  $mm'$  divide  $s' - s$  e  $s' \in [s]_{mm'}$ . Viceversa, sia  $z \in [s]_{mm'}$ , cioè sia  $z$  tale che  $z \equiv s \pmod{mm'}$ . Allora  $z \equiv s \pmod{m}$  e  $z \equiv s \pmod{m'}$ , da cui  $z \equiv b \pmod{m}$  e  $z \equiv b' \pmod{m'}$ , come volevasi.

Sia ora  $k > 2$  e si consideri il sistema:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_{k-1} \pmod{m_{k-1}}. \end{cases}$$

Per ipotesi d'induzione esiste una soluzione  $w$  di tale sistema e l'insieme delle soluzioni è  $[w]_{m_1 \dots m_{k-1}}$ . Considerata ora la generica soluzione  $w + m_1 \dots m_{k-1}y$ , con  $y \in \mathbb{Z}$ , come prima si impone che tale intero sia soluzione anche della  $k$ -esima equazione, cioè che si abbia  $w + m_1 \dots m_{k-1}y \equiv b_k \pmod{m_k}$ . Interpretando  $y$  come indeterminata, si ottiene l'equazione congruenziale  $m_1 \dots m_{k-1}y \equiv b_k - w \pmod{m_k}$ , che ha soluzione in quanto  $(m_1 \dots m_{k-1}, m_k) = 1$  (vedi 5.7.1). Detta  $l$  una tale soluzione, si ottiene che l'intero  $v := w + m_1 \dots m_{k-1}l$  è soluzione del sistema. La dimostrazione si completa poi facilmente (vedi Esercizio 5.7.4).  $\square$

Si osservi che anche la dimostrazione del Teorema 5.7.7 è costruttiva, fornendo un metodo risolutivo.

**5.7.8. Esempio.** Si consideri il sistema:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4}. \end{cases}$$

La generica soluzione della prima equazione è un intero del tipo  $4 + 5y$ , con  $y \in \mathbb{Z}$ . Si impone allora che sia soluzione della seconda, ottenendo un'equazione congruenziale nell'indeterminata  $y$ :  $4 + 5y \equiv 3 \pmod{4}$ , cioè  $5y \equiv 3 - 4 \pmod{4}$ . Da  $5 \equiv 1 \pmod{4}$  e  $-1 \equiv 3 \pmod{4}$  si ottiene  $y \equiv 3 \pmod{4}$ . Pertanto l'intero  $4 + 5 \cdot 3 = 19$  è soluzione del sistema, e l'insieme delle soluzioni è  $[19]_{20} = \{19 + 20z : z \in \mathbb{Z}\}$ .

Si noti che nello studio di un sistema di equazioni congruenziali lineari è conveniente partire dall'equazione con modulo maggiore.

**5.7.9. Esempio.** Si consideri il sistema:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5}. \end{cases}$$

Come osservato è conveniente studiare il sistema equivalente:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3}. \end{cases}$$

Come visto nell'Esempio 5.7.8, la generica soluzione del sistema costituito dalle prime due equazioni è del tipo  $19 + 20z$ , con  $z \in \mathbb{Z}$ . Imponendo che tale numero sia soluzione anche della terza equazione si ottiene la seguente equazione congruenziale in  $z$ :  $19 + 20z \equiv 2 \pmod{3}$ , cioè  $20z \equiv 2 - 19 \pmod{3}$ . Da  $20 \equiv 2 \pmod{3}$  e  $-17 \equiv 1 \pmod{3}$  segue che l'equazione da studiare diventa  $2z \equiv 1 \pmod{3}$ , che, banalmente, ha come soluzione 2. Infatti  $3 = 2 \cdot 1 + 1$  da cui  $1 = 3 - 2 \cdot 1 = 3 + 2(-1)$  sicché  $2(-1) \equiv 1 \pmod{3}$ , cioè  $2 \cdot 2 \equiv 1 \pmod{3}$ . Pertanto l'intero  $19 + 20 \cdot 2 = 59$  è soluzione del sistema, e l'insieme delle soluzioni del sistema è  $[59]_{60} = \{59 + 60v : v \in \mathbb{Z}\}$ .

Il sistema

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

con  $k \geq 2$  e  $(m_i, m_j) = 1$  per ogni  $i \neq j$ , può essere risolto anche nel seguente modo.

Si calcola innanzitutto  $m := m_1 \dots m_k$  e, per ogni  $i \in \{1, \dots, k\}$ , si determinano gli interi  $m'_i = \frac{m}{m_i}$ . Per le ipotesi ovviamente si ha che, per ogni  $i \in \{1, \dots, k\}$ , risulta  $(m'_i, m_i) = 1$ ; inoltre  $m_i$  è divisore di  $m'_j$ , per ogni  $j \neq i$ . Si studiano allora le equazioni congruenziali

$$m'_i y \equiv 1 \pmod{m_i},$$

e si determinano interi  $m''_i$  tali che  $m'_i m''_i \equiv 1 \pmod{m_i}$ . L'intero

$$s := b_1 m'_1 m''_1 + \dots + b_k m'_k m''_k$$

è soluzione del sistema. Infatti, per ogni  $i \in \{1, \dots, k\}$ , si ha  $s \equiv b_i m'_i m''_i \pmod{m_i}$ , in quanto  $m_i$  divide  $m'_j$  per ogni  $j \neq i$ . Si ha poi  $b_i m'_i m''_i \equiv b_i \pmod{m_i}$ , in quanto  $m'_i m''_i \equiv 1 \pmod{m_i}$ .

**5.7.10. Esempio.** Il sistema considerato nell'Esempio 5.7.9 ha soluzione

$$s = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 = 80 + 135 + 144 = 359,$$

perché, in tal caso, si ha  $m = 60$ ,  $m'_1 = 20$ ,  $m'_2 = 15$ ,  $m'_3 = 12$ ; si devono allora studiare le equazioni:  $20x \equiv 1 \pmod{3}$ ,  $15x \equiv 1 \pmod{4}$ ,  $12x \equiv 1 \pmod{5}$ , che diventano:  $2x \equiv 1 \pmod{3}$ ,  $3x \equiv 1 \pmod{4}$ ,  $2x \equiv 1 \pmod{5}$ , e che, ovviamente, hanno come soluzione, rispettivamente,  $m''_1 = 2$ ,  $m''_2 = 3$ ,  $m''_3 = 3$ .

Pertanto l'insieme delle soluzioni del sistema è:  $[359]_{60} = [59]_{60}$ .

Si osservi inoltre che:

**5.7.11. Si consideri il sistema**

$$\left\{ \begin{array}{l} a_1x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_kx \equiv b_k \pmod{m_k}, \end{array} \right.$$

con  $a_1, \dots, a_k, b_1, \dots, b_k$  interi e  $m_1, \dots, m_k$  interi positivi a due a due coprimi. Tale sistema ha soluzioni se e solo se ciascuna delle equazioni ha soluzioni. Precisamente, se  $s_i$  è soluzione di  $a_i x \equiv b_i \pmod{m_i}$ , il sistema considerato è equivalente al sistema:

$$\left\{ \begin{array}{l} x \equiv s_1 \pmod{m_1} \\ \vdots \\ x \equiv s_k \pmod{m_k}. \end{array} \right.$$

*Dimostrazione.* Esercizio. □

**5.7.12. Esempio.** Il sistema

$$\left\{ \begin{array}{l} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 4x \equiv 3 \pmod{11} \end{array} \right.$$

ha soluzioni ed è equivalente al sistema

$$\left\{ \begin{array}{l} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 9 \pmod{11}, \end{array} \right.$$

la cui generica soluzione è  $108 + 385z$ , con  $z \in \mathbb{Z}$ .

Si noti infine che il richiedere che i moduli delle equazioni di un sistema siano a due a due coprimi non è condizione necessaria perché il sistema abbia soluzione. Per esempio il sistema

$$\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 9 \pmod{12} \end{cases}$$

ha soluzione 81. Ciò dipende dal fatto che  $\text{MCD}(10, 12) = 2$  e 2 divide  $1 - 9$ . Si potrebbe infatti dimostrare che:

**5.7.13. Generalizzazione del teorema cinese del resto.** *Si consideri il sistema*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k}, \end{cases}$$

*con  $k \geq 2$ ,  $b_1, \dots, b_k$  interi e  $m_1, \dots, m_k$  interi positivi. Tale sistema ha soluzioni se e solo se  $\text{MCD}(m_i, m_j)$  divide  $b_i - b_j$ , per ogni  $i, j \in \{1, \dots, k\}$  con  $i \neq j$ .*

## Esercizi

**Esercizio 5.7.1.** *Si precisi se l'equazione congruenziale  $9x \equiv 5 \pmod{14}$  ha soluzioni e, in caso affermativo, le si determinino.*

**Esercizio 5.7.2.** *Si precisi se la seguente equazione congruenziale  $11x \equiv 6 \pmod{15}$  ha soluzioni e, in caso affermativo, le si determinino.*

**Esercizio 5.7.3.** *Si ridimostri la 5.7.1 utilizzando la 5.5.11.*

*Svolgimento.* Da  $(a, m) = 1$  e da 5.5.11 si ha  $\mathbb{Z}_m = \{\overline{0a}, \overline{1a}, \dots, \overline{(m-1)a}\}$ . Esiste quindi  $i \in \{0, \dots, m-1\}$  tale che  $\overline{b} = \overline{ia}$ , da cui  $ai \equiv b \pmod{m}$ .

**Esercizio 5.7.4.** *Si completi la dimostrazione di 5.7.7.*

**Esercizio 5.7.5.** *Si determini, in entrambi i modi illustrati (vedi Esempi 5.7.9 e 5.7.10), la generica soluzione dei seguenti sistemi di equazioni congruenziali:*

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 9 \pmod{11} \\ x \equiv 51 \pmod{75}. \end{cases}$$

**Esercizio 5.7.6.** *Si determini il generico intero a tale che si abbia simultaneamente:*

- (i)  $\text{rest}(a, 3) = 2, \text{rest}(a, 4) = 3, \text{rest}(a, 7) = 6;$
- (ii)  $\text{rest}(a, 18) = 15, \text{rest}(a, 19) = 16.$

**Esercizio 5.7.7.** Si determini l'unico numero naturale  $a$  compreso tra 103 e 159 tale che simultaneamente si abbia:  $a \equiv 3 \pmod{7}$  e  $a \equiv 5 \pmod{6}$ .

**Esercizio 5.7.8.** Un cesto contiene  $n$  uova. Se si prova a svuotare il cesto prendendo le uova a 2 a 2 ne resta 1, così se le si prendono a 3 a 3 o a 5 a 5. Prendendole invece a 7 a 7 non ne resta nessuna. Si determini il minimo  $n$  perché ciò accada.

**Esercizio 5.7.9.** Sette ladri devono dividere il bottino di una rapina. Hanno rubato  $n$  lingotti d'oro. Provano a dividerli in parti uguali, ma ne avanzano 6. Ne nasce un litigio cui segue una sparatoria. Uno dei ladri muore. Provano allora nuovamente a dividere il bottino ma restano 2 lingotti, il che provoca un nuovo litigio e una nuova sparatoria che causa la morte di un altro ladro. I restanti si dividono il bottino e finalmente non avanza alcun lingotto. Si determini il minimo numero  $n$  di lingotti che possono aver rubato.

**Esercizio 5.7.10.** Si dimostri 5.7.11.

## 5.8 I numeri razionali

Si è già descritto il campo dei numeri razionali

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}.$$

Tale struttura può essere costruita a partire dall'anello  $\mathbb{Z}$  degli interi, col procedimento che ora sarà illustrato.

Si consideri l'insieme  $A := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  e si introduca in  $A$  la seguente relazione:

$$(a, b) \mathcal{R} (c, d) : \iff ad = bc. \quad (5.8.1)$$

Si verifica facilmente (vedi Esercizio 5.8.1) che  $\mathcal{R}$  è una relazione d'equivalenza. Si ha poi (vedi Esercizio 5.8.2), per ogni  $b \in \mathbb{Z} \setminus \{0\}$  e per ogni  $a \in \mathbb{Z}$ :

$$[(0, b)]_{\mathcal{R}} = \{(0, y) : y \in \mathbb{Z} \setminus \{0\}\}; \quad (5.8.2)$$

$$[(b, b)]_{\mathcal{R}} = \{(y, y) : y \in \mathbb{Z} \setminus \{0\}\} = [(1, 1)]_{\mathcal{R}}; \quad (5.8.3)$$

$$[(a, b)]_{\mathcal{R}} = \{(ay, by) : y \in \mathbb{Z} \setminus \{0\}\}; \quad (5.8.4)$$

$$[(ab, b)]_{\mathcal{R}} = \{(ay, y) : y \in \mathbb{Z} \setminus \{0\}\}. \quad (5.8.5)$$

La classe  $[(a, b)]_{\mathcal{R}}$ , con  $(a, b) \in A$ , è di solito denotata col simbolo

$$\frac{a}{b}$$

e detta **frazione** di **numeratore**  $a$  e **denominatore**  $b$ . Pertanto, con  $a, c \in \mathbb{Z}$  e  $b, d \in \mathbb{Z} \setminus \{0\}$ , si ha:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

Con  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z} \setminus \{0\}$ , dalle uguaglianze (5.8.2), (5.8.3), (5.8.4) e (5.8.5) si ottiene, per ogni  $y \in \mathbb{Z} \setminus \{0\}$ :

$$\frac{0}{b} = \frac{0}{y}, \quad \frac{b}{b} = \frac{y}{y}, \quad \frac{a}{b} = \frac{ay}{by}, \quad \frac{ab}{b} = \frac{ay}{y}.$$

L'insieme quoziante  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \mathcal{R}$  è denotato col simbolo  $\mathbb{Q}$  e detto l'insieme dei numeri razionali.

Nell'insieme  $\mathbb{Q}$  si introducono le seguenti operazioni: con  $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$  si pone

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}. \quad (5.8.6)$$

Tali definizioni hanno senso, in quanto da  $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$  segue  $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$  e  $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ . Infatti per le ipotesi si ha  $ab' = ba'$  e  $cd' = dc'$ , e da ciò si ottiene immediatamente  $(ad + bc)b'd' = adb'd' + bcb'd' = (ab')(dd') + (cd')(bb') = (ba')(dd') + (dc')(bb') = (a'd' + b'c')bd$ , cioè  $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ . L'altra uguaglianza segue facilmente.

Si ha:

**5.8.1.** *L'insieme quoziante  $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \mathcal{R}$  con le operazioni di somma e prodotto definite in (5.8.6) è un campo.*

*Dimostrazione.* L'associatività e la commutatività della somma e del prodotto e la distributività del prodotto rispetto alla somma seguono facilmente (vedi Esercizio 5.8.3). Si ha poi che la classe  $\frac{0}{b}$ , con  $b \in \mathbb{Z} \setminus \{0\}$ , è elemento neutro per la somma, in quanto:  $\frac{0}{b} + \frac{c}{d} = \frac{0d+bc}{bd} = \frac{bc}{bd} = \frac{c}{d}$ , per ogni  $\frac{c}{d} \in \mathbb{Q}$ . Inoltre esiste  $-\frac{c}{d} = \frac{-c}{d}$  in quanto  $\frac{c}{d} + \frac{-c}{d} = \frac{-cd+dc}{d^2} = \frac{0}{d^2}$ , per ogni  $\frac{c}{d} \in \mathbb{Q}$ . Inoltre, qualunque sia  $b \in \mathbb{Z} \setminus \{0\}$ , la frazione  $\frac{b}{b}$  è elemento neutro per il prodotto, in quanto  $\frac{b}{b} \frac{c}{d} = \frac{bc}{bd} = \frac{c}{d}$ , per ogni  $\frac{c}{d} \in \mathbb{Q}$ . Infine, una frazione  $\frac{c}{d}$  non nulla è tale che risulta  $c \neq 0$ , sicché ha senso la frazione  $\frac{d}{c}$  e si ha  $\frac{c}{d} \cdot \frac{d}{c} = \frac{cd}{dc}$  (elemento neutro per il prodotto), cioè  $(\frac{c}{d})^{-1} = \frac{d}{c}$ . Tutto ciò assicura che  $(\mathbb{Q}, +, \cdot)$  è un campo.  $\square$

Si ha poi:

**5.8.2.** *Sia  $b \in \mathbb{Z} \setminus \{0\}$ . L'applicazione  $\varphi : z \in \mathbb{Z} \mapsto \frac{zb}{b} \in \mathbb{Q}$  è un monomorfismo di  $(\mathbb{Z}, +, \cdot)$  in  $(\mathbb{Q}, +, \cdot)$ .*

*Dimostrazione.* L'applicazione  $\varphi$  è iniettiva in quanto da  $\frac{zb}{b} = \frac{wb}{b}$ , con  $z$  e  $w$  interi, segue  $zbb = bw$ , con  $b^2 \neq 0$ , da cui  $z = w$ . Con  $z, w \in \mathbb{Z}$  si ha poi  $\varphi(z+w) = \frac{(z+w)b}{b} = \frac{(z+w)b^2}{b^2} = \frac{zb^2+wb^2}{b^2} = \frac{zb}{b} + \frac{wb}{b} = \varphi(z) + \varphi(w)$  e  $\varphi(zw) = \frac{zbw}{b} = \frac{zbw^2}{b^2} = \frac{zb}{b} \cdot \frac{wb}{b} = \varphi(z)\varphi(w)$ .  $\square$

La 5.8.2 autorizza a identificare ogni  $z \in \mathbb{Z}$  con la frazione  $\frac{zb}{b} = \frac{z1}{1} \in \mathbb{Q}$ . Si ha dunque  $\mathbb{Z} \subseteq \mathbb{Q}$  e, per ogni  $\frac{a}{b} \in \mathbb{Q}$  si ha  $\frac{a}{b} = \frac{a1}{1} \cdot \frac{1}{b1} = \frac{a1}{1}(\frac{b1}{1})^{-1} = ab^{-1}$ . Con tali identificazioni le operazioni di somma e prodotto di  $\mathbb{Q}$  “estendono” le operazioni di somma e di prodotto di  $\mathbb{Z}$ .

## Esercizi

**Esercizio 5.8.1.** *Si dimostri che la relazione  $\mathcal{R}$  definita in (5.8.1) è una relazione d'equivalenza.*

**Esercizio 5.8.2.** *Si dimostri che valgono le uguaglianze (5.8.2), (5.8.3), (5.8.4) e (5.8.5).*

**Esercizio 5.8.3.** *Si completi la dimostrazione di 5.8.1.*

**Esercizio 5.8.4.** *Con  $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$  si definisca*

$$\frac{a}{b} \sqsubseteq \frac{c}{d} : \iff (ad - bc)bd \leq 0,$$

dove  $\leq$  denota la relazione d'ordine “usuale” in  $\mathbb{Z}$ . Si provi che  $\sqsubseteq$  è una relazione d'ordine totale in  $\mathbb{Q}$ , che “estende” la relazione d'ordine usuale in  $\mathbb{Z}$ , ed è tale che

$$\begin{aligned} \frac{a}{b} \sqsubseteq \frac{c}{d} &\implies \frac{a}{b} + \frac{e}{f} \sqsubseteq \frac{c}{d} + \frac{e}{f}, \\ \frac{a}{b} \sqsubseteq \frac{c}{d} &\implies \frac{a}{b} \cdot \frac{h}{k} \sqsubseteq \frac{c}{d} \cdot \frac{h}{k}, \end{aligned}$$

per ogni  $\frac{e}{f}, \frac{h}{k} \in \mathbb{Q}$ ,  $\frac{h}{k} \geq 0$ . Ciò si esprime dicendo che  $(\mathbb{Q}, +, \cdot, \sqsubseteq)$  è un campo ordinato. Nel seguito  $\sqsubseteq$  verrà denotata semplicemente con  $\leq$ , e detta la relazione d'ordine “usuale” in  $\mathbb{Q}$ .

**Esercizio 5.8.5.** *Con  $\frac{a}{b} \in \mathbb{Q}$ ,  $\frac{a}{b} \geq 0$ , si definisca la parte intera  $\lfloor \frac{a}{b} \rfloor$  di  $\frac{a}{b}$  ponendo*

$$\left\lfloor \frac{a}{b} \right\rfloor := \max \left\{ z \in \mathbb{Z} : z \leq \frac{a}{b} \right\},$$

dove  $\leq$  denota la relazione d'ordine “usuale” in  $\mathbb{Q}$  (vedi Esercizio 5.8.4). Si provi che  $\frac{a}{b} - 1 < \lfloor \frac{a}{b} \rfloor \leq \frac{a}{b}$ , e che  $\frac{a}{b} = \lfloor \frac{a}{b} \rfloor$  se e solo se  $\frac{a}{b}$  è un intero. Si osservi inoltre che  $\lfloor \frac{a}{b} \rfloor$  coincide col quoziente della divisione in  $\mathbb{Z}$  di  $a$  per  $b$ .

Se  $\frac{a}{b} \in \mathbb{Q}$ ,  $\frac{a}{b} < 0$ , si pone anche

$$\left\lfloor \frac{a}{b} \right\rfloor := - \left\lfloor -\frac{a}{b} \right\rfloor.$$

## 5.9 I numeri reali

Esistono svariate maniere rigorose per introdurre l'insieme dei numeri reali, per esempio mediante una costruzione assiomatica (come unico campo archimedeo ordinato completo), oppure utilizzando le sezioni di Dedekind o le successioni di Cauchy. Il Lettore interessato potrà riferirsi a un qualunque testo di analisi matematica di livello universitario. Qui si preferisce invece fornire un approccio meno rigoroso ma sicuramente più intuitivo, basato sugli allineamenti decimali.

Si definisce **numero decimale** una qualunque coppia  $\alpha = (a, (c_n)_{n \in \mathbb{N}})$  dove  $a$  è un numero intero detto la **parte intera** di  $\alpha$  e  $(c_n)_{n \in \mathbb{N}}$  è una successione di numeri naturali compresi tra 0 e 9. Un tale numero decimale viene usualmente denotato con

$$\alpha = a, c_1 c_2 c_3 \dots$$

Il numero decimale  $\alpha = a, c_1 c_2 c_3 \dots$  è detto **periodico** se esistono  $p \in \mathbb{N}$  e  $k \in \mathbb{N}_0$  tali che per ogni  $r \geq p$ ,  $c_r = c_{r+m(k+1)}$  per ogni  $m \in \mathbb{N}_0$ ; in altre parole se a partire dall'indice  $p$  le  $k+1$  cifre  $c_p, c_{p+1}, \dots, c_{p+k}$  si ripetono ciclicamente. Se  $\alpha$  è periodico e  $p$  e  $k$  sono minimi per la condizione precedente, allora la  $(k+1)$ -upla  $(c_p, c_{p+1}, \dots, c_{p+k})$  è detta il **periodo** di  $\alpha$ ; se  $p > 1$  la  $(p-1)$ -upla  $(c_1, c_2, \dots, c_{p-1})$  è detta l'**antiperiodo** di  $\alpha$ , e si adotta la notazione

$$\begin{aligned} \alpha &= a, \overline{c_1 \dots c_{k+1}} && \text{se } p = 1, \\ \alpha &= a, c_1 \dots c_{p-1} \overline{c_p c_{p+1} \dots c_{p+k}} && \text{se } p > 1. \end{aligned}$$

Se  $\alpha$  è periodico di periodo (0),  $\alpha$  viene detto **limitato** e si scrive

$$\begin{aligned} \alpha &= a && \text{se } p = 1, \\ \alpha &= a, c_1 \dots c_{p-1} && \text{se } p > 1. \end{aligned}$$

Nell'insieme  $D$  dei numeri decimali si conviene che valgano le sole seguenti identificazioni:

$$a, \bar{9} = \begin{cases} a + 1 & \text{se } a \geq 0 \\ a - 1 & \text{se } a < 0, \end{cases} \quad (5.9.1)$$

$$a, c_1 \dots c_{p-1} \bar{9} = a, c_1 \dots c_{p-2} (c_{p-1} + 1) \quad \text{se } p > 1. \quad (5.9.2)$$

Sia  $D_p$  l'insieme dei decimali periodici; è possibile definire un'applicazione biettiva  $f : \mathbb{Q} \longrightarrow D_p$ . A tale scopo si ricorda (vedi Esercizio 5.8.5) che, con  $\frac{r}{s} \in \mathbb{Q}$ , il simbolo  $\left\lfloor \frac{r}{s} \right\rfloor$  denota la parte intera di  $\frac{r}{s}$ , definita ponendo:

$$\begin{aligned} \left\lfloor \frac{r}{s} \right\rfloor &:= \max \left\{ z \in \mathbb{Z} : z \leq \frac{r}{s} \right\} && \text{se } \frac{r}{s} \geq 0, \\ \left\lfloor \frac{r}{s} \right\rfloor &:= - \left\lfloor \frac{-r}{s} \right\rfloor && \text{se } \frac{r}{s} < 0. \end{aligned}$$

Considerato poi  $\frac{r}{s} \in \mathbb{Q}$  tale che  $0 \leq \frac{r}{s} < 1$ , si pone

$$\begin{aligned} r_1 &:= 10r, & c_1 &:= \left\lfloor \frac{r_1}{s} \right\rfloor, \\ r_2 &:= 10(r_1 - c_1 s), & c_2 &:= \left\lfloor \frac{r_2}{s} \right\rfloor, \\ &\vdots & &\vdots \\ r_{n+1} &:= 10(r_n - c_n s), & c_{n+1} &:= \left\lfloor \frac{r_{n+1}}{s} \right\rfloor, \\ &\vdots & &\vdots \end{aligned}$$

Si potrebbe dimostrare che  $(c_n)_{n \in \mathbb{N}}$  è una successione di numeri naturali compresi tra 0 e 9 e che se  $\frac{r}{s} = \frac{r'}{s'}$  allora le successioni che si ottengono da tali numeri con il procedimento precedente sono uguali. Inoltre è possibile provare che il numero decimale  $f(\frac{r}{s}) := 0, c_1 c_2 \dots c_n \dots$  è periodico di periodo diverso da 9.

**5.9.1. Esempi.** Si consideri il numero razionale  $\frac{1}{5}$ ; si ha  $r_1 = 10$ ,  $c_1 = \left\lfloor \frac{10}{5} \right\rfloor = 2$ ,  $r_2 = 10(10 - 2 \cdot 5) = 0$ ,  $c_2 = 0$ ,  $c_n = 0$  per ogni  $n \geq 2$ . Dunque  $f(\frac{1}{5}) = 0, 2$ . Se ora si considera  $\frac{2}{10} = \frac{1}{5}$ , si scopre facilmente che anche  $f(\frac{2}{10}) = 0, 2$ .

Si consideri ora il numero razionale  $\frac{1}{7}$ ; allora si ha  $r_1 = 10$ ,  $c_1 = \left\lfloor \frac{10}{7} \right\rfloor = 1$ ,  $r_2 = 10(10 - 1 \cdot 7) = 30$ ,  $c_2 = \left\lfloor \frac{30}{7} \right\rfloor = 4$ ,  $r_3 = 20$ ,  $c_3 = \left\lfloor \frac{20}{7} \right\rfloor = 2$ ,  $r_4 = 60$ ,  $c_4 = 8$ ,  $r_5 = 40$ ,  $c_5 = 5$ ,  $r_6 = 50$ ,  $c_6 = 7$ ,  $r_7 = 10 = r_1$ , quindi  $c_7 = c_1 = 1$ ,  $c_8 = c_2 = 4$  e così via. Dunque  $f(\frac{1}{7}) = 0, \overline{142857}$  è un decimale periodico.

Sia ora  $\frac{r}{s} \in \mathbb{Q}$ ; allora  $\left| \frac{r}{s} - \left\lfloor \frac{r}{s} \right\rfloor \right| = \frac{m}{n}$  è un numero razionale non negativo minore di 1 e scritto  $f(\frac{m}{n}) := 0, c_1 c_2 c_3 \dots$ , si definisce

$$f\left(\frac{r}{s}\right) := \left\lfloor \frac{r}{s} \right\rfloor, c_1 c_2 c_3 \dots$$

In questo modo si associa a ogni numero razionale un numero decimale periodico di periodo diverso da 9.

Viceversa si consideri il numero decimale periodico

$$\alpha = a, c_1 c_2 \dots c_{p-1} \overline{c_p c_{p+1} \dots c_{p+k}}$$

di periodo diverso da 9; allora si può provare che il numero razionale

$$\frac{r}{s} := \frac{a10^{p+k} + c_1 10^{p+k-1} + \dots + c_{p+k} - (a10^{p-1} + c_1 10^{p-2} + \dots + c_{p-1})}{(10^{k+1} - 1)10^{p-1}}$$

è l'unico elemento di  $\mathbb{Q}$  tale che  $f(\frac{r}{s}) = \alpha$ .

Tutto questo assicura che  $f$  è biettiva. Dato  $\alpha \in D_p$  l'unico  $\frac{r}{s} \in \mathbb{Q}$  tale che  $f(\frac{r}{s}) = \alpha$  è detto la **frazione generatrice** di  $\alpha$ . Si osservi che il numeratore  $r$  è la

differenza tra il numero che si ottiene scrivendo consecutivamente il numero  $a$  e le cifre  $c_1, \dots, c_{p+k}$  e quello che si ottiene giustapponendo al numero  $a$  le eventuali cifre  $c_1, \dots, c_{p-1}$ . Il denominatore  $s$  è ottenuto scrivendo consecutivamente tante cifre uguali a 9 quante sono le cifre del periodo, e tante cifre uguali a 0 quante sono le cifre dell'eventuale antiperiodo.

**5.9.2. Esempio.** Le frazioni generatrici dei numeri decimali periodici  $3,7$  e  $-5,2\overline{41}$  sono  $\frac{370-37}{90} = \frac{333}{90} = \frac{37}{10}$  e  $\frac{-5241+52}{990} = -\frac{5189}{990}$ , rispettivamente.

Siano ora  $\alpha, \beta \in D_p$  e siano  $\frac{r}{s}, \frac{p}{q} \in \mathbb{Q}$  gli unici numeri razionali tali che  $f(\frac{r}{s}) = \alpha$  e  $f(\frac{p}{q}) = \beta$ ; se si pone  $\alpha + \beta := f(\frac{r}{s} + \frac{p}{q})$  e  $\alpha \cdot \beta := f(\frac{r}{s} \cdot \frac{p}{q})$  si definiscono in  $D_p$  due operazioni interne che dotano  $D_p$  di una struttura di campo. Ponendo poi  $\alpha < \beta$  se e solo se  $\frac{r}{s} < \frac{p}{q}$  (vedi Esercizio 5.8.4) si ottiene una relazione d'ordine in  $D_p$  che ha le stesse proprietà della relazione d'ordine "usuale" su  $\mathbb{Q}$ .

Ogni numero razionale  $\frac{r}{s} \in \mathbb{Q}$  viene identificato con il decimale periodico  $f(\frac{r}{s}) \in D_p$ ; così facendo  $\mathbb{Q}$  resta identificato con  $D_p$ .

Si definisce **numero reale** ogni numero decimale, e l'insieme dei numeri reali è denotato con  $\mathbb{R}$ . Per **parte intera**  $\lfloor \alpha \rfloor$  del numero reale  $\alpha$  si intende la parte intera del numero decimale  $\alpha$ . Con l'identificazione tra numeri razionali e decimali periodici si ha che  $\mathbb{Q} \subset \mathbb{R}$ , e la parte intera del numero razionale  $\frac{r}{s}$  coincide con quella del numero reale  $\frac{r}{s}$ . Gli elementi di  $\mathbb{R} \setminus \mathbb{Q}$  sono detti numeri reali **irrazionali**.

Siano  $\alpha = a, c_1 c_2 c_3 \dots$  e  $\beta = b, d_1 d_2 d_3 \dots$  numeri reali; per ogni  $n \in \mathbb{N}$  si considerino i numeri decimali periodici limitati

$$a_n = a, c_1 c_2 \dots c_n, \quad b_n = b, d_1 d_2 \dots d_n.$$

Per ogni  $n \in \mathbb{N}$  si ha che  $a_n, b_n \in \mathbb{Q}$  e quindi sono definiti  $s_n = a_n + b_n \in \mathbb{Q}$  e  $p_n = a_n \cdot b_n \in \mathbb{Q}$ . Si dimostra che esiste  $m \in \mathbb{N}$  tale che per ogni  $n \geq m$  i numeri razionali  $s_n$  hanno tutti la stessa parte intera  $x$ , che esiste  $m_1 \in \mathbb{N}$  tale che per ogni  $n \geq m_1$  i numeri razionali  $s_n$  hanno tutti la stessa prima cifra decimale  $y_1$ , e così via. Il numero reale  $x, y_1 y_2 \dots$  è per definizione la somma  $\alpha + \beta$  dei numeri reali  $\alpha$  e  $\beta$  considerati.

Analogamente si può dimostrare che esiste  $t \in \mathbb{N}$  tale che per ogni  $n \geq t$  i numeri razionali  $p_n$  hanno tutti la stessa parte intera  $z$ , che esiste  $t_1 \in \mathbb{N}$  tale che per ogni  $n \geq t_1$  i numeri razionali  $p_n$  hanno tutti la stessa prima cifra decimale  $h_1$ , e così via. Il numero reale  $z, h_1 h_2 \dots$  è per definizione il prodotto  $\alpha \beta$  dei numeri reali  $\alpha$  e  $\beta$  considerati.

Le operazioni interne definite in questo modo dotano  $\mathbb{R}$  di struttura di campo. Per ogni  $\alpha, \beta \in \mathbb{R}$ , si pone  $\alpha < \beta$  se e solo se  $\alpha \neq \beta$  e il numero reale  $\beta - \alpha$  ha parte intera non negativa, ottenendo in  $\mathbb{R}$  una relazione d'ordine totale (il cosiddetto ordine "usuale" in  $\mathbb{R}$ ), e si ha che  $(\mathbb{R}, +, \cdot, \leq)$  è un campo ordinato (vedi Esercizio 5.8.4) completo, nel senso che ogni sottoinsieme non vuoto di  $\mathbb{R}$  che ammette maggioranti ha estremo superiore.

Sottoinsiemi notevoli di  $\mathbb{R}$  sono i cosiddetti **intervalli reali limitati**. Con

$\alpha, \beta \in \mathbb{R}$  si pone:

$$\begin{aligned} [\alpha, \beta] &:= \{x \in \mathbb{R} : \alpha \leq x \leq \beta\}, \\ [\alpha, \beta[ &:= \{x \in \mathbb{R} : \alpha \leq x < \beta\}, \\ ]\alpha, \beta] &:= \{x \in \mathbb{R} : \alpha < x \leq \beta\}, \\ ]\alpha, \beta[ &:= \{x \in \mathbb{R} : \alpha < x < \beta\}. \end{aligned}$$

Gli intervalli precedenti hanno *estremi*  $\alpha$  e  $\beta$ ; il primo è detto *chiuso*, il secondo e il terzo *semiaperti*, l'ultimo *aperto*. Ovviamente, se  $\alpha > \beta$ , si ha  $[\alpha, \beta] = \emptyset$ ; e così, se  $\alpha \geq \beta$ , si ha  $[\alpha, \beta[ = ]\alpha, \beta] = ]\alpha, \beta[ = \emptyset$ . In maniera analoga si definiscono gli *intervalli reali illimitati*. Con  $\alpha \in \mathbb{R}$  si pone:

$$\begin{aligned} [\alpha, +\infty[ &:= \{x \in \mathbb{R} : \alpha \leq x\}, \\ ]\alpha, +\infty[ &:= \{x \in \mathbb{R} : \alpha < x\}, \\ ]-\infty, \alpha] &:= \{x \in \mathbb{R} : x \leq \alpha\}, \\ ]-\infty, \alpha[ &:= \{x \in \mathbb{R} : x < \alpha\}. \end{aligned}$$

### Rappresentazione dei numeri reali in base arbitraria

Sia  $x = a, c_1 c_2 c_3 \dots$  un numero reale positivo. Ovviamente  $x$  può essere riguardato come somma della sua parte intera e della sua *parte frazionaria*  $\alpha = x - [x]$ , con  $0 \leq \alpha < 1$ .

Sia  $b \geq 2$  un numero naturale. La rappresentazione in base  $b$  del numero naturale  $a$  è già nota (vedi Paragrafo 5.2). Sia  $\alpha = 0, c_1 c_2 c_3 \dots$  la parte frazionaria di  $x$ . Allora si può scrivere

$$\alpha = \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{c_3}{10^3} + \dots = \sum_{n=1}^{\infty} \frac{c_n}{10^n}.$$

Rappresentare  $\alpha$  in base  $b$  significa determinare una successione  $\{a_n\}_{n \geq 1}$  di cifre  $a_n \in \{0, 1, \dots, b-1\}$  tale che

$$\alpha = \sum_{n=1}^{\infty} \frac{a_n}{b^n}. \quad (5.9.3)$$

Tale circostanza verrà denotata scrivendo  $\alpha = (0, a_1 a_2 a_3 \dots)_b$  o, brevemente,  $\alpha = (0, a_1 \dots a_i)_b$  se  $a_j = 0$  per ogni  $j > i$ .

Per determinare le cifre  $a_n$  si tengano presenti le considerazioni seguenti. La (5.9.3) equivale a

$$b\alpha = a_1 + \sum_{n=2}^{\infty} \frac{a_n}{b^{n-1}}, \quad (5.9.4)$$

dove  $0 \leq \frac{a_n}{b^{n-1}} < 1$  per ogni  $n \geq 2$ . La parte intera e la parte frazionaria di  $b\alpha$  sono quindi rispettivamente  $a_1$  e  $b\alpha - a_1$ ; inoltre  $a_1 \in \{0, 1, \dots, b-1\}$ .

Se  $b\alpha - a_1 = 0$  allora  $\alpha = \frac{a_1}{b}$ , pertanto  $\alpha = (0, a_1 00 \dots)_b = (0, a_1)_b$  è la rappresentazione cercata. Se invece  $b\alpha - a_1 \neq 0$ , da (5.9.4) si ricava

$$b(b\alpha - a_1) = a_2 + \sum_{n=3}^{\infty} \frac{a_n}{b^{n-2}}. \quad (5.9.5)$$

Pertanto la parte intera e la parte frazionaria di  $b(b\alpha - a_1)$  sono rispettivamente  $a_2$  e  $b(b\alpha - a_1) - a_2$ ; inoltre  $a_2 \in \{0, 1, \dots, b-1\}$ . Di nuovo, se  $b(b\alpha - a_1) - a_2 = 0$  allora  $\alpha = \frac{a_1}{b} + \frac{a_2}{b^2}$ , e  $\alpha = (0, a_1 a_2 00 \dots)_b = (0, a_1 a_2)_b$  è la rappresentazione cercata. Se invece  $b(b\alpha - a_1) - a_2 \neq 0$  si prosegue come in precedenza, ripartendo da (5.9.5), e si riesce a determinare  $a_3$ . Così continuando, ovviamente, non è detto che il procedimento termini dopo un numero finito di passi, ma si è sempre in grado di determinare il numero desiderato di cifre decimali di  $\alpha$  in base  $b$ .

**5.9.3. Esempio.** Per determinare la rappresentazione in base 5 del numero razionale

$$\alpha = \frac{84}{100} = 0, 84,$$

basta porre

$$\alpha = 0, 84 = \frac{a_1}{5} + \frac{a_2}{25} + \frac{a_3}{125} + \dots$$

Allora

$$\begin{aligned} 5\alpha &= 4, 2 = a_1 + \frac{a_2}{5} + \frac{a_3}{25} + \dots, \text{ da cui } a_1 = 4; \\ 5\alpha - a_1 &= 0, 2 = \frac{a_2}{5} + \frac{a_3}{25} + \dots; \\ 5(5\alpha - a_1) &= 1 = a_2 + \frac{a_3}{5} + \dots, \text{ da cui } a_2 = 1; \\ 5(5\alpha - a_1) - a_2 &= 0. \end{aligned}$$

Dunque  $\alpha = (0, 41)_5$ .

**5.9.4. Esempio.** Per determinare la rappresentazione in base 5 del numero razionale

$$\alpha = \frac{85}{100} = 0, 85,$$

si ponga

$$\alpha = 0, 85 = \frac{a_1}{5} + \frac{a_2}{25} + \frac{a_3}{125} + \dots$$

Allora

$$\begin{aligned} 5\alpha &= 4, 25 = a_1 + \frac{a_2}{5} + \frac{a_3}{25} + \dots, \text{ da cui } a_1 = 4; \\ 5\alpha - a_1 &= 0, 25 = \frac{a_2}{5} + \frac{a_3}{25} + \dots; \end{aligned}$$

$$\begin{aligned}5(5\alpha - a_1) &= 1,25 = a_2 + \frac{a_3}{5} + \dots, \text{ da cui } a_2 = 1; \\5(5\alpha - a_1) - a_2 &= 0,25 = \frac{a_3}{5} + \dots; \\5(5(5\alpha - a_1) - a_2) &= 1,25 = a_3 + \frac{a_4}{5} + \dots, \text{ da cui } a_3 = 1.\end{aligned}$$

Il procedimento non ha termine. Però siccome per  $n \geq 2$  le cifre  $a_n$  si ripetono costantemente, si può scrivere  $\alpha = (0,41111\dots)_5$ . Si noti che in questo caso la rappresentazione decimale di  $\alpha$  è limitata, mentre quella in base 5 non lo è.

**5.9.5. Esempio.** Si voglia determinare, fino alle prime 3 cifre decimali, la rappresentazione in base 5 del numero reale irrazionale  $\pi = 3,14159\dots$ . La parte frazionaria di  $\pi$  è  $\alpha = 0,14159\dots$ . Si scriva

$$\alpha = 0,14159\dots = \frac{a_1}{5} + \frac{a_2}{25} + \frac{a_3}{125} + \dots$$

Allora

$$\begin{aligned}5\alpha &= 0,70795\dots = a_1 + \frac{a_2}{5} + \frac{a_3}{25} + \dots, \text{ da cui } a_1 = 0; \\5\alpha - a_1 &= 0,70795\dots = \frac{a_2}{5} + \frac{a_3}{25} + \dots; \\5(5\alpha - a_1) &= 3,53975\dots = a_2 + \frac{a_3}{5} + \frac{a_4}{25} + \dots, \text{ da cui } a_2 = 3; \\5(5\alpha - a_1) - a_2 &= 0,53975\dots = \frac{a_3}{5} + \frac{a_4}{25} + \dots; \\5(5(5\alpha - a_1) - a_2) &= 2,69875\dots = a_3 + \frac{a_4}{5} + \dots, \text{ da cui } a_3 = 2.\end{aligned}$$

Quindi  $\alpha = (0,032\dots)_5$  e  $\pi = (3,032\dots)_5$ .

**Osservazione.** Si potrebbe verificare che se si adotta per i numeri reali la rappresentazione in base arbitraria  $b \geq 2$ , le identificazioni (5.9.1) e (5.9.2) inducono analoghe uguaglianze, dove ovviamente si sostituisca la cifra 9 con la cifra  $b - 1$ . Per esempio, in base  $b = 2$ , risulta

$$(0,10011111\dots)_2 = (0,101)_2 = \frac{5}{8}.$$

Inoltre si può dimostrare che esiste un'applicazione biettiva tra l'intervallo reale  $[0, 1[$  e l'insieme delle successioni a valori interi compresi tra 0 e  $b - 1$  e non definitivamente uguali a  $b - 1$ .

## Esercizi

**Esercizio 5.9.1.** Di ciascuno dei seguenti numeri reali si individui la parte intera, la parte frazionaria, l'eventuale periodo, l'eventuale antiperiodo e, per quelli

razionali, la frazione generatrice:

$$\begin{array}{lll} 2,\overline{369} & -3,0007 & 3,000\overline{7} \\ \sqrt{2} & (3,1\overline{2})^2 & 2\sqrt{5} \\ \sqrt{2}\sqrt{3} & -\pi\sqrt{3} & 2\sqrt{5} + 1. \end{array}$$

**Esercizio 5.9.2.** Si determini la rappresentazione in base 8 del numero razionale

$$\alpha = \frac{9}{5} = 1,8.$$

**Esercizio 5.9.3.** Si determini la rappresentazione in base 9 del numero razionale

$$\alpha = \frac{288}{100} = 2,88.$$

**Esercizio 5.9.4.** Si determini, fino alle prime 4 cifre decimali, la rappresentazione in base 6 del numero irrazionale  $\pi^2$ .

**Esercizio 5.9.5.** Si stabilisca se il numero reale  $0,43\overline{42}$  è razionale, e se ne determini la rappresentazione in base 5 fino alle prime 4 cifre decimali.

**Esercizio 5.9.6.** Si determini, fino alle prime 5 cifre decimali, la rappresentazione in base 4 del numero reale  $\sqrt{6}$ .

## 5.10 I numeri complessi

Il campo  $\mathbb{C}$  dei numeri complessi nasce dall'esigenza di "ampliare" il campo  $\mathbb{R}$  dei numeri reali per far sì che esistano elementi il cui quadrato è negativo.

Una possibile costruzione è la seguente. Si ponga  $\mathbb{C} = \mathbb{R} \times \mathbb{R}$  e si introducano in  $\mathbb{C}$  le seguenti operazioni:

$$\begin{aligned} (a, b) + (c, d) &:= (a + c, b + d), \\ (a, b) \cdot (c, d) &:= (ac - bd, ad + bc). \end{aligned}$$

La struttura  $(\mathbb{C}, +)$  è un gruppo abeliano, in quanto struttura prodotto di  $(\mathbb{R}, +)$  con se stesso; la coppia  $(0, 0)$  è l'elemento neutro, denotato anche con 0, e risulta  $-(a, b) = (-a, -b)$ , per ogni  $(a, b) \in \mathbb{C}$ . Si ha poi:

**5.10.1.** La struttura algebrica  $(\mathbb{C}, +, \cdot)$  è un campo.

*Dimostrazione.* Si prova facilmente che il prodotto è associativo, commutativo e distributivo rispetto alla somma (vedi Esercizio 5.10.1). La coppia  $(1, 0)$  è elemento neutro per il prodotto in quanto  $(1, 0)(a, b) = (1a - 0b, 1b + 0a) = (a, b)$ ,

per ogni  $(a, b) \in \mathbb{C}$ . Supposto  $(a, b) \in \mathbb{C} \setminus \{0\}$  si ha che  $a^2 + b^2 \neq 0$  essendo  $a \neq 0$  oppure  $b \neq 0$ , e la coppia  $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$  è l'inverso di  $(a, b)$  poiché

$$\begin{aligned}(a, b) \left( \frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) &= \left( a \frac{a}{a^2+b^2} - b \frac{-b}{a^2+b^2}, a \frac{-b}{a^2+b^2} + b \frac{a}{a^2+b^2} \right) \\ &= \left( \frac{a^2+b^2}{a^2+b^2}, \frac{0}{a^2+b^2} \right) = (1, 0).\end{aligned}$$

Quanto detto prova che  $(\mathbb{C}, +, \cdot)$  è un campo.  $\square$

Si ha inoltre:

**5.10.2.** L'applicazione  $\psi : r \in \mathbb{R} \mapsto (r, 0) \in \mathbb{C}$  è un monomorfismo tra le strutture  $(\mathbb{R}, +, \cdot)$  e  $(\mathbb{C}, +, \cdot)$ .

*Dimostrazione.* Esercizio.  $\square$

La 5.10.2 permette di identificare ogni numero reale con la coppia  $(r, 0)$ . Pertanto si ha  $\mathbb{R} \subseteq \mathbb{C}$  e la somma e il prodotto di  $\mathbb{C}$  “estendono” la somma e il prodotto di  $\mathbb{R}$ . La coppia  $(0, 1) \in \mathbb{C}$  è tale che

$$(0, 1)(0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0).$$

Pertanto, posto  $i := (0, 1)$  (la cosiddetta **unità immaginaria**) e utilizzando l'identificazione precedentemente introdotta, si ha  $i^2 = -1$ . Risulta poi, sempre con le notazioni precedenti che, per ogni  $(a, b) \in \mathbb{C}$ , riesce

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi.$$

Pertanto

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

Gli elementi di  $\mathbb{C}$  si dicono **numeri complessi**. Si ha  $a + bi = c + di$  se e solo se  $a = c$  e  $b = d$ , e le operazioni di somma e prodotto tra numeri complessi acquistano l'usuale espressione:

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i, \\ (a + bi) \cdot (c + di) &= (ac - bd) + (ad + bc)i,\end{aligned}$$

per ogni  $a, b, c, d \in \mathbb{R}$ .

Sia  $\alpha = a + bi$  un numero complesso. Il numero complesso

$$\overline{\alpha} := a + (-b)i$$

è detto il **coniugato** di  $\alpha$ , e il numero reale

$$N(\alpha) := a^2 + b^2$$

la **norma** di  $\alpha$ . Si prova facilmente che:

**5.10.3.** *Si ha:*

- (i)  $N(\alpha)$  è un numero reale non negativo, per ogni  $\alpha \in \mathbb{C}$ ;
- (ii)  $N(\alpha) = 0$  se e solo se  $\alpha = 0$ ;
- (iii)  $\alpha\bar{\alpha} = N(\alpha)$ , per ogni  $\alpha \in \mathbb{C}$ ;
- (iv)  $N(\alpha\beta) = N(\alpha)N(\beta)$ , per ogni  $\alpha, \beta \in \mathbb{C}$ ;
- (v)  $\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}$ , per ogni  $\alpha \in \mathbb{C} \setminus \{0\}$ .

*Dimostrazione.* Esercizio. □

Il campo complesso  $\mathbb{C}$ , come osservato, è tale che in esso esistono elementi il cui quadrato è  $-1$ , cioè esistono soluzioni dell'equazione  $x^2 + 1 = 0$ . Più in generale, il cosiddetto **teorema fondamentale dell'algebra**, di cui non si fornisce la dimostrazione, assicura che una qualunque equazione di grado  $n > 0$  a coefficienti complessi ha soluzioni  $c_1, \dots, c_n$  (non necessariamente distinte) in  $\mathbb{C}$ . Ciò si esprime dicendo che  $\mathbb{C}$  è **algebricamente chiuso**.

Si noti infine che non è possibile definire in  $\mathbb{C}$  una relazione d'ordine totale  $\leq$  tale che da  $\alpha \leq \beta$  segua  $\alpha + \gamma \leq \beta + \gamma$ , per ogni  $\gamma \in \mathbb{C}$ , e  $\alpha\delta \leq \beta\delta$ , per ogni  $\delta \in \mathbb{C}$ ,  $\delta > 0$  (vedi Esercizio 5.10.4).

## Esercizi

**Esercizio 5.10.1.** *Si dimostri che il prodotto di numeri complessi è associativo, commutativo e distributivo rispetto alla somma.*

**Esercizio 5.10.2.** *Si dimostri 5.10.2.*

**Esercizio 5.10.3.** *Si provi 5.10.3.*

**Esercizio 5.10.4.** *Si dimostri che non è possibile definire in  $\mathbb{C}$  una relazione d'ordine totale  $\leq$  tale che da  $\alpha \leq \beta$  segua  $\alpha + \gamma \leq \beta + \gamma$ , per ogni  $\gamma \in \mathbb{C}$ , e  $\alpha\delta \leq \beta\delta$ , con  $\delta \in \mathbb{C}$ ,  $\delta > 0$ .*

*Svolgimento.* Per assurdo sia  $\leq$  una relazione d'ordine totale in  $\mathbb{C}$  soddisfacente le condizioni dell'enunciato. Allora si osservi innanzitutto che, se  $\alpha \in \mathbb{C} \setminus \{0\}$ , si ha  $\alpha > 0$  se e solo se  $-\alpha < 0$ . Infatti, supposto  $\alpha > 0$ , si ha  $\alpha + (-\alpha) > -\alpha$ , cioè  $0 > -\alpha$ . Analogamente  $-\alpha < 0$  implica  $-\alpha + \alpha < 0 + \alpha$ , cioè  $0 < \alpha$ . Si osservi poi che considerato un qualunque  $\alpha \in \mathbb{C} \setminus \{0\}$ , si ha che  $\alpha^2 > 0$ . Infatti, se  $\alpha > 0$ , si ha  $\alpha \cdot \alpha > \alpha \cdot 0 = 0$ ; se invece  $\alpha < 0$ , si ha  $-\alpha > 0$  e quindi  $0 = 0 \cdot (-\alpha) < (-\alpha)(-\alpha) = \alpha^2$ . In particolare si ha dunque  $1 = 1^2 > 0$  e  $-1 = i^2 > 0$ , il che è assurdo. □

## 5.11 Metodi di fattorizzazione

Sia  $n \geq 2$  un numero intero. Il problema di fattorizzare  $n$  consiste nel determinare tutti i primi  $p_1 \leq p_2 \leq \dots \leq p_N$  tali che  $n = p_1 p_2 \dots p_N$ . Esistono numerosi metodi per affrontare tale problema, che per numeri molto grandi può rivelarsi praticamente irrisolvibile con le risorse oggi disponibili, a causa dell'elevatissimo "costo computazionale". Qui verranno presentati tre metodi di fattorizzazione che, pur essendo molto semplici, hanno un notevole interesse teorico.

### Il metodo “standard”

Si tratta in sostanza della formalizzazione del metodo di fattorizzazione in primi che tutti conoscono fin dalle scuole medie. Nella sua descrizione si farà uso del crivello di Eratostene (vedi 5.1.5), nella seguente versione equivalente, di cui si preferisce fornire anche la dimostrazione:

**5.11.1. Lemma.** *Sia  $n \geq 2$  un numero naturale. Allora  $n$  è primo oppure possiede un divisore  $d$  con  $1 < d \leq \lfloor \sqrt{n} \rfloor$ .*

*Dimostrazione.* Se  $n$  non è primo, esistono naturali positivi  $a, b \neq 1$  tali che  $n = ab$ . Se  $a > \lfloor \sqrt{n} \rfloor$  allora  $a - 1 \geq \lfloor \sqrt{n} \rfloor$ , da cui  $a \geq \sqrt{n} + 1 > \sqrt{n}$ . Ne segue che  $n = ab > \sqrt{n}b$ , sicché  $b < \frac{n}{\sqrt{n}} = \sqrt{n}$  e quindi  $b \leq \lfloor \sqrt{n} \rfloor$ .  $\square$

Si consideri il numero naturale  $n \geq 2$ . Sia  $I_1 := \mathbb{N} \cap [2, \sqrt{n}]$  l'insieme dei numeri naturali appartenenti all'intervallo reale  $[2, \sqrt{n}]$ . Se  $I_1 = \emptyset$  allora  $n \in \{2, 3\}$  e il problema è risolto. Sia allora  $I_1 \neq \emptyset$ . Per il Lemma 5.11.1, se nessun elemento di  $I_1$  divide  $n$  allora  $n$  è primo. Altrimenti, sia  $k_1$  il più piccolo elemento di  $I_1$  che divide  $n$ . Se  $t$  fosse divisore di  $k_1$  per qualche naturale  $t$  con  $2 \leq t < k_1$ , allora  $t$  dividerebbe  $n$ , contro la minimalità di  $k_1$  come elemento di  $I_1$  divisore di  $n$ . Pertanto  $k_1$  è primo. Si ponga  $n_1 := \frac{n}{k_1}$ .

Sia ora  $I_2 := \mathbb{N} \cap [k_1, \sqrt{n_1}]$ . Se  $h$  dividesse  $n_1$  per qualche naturale  $h$  con  $2 \leq h < k_1$  allora  $h$  dividerebbe  $n$ , assurdo perché  $h < k_1$ . Da ciò e dal Lemma 5.11.1 segue che se  $I_2 = \emptyset$  oppure nessun elemento di  $I_2$  divide  $n_1$  allora  $n_1$  è primo. In tal caso  $n = k_1 n_1$  risulta fattorizzato nel prodotto di primi. In caso contrario, sia  $k_2$  il più piccolo elemento di  $I_2$  che divide  $n_1$ . Si supponga ora  $h$  divisore di  $k_2$ , con  $2 \leq h < k_2$ . Da  $h \geq k_1$  seguirebbe  $h \in I_2$ , e ciò è assurdo per la definizione di  $k_2$ ; quindi deve essere  $h < k_1$ , ma anche questo è impossibile per la minimalità di  $k_1$  come elemento di  $I_1$  divisore di  $n$ . Pertanto  $k_2$  è primo. Si ponga  $n_2 := \frac{n_1}{k_2}$ .

Iterando il procedimento, per ogni  $j \geq 3$  si ponga  $I_j := \mathbb{N} \cap [k_{j-1}, \sqrt{n_{j-1}}]$ . Se  $I_j = \emptyset$  oppure nessun elemento di  $I_j$  divide  $n_{j-1}$  allora  $n_{j-1}$  è primo, ed  $n = k_1 k_2 \dots k_{j-1} n_{j-1}$  risulta fattorizzato in prodotto di primi. In caso contrario si costruisca l'intervallo naturale  $I_{j+1}$ . Siccome l'ampiezza degli intervalli naturali  $I_j$  diminuisce al crescere di  $j$ , l'algoritmo descritto deve necessaria-

mente terminare dopo un numero finito di passi, dando luogo alla fattorizzazione richiesta.

**5.11.2. Esempio.** Per fattorizzare  $n = 462$  utilizzando il metodo “standard”, si procede nel modo seguente:

$$\begin{array}{llll} \lfloor \sqrt{462} \rfloor = 21 & I_1 = \mathbb{N} \cap [2, 21] & k_1 = 2 & n_1 = \frac{462}{2} = 231 \\ \lfloor \sqrt{231} \rfloor = 15 & I_2 = \mathbb{N} \cap [2, 15] & k_2 = 3 & n_2 = \frac{231}{3} = 77 \\ \lfloor \sqrt{77} \rfloor = 8 & I_3 = \mathbb{N} \cap [3, 8] & k_3 = 7 & n_3 = \frac{77}{7} = 11 \\ \lfloor \sqrt{11} \rfloor = 3 & I_4 = \emptyset. & & \end{array}$$

Pertanto  $n = 2 \cdot 3 \cdot 7 \cdot 11$  è la fattorizzazione richiesta.

**5.11.3. Esempio.** Per fattorizzare  $n = 860$  utilizzando il metodo “standard”, si procede come segue:

$$\begin{array}{llll} \lfloor \sqrt{860} \rfloor = 29 & I_1 = \mathbb{N} \cap [2, 29] & k_1 = 2 & n_1 = \frac{860}{2} = 430 \\ \lfloor \sqrt{430} \rfloor = 20 & I_2 = \mathbb{N} \cap [2, 20] & k_2 = 2 & n_2 = \frac{430}{2} = 215 \\ \lfloor \sqrt{215} \rfloor = 14 & I_3 = \mathbb{N} \cap [2, 14] & k_3 = 5 & n_3 = \frac{215}{5} = 43 \\ \lfloor \sqrt{43} \rfloor = 6 & I_4 = \mathbb{N} \cap [5, 6] & \nexists k_4. & \end{array}$$

Pertanto  $n = 2 \cdot 2 \cdot 5 \cdot 43$  è la fattorizzazione richiesta.

## Il metodo di Fermat

Il metodo di Fermat consente di scomporre un naturale dispari non primo nel prodotto di due fattori, non necessariamente primi, ma più piccoli e quindi più agevoli da fattorizzare. Il metodo si basa su un’idea molto semplice, che è essenzialmente contenuta nel seguente lemma.

**5.11.4. Lemma.** *Sia  $n$  un numero naturale dispari. Le seguenti condizioni sono equivalenti:*

- (i) esistono  $a, b \in \mathbb{N}$  con  $1 < a < b < n$  tali che  $n = ab$ ;
- (ii) esistono  $x, y \in \mathbb{N}$  con  $0 < y + 1 < x < n$  tali che  $n = x^2 - y^2$ .

*Dimostrazione.* (i)  $\Rightarrow$  (ii). Posto  $x = \frac{b+a}{2}$  e  $y = \frac{b-a}{2}$  risulta  $x, y \in \mathbb{N}$  perché  $n$  è dispari. Inoltre  $x^2 - y^2 = ab = n$  e  $0 < y + 1 < x < n$  in quanto  $x = y + 1$  comporterebbe  $a = -a + 2$  e dunque  $a = 1$  contro le ipotesi.

(ii)  $\Rightarrow$  (i). Posto  $a = x-y$  e  $b = x+y$  si ha  $n = x^2 - y^2 = (x-y)(x+y) = ab$ . Inoltre da  $y + 1 < x$  segue che  $1 < a < b < n$ .  $\square$

Sia  $n \geq 3$  un numero naturale dispari non primo. Se  $n$  è il quadrato di un numero naturale  $a$ , allora  $a > 1$  e  $n = aa$  è la fattorizzazione richiesta. Se invece  $n$  non è un quadrato, esistono  $a, b \in \mathbb{N}$  con  $1 < a < b < n$  tali che  $n = ab$ . Per il Lemma 5.11.4 esistono  $x, y \in \mathbb{N}$  con  $0 < y + 1 < x < n$  tali che  $n = x^2 - y^2$ . Siccome deve essere  $x > \lfloor \sqrt{n} \rfloor$ , per determinare  $x$  e  $y$  si comincia verificando al primo passo se  $m_1 = (\lfloor \sqrt{n} \rfloor + 1)^2 - n$  è un quadrato. In caso contrario si prosegue, verificando al passo  $i$ -esimo se  $m_i = (\lfloor \sqrt{n} \rfloor + i)^2 - n$  è un quadrato. Il Lemma 5.11.4 assicura che, dopo al più  $n - \lfloor \sqrt{n} \rfloor$  passi, questo algoritmo consente di determinare un intero positivo  $i$  tale che  $m_i$  è un quadrato. Posto allora  $x = \lfloor \sqrt{n} \rfloor + i$  e  $y = \sqrt{x^2 - n}$  risulta  $n = x^2 - y^2$ . Pertanto  $n = (x - y)(x + y)$  è la fattorizzazione richiesta.

**5.11.5. Esempio.** Per fattorizzare  $n = 462$  utilizzando il metodo di Fermat, si osservi innanzitutto che  $462 = 2 \cdot 231$ . Inoltre  $\lfloor \sqrt{231} \rfloor = 15$ , e  $m_1 = 16^2 - 231 = 25$  è un quadrato. Pertanto  $x = 16$ ,  $y = 5$ , e  $231 = (16 - 5)(16 + 5) = 11 \cdot 21$ . Siccome  $21 = 3 \cdot 7$ , in definitiva  $462 = 2 \cdot 3 \cdot 7 \cdot 11$  è la fattorizzazione richiesta.

**5.11.6. Esempio.** Per fattorizzare  $n = 860$  utilizzando il metodo di Fermat, si osservi innanzitutto che  $860 = 2 \cdot 2 \cdot 215$ . Risulta poi  $\lfloor \sqrt{215} \rfloor = 14$ , e si ha:

$$\begin{array}{ll} m_1 = 15^2 - 215 = 10 & \text{non è un quadrato;} \\ m_2 = 16^2 - 215 = 41 & \text{non è un quadrato;} \\ m_3 = 17^2 - 215 = 74 & \text{non è un quadrato;} \\ m_4 = 18^2 - 215 = 109 & \text{non è un quadrato;} \\ m_5 = 19^2 - 215 = 146 & \text{non è un quadrato;} \\ m_6 = 20^2 - 215 = 185 & \text{non è un quadrato;} \\ m_7 = 21^2 - 215 = 226 & \text{non è un quadrato;} \\ m_8 = 22^2 - 215 = 269 & \text{non è un quadrato;} \\ m_9 = 23^2 - 215 = 314 & \text{non è un quadrato;} \\ m_{10} = 24^2 - 215 = 361 = 19^2. & \end{array}$$

Pertanto  $x = 24$ ,  $y = 19$ , e  $215 = (24 - 19)(24 + 19) = 5 \cdot 43$  è già prodotto di primi. In definitiva  $860 = 2 \cdot 2 \cdot 5 \cdot 43$  è la fattorizzazione richiesta.

## Il metodo $p - 1$ di Pollard

Si consideri un numero naturale  $n > 2$  e si fissi un numero naturale  $a$  tale che  $1 < a < n$  e  $\text{MCD}(a, n) = 1$ . Si costruisca una sequenza  $a_1, a_2, \dots, a_i, \dots$  di numeri naturali ponendo:

$$a_1 := a, \quad a_2 := \text{rest}(a_1^2, n), \quad \dots, \quad a_i := \text{rest}(a_{i-1}^i, n), \quad \dots$$

Per ogni  $i \in \mathbb{N}$  si ha allora  $0 \leq a_i < n$  e  $a_i \equiv a^{i!} \pmod{n}$ , in quanto  $a_2 \equiv a_1^2 \pmod{n}$ ,  $a_3 \equiv a_2^3 \equiv a_1^{2 \cdot 3} \pmod{n}$  e così via. Per ogni  $i \in \mathbb{N}$  si ponga poi:

$$b_i := \text{MCD}(a_i - 1, n).$$

Ovviamente, non appena si ha  $b_i \neq 1$ , si è individuato un divisore  $d$  di  $n$ , con  $d \neq 1$ . Il metodo è efficace, come mostra la seguente:

**5.11.7.** *Sia  $n$  un numero naturale,  $n > 2$ , e sia  $a > 1$  tale che  $\text{MCD}(a, n) = 1$ . Se  $p$  è un primo divisore di  $n$  e  $p - 1$  divide  $c!$ , con  $c \in \mathbb{N}$ , allora  $p$  divide  $\text{MCD}(a^{c!} - 1, n)$ .*

*Dimostrazione.* Da  $p$  divisore di  $n$  e da  $(a, n) = 1$  segue che  $(a, p) = 1$ , sicché, per il teorema di Fermat-Eulero, si ha  $a^{p-1} \equiv 1 \pmod{p}$ . L'ipotesi  $p - 1$  divisore di  $c!$  comporta allora  $a^{c!} \equiv 1 \pmod{p}$ , sicché  $p$  divide  $a^{c!} - 1$ , come volevasi.  $\square$

Si osservi che se  $p$  divide  $\text{MCD}(a^{c!} - 1, n)$ , allora si ha anche  $p$  divisore di  $a_c - 1$ , per le proprietà degli  $a_i$ , e dunque  $p$  divide  $b_c$ . È opportuno rilevare che, perché  $p - 1$  divida  $c!$ , con  $c$  naturale positivo, è sufficiente che, considerato un qualunque primo  $q$  che divide  $p - 1$  e detta  $q^\alpha$  la massima potenza di  $q$  che divide  $p - 1$ , risulti  $c \geq q^\alpha$ . Per esempio, per  $p = 2521$ , si ha  $p - 1 = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$  sicché  $p - 1$  divide  $9!$ . Si noti anche che, messa in evidenza la massima potenza di 2 che divide  $n$ , si ha  $n = 2^l m$ , con  $\text{MCD}(m, 2) = 1$ , ed è conveniente scegliere  $a = 2$ .

**5.11.8. Esempio.** Si consideri  $n = 3094$ . Ovviamente  $n$  è divisibile per 2 e si ha  $n = 2 \cdot 1547$ , con  $\text{MCD}(2, 1547) = 1$ . Posto  $m = 1547$  si scelga  $a = 2$ . Allora  $a_1 = a = 2$  e  $b_1 = 1$ ,  $a_2 = \text{rest}(2^2, m) = 4$  e  $b_2 = (3, m) = 1$ ,  $a_3 = \text{rest}(4^3, m) = \text{rest}(64, m) = 64$  e  $b_3 = (63, m) = 7$ . Pertanto 7 divide  $m$  e si ha infatti  $1547 = 7 \cdot 221 = 7 \cdot 13 \cdot 17$ . Dunque  $3094 = 2 \cdot 7 \cdot 13 \cdot 17$ .

**5.11.9. Esempio.** Si consideri  $n = 5746$ . Ovviamente  $n$  è divisibile per 2 e si ha  $n = 2 \cdot 2873$ , con  $(2873, 2) = 1$ . Posto  $m = 2873$ , si scelga  $a = 2$ . Allora  $a_1 = a = 2$  e  $b_1 = 1$ ,  $a_2 = \text{rest}(2^2, m) = 4$  e  $b_2 = (3, m) = 1$ ,  $a_3 = \text{rest}(4^3, m) = \text{rest}(64, m) = 64$  e  $b_3 = (63, m) = 1$ ,  $a_4 = \text{rest}(64^4, m)$ . Per determinare tale numero, si osservi che  $64^2 = 4096 \equiv 1223 \pmod{m}$ ,  $64^3 \equiv 1223 \cdot 64 = 78272 \equiv 701 \pmod{m}$ ,  $64^4 \equiv 701 \cdot 64 = 44864 \equiv 1769 \pmod{m}$  e si ha  $b_4 = (1768, m) = 221$ . Pertanto  $221 = 13 \cdot 17$  è un divisore di  $m$  e si ha  $m = 221 \cdot 13 = 13 \cdot 13 \cdot 17$ . Dunque  $5746 = 2 \cdot 13 \cdot 13 \cdot 17$ .

**5.11.10. Esempio.** Si consideri  $n = 2444$ . Ovviamente  $n$  è divisibile per 2 e si ha  $n = 2^2 \cdot 611$  con  $(611, 2) = 1$ . Posto  $m = 611$ , si scelga  $a = 2$ . Allora  $a_1 = a = 2$  e  $b_1 = 1$ ,  $a_2 = \text{rest}(2^2, m) = 4$ , e  $b_2 = (3, m) = 1$ ,  $a_3 = \text{rest}(4^3, m) = \text{rest}(64, m) = 64$  e  $b_3 = (63, m) = 1$ ,  $a_4 = \text{rest}(64^4, m)$ . Per determinare tale numero si osservi che  $64^2 = 4096 \equiv 430 \pmod{m}$ ,  $64^3 \equiv 430 \cdot 64 = 27520 \equiv 25 \pmod{m}$ ,  $64^4 = 25 \cdot 64 = 1600 \equiv 378 \pmod{m}$  e si ha  $b_4 = (377, m) = 13$ . Pertanto 13 divide 611 e riesce  $611 = 13 \cdot 47$ , con 47 numero primo. Dunque  $2444 = 2 \cdot 2 \cdot 13 \cdot 47$ .

## Esercizi

**Esercizio 5.11.1.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 548$ .

**Esercizio 5.11.2.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 814$ .

**Esercizio 5.11.3.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 146$ .

**Esercizio 5.11.4.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 824$ .

**Esercizio 5.11.5.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 999$ .

**Esercizio 5.11.6.** Si fattorizzi, utilizzando prima il metodo “standard” e poi il metodo di Fermat, il numero intero  $n = 2205$ .

**Esercizio 5.11.7.** Si fattorizzi, utilizzando prima il metodo di Fermat e poi il metodo  $p - 1$  di Pollard, il numero intero  $n = 10961$ .

**Esercizio 5.11.8.** Si fattorizzi, utilizzando il metodo  $p - 1$  di Pollard, il numero intero  $n = 12871$ .

## 5.12 Esercizi di riepilogo

**Esercizio 5.12.1.** Si determinino le seguenti rappresentazioni:

$$\begin{array}{ll} (401)_{10} = (\dots)_2, & (120101)_3 = (\dots)_{10}, \\ (491)_{10} = (\dots)_6, & (100110100)_2 = (\dots)_{10}, \\ (539)_{10} = (\dots)_4, & (20431)_5 = (\dots)_{10}, \\ (329)_{10} = (\dots)_2; & (319)_{10} = (\dots)_3, \\ (1420)_6 = (\dots)_{10}, & (100011100)_2 = (\dots)_{10}, \\ (13201)_4 = (\dots)_{10}, & (2164)_{10} = (\dots)_5. \end{array}$$

**Esercizio 5.12.2.** Si verifichi, utilizzando il crivello di Eratostene e criteri di divisibilità (quando possibile), che i seguenti numeri sono primi: 149, 167, 173, 179, 191.

**Esercizio 5.12.3.** Si determinino tutte le soluzioni delle seguenti equazioni congruenziali:  $25x \equiv 24 \pmod{16}$ ,  $20x \equiv 30 \pmod{26}$ ,  $33x \equiv 24 \pmod{12}$ .

**Esercizio 5.12.4.** Con  $x \in \mathbb{N}_0$ , si indichi con  $\text{rest}(x, 3)$  il resto della divisione di  $x$  per 3. Si considerino poi in  $\mathbb{N}_0$  le relazioni binarie definite da:

$$\begin{aligned} x \mathcal{R}_1 y &: \iff \text{rest}(x, 3) = \text{rest}(y, 3), \\ x \mathcal{R}_2 y &: \iff x = y \text{ oppure } \text{rest}(x, 3) < \text{rest}(y, 3). \end{aligned}$$

Si precisi se le seguenti affermazioni sono esatte:

$$15 \mathcal{R}_1 5, \quad 3 \mathcal{R}_1 12, \quad 4 \mathcal{R}_1 14, \quad 11 \mathcal{R}_1 5,$$

e se è vero che:

$$13 \mathcal{R}_2 13, \quad 25 \mathcal{R}_2 31, \quad 10 \mathcal{R}_2 18, \quad 6 \mathcal{R}_2 11.$$

Si provi che  $\mathcal{R}_1$  è una relazione d'equivalenza in  $\mathbb{N}_0$  e che  $\mathcal{R}_2$  è una relazione d'ordine in  $\mathbb{N}_0$ .

**Esercizio 5.12.5.** Si descrivano gli interi a tali che simultaneamente si abbia  $\text{rest}(a, 19) = 16$ ,  $\text{rest}(a, 20) = 17$ , e se ne determini l'unico compreso tra 1000 e 1500.

**Esercizio 5.12.6.** Si determini l'unico numero naturale a compreso tra 103 e 600 tale che simultaneamente si abbia:  $a \equiv 4 \pmod{9}$ ,  $a \equiv 5 \pmod{8}$ ,  $a \equiv 3 \pmod{7}$ .

**Esercizio 5.12.7.** Considerati l'anello  $(\mathbb{Z}_6, +, \cdot)$  e l'intero positivo  $t$ , si dimostri che la parte  $t\mathbb{Z}_6 = \{t[z]_6 : [z]_6 \in \mathbb{Z}_6\} = \{[tz]_6 : z \in \mathbb{Z}\}$  è stabile. Si determini poi  $(2\mathbb{Z}_6, +, \cdot)$  e se ne studino le proprietà.

**Esercizio 5.12.8.** Si verifichi che le seguenti sono applicazioni di  $\mathbb{Z}_5$  in  $\mathbb{Z}_{15}$ , se ne studi l'iniettività e la suriettività, si stabilisca infine se sono omomorfismi di  $(\mathbb{Z}_5, +, \cdot)$  in  $(\mathbb{Z}_{15}, +, \cdot)$ :

$$\begin{aligned} f : [z]_5 \in \mathbb{Z}_5 &\longmapsto [0]_{15} \in \mathbb{Z}_{15}; \\ g : [z]_5 \in \mathbb{Z}_5 &\longmapsto [1]_{15} \in \mathbb{Z}_{15}; \\ h : [z]_5 \in \mathbb{Z}_5 &\longmapsto [3z]_{15} \in \mathbb{Z}_{15}; \\ k : [z]_5 \in \mathbb{Z}_5 &\longmapsto [6z]_{15} \in \mathbb{Z}_{15}. \end{aligned}$$

**Esercizio 5.12.9.** Si consideri, nell'insieme  $\mathbb{Z}_5$ , l'operazione interna  $\star$  definita ponendo, con  $[x]_5, [y]_5 \in \mathbb{Z}_5$ :

$$[x]_5 \star [y]_5 := [x + y + 3]_5.$$

Si verifichi che tale posizione ha senso, e si studi la struttura  $(\mathbb{Z}_5, \star)$ , scrivendone anche una tavola di moltiplicazione. Si dimostri che la posizione

$$f : [x]_5 \in \mathbb{Z}_5 \longmapsto [x + 2]_5 \in \mathbb{Z}_5$$

definisce un'applicazione e che tale applicazione è biettiva, se ne determini l'inversa, e si provi che  $f$  è un omomorfismo di  $(\mathbb{Z}_5, +)$  in  $(\mathbb{Z}_5, \star)$ .

# 6

## Alcune strutture algebriche notevoli

In questo capitolo sarà approfondito lo studio di alcune delle strutture introdotte nel Capitolo 4.

### 6.1 Semigruppi

Sia  $S$  un insieme dotato di un'operazione interna associativa, denotata come al solito con  $\cdot$ ; allora la struttura algebrica semplice  $(S, \cdot)$  è un semigruppo. Oltre agli esempi notevoli già considerati nel Capitolo 4, molto interessante risulta il seguente:

**6.1.1. Esempio.** Sia  $A$  un insieme, detto **alfabeto**, si consideri l'insieme  $A^+$  costituito dalle sequenze  $w = a_1 \dots a_n$ , con  $n \geq 1$  e  $a_1, \dots, a_n \in A$ , e si ponga  $a_1 \dots a_n = a'_1 \dots a'_m$  se e solo se  $n = m$  e  $a_1 = a'_1, \dots, a_n = a'_n$ . Una siffatta sequenza è detta una **parola** sull'alfabeto  $A$  e l'intero  $n$  è detto la **lunghezza** della parola  $w$ . Si scrive  $l(w) = n$  o anche  $|w| = n$ .

Nell'insieme  $A^+$  si introduce l'operazione di “concatenazione” o “giustapposizione” ponendo

$$a_1 \dots a_n \cdot b_1 \dots b_s := a_1 \dots a_n b_1 \dots b_s.$$

È immediato verificare che tale operazione è associativa e che, con  $w, w' \in A^+$ , si ha  $l(w \cdot w') = l(w) + l(w')$ . La struttura  $(A^+, \cdot)$  è detta il **semigruppo delle parole** sull'alfabeto  $A$ .

Si noti che, identificati gli elementi di  $A$  con le relative parole di lunghezza 1, si ha  $A \subseteq A^+$ .

Sia  $(S, \cdot)$  un semigruppo. Una parte  $T$  di  $S$  è detta un **sottosemigruppo** se è una parte stabile di  $S$  e la struttura indotta  $(T, \cdot)$  è un semigruppo. Per la (i) di 4.2.2 si ha ovviamente che  $T$  è un sottosemigruppo di  $S$  se e solo se è una parte stabile di  $S$ .

**6.1.2. Esempi.**  $S$  e  $\emptyset$  sono sempre sottosemigruppi di  $(S, \cdot)$ .  $\mathbb{N}_p$  è un sottosemigruppo di  $(\mathbb{N}, +)$ ,  $\mathbb{N}_d$  non lo è.

Per ogni intero  $t$ ,  $t\mathbb{Z}$  è un sottosemigruppo sia di  $(\mathbb{Z}, +)$  che di  $(\mathbb{Z}, \cdot)$ .

Quanto provato nel Capitolo 4 assicura che, considerato un semigruppo  $(S, \cdot)$ , l'intersezione di una famiglia di suoi sottosemigruppi è un sottosemigruppo, e che, se  $X$  è una parte di  $S$ , resta definito il sottosemigruppo **generato** da  $X$ , coincidente con  $\overline{X}$ . Pertanto  $\overline{\emptyset} = \emptyset$ ,  $\overline{X} = \{x_1 \dots x_n : n \in \mathbb{N}, x_1, \dots, x_n \in X\}$ , e se  $X = \{x\}$ , allora  $\overline{\{x\}} = \{x^n : n \in \mathbb{N}\}$ .

**6.1.3. Esempi.** In  $(\mathbb{N}, +)$  si ha  $\overline{\{1\}} = \mathbb{N}$ ,  $\overline{\{2\}} = \mathbb{N}_p$ ,  $\overline{\{2, 3\}} = \mathbb{N} \setminus \{1\}$ .

Se  $A$  è un alfabeto, come nell'Esempio 6.1.1, allora  $A^+ = \overline{A}$ .

Sia  $(S, \cdot)$  un semigruppo. Una parte  $X$  di  $S$  è detta una **base** di  $S$  se  $S = \overline{X}$  e da  $x_1 \dots x_n = x'_1 \dots x'_m$ , con  $n, m \in \mathbb{N}, x_1, \dots, x_n, x'_1, \dots, x'_m \in X$ , segue

$$n = m, \quad x_1 = x'_1, \dots, x_n = x'_n. \quad (6.1.1)$$

Un semigruppo  $(S, \cdot)$  è detto **libero** (e di base  $X$ ) se ammette una base (e  $X$  ne è una base).

**6.1.4. Esempi.** Ovviamente il semigruppo vuoto è libero di base l'insieme  $\emptyset$ .

$(\mathbb{N}, +)$  è libero di base  $\{1\}$ .

Il semigruppo delle parole  $A^+$  sull'alfabeto  $A$  è libero di base  $A$ .

Per la (6.1.1), il sottoinsieme  $\{2, 3\}$  non è una base di  $(\mathbb{N} \setminus \{1\}, +)$ , in quanto  $6 = 2 + 2 + 2 = 3 + 3$  o anche  $5 = 2 + 3 = 3 + 2$ .

Se  $(S, \cdot)$  è un semigruppo commutativo non vuoto, libero di base  $X$ , allora necessariamente  $|X| = 1$ , in quanto, supposto per assurdo  $|X| > 1$ , e considerati  $x, y \in X$  con  $x \neq y$ , si ha  $xy = yx$ , contro la (6.1.1). Si osservi inoltre che, se  $X$  è una base non vuota di un semigruppo libero  $S$ , allora  $S$  è infinito, in quanto, supposto  $x \in S$ , la (6.1.1) assicura che  $x^n \neq x^m$ , per ogni  $n, m \in \mathbb{N}$  con  $n \neq m$ .

**6.1.5. Esempi.**  $(\mathbb{N} \setminus \{1\}, +)$  non è libero, poiché nessun singleton genera  $\mathbb{N} \setminus \{1\}$ , e nessun  $X \subseteq \mathbb{N} \setminus \{1\}$ , con  $|X| > 1$  soddisfa la (6.1.1).

Ogni semigruppo finito non vuoto non è libero.

Per i semigruppi liberi sussiste la notevole:

**6.1.6. Proprietà universale dei semigruppi liberi.** *Sia  $(S, \cdot)$  un semigruppo libero di base  $X$  e si denoti con  $i$  l'immersione di  $X$  in  $S$ . Per ogni semigruppo  $(T, \cdot)$  e per ogni applicazione  $f : X \longrightarrow T$  esiste uno e un sol omomorfismo  $\varphi : S \longrightarrow T$  tale che  $\varphi \circ i = f$ , tale cioè che la restrizione di  $\varphi$  a  $X$  coincida con  $f$ .*

*Dimostrazione.* L'asserto è ovvio se  $X$  è vuoto. Sia  $X \neq \emptyset$ . Ogni elemento  $s$  di  $S$  si scrive, e in unico modo, nella forma  $s = x_1 \dots x_n$ , con  $n \geq 1$  e con  $x_1, \dots, x_n \in X$ . Ha allora senso definire  $\varphi(s) := f(x_1) \dots f(x_n)$ , ed è immediato verificare che l'applicazione  $\varphi : S \longrightarrow T$  è un omomorfismo che gode della proprietà richiesta. Se poi  $\psi : S \longrightarrow T$  è un omomorfismo con  $\psi \circ i = f$ , allora si ha  $\psi(s) = \psi(x_1 \dots x_n) = \psi(x_1) \dots \psi(x_n) = (\psi \circ i)(x_1) \dots (\psi \circ i)(x_n) = f(x_1) \dots f(x_n) = \varphi(s)$ , per ogni  $s = x_1 \dots x_n \in S$ .  $\square$

La precedente proprietà illustra il significato del termine “libero” usato per un semigruppo  $S$  dotato di base  $X$ : per definire un omomorfismo di  $S$  in un semigruppo  $T$ , basta fissare “liberamente” le immagini di ogni  $x \in X$  e utilizzare poi la suddetta proprietà.

Conseguenza immediata di 6.1.6 è il seguente:

**6.1.7. Teorema.** *Sia  $(S, \cdot)$  un semigruppo libero di base  $X$ . Allora  $S$  è isomorfo al semigruppo delle parole sull’alfabeto  $X$ .*

*Dimostrazione.* Siano  $i$  l’immersione di  $X$  in  $S$  e  $j$  l’immersione di  $X$  in  $X^+$ . Per la proprietà universale restano determinati omomorfismi  $\varphi : S \longrightarrow X^+$  e  $\psi : X^+ \longrightarrow S$  tali che  $\varphi \circ i = j$  e  $\psi \circ j = i$ . Sempre utilizzando la proprietà universale si verifica allora facilmente che  $\varphi \circ \psi = \text{id}_{X^+}$  e  $\psi \circ \varphi = \text{id}_S$ , sicché  $\varphi$  e  $\psi$  sono isomorfismi, l’uno l’inverso dell’altro (vedi anche 2.2.16).  $\square$

Sia  $(S, \cdot)$  un semigruppo. Col simbolo  $(S^{(1)}, \cdot)$  si denota il cosiddetto **monoide associato** a  $S$ , definito da:  $(S^{(1)}, \cdot) = (S, \cdot)$  se  $S$  è unitario,  $S^{(1)} = S \cup \{1\}$ , con 1 oggetto non appartenente a  $S$ , e dove  $x \cdot y$  in  $S^{(1)}$  coincide con  $x \cdot y$  in  $S$  se  $x, y \in S$ , e  $1 \cdot x = x \cdot 1 = x$ , per ogni  $x \in S^{(1)}$ , altrimenti. Si verifica subito che  $S$  è un sottosemigruppo di  $(S^{(1)}, \cdot)$ . Si ha poi:

**6.1.8.** *Sia  $(S, \cdot)$  un semigruppo e sia  $V = (S^{(1)}, \cdot)$  il monoide associato a  $S$ . Allora l’applicazione  $\varphi : s \in S \longmapsto \varphi_s \in V^V$ , dove  $\varphi_s : x \in V \longmapsto xs \in V$ , è un monomorfismo di  $(S, \cdot)$  in  $(V^V, \cdot)$ .*

*Dimostrazione.* Esercizio.  $\square$

## Esercizi

**Esercizio 6.1.1.** *Sia  $(S, \cdot)$  un semigruppo e si consideri in  $\mathcal{P}(S)$  la seguente operazione:  $X \cdot Y := \{xy : x \in X, y \in Y\}$ , con  $X, Y \in \mathcal{P}(S)$ . Si provi che  $(\mathcal{P}(S), \cdot)$  è un semigruppo.*

**Esercizio 6.1.2.** *Si provi che se  $(S, \cdot)$  è un semigruppo libero di base  $X$  e si ha  $S = \overline{Y}$ , con  $Y \subseteq S$ , allora  $Y \supseteq X$ . Se ne deduca che un semigruppo libero ha un’unica base.*

**Esercizio 6.1.3.** *Si verifichi che il semigruppo delle parole su  $A$ , con  $|A| = 1$ , è isomorfo al semigruppo libero  $(\mathbb{N}, +)$ .*

**Esercizio 6.1.4.** *Sia  $(A^+, \cdot)$  il semigruppo delle parole sull’alfabeto  $A$ . Si dimostri che l’applicazione  $l : w \in A^+ \longmapsto l(w) \in \mathbb{N}$  è un omomorfismo tra i semigruppi  $(A^+, \cdot)$  e  $(\mathbb{N}, +)$ , suriettiva se e solo se  $A \neq \emptyset$ , iniettiva se e solo se  $|A| = 1$ .*

**Esercizio 6.1.5.** Si provi che, per ogni  $m, t \geq 0$ ,  $t\mathbb{Z}_m$  è un sottosemigruppo sia di  $(\mathbb{Z}_m, +)$  che di  $(\mathbb{Z}_m, \cdot)$ .

**Esercizio 6.1.6.** Si completi la dimostrazione di 6.1.7.

**Esercizio 6.1.7.** Si dimostri 6.1.8.

## 6.2 Monoidi

Sia  $M$  un insieme dotato di un’operazione interna  $\cdot$  associativa con elemento neutro  $1$ , che talvolta è per comodità indicato con  $1_M$ . Allora la struttura algebrica semplice  $(M, \cdot)$  è un monoide.

**6.2.1. Esempio.** Come si è osservato nel paragrafo precedente, ogni semigruppo  $(S, \cdot)$  individua un monoide  $(S^{(1)}, \cdot)$ . In particolare, se  $A$  è un alfabeto, il semigruppo  $A^+$  delle parole su  $A$  individua il **monoide delle parole** su  $A$ , denotato con  $A^*$ , e ottenuto “aggiungendo” ad  $A^+$  la sequenza vuota  $1$ , detta anche la **parola vuota** su  $A$ .

È importante sottolineare che, nello studio dei monoidi, il comportamento dell’unità è “controllato”. Per esempio, se  $(M, \cdot)$  è un monoide e  $N$  è un suo sottoinsieme, si dice che  $N$  è un **sottomonoide di  $M$**  se è stabile e  $N$  con la legge indotta è un monoide avente la stessa unità di  $M$ .

**6.2.2. Esempi.** Ovviamente  $M$  è un sottomonoide di  $(M, \cdot)$ , mentre non lo è l’insieme vuoto.

La parte  $\mathbb{N}$  non è un sottomonoide di  $(\mathbb{N}_0, +)$ , perché  $0 \notin \mathbb{N}$ .

Il sottoinsieme  $4\mathbb{Z}_{12}$  non è un sottomonoide di  $(\mathbb{Z}_{12}, \cdot)$ , pur essendo stabile e tale che  $(4\mathbb{Z}_{12}, \cdot)$  è un monoide di unità  $[4]_{12}$ , in quanto  $[1]_{12} \notin 4\mathbb{Z}_{12}$ .

Con  $V$  insieme e  $X \subseteq V$ , il sottoinsieme  $\{\emptyset, X\}$  è un sottomonoide di  $(\mathcal{P}(V), \cup)$ , non di  $(\mathcal{P}(V), \cap)$  se  $X \neq V$ .

Con la definizione appena data si ha facilmente che, se  $(M, \cdot)$  è un monoide, l’intersezione di una famiglia non vuota di sottomonoidi di  $M$  è ancora un sottomonoide di  $M$ . Si può dunque definire il sottomonoide **[ $X$ ] generato** da una parte  $X$  di  $M$  come l’intersezione dei sottomonoidi di  $M$  contenenti  $X$ . Ancora si prova agevolmente che:

**6.2.3. Siano  $(M, \cdot)$  un monoide e  $X \subseteq M$ . Allora:  $K = [X]$  se e solo se:**

- (i)  $K$  è un sottomonoide di  $M$ ;
- (ii)  $K \supseteq X$ ;
- (iii)  $T$  sottomonoide di  $M$ ,  $T \supseteq X \implies T \supseteq K$ .

*Dimostrazione.* Esercizio. □

**6.2.4.** Siano  $(M, \cdot)$  un monoide e  $X \subseteq M$ . Allora:

- (i) se  $X = \emptyset$ , si ha  $[X] = \{1\}$ ;
- (ii) se  $X \neq \emptyset$ , si ha  $[X] = \{x_1 \dots x_n : n \in \mathbb{N}_0, x_1, \dots, x_n \in X\}$ , dove per  $n = 0$  si pone  $x_1 \dots x_n = 1$ .

In particolare si ha  $[x] := [\{x\}] = \{x^n : n \in \mathbb{N}_0\}$ , per ogni  $x \in M$ .

*Dimostrazione.* Esercizio. □

**6.2.5. Esempi.** Con  $A$  alfabeto si ha  $A^* = [A]$ .

In  $(\mathbb{N}_0, +)$  si ha  $[2] = 2\mathbb{N}_0$ , in  $(\mathbb{Z}_{12}, \cdot)$  si ha  $[4\mathbb{Z}_{12}] = 4\mathbb{Z}_{12} \cup \{[1]_{12}\}$ .

Attenzione va posta anche nella definizione di omomorfismo tra monoidi. Se  $(M, \cdot)$  e  $(N, \cdot)$  sono monoidi, un'applicazione  $f : M \longrightarrow N$  è detta un **omomorfismo (di monoidi)** se  $f(xy) = f(x)f(y)$ , per ogni  $x, y \in M$ , e inoltre  $f(1_M) = 1_N$ .

Si noti quindi che, se  $(M, \cdot)$  e  $(N, \cdot)$  sono monoidi, un omomorfismo di monoidi  $f : M \longrightarrow N$  è sempre un omomorfismo tra i semigruppi  $(M, \cdot)$  e  $(N, \cdot)$ , ma non vale il viceversa.

**6.2.6. Esempi.** L'applicazione  $g : x \in \mathbb{N}_0 \longmapsto 0 \in \mathbb{N}_0$  è un endomorfismo del semigruppo  $(\mathbb{N}_0, \cdot)$ , ma non è un omomorfismo del monoide  $(\mathbb{N}_0, \cdot)$  in sé.

Con  $m$  intero, l'applicazione  $h : x \in \mathbb{Z} \longrightarrow [x]_m \in \mathbb{Z}_m$  è un omomorfismo tra i monoidi  $(\mathbb{Z}, \cdot)$  e  $(\mathbb{Z}_m, \cdot)$ .

Anche per i monoidi sussiste il concetto di base di un monoide e di monoide libero. Una parte  $X$  di un monoide  $(M, \cdot)$  è detta una **base** di  $M$  se  $M = [X]$  e se da  $x_1 \dots x_n = x'_1 \dots x'_m$ , con  $n, m \in \mathbb{N}_0, x_1, \dots, x_n, x'_1, \dots, x'_m \in X$ , segue

$$n = m, \quad x_1 = x'_1, \dots, x_n = x'_n, \tag{6.2.1}$$

dove ancora, per  $n = 0$ , si pone  $x_1 \dots x_n = 1$ . Un monoide  $(M, \cdot)$  è detto **libero** (e di base  $X$ ) se ammette una base (e  $X$  ne è una base).

**6.2.7. Esempi.**  $(\{1\}, \cdot)$  è libero di base  $\emptyset$ .  $(\mathbb{N}_0, +)$  è libero di base  $\{1\}$ .

$(A^*, \cdot)$  è libero di base  $A$ .

Ancora sussistono la proprietà universale e un risultato analogo a 6.1.7 (vedi Esercizio 6.2.3 e Esercizio 6.2.5).

## Esercizi

**Esercizio 6.2.1.** Si dimostri 6.2.3.

**Esercizio 6.2.2.** Si dimostri 6.2.4.

**Esercizio 6.2.3.** Si enunci e si dimostri per i monoidi liberi una proprietà universale analoga a 6.1.6.

**Esercizio 6.2.4.** Si provi che se  $(M, \cdot)$  è un monoide libero di base  $X$  e si ha  $M = [Y]$ , con  $Y \subseteq M$ , allora  $Y \supseteq X$ . Se ne deduca che un monoide libero ha un'unica base.

**Esercizio 6.2.5.** Sia  $(M, \cdot)$  un monoide libero di base  $X$ . Allora  $M$  è isomorfo al monoide delle parole sull'alfabeto  $X$ .

## 6.3 Gruppi

Come già definito nel Capitolo 4, un gruppo  $(G, \cdot)$  è un monoide in cui tutti gli elementi sono dotati di inverso. Nel seguito talvolta si indicherà un tale gruppo semplicemente col simbolo  $G$ .

Si osservi che in un gruppo ogni elemento è regolare in quanto simmetrizzabile (vedi 4.1.15).

Nel gruppo  $(G, \cdot)$  ha senso considerare le potenze  $x^n$  di ogni elemento  $x \in G$ , per ogni  $n \in \mathbb{Z}$ , e valgono le note proprietà (4.1.3) e (4.1.4) e, se  $\cdot$  è commutativa, anche (4.1.5). Ovviamente, se si utilizza la notazione additiva, in  $(G, +)$  si possono considerare i multipli  $nx$ , al variare di  $x$  in  $G$  e di  $n$  in  $\mathbb{Z}$  e ancora valgono le usuali proprietà (4.1.1) e (4.1.2) e, se  $+$  è commutativa, anche (4.1.5).

Un gruppo commutativo è detto anche **gruppo abeliano**, dal nome del matematico norvegese Abel.

**6.3.1. Esempi.** Sono gruppi abeliani:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}_m, +)$  con  $m$  intero  $\geq 0$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathcal{P}(V), \cup)$  con  $V$  insieme, e, per la 4.2.3,  $(\{-1, 1\}, \cdot)$ ,  $(\mathbb{Z}_m^*, \cdot)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{C} \setminus \{0\}, \cdot)$ .

Se  $V$  è un insieme non vuoto, il gruppo  $(S_V, \cdot)$  definito in 4.2.4 è non abeliano se e solo se  $|V| > 2$ .

Se  $(G, \cdot)$  e  $(H, \cdot)$  sono gruppi (abeliani), la struttura prodotto  $(G \times H, \cdot)$  definita nel Paragrafo 4.1 è un gruppo (abeliano).

Sia  $(G, \cdot)$  un gruppo. Una parte  $H$  di  $G$  è detta un **sottogruppo** di  $G$ , e si scrive  $H \leq G$ , se è stabile e la struttura indotta  $(H, \cdot)$  è un gruppo. Ovviamente riesce sempre  $\{1\} \leq G$  e  $G \leq G$ , e questi sono detti i sottogruppi **banali** di  $G$ .

Le seguenti caratterizzazioni dei sottogruppi sono notevoli.

**6.3.2.** Siano  $(G, \cdot)$  un gruppo e  $H$  un sottoinsieme di  $G$ . Si ha  $H \leq G$  se e solo se valgono le seguenti proprietà:

- (i)  $H$  è stabile,
- (ii)  $1_G \in H$ ,
- (iii)  $x^{-1} \in H$ , per ogni  $x \in H$ .

*Dimostrazione.* Ovviamente, se gode delle tre proprietà suddette,  $H$  è un sottogruppo di  $G$  (vedi 4.2.2). Viceversa, se  $H$  è un sottogruppo, è soddisfatta la (i). Da  $(H, \cdot)$  gruppo segue che esiste l'unità  $1_H$  in  $H$  e risulta  $1_H 1_H = 1_H = 1_H 1_G$ , da cui, per la cancellabilità,  $1_H = 1_G$ . Infine, se  $x \in H$  e  $x'$  è l'inverso di  $x$  in

$H$ , si ha  $xx' = 1_H = 1_G = xx^{-1}$ , e, ancora per la cancellabilità di  $x$ , segue che  $x^{-1} = x' \in H$ .  $\square$

**6.3.3.** Siano  $(G, \cdot)$  un gruppo e  $H$  un sottoinsieme non vuoto di  $G$ . Allora  $H \leq G$  se e solo se  $x^{-1}y \in H$ , per ogni  $x, y \in H$ .

*Dimostrazione.* Se  $H$  è un sottogruppo di  $G$  e  $x, y$  sono elementi di  $H$ , si ha  $x^{-1} \in H$  per la (iii) di 6.3.2 e poi  $x^{-1}y \in H$  per la (i) di 6.3.2.

Viceversa, da  $H \neq \emptyset$  segue che esiste  $z \in H$  e dunque  $1 = z^{-1}z \in H$  per le ipotesi. Per ogni  $h \in H$  si ha poi  $h, 1 \in H$  e dunque  $h^{-1} = h^{-1}1 \in H$ . Infine, supposto  $x, y \in H$ , si ha  $x^{-1} \in H$  per quanto appena osservato, e di conseguenza  $xy = (x^{-1})^{-1}y \in H$ .  $\square$

In maniera analoga si prova:

**6.3.4.** Siano  $(G, \cdot)$  un gruppo e  $H$  un sottoinsieme non vuoto di  $G$ . Allora  $H \leq G$  se e solo se  $xy^{-1} \in H$ , per ogni  $x, y \in H$ .

Se si utilizza la notazione additiva per l'operazione del gruppo  $G$ , le 6.3.2, 6.3.3, 6.3.4 diventano:

**6.3.5.** Siano  $(G, +)$  un gruppo e  $H$  un sottoinsieme di  $G$ . Si ha  $H \leq G$  se e solo se valgono le seguenti proprietà:

- (i)  $H$  è stabile,
- (ii)  $0_G \in H$ ,
- (iii)  $-x \in H$ , per ogni  $x \in H$ .

**6.3.6.** Siano  $(G, +)$  un gruppo e  $H$  un sottoinsieme non vuoto di  $G$ . Allora  $H \leq G$  se e solo se  $-x + y \in H$ , per ogni  $x, y \in H$ .

**6.3.7.** Siano  $(G, +)$  un gruppo e  $H$  un sottoinsieme non vuoto di  $G$ . Allora  $H \leq G$  se e solo se  $x + (-y) \in H$ , per ogni  $x, y \in H$ .

**6.3.8. Esempi.**  $\mathbb{Z}$  è un sottogruppo di  $(\mathbb{Q}, +)$ ,  $\mathbb{N}_0$  non è un sottogruppo di  $(\mathbb{Z}, +)$ ,  $m\mathbb{Z}$ , per ogni  $m \geq 0$ , è un sottogruppo di  $(\mathbb{Z}, +)$ ,  $\{1, -1\}$  è un sottogruppo di  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $\{\bar{0}, \bar{3}\}$  e  $\{\bar{0}, \bar{2}, \bar{4}\}$  sono sottogruppi di  $(\mathbb{Z}_6, +)$ .

È facile individuare in un gruppo gli eventuali sottogruppi di ordine 2. Si ha infatti:

**6.3.9.** Se  $(G, \cdot)$  è un gruppo e  $x \in G \setminus \{1\}$ , il sottoinsieme  $\{1, x\}$  è un sottogruppo di  $G$  se e solo se  $x = x^{-1}$ .

*Dimostrazione.* Esercizio. □

Esiste un'efficace descrizione dei sottogruppi di  $(\mathbb{Z}, +)$ :

**6.3.10.** *Sia  $H$  un sottoinsieme di  $\mathbb{Z}$ . Allora  $H$  è un sottogruppo di  $\mathbb{Z}$  se e solo se esiste (un unico)  $m \geq 0$  tale che  $H = m\mathbb{Z}$ .*

*Dimostrazione.* Esercizio. □

Utilizzando la 6.3.2 si prova facilmente che l'intersezione di una famiglia non vuota di sottogruppi di un gruppo è ancora un sottogruppo. Ciò permette di definire come sottogruppo **generato** dalla parte  $X$  del gruppo  $(G, \cdot)$  l'intersezione della famiglia dei sottogruppi di  $G$  che contengono  $X$ . Tale sottogruppo viene denotato con  $\langle X \rangle$  e si osserva facilmente che:

**6.3.11.** *Siano  $(G, \cdot)$  un gruppo e  $X \subseteq G$ . Si ha  $K = \langle X \rangle$  se e solo se valgono le seguenti proprietà:*

- (i)  $K \leq G$ ,
- (ii)  $K \supseteq X$ ,
- (iii)  $H \leq G, H \supseteq X \implies H \supseteq K$ .

*Dimostrazione.* Esercizio. □

Tale proposizione permette di ottenere la descrizione seguente:

**6.3.12.** *Siano  $(G, \cdot)$  un gruppo e  $X$  un sottoinsieme di  $G$ . Si ha:*

- (i) se  $X = \emptyset$ , allora  $\langle X \rangle = \{1\}$ ;
- (ii) se  $X \neq \emptyset$ , allora  $\langle X \rangle = \{x_1 \dots x_t : t \in \mathbb{N}, x_1, \dots, x_t \in X \cup X^{-1}\}$ , dove  $X^{-1} = \{x^{-1} : x \in X\}$ .

*Dimostrazione.* Esercizio. □

In particolare si ha:

**6.3.13.** *Siano  $(G, \cdot)$  un gruppo e  $x \in G$ . Si ha:*

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\} = \langle x^{-1} \rangle.$$

**6.3.14. Esempi.** In  $(\mathbb{Z}, +)$  si ha  $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$ , più in generale  $\langle t \rangle = \langle -t \rangle = t\mathbb{Z}$ , per ogni  $t \geq 0$ .

In  $(\mathbb{Z}_m, +)$  si ha  $\langle \bar{1} \rangle = \mathbb{Z}_m = \langle \overline{m-1} \rangle$ . In  $(\mathbb{Z}_{12}, +)$ ,  $\langle \bar{4}, \bar{6} \rangle = 2\mathbb{Z}_{12}$ .

Un gruppo  $G$  è detto **ciclico** se esiste  $x \in G$  tale che  $G = \langle x \rangle$ .

**6.3.15. Esempi.** I gruppi  $(\mathbb{Z}, +)$  e  $(\mathbb{Z}_m, +)$  per ogni  $m \geq 0$  sono gruppi ciclici. Si proverà (vedi 6.3.26) che essi sono gli unici gruppi ciclici, a meno di isomorfismi.

Il gruppo  $(V_4, \cdot)$  dell'Esercizio 6.3.3 non è ciclico, in quanto:  $\langle 1 \rangle = \{1\}$ ,  $\langle a \rangle = \{1, a\}$ ,  $\langle b \rangle = \{1, b\}$ ,  $\langle c \rangle = \{1, c\}$ .

Si noti che un gruppo ciclico è abeliano a causa della (4.1.3), ma non sussiste il viceversa, come prova il gruppo  $V_4$ .

Siano  $(G, \cdot)$  e  $(K, \cdot)$  gruppi. Si ricorda che un'applicazione  $f : G \rightarrow K$  è detta un omomorfismo se per ogni  $x, y \in G$  risulta  $f(xy) = f(x)f(y)$ . Per gli omomorfismi tra gruppi sussistono le seguenti interessanti proprietà:

**6.3.16.** Sia  $f : G \rightarrow K$  un omomorfismo tra i gruppi  $(G, \cdot)$  e  $(K, \cdot)$ . Allora:

- (i)  $f(1_G) = 1_K$ ;
- (ii)  $f(x^{-1}) = f(x)^{-1}$ , per ogni  $x \in G$ ;
- (iii)  $f(x^n) = f(x)^n$ , per ogni  $x \in G$  e ogni  $n \in \mathbb{Z}$ ;
- (iv) da  $H \leq G$  segue  $f(H) \leq K$ ;
- (v) da  $L \leq K$  segue  $f^{-1}(L) \leq G$ ;
- (vi)  $f(\langle X \rangle) = \langle f(X) \rangle$ , per ogni  $X \subseteq G$ .

*Dimostrazione.* (i) Si ha  $f(1_G)1_K = f(1_G) = f(1_G1_G) = f(1_G)f(1_G)$ , da cui, per la cancellabilità,  $f(1_G) = 1_K$ .

(ii) Si ha  $f(x)f(x)^{-1} = 1_K = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})$ , da cui, sempre per la cancellabilità,  $f(x)^{-1} = f(x^{-1})$ .

(iii), (v), (vi) Esercizio.

(iv) Supposto  $H \leq G$ , si ha  $1_K = f(1_G) \in f(H)$ , e quindi  $f(H) \neq \emptyset$ . Per ogni  $a, b \in f(H)$  si ha poi  $a = f(x), b = f(y)$ , con  $x, y \in H$ , e quindi anche  $a^{-1}b = f(x)^{-1}f(y) = f(x^{-1}y) \in f(H)$ , poiché  $x^{-1}y \in H$ .  $\square$

**6.3.17.** Sia  $f : G \rightarrow K$  un omomorfismo tra i gruppi  $(G, \cdot)$  e  $(K, \cdot)$ . L'insieme

$$\text{Ker } f := \{x \in G : f(x) = 1_K\}$$

è un sottogruppo di  $G$ , detto **nucleo** di  $f$  (e talvolta denotato anche con  $N_f$ ). Inoltre  $f$  è un monomorfismo se e solo se  $\text{Ker } f = \{1_G\}$ .

*Dimostrazione.* Per la (i) di 6.3.16 si ha  $1_G \in \text{Ker } f$  e dunque  $\text{Ker } f \neq \emptyset$ . Per ogni  $x, y \in \text{Ker } f$ , dalla (ii) di 6.3.16 segue poi  $f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) = 1^{-1} \cdot 1 = 1$ , sicché  $x^{-1}y \in \text{Ker } f$ . Pertanto  $\text{Ker } f \leq G$ .

Supposto  $f$  monomorfismo e  $x \in \text{Ker } f$ , si ha  $f(x) = 1_K = f(1_G)$  e dunque  $x = 1_G$ . Viceversa, supposto  $\text{Ker } f = \{1_G\}$  e  $f(x) = f(y)$ , si ha  $1_K = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ , sicché  $xy^{-1} \in \text{Ker } f$  e quindi  $xy^{-1} = 1_G$ , da cui  $x = y$ .  $\square$

Sussiste un'efficace descrizione delle congruenze di un gruppo, e più in generale delle relazioni d'equivalenza compatibili da un lato, come ora si illustrerà.

Sia  $H$  un sottogruppo del gruppo  $(G, \cdot)$ . Le posizioni:

$$x \mathcal{R}'_H y : \iff x^{-1}y \in H,$$

$$x \mathcal{R}''_H y : \iff xy^{-1} \in H,$$

con  $x, y \in G$ , definiscono relazioni d'equivalenza in  $G$ . Infatti, per esempio, da  $1_G \in H$  segue  $x^{-1}x = 1_G \in H$  e quindi  $x \mathcal{R}'_H x$ , per ogni  $x \in G$ , sicché  $\mathcal{R}'_H$  è riflessiva. Da  $x \mathcal{R}'_H y$  segue  $x^{-1}y \in H$  e quindi, per 4.1.11, anche  $y^{-1}x = (x^{-1}y)^{-1} \in H$ , sicché  $y \mathcal{R}'_H x$  e dunque  $\mathcal{R}'_H$  è simmetrica. Infine, supposto  $x \mathcal{R}'_H y$  e  $y \mathcal{R}'_H z$ , cioè  $x^{-1}y, y^{-1}z \in H$ , si ha, per la stabilità di  $H$ ,  $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ , il che assicura la transitività di  $\mathcal{R}'_H$ .

È facile provare (vedi Esercizio 6.3.7) che, con  $x \in G$ , si ha:

$$[x]_{\mathcal{R}'_H} = \{xh : h \in H\},$$

e

$$[x]_{\mathcal{R}''_H} = \{hx : h \in H\}.$$

Tali insiemi vengono denotati rispettivamente coi simboli  $xH$  e  $Hx$  e detti il *laterale sinistro (destro)* di  $H$  in  $G$  individuato da  $x$ . Pertanto:

$$xH = yH \iff x^{-1}y \in H,$$

$$Hx = Hy \iff xy^{-1} \in H.$$

Si noti che  $[1]_{\mathcal{R}'_H} = \{h : h \in H\} = H = [1]_{\mathcal{R}''_H}$ , pertanto  $H$  è un laterale sinistro (destro), e si ha:

$$xH = H \iff x \in H,$$

$$Hx = H \iff x \in H.$$

Sono ovviamente biettive le applicazioni

$$f : h \in H \longmapsto xh \in xH,$$

$$g : h \in H \longmapsto hx \in Hx,$$

e gli insiemi quoziante

$$G/\mathcal{R}'_H = \{xH : x \in G\},$$

$$G/\mathcal{R}''_H = \{Hx : x \in G\}$$

sono partizioni di  $G$ . In più risulta:

**6.3.18.** *Con  $(G, \cdot)$  gruppo e  $H \leq G$  si ha che la posizione*

$$\varphi(xH) := Hx^{-1},$$

*per ogni  $x \in G$ , definisce un'applicazione biettiva di  $G/\mathcal{R}'_H$  in  $G/\mathcal{R}''_H$ .*

*Dimostrazione.* Con  $x, y \in G$  si ha  $xH = yH$  se e solo se  $x^{-1}y \in H$ . Da  $x^{-1}y = x^{-1}(y^{-1})^{-1}$  segue quindi che ciò equivale a  $Hx^{-1} = Hy^{-1}$ . Pertanto  $\varphi$  è un'applicazione ed è iniettiva. Si ha poi  $Hy = H(y^{-1})^{-1} = \varphi(y^{-1}H)$  per ogni  $y \in G$ , sicché  $\varphi$  è anche suriettiva.  $\square$

Se  $G$  è finito e  $H \leq G$ , si ha quindi  $|G/\mathcal{R}'_H| = |G/\mathcal{R}''_H|$  e tale numero viene detto l'*indice* di  $H$  in  $G$  e denotato col simbolo  $|G : H|$ .

Per i gruppi finiti sussiste il seguente semplice ma importante risultato:

**6.3.19. Teorema di Lagrange.** *Siano  $G$  un gruppo finito e  $H$  un suo sottogruppo. Allora*

$$|G| = |H| \cdot |G : H|.$$

*Pertanto sia l'ordine di  $H$  che l'indice di  $H$  in  $G$  sono divisori dell'ordine di  $G$ .*

*Dimostrazione.* Sia  $|G : H| = t = |G/\mathcal{R}'_H|$ . Si ha  $G/\mathcal{R}'_H = \{x_1H, \dots, x_tH\}$ , e dall'essere  $G/\mathcal{R}'_H$  una partizione di  $G$  segue che  $G = x_1H \dot{\cup} \dots \dot{\cup} x_tH$ . Da ciò, osservato che  $|x_iH| = |H|$  per ogni  $i = 1, \dots, t$  a causa di 2.2.9, si ottiene

$$|G| = |x_1H| + \dots + |x_tH| = \underbrace{|H| + \dots + |H|}_t = t|H| = |G : H| \cdot |H|,$$

come volevasi.  $\square$

Come semplice conseguenza del teorema di Lagrange si ottiene che un gruppo di ordine primo ha come sottogruppi solo quelli banali. Pertanto un gruppo  $G$  di ordine primo è sempre ciclico essendo  $\langle x \rangle = G$  per ogni  $x \in G \setminus \{1\}$ .

È immediato verificare che la relazione  $\mathcal{R}'_H$  è compatibile a sinistra col prodotto di  $G$ , in quanto da  $x\mathcal{R}'_H y$  e  $a \in G$  segue  $ax\mathcal{R}'_H ay$ , essendo  $(ax)^{-1}ay = x^{-1}a^{-1}ay = x^{-1}y$ . Analogamente si prova che  $\mathcal{R}''_H$  è compatibile a destra col prodotto di  $G$ . In più si ha:

**6.3.20.** *Siano  $G$  un gruppo e  $\mathcal{R}$  una relazione d'equivalenza in  $G$ . La relazione  $\mathcal{R}$  è compatibile a sinistra (a destra) col prodotto di  $G$  se e solo se esiste  $H \leq G$  tale che  $\mathcal{R} = \mathcal{R}'_H$  (rispettivamente  $\mathcal{R} = \mathcal{R}''_H$ ).*

*Dimostrazione.* Se  $\mathcal{R}$  è compatibile a sinistra (destra) si verifica facilmente che l'insieme  $H = [1]_{\mathcal{R}}$  è un sottogruppo di  $G$ : ovviamente  $1 \in H$ , da  $x, y \in H$  segue  $x\mathcal{R} 1, y\mathcal{R} 1$ , quindi  $xy\mathcal{R} x1$ , cioè  $xy\mathcal{R} x$  (rispettivamente  $xy\mathcal{R} y$ ) per la compatibilità e  $xy\mathcal{R} 1$  per la proprietà transitiva, cioè  $xy \in H$ , infine da  $x \in H$  segue  $x\mathcal{R} 1$  da cui  $x^{-1}x\mathcal{R} x^{-1}$  (risp.  $xx^{-1}\mathcal{R} x^{-1}$ ), quindi  $1\mathcal{R} x^{-1}$ , cioè  $x^{-1} \in H$ .

Con  $x, y \in G$  si ha poi  $x\mathcal{R}'_H y$  (risp.  $x\mathcal{R}''_H y$ ) se e solo se  $x^{-1}y \in H = [1]_{\mathcal{R}}$  (risp.  $xy^{-1} \in H = [1]_{\mathcal{R}}$ ), cioè  $x^{-1}y\mathcal{R} 1$  (risp.  $xy^{-1}\mathcal{R} 1$ ), il che equivale per la compatibilità a  $y\mathcal{R} x$  (risp.  $x\mathcal{R} y$ ), cioè  $x\mathcal{R} y$ .  $\square$

Un sottogruppo  $H$  di  $G$  è detto **normale** in  $G$ , e si scrive  $H \trianglelefteq G$  se  $\mathcal{R}'_H = \mathcal{R}''_H$ . In tal caso la relazione  $\mathcal{R}_H := \mathcal{R}'_H = \mathcal{R}''_H$  è una congruenza. In più da 6.3.20 segue che:

**6.3.21.** *Siano  $G$  un gruppo e  $\mathcal{R}$  una relazione d'equivalenza in  $G$ . Allora  $\mathcal{R}$  è una congruenza se e solo se esiste  $H \trianglelefteq G$  tale che  $\mathcal{R} = \mathcal{R}_H$ .*

**6.3.22. Esempi.** I sottogruppi banali sono normali in quanto  $\mathcal{R}'_{\{1\}} = \text{id}_G = \mathcal{R}''_{\{1\}}$  e  $\mathcal{R}'_G = \mathcal{R}_t = \mathcal{R}''_G$ .

Se  $G$  è un gruppo abeliano, si ha  $H \trianglelefteq G$ , per ogni  $H \leq G$ , in quanto  $x^{-1}y \in H$  equivale a  $yx^{-1} \in H$ . Un gruppo non abeliano può avere sottogruppi non normali come prova l'Esercizio 6.3.24.

Siano  $G$  un gruppo e  $H \trianglelefteq G$ . Si denoti con  $G/H$  l'insieme quoziante  $G/\mathcal{R}_H = \{xH : x \in G\}$ . La compatibilità di  $\mathcal{R}_H$  assicura che la posizione

$$xH \cdot yH := (xy)H,$$

con  $x, y \in G$ , definisce l'operazione quoziante in  $G/H$ . La struttura quoziante  $(G/H, \cdot)$ , come osservato nel Capitolo 4 (vedi 4.2.10), è un gruppo, detto il **gruppo quoziante** di  $G$  rispetto ad  $H$ .

**6.3.23. Esempio.** Considerati il gruppo  $(\mathbb{Z}, +)$  e il suo sottogruppo  $H = m\mathbb{Z}$ , con  $m$  intero  $\geq 0$ , si ha ovviamente  $(\mathbb{Z}/m\mathbb{Z}, +) = (Z_m, +)$ .

Un esempio notevole di sottogruppo normale è il nucleo di un omomorfismo, come contenuto nel seguente:

**6.3.24. Teorema di omomorfismo (nei gruppi).** *Siano  $G$  e  $K$  gruppi e sia  $f : G \longrightarrow K$  un omomorfismo. Allora si ha:*

- (i)  $\text{Im } f$  è un sottogruppo di  $K$ ;
- (ii)  $\text{Ker } f \trianglelefteq G$ ;
- (iii) ha senso l'applicazione

$$g : x \text{Ker } f \in G/\text{Ker } f \longmapsto f(x) \in \text{Im } f$$

*ed è un isomorfismo tra i gruppi  $(G/\text{Ker } f, \cdot)$  e  $(\text{Im } f, \cdot)$ .*

*Dimostrazione.* La (i) segue dalla (iv) di 6.3.16.

Si è già osservato che  $\text{Ker } f \leq G$ . Siano ora  $x, y \in G$ , si ha  $x \mathcal{R}'_{\text{Ker } f} y$  se e solo se  $x^{-1}y \in \text{Ker } f$ , cioè se e solo se  $1 = f(x^{-1}y) = f(x)^{-1}f(y)$ . Ciò equivale a  $f(x) = f(y)$  o anche a  $1 = f(x)f(y)^{-1} = f(xy^{-1})$ , il che significa  $x \mathcal{R}''_{\text{Ker } f} y$ . Si è così provato che  $\mathcal{R}'_{\text{Ker } f} = \mathcal{R}_f = \mathcal{R}''_{\text{Ker } f}$ .

La (iii) segue poi dalla (iii) del teorema di omomorfismo (vedi 4.3.7).  $\square$

Ogni sottogruppo normale è il nucleo di un omomorfismo. Precisamente si ha:

**6.3.25.** *Siano  $G$  un gruppo e  $H \trianglelefteq G$ . La proiezione canonica*

$$\pi : x \in G \longmapsto xH \in G/H$$

*è un epimorfismo tale che  $\text{Ker } \pi = H$ .*

*Dimostrazione.* Ovviamente si ha  $\pi(x) = H$  se e solo se  $xH = H$ , cioè se e solo se  $x \in H$ .  $\square$

Si osservi anche che, se  $H = \{1\}$ ,  $\pi$  è pure iniettiva, sicché risulta  $G \simeq G/\{1\}$ .

Un'interessante applicazione del teorema di omomorfismo (vedi 6.3.24) è la proposizione seguente:

**6.3.26.** *Sia  $(G, \cdot)$  un gruppo ciclico,  $G = \langle x \rangle$ . Allora si ha:*

- (i) *se  $G$  è infinito,  $G$  è isomorfo a  $(\mathbb{Z}, +)$ ;*
- (ii) *se  $G$  è finito di ordine  $m$ ,  $G$  è isomorfo a  $(\mathbb{Z}_m, +)$ .*

*Dimostrazione.* L'applicazione  $f : n \in \mathbb{Z} \longmapsto x^n \in G$  è un epimorfismo di  $(\mathbb{Z}, +)$  in  $(G, \cdot)$ , in quanto  $f(\mathbb{Z}) = \{f(n) : n \in \mathbb{Z}\} = \{x^n : n \in \mathbb{Z}\} = G$ , e, per ogni  $n, t \in \mathbb{Z}$  si ha  $f(n+t) = x^{n+t} = x^n x^t = f(n)f(t)$ . Pertanto  $G \simeq \mathbb{Z}/\text{Ker } f$ . Per la 6.3.10 esiste uno e un solo  $s \geq 0$  tale che  $\text{Ker } f = s\mathbb{Z}$ . Quindi, se  $G$  è infinito, tale risulta  $\mathbb{Z}/s\mathbb{Z}$ , sicché  $s = 0$  e  $G \simeq \mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ . Se invece  $G$  ha ordine  $m$ , riesce  $s = m$  e  $G \simeq \mathbb{Z}_m$ .  $\square$

Da 6.3.26 e dalla (iii) del teorema di omomorfismo (vedi 6.3.24) si ottiene che se  $G = \langle x \rangle$  è infinito allora l'applicazione  $f : n \in \mathbb{Z} \longmapsto x^n \in G$  è un isomorfismo, e che se  $G = \langle x \rangle$  ha ordine  $m$  allora l'applicazione  $g : [n]_m \in \mathbb{Z}_m \longmapsto x^n \in G$  è un isomorfismo. Se ne deducono facilmente le seguenti interessanti proprietà:

**6.3.27.** *Sia  $(G, \cdot)$  un gruppo ciclico infinito,  $G = \langle x \rangle$ . Allora:*

- (i)  $x^n = x^m$  se e solo se  $n = m$ ;
- (ii)  $x^n = 1$  se e solo se  $n = 0$ ;
- (iii)  $G = \langle x^n \rangle$  se e solo se  $n = 1$  o  $n = -1$ ;
- (iv)  $H \leq G$  se e solo se esiste  $m \geq 0$  tale che  $H = \langle x^m \rangle$ .

*Dimostrazione.* Esercizio.  $\square$

**6.3.28.** *Sia  $(G, \cdot)$  un gruppo ciclico finito di ordine  $m$ ,  $G = \langle x \rangle$ . Allora:*

- (i)  $x^n = x^t$  se e solo se  $n \equiv t \pmod{m}$ ;
- (ii)  $x^n = 1$  se e solo se  $m$  divide  $n$ ;
- (iii)  $G = \{1, x, \dots, x^{m-1}\}$  ed  $m$  è il minimo intero positivo  $i$  tale che  $x^i = 1$ .

*Dimostrazione.* Esercizio. □

Come immediata applicazione delle proprietà dei gruppi ciclici finiti si ha il seguente interessante risultato.

**6.3.29.** *Sia  $G$  un gruppo finito. Allora  $x^{|G|} = 1$ , per ogni  $x \in G$ .*

*Dimostrazione.* Sia  $x \in G$ . Per il teorema di Lagrange (vedi 6.3.19) si ha che  $\langle x \rangle$  è finito e  $|\langle x \rangle|$  è un divisore di  $|G|$ . Pertanto il risultato segue da (ii) di 6.3.28. □

Come corollario si ritrova il teorema di Fermat-Eulero (vedi 5.6.3). Infatti da  $a$  coprimo con  $m$  segue (vedi 5.5.12) che  $[a]_m \in U(\mathbb{Z}_m) = \mathbb{Z}_m^*$ , con  $|\mathbb{Z}_m^*| = \varphi(m)$ . Pertanto  $[1]_m = [a]^{\varphi(m)} = [a^{\varphi(m)}]_m$  e quindi  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

## Esercizi

**Esercizio 6.3.1.** *Sia  $G$  un gruppo, con  $|G| = 2$ ,  $G = \{1, a\}$ . Si verifichi che la tavola di moltiplicazione di  $G$  è la seguente:*

	1	$a$
1	1	$a$
$a$	$a$	1

e che  $G$  è isomorfo a  $(\mathbb{Z}_2, +)$ .

**Esercizio 6.3.2.** *Sia  $G$  un gruppo, con  $|G| = 3$ ,  $G = \{1, a, b\}$ . Si verifichi che la tavola di moltiplicazione di  $G$  è la seguente:*

	1	$a$	$b$
1	1	$a$	$b$
$a$	$a$	$b$	1
$b$	$b$	1	$a$

e che  $G$  è isomorfo a  $(\mathbb{Z}_3, +)$ .

**Esercizio 6.3.3.** *Sia  $V_4 = \{1, a, b, c\}$  strutturato con l'operazione  $\cdot$  data dalla seguente tavola:*

	1	$a$	$b$	$c$
1	1	$a$	$b$	$c$
$a$	$a$	1	$c$	$b$
$b$	$b$	$c$	1	$a$
$c$	$c$	$b$	$a$	1

Si verifichi che  $(V_4, \cdot)$  è un gruppo abeliano provando che l'applicazione  $\varphi$  definita ponendo  $\varphi(1) = (\bar{0}, \bar{0})$ ,  $\varphi(a) = (\bar{1}, \bar{0})$ ,  $\varphi(b) = (\bar{0}, \bar{1})$ ,  $\varphi(c) = (\bar{1}, \bar{1})$ , è un isomorfismo di  $(V_4, \cdot)$  nella struttura prodotto  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ . Tale gruppo è detto **gruppo quadrinomio o gruppo di Klein**.

**Esercizio 6.3.4.** Si verifichi che il gruppo  $(V_4, \cdot)$  dell'Esercizio 6.3.3 non è isomorfo al gruppo  $(\mathbb{Z}_4, +)$ . Si dimostri poi che un gruppo  $(G, \cdot)$  di ordine 4 è isomorfo a  $(\mathbb{Z}_4, +)$  o a  $(V_4, \cdot)$ .

**Esercizio 6.3.5.** Siano  $X$  e  $Y$  insiemi e sia  $\varphi : X \longrightarrow Y$  un'applicazione biettiva. Si provi che i gruppi simmetrici  $(S_X, \cdot)$  e  $(S_Y, \cdot)$  sono isomorfi.

*Suggerimento.* Si dimostri che l'applicazione  $\psi$  definita nell'Esercizio 3.4.1 è un isomorfismo di gruppi.

**Esercizio 6.3.6.** Sia  $G$  un gruppo e siano  $H$  e  $K$  sottogruppi di  $G$ . Si provi che  $H \cup K$  è un sottogruppo di  $G$  se e solo se  $H \subseteq K$  o  $K \subseteq H$ . Se ne deduca che un gruppo non è mai unione di due suoi sottogruppi  $H, K \neq G$ .

*Suggerimento.* Supposto  $H \cup K \leq G$ , si sfrutti il fatto che  $H \cup K$  è stabile.

**Esercizio 6.3.7.** Siano  $G$  un gruppo e  $H \leq G$ . Si provi che, per ogni  $x \in G$ ,  $[x]_{R'_H} = xH$  e  $[x]_{R''_H} = Hx$ .

**Esercizio 6.3.8.** Siano  $G$  un gruppo e  $H \leq G$ . Si provi che sono equivalenti:

- (i)  $H \trianglelefteq G$ ;
- (ii)  $x^{-1}Hx := \{x^{-1}hx : h \in H\} = H$ , per ogni  $x \in G$ ;
- (iii)  $x^{-1}Hx \subseteq H$ , per ogni  $x \in G$ ;
- (iv)  $x^{-1}hx \in H$ , per ogni  $x \in G$  e  $h \in H$ .

**Esercizio 6.3.9.** Sia  $(S_3, \cdot)$  il gruppo delle permutazioni su  $X = \{1, 2, 3\}$ . Si verifichi che gli elementi di  $S_3$  sono:

$$\text{id}_X = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

dove le applicazioni sono state rappresentate scrivendo nel primo rigo gli elementi di  $X$  e, in corrispondenza, nel secondo rigo, le loro immagini.

**Esercizio 6.3.10.** Con le notazioni dell'Esercizio 6.3.9, si provi che la tavola di moltiplicazione di  $(S_3, \cdot)$  è la seguente:

$\cdot$	1	a	b	c	d	f
1	1	a	b	c	d	f
a	a	1	f	d	c	b
b	b	d	1	f	a	c
c	c	f	d	1	b	a
d	d	b	c	a	f	1
f	f	c	a	b	1	d

**Esercizio 6.3.11.** Si verifichi che, con le notazioni dell'Esercizio 6.3.9, i sottogruppi del gruppo  $(\mathbb{S}_3, \cdot)$  sono:  $\{1\}$ ,  $\{1, a\}$ ,  $\{1, b\}$ ,  $\{1, c\}$ ,  $\{1, d, f\}$ .

**Esercizio 6.3.12.** Si dimostri 6.3.9.

**Esercizio 6.3.13.** Siano  $G$  un gruppo e  $X \subseteq G$ . Si provi che:  $(X^{-1})^{-1} = X$  e che  $\langle X \rangle = \langle X^{-1} \rangle$ .

**Esercizio 6.3.14.** Si dimostri 6.3.10.

**Esercizio 6.3.15.** Sia  $m \geq 1$  un intero e sia  $a \in \mathbb{Z}$ . Si provi che si ha  $\mathbb{Z}_m = \langle \bar{a} \rangle$  se e solo se  $(a, m) = 1$ .

**Esercizio 6.3.16.** Si consideri il gruppo  $(\mathbb{Z}, +)$  e siano  $s, t \in \mathbb{Z} \setminus \{0\}$ . Si provi che:

- (i)  $s\mathbb{Z} \subseteq t\mathbb{Z} \iff t|s$ ;
- (ii)  $s\mathbb{Z} = t\mathbb{Z} \iff s = \pm t$ ;
- (iii)  $s\mathbb{Z} \cap t\mathbb{Z} = m\mathbb{Z}$ , con  $m = \text{mcm}(s, t)$ ;
- (iv)  $\langle s, t \rangle = d\mathbb{Z}$ , con  $d = \text{MCD}(s, t)$ .

**Esercizio 6.3.17.** Si provi 6.3.11.

**Esercizio 6.3.18.** Si provi 6.3.12.

**Esercizio 6.3.19.** Si provi che sottogruppi e quoienti di un gruppo ciclico sono ciclici.

**Esercizio 6.3.20.** Sia  $(G, \cdot)$  un gruppo ciclico finito, di ordine  $m$ ,  $G = \langle x \rangle$ . Si provi che  $G = \langle x^t \rangle$  se e solo se  $(t, m) = 1$ .

*Suggerimento.* Si utilizzino 6.3.26 e l'Esercizio 6.3.15.

**Esercizio 6.3.21.** Si dimostrino (iii), (v) e (vi) di 6.3.16.

**Esercizio 6.3.22.** Si dimostri 6.3.27.

**Esercizio 6.3.23.** Si dimostri 6.3.28.

**Esercizio 6.3.24.** Si provi che i sottogruppi di ordine 2 di  $\mathbb{S}_3$  non sono normali in  $\mathbb{S}_3$ , mentre lo è quello di ordine 3.

**Esercizio 6.3.25.** Si provi che un sottogruppo d'indice 2 in un gruppo  $G$  è sempre normale in  $G$ .

**Esercizio 6.3.26.** Siano  $G$  un gruppo e  $H \trianglelefteq G$ . Si provi che  $K'$  è un sottogruppo di  $G/H$  se e solo se esiste  $K \leq G$  con  $K \supseteq H$  tale che  $K' = K/H$ .

*Suggerimento.* Supposto  $K' \leq G/H$ , si ponga  $K = \{x \in G : xH \in K'\}$ .

**Esercizio 6.3.27.** Si considerino il gruppo  $(\mathbb{Q}, +)$  dei numeri razionali, il suo sottogruppo  $\mathbb{Z}$  dei numeri interi e il gruppo quoziante  $(\mathbb{Q}/\mathbb{Z}, +)$ . Si ponga

$$f : x \in \mathbb{Q} \longmapsto 3x + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}.$$

Si provi che:

- (i)  $f$  è un epimorfismo di gruppi;
- (ii) il nucleo  $\text{Ker } f$  di  $f$  è un sottogruppo di  $\mathbb{Q}$  contenente  $\mathbb{Z}$ ;
- (iii) il gruppo quoziante  $\text{Ker } f/\mathbb{Z}$  ha ordine 3.

**Esercizio 6.3.28.** Nell'insieme  $G = \mathbb{Z} \times \{1, -1\}$  si definisca un'operazione  $\star$  ponendo, per ogni  $(a, x), (b, y) \in \mathbb{Z} \times \{1, -1\}$ ,

$$(a, x) \star (b, y) := (a + xb, xy).$$

- (i) Si dimostri che  $(G, \star)$  è un gruppo.
- (ii) Si dimostri che la proiezione canonica  $\pi : (a, x) \in G \longmapsto x \in \{1, -1\}$  è un omomorfismo del gruppo  $(G, \star)$  nel gruppo  $(\{1, -1\}, \cdot)$ .
- (iii) Si dimostri che  $H = \{(a, 1) : a \in \mathbb{Z}\}$  è un sottogruppo normale di  $G$ .
- (iv) Si calcoli l'indice  $|G : H|$ .

**Esercizio 6.3.29.** Si considerino i gruppi  $(\mathbb{Z}_2, +)$ ,  $(\mathbb{Z}_6, +)$  e il gruppo prodotto  $G = (\mathbb{Z}_2 \times \mathbb{Z}_6, +)$ .

- (i) Si scrivano gli elementi di  $G$ .
- (ii) Si provi che il sottoinsieme  $T = \{(a, 2b) : a \in \mathbb{Z}_2, b \in \mathbb{Z}_6\}$  è un sottogruppo di  $G$  e si determini la struttura del gruppo  $(T, +)$ .
- (iii) Posto  $H = \langle(\bar{0}, \bar{4})\rangle$ , si scrivano gli elementi di  $H$ .
- (iv) Si studi il gruppo quoziante  $(G/H, +)$  determinandone la struttura e gli elementi.

## 6.4 Gruppi di permutazioni

Si è già osservato che un esempio notevole di gruppo è il gruppo simmetrico  $(\mathbb{S}_X, \cdot)$ , dove  $X$  è un insieme,  $\mathbb{S}_X$  l'insieme delle permutazioni di  $X$ , e  $f \cdot g = g \circ f$ , per ogni  $f, g \in \mathbb{S}_X$ .

Tale gruppo è di solito non abeliano (vedi 6.3.1); se  $X$  è finito e di ordine  $n \geq 1$ , è lecito assumere  $X = \{1, \dots, n\}$  e denotare  $\mathbb{S}_X$  col simbolo  $\mathbb{S}_n$  (vedi Paragrafo 3.4) e si ha  $|\mathbb{S}_n| = n!$  (vedi 3.4.2).

Come indicato nel paragrafo precedente, un elemento  $f \in \mathbb{S}_n$  può essere scritto nel seguente modo:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}. \quad (6.4.1)$$

Si dice **supporto** di  $f$ , e si indica con  $\text{supp}(f)$ , il sottoinsieme di  $X$  costituito dagli elementi  $x \in X$  non fissati da  $f$ , tali cioè che  $f(x) \neq x$ . Per esempio,

$$\text{supp}(\text{id}_X) = \emptyset, \text{supp}(h) = \{1, 3, 4\} \text{ con } h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \in \mathbb{S}_5.$$

Talvolta, se l'insieme  $X$  è ben precisato, l'identità di  $X$  viene denotata con  $1_X$  o solo con 1, e, se  $f \in \mathbb{S}_n$  è diversa dall'identità, nella scrittura di  $f$  introdotta in (6.4.1) si omettono gli elementi non appartenenti al supporto. Per esempio, con le notazioni precedenti, si scrive  $h = \begin{pmatrix} 1 & 3 & 4 \\ 4 & 1 & 3 \end{pmatrix}$ .

Sono di notevole interesse, tra le permutazioni, i cosiddetti cicli di lunghezza  $k$ , con  $2 \leq k \leq n$ . Una permutazione  $f \in \mathbb{S}_n$  è detta un *ciclo* di *lunghezza*  $k$ , o un  $k$ -ciclo, se esistono elementi  $i_1, \dots, i_k \in X$ , a due a due distinti, tali che  $\text{supp}(f) = \{i_1, \dots, i_k\}$  e  $f(i_1) = i_2, \dots, f(i_{k-1}) = i_k, f(i_k) = i_1$ . Si scrive allora anche:

$$f = (i_1 i_2 \dots i_k).$$

Un ciclo di lunghezza 2 è anche detto una *trasposizione*.

**6.4.1. Esempi.** La permutazione  $h \in \mathbb{S}_5$  prima definita è un 3-ciclo e si può scrivere  $h = (143)$ . La permutazione  $v = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$  non è un ciclo.

Il termine *ciclo* è giustificato dalla seguente osservazione. Se  $f = (i_1 \dots i_k)$  e si scrivono in senso orario i numeri  $i_1, \dots, i_k$  su una circonferenza e la si percorre in questo verso, allora l'immagine di ogni  $i_j$  è il numero che compare subito dopo. Dopo  $k$  passi si ritorna al punto di partenza. Ciò giustifica anche l'espressione “ $f$  permuta ciclicamente  $i_1, \dots, i_k$ ” a volte usata per descrivere  $f$ . Risulta quindi chiaro che  $f = (i_1 i_2 \dots i_k)$  può anche essere scritta come  $(i_2 i_3 \dots i_k i_1)$  o come  $(i_3 i_4 \dots i_k i_1 i_2)$  e così via. Pertanto, come ciclo,  $f$  ammette  $k$  scritture distinte.

**6.4.2. Esempio.** La permutazione  $h = (143) \in \mathbb{S}_5$  può essere scritta come  $h = (431)$  o come  $h = (314)$ .

Si osservi che:

**6.4.3.** Sia  $f$  un  $k$ -ciclo di  $\mathbb{S}_n$ ,  $f = (i_1 \dots i_k)$ . Allora si ha:

$$f(i_1) = i_2, f^2(i_1) = i_3, \dots, f^{k-1}(i_1) = i_k, f^k(i_1) = i_1.$$

Quindi  $\text{supp}(f) = \{f^s(i) : s \in \{1, \dots, k\}\}$ , per ogni  $i \in \text{supp}(f)$ .

*Dimostrazione.* Esercizio. □

Permutazioni  $f, g$  di  $\mathbb{S}_n$  sono dette *disgiunte* se  $\text{supp}(f) \cap \text{supp}(g) = \emptyset$ . Si ha:

**6.4.4.** Siano  $f, g \in \mathbb{S}_n$ . Se  $f$  e  $g$  sono disgiunte, allora  $f \cdot g = g \cdot f$ .

*Dimostrazione.* Esercizio. □

**6.4.5. Esempi.** L'unico elemento  $\neq 1$  di  $\mathbb{S}_2$  è un 2-ciclo:  $\mathbb{S}_2 = \{1, (12)\}$ . Gli elementi  $\neq 1$  di  $\mathbb{S}_3$  sono tutti cicli: infatti, con la notazione dell'Esercizio 6.3.9, si ha  $\mathbb{S}_3 = \{1, a = (23), b = (13), c = (12), d = (123), f = (132)\}$ . Come già osservato, non tutti gli elementi  $\neq 1$  di  $\mathbb{S}_4$  sono cicli. Si noti però che la permutazione  $v$  dell'Esempio 6.4.1 coincide col prodotto delle trasposizioni disgiunte  $(14)$  e  $(23)$ .

Più in generale si ha:

**6.4.6.** Sia  $f$  una permutazione di  $\mathbb{S}_n$ ,  $f \neq 1$ . Allora  $f$  è prodotto di cicli a due a due disgiunti e la fattorizzazione è unica a meno dell'ordine dei fattori.

*Dimostrazione.* Sia  $i \in \text{supp}(f)$ . Si ponga allora  $i_1 = i$ ,  $i_2 = f(i_1)$ , e così via. Siccome  $X$  è finito e  $f \neq 1$ , esiste un minimo  $k_1$ , con  $2 \leq k_1 \leq n$ , tale che  $f(i_{k_1}) = i_1$ . Si è quindi individuato il ciclo  $\sigma_1 = (i_1 \dots i_{k_1})$ . Se  $\text{supp}(f) = \{i_1, \dots, i_{k_1}\}$ , si ha  $f = \sigma_1$ . Altrimenti si consideri  $j \in \text{supp}(f) \setminus \{i_1, \dots, i_{k_1}\}$ . Si ponga allora  $j_1 = j$ ,  $j_2 = f(j_1), \dots$ , e sia  $k_2 \geq 2$  il minimo intero  $\leq n$  tale che  $f(j_{k_2}) = j_1$ . Si è così ottenuto il ciclo  $\sigma_2 = (j_1 \dots j_{k_2})$ , disgiunto da  $\sigma_1$ . Se  $\text{supp}(f) = \{i_1, \dots, i_{k_1}\} \cup \{j_1, \dots, j_{k_2}\}$ , allora è  $f = \sigma_1 \sigma_2 = \sigma_2 \sigma_1$ . Altrimenti si continua il procedimento, ottenendo la richiesta decomposizione. L'unicità della fattorizzazione segue facilmente da 6.4.3.  $\square$

**6.4.7. Esempio.** Siano

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix} \in \mathbb{S}_6, \quad g' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 6 & 7 & 5 & 9 & 2 & 3 & 8 & 4 \end{pmatrix} \in \mathbb{S}_9.$$

Si ha:  $g = (125)(36)$ ,  $g' = (26)(37)(459)$ .

Interessante è la seguente:

**6.4.8.** Sia  $n \geq 2$ . Ogni  $k$ -ciclo ( $2 \leq k \leq n$ ) di  $\mathbb{S}_n$  si decomponete nel prodotto di  $k - 1$  trasposizioni. Ne segue che qualsiasi  $f \in \mathbb{S}_n$  è prodotto di trasposizioni.

*Dimostrazione.* Sia  $\sigma = (i_1 i_2 \dots i_k) \in \mathbb{S}_n$ . È immediato verificare che si ha:  $\sigma = (i_1 i_2)(i_1 i_3) \dots (i_1 i_k)$ . Banalmente  $f = (12)(12)$  se  $f = 1$ . Se poi  $f$  è una qualunque permutazione di  $\mathbb{S}_n \setminus \{1\}$ , basta utilizzare quanto provato insieme alla 6.4.6.  $\square$

**6.4.9. Esempi.** Con  $g = (125)(36) \in \mathbb{S}_6$ , si ha  $g = (12)(15)(36)$  e anche  $g = (12)(34)(15)(34)(36) = (12)(12)(12)(36)(15) = \dots$ .

Con  $h = (13786)(254) \in \mathbb{S}_8$ , si ha  $h = (13)(17)(18)(16)(25)(24)$ .

Si noti che ovviamente la decomposizione in trasposizioni di un  $k$ -ciclo, e quindi di una generica permutazione, non è unica e che le trasposizioni che compaiono come fattori sono in generale non disgiunte se  $k > 2$ .

Si può provare che:

**6.4.10.** *Sia  $n \geq 2$  e sia  $f \in \mathbb{S}_n$ , con  $f = \tau_1 \dots \tau_s = \mu_1 \dots \mu_t$ , con  $s, t \geq 1$  e  $\tau_1, \dots, \tau_s, \mu_1, \dots, \mu_t$  trasposizioni. Allora  $s$  e  $t$  sono o entrambi pari o entrambi dispari.*

Ha quindi senso la definizione seguente. Una permutazione  $f \in \mathbb{S}_n$  ( $n \geq 2$ ) è detta *pari* se è prodotto di un numero pari di trasposizioni, *dispari* altrimenti. Si definisce poi *segnatura* di  $f$ , e si denota con  $\text{sign}(f)$ , il numero 1 se  $f$  è pari, il numero  $-1$  altrimenti. In particolare, ovviamente, un  $k$ -ciclo è pari e dunque di segnatura 1 se  $k$  è dispari, è dispari e dunque di segnatura  $-1$ , se  $k$  è pari. Si ha poi:

**6.4.11.** *L'applicazione  $\theta : f \in \mathbb{S}_n \longmapsto \text{sign}(f) \in \{1, -1\}$  è un epimorfismo di  $(\mathbb{S}_n, \cdot)$  in  $(\{1, -1\}, \cdot)$ .*

*Dimostrazione.* Esercizio. □

Il nucleo dell'epimorfismo  $\theta$  è un sottogruppo normale di  $\mathbb{S}_n$ , denotato con  $\mathbb{A}_n$ ; il gruppo  $(\mathbb{A}_n, \cdot)$  è detto il *gruppo alterno* di *n*. Da  $\mathbb{S}_n/\mathbb{A}_n \simeq \{1, -1\}$  segue poi che

$$|\mathbb{A}_n| = \frac{|\mathbb{S}_n|}{2} = \frac{n!}{2}.$$

**6.4.12. Esempio.** Si ha:  $\mathbb{A}_2 = \{1\}$ ,  $\mathbb{A}_3 = \{1, (123), (132)\}$ . Gli elementi di  $\mathbb{A}_4$  sono: 1,  $(12)(34)$ ,  $(13)(24)$ ,  $(14)(23)$ ,  $(123)$ ,  $(132)$ ,  $(124)$ ,  $(142)$ ,  $(134)$ ,  $(143)$ ,  $(234)$ ,  $(243)$ .

## Esercizi

**Esercizio 6.4.1.** *Si dimostri 6.4.3.*

**Esercizio 6.4.2.** *Si dimostri 6.4.4.*

**Esercizio 6.4.3.** *Si dimostri 6.4.11.*

**Esercizio 6.4.4.** *Sia  $\sigma = (i_1 \dots i_k) \in \mathbb{S}_n$ , con  $n \geq 2$ ,  $2 \leq k \leq n$ . Si provi che  $\sigma^{-1} = (i_k i_{k-1} \dots i_2 i_1) = (i_1 i_k i_{k-1} \dots i_2)$ .*

**Esercizio 6.4.5.** *Supposto  $n \geq 2$ , senza fare uso di 6.4.11 si verifichi che l'inversa di una permutazione pari (dispari) è pari (rispettivamente dispari).*

**Esercizio 6.4.6.** *Si provi che  $\mathbb{A}_n \cup \{(12)f : f \in \mathbb{A}_n\} = \mathbb{S}_n$ , per ogni  $n \geq 2$ .*

**Esercizio 6.4.7.** Si considerino le seguenti permutazioni di  $\mathbb{S}_5$ :

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix},$$

$$f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix},$$

$$f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}, \quad f_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

Si precisi se esse appartengono o no ad  $\mathbb{A}_5$ .

**Esercizio 6.4.8.** Di ciascuna delle seguenti permutazioni di  $\mathbb{S}_9$  si scriva la decomposizione in cicli disgiunti e si precisi la parità; si determini poi l'inversa e se ne individui una decomposizione in trasposizioni:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 7 & 6 & 3 & 8 & 5 & 2 & 9 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 7 & 2 & 9 & 1 & 5 & 8 \end{pmatrix}.$$

## 6.5 Anelli, corpi e campi

Sia  $(R, +, \cdot)$  un anello, sia cioè l'insieme  $R$  dotato di due operazioni interne tali che  $(R, +)$  è un gruppo abeliano,  $\cdot$  è associativa e distributiva rispetto alla somma. Si ricordi che  $(R, +, \cdot)$  è detto commutativo se  $\cdot$  è commutativa, unitario se esiste elemento neutro 1 rispetto a  $\cdot$ . L'anello unitario  $(R, +, \cdot)$  è poi un corpo se  $R$  ha più di un elemento e ogni elemento di  $R \setminus \{0\}$  è invertibile; è un campo se è un corpo commutativo.

**6.5.1. Esempi.** Oltre agli esempi già citati nel Capitolo 4, una classe interessante di anelli commutativi unitari è quella degli  $(\mathbb{Z}_m, +, \cdot)$ , con  $m$  intero  $> 0$  (vedi 5.5.3). In particolare si ha che  $\mathbb{Z}_m$  è un campo se e solo se  $m$  è un numero primo (vedi 5.5.13).

Ogni gruppo abeliano  $(G, +)$  può essere strutturato ad anello mediante la posizione  $xy := 0$ , per ogni  $x, y \in G$ . Tale anello è ovviamente commutativo, ed è unitario se e solo se  $|G| = 1$ .

In analogia a quanto fatto nell'Esempio 4.1.19, per ogni  $m > 0$  si costruisce l'anello  $(M_2(\mathbb{Z}_m), +, \cdot)$ . Ciò fornisce un'ulteriore classe di anelli non commutativi; altri esempi sono descritti nel Capitolo 10.

Se  $(R, +, \cdot)$  e  $(S, +, \cdot)$  sono anelli, la struttura prodotto  $(R \times S, +, \cdot)$  è un anello, che risulta commutativo (rispettivamente unitario) se e solo se  $(R, +, \cdot)$  e  $(S, +, \cdot)$  sono entrambi commutativi (risp. unitari).

Se  $(R, +, \cdot)$  è un anello, esiste in  $(R, +)$  elemento neutro 0 e ogni elemento  $a \in R$  è dotato di opposto  $-a$ , sono definiti i multipli  $na$ , con  $n \in \mathbb{Z}$  e  $a \in R$  e sussistono

le usuali proprietà (vedi (4.1.1), (4.1.2) e (4.1.5)). Con  $a, b \in R$  si pone inoltre  $a - b := a + (-b)$ . Valgono le seguenti regole di calcolo:

**6.5.2.** *Sia  $(R, +, \cdot)$  un anello. Allora, per ogni  $a, b, c \in R$ , si ha:*

- (i)  $a0 = 0 = 0a$ ;
- (ii)  $(-a)b = a(-b) = -(ab)$ ;
- (iii)  $(a - b)c = ac - bc$ ;
- (iv)  $a(b - c) = ab - ac$ ;
- (v)  $(na)b = n(ab) = a(nb)$ , per ogni  $n \in \mathbb{Z}$ ;
- (vi)  $(na)(mb) = nm(ab) = (ma)(nb)$ , per ogni  $n, m \in \mathbb{Z}$ .

*Dimostrazione.* (i) Da 0 neutro per la somma e in particolare da  $0 = 0 + 0$  segue, per ogni  $a \in R$ ,  $0 + 0a = 0a = (0 + 0)a = 0a + 0a$ , per la proprietà distributiva del prodotto rispetto alla somma, sicché  $0 = 0a$  per la regolarità di  $0a$  in  $(R, +)$ ; analogamente si prova che  $a0 = 0$ .

(ii) Per ogni  $a, b \in R$ , da  $0 = a + (-a)$  e dalla (i) segue, sempre per la proprietà distributiva,  $0 = 0b = (a + (-a))b = ab + (-a)b$ , da cui  $(-a)b = -(ab)$ ; analogamente  $a(-b) = -(ab)$ .

(iii) Si ha:  $(a - b)c = (a + (-b))c = ac + (-b)c = ac + (-bc) = ac - bc$ .

(iv), (v), (vi) Esercizio.  $\square$

Dalla (i) di 6.5.2 segue che, in un anello  $(R, +, \cdot)$ , si ha  $ab = 0$  se  $a = 0$  o  $b = 0$ . Il viceversa, valido nell'aritmetica elementare (vedi (1.2.11)), non è sempre vero, per esempio in  $(\mathbb{Z}_6, +, \cdot)$  si ha  $[2]_6[3]_6 = [0]_6$ , con  $[2]_6, [3]_6 \neq [0]_6$ .

Si dice che in un anello  $(R, +, \cdot)$  vale la **legge di annullamento del prodotto** se, con  $a, b \in R$ , si ha:

$$ab = 0 \iff a = 0 \text{ o } b = 0.$$

Un anello commutativo in cui valga la legge di annullamento del prodotto è detto un **dominio d'integrità**.

**6.5.3. Esempi.**  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  sono domini d'integrità,  $\mathbb{Z}_6$  non lo è.

Con  $V$  insieme,  $(\mathcal{P}(V), \cup, \cap)$  è un dominio d'integrità se e solo se  $|V| \leq 1$ , in quanto  $X \cap (V \setminus X) = \emptyset$  per ogni  $X \in \mathcal{P}(V)$ .

In un corpo  $(R, +, \cdot)$  vale la legge di annullamento del prodotto, in quanto, supposto  $ab = 0$ , con  $a, b \in R$  e  $a \neq 0$ , si ha l'esistenza di  $a^{-1}$  in  $R$ , e quindi, per la (i) di 6.5.2,  $0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$ . Pertanto un campo è un dominio d'integrità. Si noti che  $(\mathbb{Z}, +, \cdot)$  è un dominio d'integrità unitario ma non è un campo.

Sia  $(R, +, \cdot)$  un anello. Un elemento  $a \in R$  è detto un **divisore sinistro** (rispettivamente **divisore destro**) **dello 0** se  $a \neq 0$  ed esiste  $b \neq 0$  tale che  $ab = 0$  (risp.  $ba = 0$ ). L'elemento  $a$  è detto un **divisore dello 0** se è divisore sinistro o destro dello 0.

Ovviamente ogni elemento di un anello è regolare rispetto alla somma in quanto  $(R, +)$  è un gruppo. Si ha poi:

**6.5.4.** *Sia  $(R, +, \cdot)$  un anello,  $R \neq \{0\}$ . Allora:*

- (i)  *$0$  non è regolare in  $(R, \cdot)$ ,*
- (ii) *un elemento  $a \in R \setminus \{0\}$  è regolare in  $(R, \cdot)$  se e solo se non è un divisore dello  $0$ .*

*Dimostrazione.* La (i) discende da (i) di 6.5.2. Per la (ii) si osservi che, ovviamente, se  $a$  è regolare,  $a$  non è un divisore dello  $0$ , per la (i) di 6.5.2. Viceversa sia  $a$  non un divisore dello  $0$ , con  $a \neq 0$ . Supposto per esempio  $ab = ac$ , si ha  $0 = ab - ac = a(b - c)$ , da cui  $b - c = 0$ , cioè  $b = c$ .  $\square$

È immediato verificare che:

**6.5.5.** *Sia  $(R, +, \cdot)$  un anello. Allora sono equivalenti:*

- (i) *in  $R$  vale la legge di annullamento del prodotto;*
- (ii) *in  $R$  non esistono divisori dello  $0$ ;*
- (iii)  *$R \setminus \{0\}$  è stabile per il prodotto.*

*Dimostrazione.* Esercizio.  $\square$

Dai due risultati precedenti segue quindi che:

**6.5.6.** *Un anello  $(R, +, \cdot)$  è un corpo se, e solo se,  $R \setminus \{0\}$  è stabile per il prodotto e  $(R \setminus \{0\}, \cdot)$  è un gruppo.*

*Dimostrazione.* Se  $(R, +, \cdot)$  è un corpo, ogni elemento  $x \in R \setminus \{0\}$  è simmetrizzabile e quindi regolare in  $(R, \cdot)$ , sicché  $R \setminus \{0\}$  è stabile per  $\cdot$ .  $\square$

È importante sottolineare che sussiste il seguente notevole teorema, di cui si omette la non elementare dimostrazione:

**6.5.7. Teorema di Wedderburn.** *Ogni corpo finito è un campo.*

Esistono invece corpi (infiniti) non commutativi, un primo esempio è il cosiddetto corpo dei **quaternioni reali** che, per brevità, non viene qui descritto.

Sia  $(R, +, \cdot)$  un anello. Una parte  $H \subseteq R$  è detta un **sottoanello** di  $R$  se è stabile per  $+$  e  $\cdot$  e la struttura indotta  $(H, +, \cdot)$  è un anello.

**6.5.8. Esempi.** Qualunque sia l'anello  $R$ ,  $\{0\}$  e  $R$  sono sottoanelli di  $(R, +, \cdot)$ , detti i **sottoanelli banali**.

L'anello  $(\mathbb{Z}, +, \cdot)$  è un sottoanello di  $(\mathbb{Q}, +, \cdot)$ .

Dalla definizione segue subito che:

**6.5.9.** *Sia  $(R, +, \cdot)$  un anello e sia  $H \subseteq R$ . Allora  $H$  è un sottoanello di  $R$  se e solo se  $H$  è un sottogruppo di  $(R, +)$  stabile per il prodotto.*

*Dimostrazione.* Esercizio. □

Da 6.3.5 si ottiene facilmente che:

**6.5.10.** *Sia  $(R, +, \cdot)$  un anello e sia  $H \subseteq R$ . Allora  $H$  è un sottoanello di  $R$  se e solo se valgono le seguenti proprietà:*

- (i)  $x + y \in H$ , per ogni  $x, y \in H$ ;
- (ii)  $0 \in H$ ;
- (iii)  $-x \in H$ , per ogni  $x \in H$ ;
- (iv)  $xy \in H$ , per ogni  $x, y \in H$ .

*Dimostrazione.* Esercizio. □

**6.5.11.** *Sia  $(R, +, \cdot)$  un anello e sia  $H \subseteq R$ ,  $H \neq \emptyset$ . Allora  $H$  è un sottoanello di  $R$  se e solo valgono le seguenti proprietà:*

- (i)  $x - y \in H$ , per ogni  $x, y \in H$ ;
- (ii)  $xy \in H$ , per ogni  $x, y \in H$ .

*Dimostrazione.* Esercizio. □

**6.5.12. Esempi.** Per ogni  $m \geq 0$  si ha che  $m\mathbb{Z}$  è un sottoanello di  $(\mathbb{Z}, +, \cdot)$ . Pertanto per la 6.5.9 e la 6.3.10 questi sono tutti e soli i sottoanelli di  $(\mathbb{Z}, +, \cdot)$ .

Con  $V$  insieme, in  $(\mathcal{P}(V), \cup, \cap)$  la parte  $\{\emptyset, X\}$  è un sottoanello per ogni  $X \subseteq V$ .

Il sottoinsieme

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$$

è un sottoanello di  $M_2(\mathbb{R})$ ; si noti che  $H$  è unitario e ha come unità la matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Da 6.5.9 segue subito che:

**6.5.13.** *Sia  $(R, +, \cdot)$  un anello e sia  $(H_i)_{i \in I}$  una famiglia non vuota di sottoanelli di  $R$ . Allora  $\bigcap_{i \in I} H_i$  è un sottoanello di  $R$ .*

Ciò suggerisce, come al solito, di definire il sottoanello ***generato*** da una parte  $X$  dell'anello  $(R, +, \cdot)$  come l'intersezione della famiglia dei sottoanelli di  $R$  contenenti  $X$ . Tale sottoanello resta caratterizzato come l'unico sottoanello di  $R$  contenente  $X$  e contenuto in ogni sottoanello di  $R$  contenente  $X$ .

Nello studio delle congruenze di un anello risulta essenziale il seguente concetto. Sia  $(R, +, \cdot)$  un anello e sia  $I \subseteq R$ . L'insieme  $I$  è detto un ***ideale sinistro*** (***destro***) di  $R$  se  $I$  è un sottogruppo di  $(R, +)$  e si ha  $ax \in I$  (rispettivamente  $xa \in I$ ), per ogni  $a \in R$  e  $x \in I$ . L'insieme  $I$  è detto un ***ideale bilatero*** se è un ideale sia destro che sinistro.

Ovviamente ogni ideale sinistro (destro) è un sottoanello,  $\{0\}$  e  $R$  sono ideali bilateri di  $(R, +, \cdot)$ , detti gli ***ideali banali***, e, se l'anello è commutativo, ogni ideale sinistro o destro è bilatero. Da 6.3.7 segue subito che:

**6.5.14.** *Sia  $I$  una parte non vuota di un anello  $(R, +, \cdot)$ . Allora  $I$  è un ideale sinistro (destro) di  $R$  se e solo se valgono le seguenti proprietà:*

- (i)  $x - y \in I$ , per ogni  $x, y \in I$ ,
- (ii)  $ax \in I$  (rispettivamente  $xa \in I$ ), per ogni  $a \in R$  e  $x \in I$ .

*Dimostrazione.* Esercizio. □

Si noti che:

**6.5.15.** *Sia  $(R, +, \cdot)$  un anello unitario. Allora:*

- (i) *se  $I$  è un ideale sinistro (destro) di  $R$  tale che  $1 \in I$ , allora  $I = R$ ;*
- (ii) *se  $I$  è un ideale sinistro (destro) di  $R$  cui appartiene un elemento invertibile dell'anello, allora  $I = R$ ;*
- (iii) *se  $R$  è un campo, allora gli unici ideali sono quelli banali.*

*Dimostrazione.* Esercizio. □

**6.5.16. Esempi.** Tutti e soli gli ideali di  $(\mathbb{Z}, +, \cdot)$  sono i sottoinsiemi  $m\mathbb{Z}$ , con  $m \geq 0$ .

Con  $V$  insieme  $\{\emptyset, X\}$  è un ideale di  $(\mathcal{P}(V), \dot{\cup}, \cap)$  se e solo se  $|X| \leq 1$ . Si noti che, se  $|X| > 1$ ,  $\{\emptyset, X\}$  è un sottoanello ma non un ideale di  $\mathcal{P}(V)$ .

L'insieme

$$\left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \in \mathbb{R} \right\}$$

è un ideale sinistro, non destro di  $(M_2(\mathbb{R}), +, \cdot)$ ; l'insieme

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

è un ideale destro, non sinistro di  $(M_2(\mathbb{R}), +, \cdot)$ ; l'insieme

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$$

è un sottoanello, non un ideale né sinistro né destro di  $(M_2(\mathbb{R}), +, \cdot)$ .

Sia  $(R, +, \cdot)$  un anello. Da 6.3.21 segue che tutte e sole le congruenze di  $(R, +)$  sono le relazioni  $\mathcal{R}_H = \mathcal{R}'_H = \mathcal{R}''_H$ , con  $H$  sottogruppo di  $(R, +)$ , dove si ricorda che  $x \mathcal{R}_H y : \iff x - y \in H$  e  $[x]_{\mathcal{R}_H} = \{x + h : h \in H\} = x + H$ , per ogni  $x, y \in R$ . Sussiste il seguente notevole risultato:

**6.5.17.** *Siano  $(R, +, \cdot)$  un anello e  $H$  un sottogruppo di  $(R, +)$ . Allora  $\mathcal{R}_H$  è compatibile a sinistra (a destra) col prodotto se e solo se  $H$  è un ideale sinistro (rispettivamente destro) di  $R$ . Pertanto tutte e sole le congruenze dell'anello  $(R, +, \cdot)$  sono le relazioni  $\mathcal{R}_H$  con  $H$  ideale bilatero di  $R$ .*

*Dimostrazione.* Esercizio. □

Siano ora  $(R, +, \cdot)$  un anello e  $I$  un ideale bilatero di  $R$ . Indicata ancora con  $I$  la relazione  $\mathcal{R}_I$ , dalle 6.5.17 e 4.2.10 si ha che l'insieme quoziante

$$R/I = \{x + I : x \in R\},$$

strutturato con la somma e il prodotto quozianti, è anch'esso un anello, detto l'**anello quoziante** di  $R$  rispetto a  $I$ .

**6.5.18. Esempio.** Con  $m \geq 0$  l'anello quoziante di  $(\mathbb{Z}, +, \cdot)$  rispetto all'ideale  $m\mathbb{Z}$  coincide con l'anello  $(\mathbb{Z}_m, +, \cdot)$ .

Siano ora  $(R, +, \cdot)$  e  $(S, +, \cdot)$  anelli. Si ricorda che un'applicazione  $f : R \rightarrow S$  è detta un omomorfismo (di anelli) se, per ogni  $x, y \in R$ , si ha

$$\begin{cases} f(x+y) = f(x) + f(y), \\ f(xy) = f(x)f(y). \end{cases}$$

**6.5.19. Esempi.** L'applicazione  $f : x \in R \mapsto 0_S \in S$  è un omomorfismo, qualunque siano gli anelli  $R$  e  $S$ , detto l'**omomorfismo nullo**.

L'applicazione  $\pi : x \in R \mapsto x + I \in R/I$ , con  $R$  anello e  $I$  ideale bilatero di  $R$ , è un epimorfismo, detto l'**epimorfismo canonico** di  $(R, +, \cdot)$  in  $(R/I, +, \cdot)$ .

L'applicazione  $i : x \in H \mapsto x \in R$ , con  $R$  anello e  $H$  sottoanello di  $R$ , è un monomorfismo di  $(H, +, \cdot)$  in  $(R, +, \cdot)$ , detto l'**immersione** di  $H$  in  $R$ .

Un omomorfismo  $f : R \rightarrow S$  tra gli anelli  $(R, +, \cdot)$  e  $(S, +, \cdot)$  è anche ovviamente un omomorfismo tra i gruppi  $(R, +)$  e  $(S, +)$  e tra i semigruppi  $(R, \cdot)$  e  $(S, \cdot)$ . Pertanto si ha:  $f(0_R) = 0_S$ , e, per ogni  $x \in R, n \in \mathbb{Z}, t \in \mathbb{N}$ , riesce

$$f(-x) = -f(x), \quad f(nx) = nf(x), \quad f(x^t) = f(x)^t.$$

Ancora l'insieme  $\text{Ker } f = \{x \in R : f(x) = 0_S\}$  è detto **nucleo** dell'omomorfismo  $f$  e si ha:  $\text{Ker } f = \{0\}$  se e solo se  $f$  è un monomorfismo. Vale inoltre il seguente:

**6.5.20. Teorema di omomorfismo (negli anelli).** Sia  $f : R \rightarrow S$  un omomorfismo tra gli anelli  $(R, +, \cdot)$  e  $(S, +, \cdot)$ . Allora:

- (i)  $\text{Im } f$  è un sottoanello di  $S$ ;
- (ii)  $\text{Ker } f$  è un ideale bilatero di  $R$ ;
- (iii) l'anello quoziante  $(R/\text{Ker } f, +, \cdot)$  è isomorfo all'anello  $(\text{Im } f, +, \cdot)$  e l'applicazione

$$g : x + \text{Ker } f \in R/\text{Ker } f \longmapsto f(x) \in \text{Im } f$$

è un isomorfismo di anelli.

*Dimostrazione.* La (i) segue subito da 6.3.24 e da (i) di 4.3.7.

Per la (ii) si osservi che ovviamente  $\text{Ker } f$  è un sottogruppo di  $(R, +)$ . Si ha poi  $f(ax) = f(a)f(x) = f(a)0 = 0 = 0f(a) = f(x)f(a) = f(xa)$ , per ogni  $x \in \text{Ker } f$  e  $a \in R$ .

La (iii) segue subito da 6.3.24 e da (iii) di 4.3.7.  $\square$

Un concetto fondamentale relativo agli anelli unitari è quello di caratteristica. Sia  $(R, +, \cdot)$  un anello unitario, di unità  $1_R$ . La parte  $\{n1_R : n \in \mathbb{Z}\}$  costituita dai multipli di  $1_R$  in  $R$  è un sottoanello di  $R$ , detto il **sottoanello fondamentale** di  $R$ , e denotato con  $E$ . Si ha infatti che  $E$  coincide col sottogruppo generato da  $1_R$  in  $(R, +)$ , e inoltre per la 6.5.2 per ogni  $n, s \in \mathbb{Z}$  risulta  $(n1_R)(s1_R) = (ns)(1_R1_R) = (ns)1_R \in E$ . L'anello  $R$  è detto di **caratteristica 0** se  $E$  è infinito, di caratteristica  $c > 0$  se  $E$  è finito di ordine  $c$ . La caratteristica di  $R$  è dunque un intero  $\geq 0$ , ed è di solito denotata con  $\text{car } R$  o con  $\text{char } R$ .

**6.5.21. Esempi.** Il sottoanello fondamentale di  $(\mathbb{Z}, +, \cdot)$ , di  $(\mathbb{Q}, +, \cdot)$ , di  $(\mathbb{R}, +, \cdot)$ , di  $(\mathbb{C}, +, \cdot)$  è l'insieme  $\mathbb{Z}$ , pertanto  $\text{car } \mathbb{Z} = 0 = \text{car } \mathbb{Q} = \text{car } \mathbb{R} = \text{car } \mathbb{C}$ .

Il sottoanello fondamentale di  $(\mathbb{Z}_m, +, \cdot)$  con  $m \geq 0$  è lo stesso  $\mathbb{Z}_m$ , sicché  $\text{car } \mathbb{Z}_m = m$ .

Esistono pertanto anelli di caratteristica  $c$ , per ogni intero  $c \geq 0$ . Inoltre è ovvio che un anello finito ha caratteristica diversa da 0, e che un sottoanello di un anello unitario, avente la stessa unità dell'anello, ha anche lo stesso sottoanello fondamentale e dunque la stessa caratteristica.

Il significato profondo del concetto di caratteristica è illustrato nella proposizione seguente:

**6.5.22.** Sia  $(R, +, \cdot)$  un anello unitario. Allora:

- (i)  $R$  ha caratteristica 0 se e solo se  $n1_R \neq 0$ , per ogni  $n \in \mathbb{N}$ ; ha caratteristica  $c > 0$  se e solo se  $c$  è il minimo intero positivo  $s$  tale che  $s1_R = 0$ .
- (ii) Se  $R$  ha caratteristica  $c > 0$ , allora  $n1_R = 0$  se e solo se  $c$  divide  $n$ .
- (iii) Se  $R$  ha caratteristica  $c > 0$ , si ha  $ca = 0$ , per ogni  $a \in R$ .

*Dimostrazione.* Sia  $E$  il sottoanello fondamentale di  $R$ ,  $E = \{n1_R : n \in \mathbb{Z}\}$ . Allora  $E$  coincide col sottogruppo generato in  $(R, +)$  da  $1_R$ , sicché (i) e (ii)

seguono immediatamente da 6.3.27 e 6.3.28. Per la (iii) basta osservare che, per ogni  $a \in R$ , da 6.5.2 segue  $ca = c(1_R a) = (c1_R)a = 0a = 0$ .  $\square$

**6.5.23. Esempi.** La caratteristica dell'anello unitario  $(R, +, \cdot)$  è 1 se e solo se  $R = \{0\}$ .

Con  $V$  insieme non vuoto, l'anello  $(\mathcal{P}(V), \dot{\cup}, \cap)$  ha caratteristica 2: infatti  $2X = X \dot{\cup} X = \emptyset$ , per ogni  $X \in \mathcal{P}(V)$ .

L'esempio precedente mostra che esistono anelli infiniti con caratteristica diversa da 0. Si ha poi:

**6.5.24.** *Sia  $(R, +, \cdot)$  un anello unitario non nullo e privo di divisori dello zero. Allora la caratteristica di  $R$  è 0 oppure un numero primo.*

*Dimostrazione.* Sia  $c := \text{car } R$  e si supponga  $c \neq 0$ . Da  $R \neq \{0\}$  segue  $c \neq 1$ . Se per assurdo  $c = c_1 c_2$ , con  $1 < c_1, c_2 < c$ , allora  $0 = c1_R = (c_1 c_2)1_R = (c_1 1_R)(c_2 1_R)$ , da cui, per le ipotesi,  $c_1 1_R = 0$  o  $c_2 1_R = 0$ , contro la (i) di 6.5.22.  $\square$

## Esercizi

**Esercizio 6.5.1.** Si dimostrino (iv), (v), (vi) di 6.5.2.

**Esercizio 6.5.2.** Si dimostri 6.5.5.

**Esercizio 6.5.3.** Si provi che se  $R$  è un anello unitario si ha  $1 = 0$  se e solo se  $R = \{0\}$ .

**Esercizio 6.5.4.** Sia  $(R, +, \cdot)$  un anello finito non nullo. Si provi che  $(R, +, \cdot)$  è un campo se e solo se è privo di divisori dello 0.

**Esercizio 6.5.5.** Si dimostrino 6.5.9, 6.5.10 e 6.5.11.

**Esercizio 6.5.6.** Si dimostrino 6.5.14 e 6.5.15.

**Esercizio 6.5.7.** Si dimostri 6.5.17.

**Esercizio 6.5.8.** Sia  $R = \mathbb{R} \times \mathbb{Z}_8$  l'anello prodotto del campo  $(\mathbb{R}, +, \cdot)$  dei numeri reali e dell'anello  $(\mathbb{Z}_8, +, \cdot)$  degli interi modulo 8.

- (i) Si provi che l'anello  $(R, +, \cdot)$  è commutativo e unitario e si stabilisca se esso è un dominio d'integrità.
- (ii) Si dimostri che le parti  $\{0\} \times \mathbb{Z}_8$  e  $\mathbb{R} \times \{\bar{0}\}$  sono ideali di  $R$ .

**Esercizio 6.5.9.** Si consideri l'anello  $A = \mathbb{Z}_6 \times \mathbb{Z}_3$ .

- (i) Si determinino l'ordine di  $A$ , la sua caratteristica, il sottoanello fondamentale  $E$ , i divisori dello zero in  $A$ , e si dica se  $E$  è un campo.
- (ii) Posto  $a = (\bar{4}, \bar{2}) \in A$  si determinino il sottogruppo generato da  $a$  in  $A(+)$ , l'ideale  $K$  generato da  $a$  in  $A(+, \cdot)$  e si studi l'anello quoziente  $A/K$ .

(iii) Posto infine

$$f : (x, y) \in A \mapsto (5x, 2y) \in A$$

e

$$g : (x, y) \in A \mapsto 4x \in \mathbb{Z}_6$$

si stabilisca se  $f, g$  sono iniettive, suriettive, omomorfismi di anelli.

**Esercizio 6.5.10.** Sia  $(G, +)$  un gruppo abeliano e si indichi con  $\text{End } G$  l'insieme degli endomorfismi di  $G$ . Si provi che, con  $f, g \in \text{End } G$ , le applicazioni  $f + g$  e  $f \cdot g$  definite ponendo, per ogni  $x \in G$ ,

$$(f + g)(x) := f(x) + g(x), \\ (f \cdot g)(x) := (g \circ f)(x) = g(f(x)),$$

sono elementi di  $\text{End } G$  e che la struttura  $(\text{End } G, +, \cdot)$  è un anello unitario, in generale non commutativo.

**Esercizio 6.5.11.** Si provi che il sottoanello  $2\mathbb{Z}_{12}$  di  $(\mathbb{Z}_{12}, +, \cdot)$  è, con le operazioni indotte, un anello non unitario, mentre  $(4\mathbb{Z}_{12}, +, \cdot)$  è unitario, di unità  $[4]_{12}$ . Si noti che ciò mostra che un sottoanello di un anello non unitario può essere unitario.

**Esercizio 6.5.12.** Si determini la caratteristica dei seguenti anelli:  $(M_2(\mathbb{Z}), +, \cdot)$ ,  $(M_2(\mathbb{Z}_m), +, \cdot)$  con  $m > 0$ ,  $(M_2(\mathbb{Q}), +, \cdot)$ ,  $(M_2(\mathbb{R}), +, \cdot)$ ,  $(M_2(\mathbb{C}), +, \cdot)$ .

**Esercizio 6.5.13.** Siano  $(R, +, \cdot)$  e  $(S, +, \cdot)$  anelli unitari. Si provi che:

- (i) l'anello prodotto ha caratteristica 0 se e solo se  $\text{car } R = 0$  o  $\text{car } S = 0$ ,
- (ii) l'anello prodotto ha caratteristica  $c > 0$  se e solo se  $c = \text{lcm}(\text{car } R, \text{car } S)$ , con  $\text{car } R > 0, \text{car } S > 0$ .

**Esercizio 6.5.14.** Sia  $(R, +, \cdot)$  un anello commutativo unitario e siano  $a, b \in R$ ,  $n \in \mathbb{N}_0$ . Si provi che:

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Se ne deduca che, se  $R$  ha caratteristica un primo  $p$ , si ha, per ogni  $a, b \in R$ :

$$(a + b)^p = a^p + b^p.$$

**Esercizio 6.5.15.** Sia  $(R, +, \cdot)$  un anello unitario, di unità  $1_R$ . Si provi che l'applicazione

$$f : n \in \mathbb{Z} \mapsto n1_R \in R$$

è un omomorfismo di anelli, di immagine  $E$ , e che  $f$  è un monomorfismo se e solo se  $\text{car } R = 0$ .

**Esercizio 6.5.16.** Sia  $(R, +, \cdot)$  un anello commutativo unitario e si consideri la struttura  $(M_2(R), +, \cdot)$ , dove la somma di matrici e il prodotto “righe per colonne” sono definiti in analogia a quanto fatto nell’Esempio 4.1.19.

- (i) Si provi che la struttura  $(M_2(R), +, \cdot)$  è un anello unitario, non commutativo se  $R \neq \{0\}$ , e se ne determinino la caratteristica e il sottoanello fondamentale.
- (ii) Per ogni

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R),$$

posto

$$\det X = ad - bc,$$

si provi che la matrice  $X$  è invertibile in  $(M_2(R), +, \cdot)$  se e solo se  $\det X$  è invertibile in  $(R, +, \cdot)$ .

- (iii) Il gruppo  $(U(M_2(R)), \cdot)$  degli elementi invertibili in  $(M_2(R), \cdot)$  viene denotato con il simbolo  $(\mathrm{GL}(2, R), \cdot)$  ed è detto **gruppo generale lineare** di dimensione 2 su  $R$ . Si provi che  $(\mathrm{GL}(2, R), \cdot)$  è un gruppo non abeliano se  $R \neq \{0\}$ .

**Esercizio 6.5.17.** Sia  $(D, +, \cdot)$  un dominio d’integrità. Si costruiscano un campo  $(F, +, \cdot)$  e un monomorfismo di  $(D, +, \cdot)$  in  $(F, +, \cdot)$ , generalizzando il procedimento seguito nel Capitolo 5 per costruire il campo  $\mathbb{Q}$  dei razionali a partire dall’anello  $\mathbb{Z}$  degli interi.

## 6.6 Anelli di polinomi

Sia  $(R, +, \cdot)$  un anello commutativo unitario. Una scrittura del tipo

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

con  $n$  intero non negativo,  $a_0, \dots, a_n \in R$ ,  $a_n \neq 0$ , viene detto un **polinomio** non nullo nell’indeterminata  $x$  a coefficienti in  $R$ . L’intero  $n$  viene detto il **grado** di  $f(x)$  e denotato con  $v(f(x))$  o anche con  $\delta(f(x))$ . Gli elementi  $a_0, \dots, a_n$  sono detti i **coefficienti** di  $f(x)$ , in particolare  $a_n$  è detto il **coefficiente direttivo** o **parametro direttore** di  $f(x)$ . Con  $a_0 + a_1x + \cdots + a_nx^n$ ,  $b_0 + b_1x + \cdots + b_mx^m$  polinomi non nulli a coefficienti in  $R$ , si pone

$$a_0 + a_1x + \cdots + a_nx^n = b_0 + b_1x + \cdots + b_mx^m : \iff \begin{cases} n = m, \\ a_0 = b_0, \\ \vdots \\ a_n = b_n. \end{cases}$$

Si pone poi

$$R[x] := \{0\} \cup \{f(x) = a_0 + a_1x + \cdots + a_nx^n : n \in \mathbb{N}_0, a_0, \dots, a_n \in R, a_n \neq 0\}.$$

I polinomi di grado 0 sono tutti e soli gli elementi non nulli di  $R$ , e, con lo 0, sono detti i **polinomi costanti** di  $R[x]$ .

A volte per denotare il polinomio  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  è conveniente utilizzare la scrittura

$$f(x) = \sum_{i \in \mathbb{N}_0} a_i x^i,$$

dove  $a_j = 0$ , per ogni  $j > n$ . Tale scrittura permette anche di rappresentare lo 0, il cosiddetto **polinomio nullo**, con  $a_i = 0$  per ogni  $i \in \mathbb{N}_0$ .

Siano  $f(x) = \sum_{i \in \mathbb{N}_0} a_i x^i$  e  $g(x) = \sum_{i \in \mathbb{N}_0} b_i x^i$  elementi di  $R[x]$ . Si pone:

$$f(x) + g(x) := \sum_{i \in \mathbb{N}_0} c_i x^i, \quad \text{con } c_i := a_i + b_i,$$

$$f(x) \cdot g(x) := \sum_{i \in \mathbb{N}_0} d_i x^i, \quad \text{dove } d_i := \sum_{s+t=i} a_s b_t.$$

Si noti che tali operazioni hanno senso: ciò è ovvio se uno dei due polinomi è nullo, altrimenti, posto  $m = v(f(x))$  e  $l = v(g(x))$ , si ha che  $c_i = 0$  per ogni  $i > \max\{m, l\}$  e  $d_i = 0$ , per ogni  $i > m + l$ . E infatti:

$$\begin{aligned} f(x) + 0 &= f(x), \\ 0 + g(x) &= g(x), \\ f(x) \cdot 0 &= 0, \\ 0 \cdot g(x) &= 0 \end{aligned}$$

e, supposto  $f(x)$  e  $g(x)$  polinomi non nulli di rispettivi gradi  $m$  e  $l$ , con  $m \leq l$ :

$$\begin{aligned} (a_0 + a_1x + \cdots + a_mx^m) + (b_0 + b_1x + \cdots + b_lx^l) &= \\ (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \cdots + b_lx^l, \end{aligned}$$

e inoltre

$$\begin{aligned} (a_0 + a_1x + \cdots + a_mx^m) \cdot (b_0 + b_1x + \cdots + b_lx^l) &= \\ a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_mb_lx^{m+l}. \end{aligned}$$

La struttura  $(R[x], +, \cdot)$  è un anello commutativo unitario (vedi Esercizio 6.6.1), di unità  $1_R$ . In particolare, un polinomio non nullo  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  ha opposto  $-f(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$ .

In più si ha:  $\text{car } R[x] = \text{car } R$ , poiché  $R$  e  $R[x]$  hanno la stessa unità.

Nella scrittura di un polinomio non nullo  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ , è conveniente trascurare i termini relativi a coefficienti nulli. Con questa convenzione, un qualunque polinomio del tipo  $f(x) = a_nx^n$  è detto un **monomio**. Si ritrova così che, come familiare al Lettore, un polinomio non nullo è somma di monomi.

Un polinomio non nullo è detto **monico** se il suo coefficiente direttivo è 1. Di semplice dimostrazione, ma di notevole interesse è il seguente:

**6.6.1. Teorema di addizione dei gradi.** *Sia  $(R, +, \cdot)$  un dominio d'integrità unitario. Se  $f(x), g(x)$  sono polinomi non nulli di  $R[x]$ , allora  $f(x)g(x) \neq 0$  e*

$$v(f(x)g(x)) = v(f(x)) + v(g(x)).$$

Pertanto  $R[x]$  è un dominio d'integrità.

**Dimostrazione.** Si considerino i polinomi  $f(x) = a_0 + a_1x + \cdots + a_mx^m$  e  $g(x) = b_0 + b_1x + \cdots + b_sx^s$ , con  $v(f(x)) = m$  e  $v(g(x)) = s$ . Allora, da  $a_m \neq 0, b_s \neq 0$ , segue  $a_m b_s \neq 0$ , sicché  $f(x)g(x) \neq 0$  e  $a_m b_s$  è il coefficiente direttivo di  $f(x)g(x)$ . Dunque  $v(f(x)g(x)) = m + s = v(f(x)) + v(g(x))$ .  $\square$

Fondamentale è il seguente:

**6.6.2. Algoritmo della divisione.** *Sia  $(R, +, \cdot)$  un campo e siano  $f(x), g(x) \in R[x]$ , con  $g(x) \neq 0$ . Allora esistono, e sono univocamente individuati, polinomi  $q(x), r(x) \in R[x]$  tali che risulti:*

$$f(x) = g(x)q(x) + r(x),$$

con  $r(x) = 0$  o  $v(r(x)) < v(g(x))$ . Tali polinomi  $q(x)$  e  $r(x)$  sono detti, rispettivamente, il **quoziente** e il **resto** della divisione di  $f(x)$  per  $g(x)$ .

**Dimostrazione.** Si proverà innanzitutto l'esistenza di siffatti polinomi  $q(x)$  e  $r(x)$ . Se  $f(x) = 0$  o  $v(f(x)) < v(g(x))$ , basta porre  $q(x) = 0$  e  $r(x) = f(x)$ . Si supponga dunque  $f(x) = a_0 + a_1x + \cdots + a_mx^m$ ,  $g(x) = b_0 + b_1x + \cdots + b_sx^s$ , con  $v(f(x)) = m \geq s = v(g(x))$ . Si procederà per induzione su  $m$ . Se  $m = 0$ , allora  $s = 0$ ,  $f(x) = a_0$ ,  $g(x) = b_0$  e si ha l'asserto con  $q(x) = b_0^{-1}a_0$  e  $r(x) = 0$ . Sia ora  $m > 0$ . Posto  $q_1(x) = b_s^{-1}a_mx^{m-s}$  si ha

$$g(x)q_1(x) = b_0b_s^{-1}a_mx^{m-s} + b_1b_s^{-1}a_mx^{m-s+1} + \cdots + b_sb_s^{-1}a_mx^m,$$

sicché  $g(x)q_1(x)$  ha grado  $m$  e coefficiente direttivo  $a_m$ . Pertanto il polinomio  $f(x) - g(x)q_1(x)$  o è nullo o è di grado  $< m$ , sicché esistono, per l'ipotesi d'induzione, polinomi  $q^*(x), r^*(x)$  tali che  $f(x) - g(x)q_1(x) = g(x)q^*(x) + r^*(x)$ , cioè  $f(x) = g(x)(q_1(x) + q^*(x)) + r^*(x)$ , con  $r^*(x) = 0$  o  $v(r^*(x)) < v(g(x))$ .

Per provare l'unicità si osservi che, supposto

$$f(x) = g(x)q(x) + r(x) = g(x)\bar{q}(x) + \bar{r}(x),$$

con  $r(x) = 0$  o  $v(r(x)) < v(g(x))$ ,  $\bar{r}(x) = 0$  o  $v(\bar{r}(x)) < v(g(x))$ , si ha

$$g(x)(q(x) - \bar{q}(x)) = \bar{r}(x) - r(x),$$

con  $\bar{r}(x) - r(x) = 0$  o  $v(\bar{r}(x) - r(x)) \leq \max\{v(r(x)), v(\bar{r}(x))\} < v(g(x))$ . Dal teorema di addizione dei gradi segue allora  $\bar{r}(x) - r(x) = 0 = g(x)(q(x) - \bar{q}(x))$ , sicché  $q(x) = \bar{q}(x)$ ,  $r(x) = \bar{r}(x)$ .  $\square$

**6.6.3. Esempi.** La prima parte della dimostrazione del precedente risultato fornisce anche un metodo per individuare quoziente e resto di una divisione, come mostrano gli esempi seguenti. In  $\mathbb{R}[x]$  si considerino i polinomi:

$$f(x) = 3 + 5x - 4x^2 + 7x^3,$$

$$g(x) = x - 2,$$

$$g_1(x) = 6x^2 - x + 3,$$

$$g_2(x) = 5x^3 + 9x + 11,$$

$$g_3(x) = 2x^4 + 7x^2 + 20.$$

Si ha:

$$\begin{array}{r} 7x^3 & -4x^2 & +5x & +3 \\ \hline 7x^3 & -14x^2 & & \\ \hline & 10x^2 & +5x & +3 \\ & 10x^2 & -20x & \\ \hline & 25x & +3 & \\ & 25x & -50 & \\ \hline & & & 53 \end{array} \left| \begin{array}{l} x-2 \\ \hline 7x^2+10x+25 \end{array} \right.$$

quindi  $f(x) = g(x)(7x^2 + 10x + 25) + 53$ ;

$$\begin{array}{r} 7x^3 & -4x^2 & +5x & +3 \\ \hline 7x^3 & -\frac{7}{6}x^2 & +\frac{7}{2}x & \\ \hline -\frac{17}{6}x^2 & +\frac{3}{2}x & +3 \\ -\frac{17}{6}x^2 & +\frac{17}{36}x & -\frac{17}{12} \\ \hline \frac{37}{36}x & +\frac{53}{12} \end{array} \left| \begin{array}{l} 6x^2-x+3 \\ \hline \frac{7}{6}x-\frac{17}{36} \end{array} \right.$$

cioè  $f(x) = g_1(x)(\frac{7}{6}x - \frac{17}{36}) + (\frac{37}{36}x + \frac{53}{12})$ ;

$$\begin{array}{r} 7x^3 & -4x^2 & +5x & +3 \\ \hline 7x^3 & & +\frac{63}{5}x & +\frac{77}{5} \\ \hline -4x^2 & -\frac{38}{5}x & -\frac{62}{5} \end{array} \left| \begin{array}{l} 5x^3+9x+11 \\ \hline \frac{7}{5} \end{array} \right.$$

da cui  $f(x) = g_2(x)(\frac{7}{5}) + (-4x^2 - \frac{38}{5}x - \frac{62}{5})$ ; e infine ovviamente, essendo  $v(f(x)) < v(g_3(x))$ , si ha  $f(x) = g_3(x)0 + f(x)$ .

Si noti che, come mostrato dalla dimostrazione di 6.6.2, continua a valere l'algoritmo della divisione per polinomi  $f(x)$  e  $g(x)$  a coefficienti in un anello commutativo unitario  $R$  purché il coefficiente direttivo di  $g(x)$  sia un elemento invertibile di  $R$ . In particolare, ciò è sempre vero quando  $g(x)$  è monico.

Se il resto della divisione di  $f(x)$  per  $g(x)$  è il polinomio nullo, si dice anche, come al solito, che  $g(x)$  *divide*  $f(x)$  in  $R[x]$  (o che  $f(x)$  è *multiplo* in  $R[x]$  di  $g(x)$ ).

Sia  $(R, +, \cdot)$  un anello commutativo unitario. Dati un qualsiasi polinomio  $f(x) = a_0 + a_1x + \dots + a_mx^m \in R[x]$  e un elemento  $c \in R$ , si pone:

$$f(c) := a_0 + a_1c + \dots + a_mc^m.$$

Se  $f(x)$  è il polinomio nullo, è  $f(c) = 0$ . Si osservi che, se  $f(x), g(x) \in R[x]$  e  $c \in R$ , allora:

$$\begin{aligned} (f+g)(c) &= f(c) + g(c), \\ (fg)(c) &= f(c)g(c). \end{aligned}$$

L'elemento  $c$  è detto *radice* del polinomio  $f(x)$  se si ha  $f(c) = 0$ .

**6.6.4. Esempi.** Il polinomio nullo ha per radici tutti gli elementi di  $R$ .

Un polinomio costante non nullo non ha radici, in quanto, se  $f(x) = a_0$ , si ha  $f(c) = a_0$ , per ogni  $c \in R$  (ciò giustifica anche il termine “costante”).

Un polinomio  $f(x) = a_1x + a_0$  di grado 1 ha sempre una (e una sola) radice  $c = -a_0a_1^{-1}$  se  $a_1$  è invertibile in  $R$ . Pertanto, se  $R$  è un campo, ogni polinomio di primo grado ha una e una sola radice in  $R$ . Il polinomio  $f(x) = 3x + 2$  non ha radici in  $\mathbb{Z}$ .

In  $\mathbb{R}[x]$  il polinomio  $x^2 - 5x + 6$  ha radici 2 e 3, il polinomio  $x^2 - 4x + 4$  ha radice il solo 2, il polinomio  $x^2 + 1$  non ha radici in  $\mathbb{R}$ .

Dall'algoritmo della divisione segue subito il fondamentale, ben noto:

**6.6.5. Teorema di Ruffini.** Sia  $(R, +, \cdot)$  un anello commutativo unitario e siano  $f(x) \in R[x]$  e  $c \in R$ . Allora  $c$  è radice di  $f(x)$  se e solo se il polinomio  $x - c$  divide  $f(x)$ .

*Dimostrazione.* Se  $x - c$  divide  $f(x)$ , si ha  $f(x) = (x - c)q(x)$ , da cui  $f(c) = (c - c)q(c) = 0$ . Viceversa, sia  $f(c) = 0$ . Applicando l'algoritmo della divisione ai polinomi  $f(x)$  e  $x - c$ , si ha  $f(x) = (x - c)q(x) + r(x)$ , per opportuni polinomi  $q(x), r(x) \in R[x]$ , con  $r(x) = 0$  o  $v(r(x)) < v(x - c) = 1$ . Pertanto  $r(x) = a_0 \in R$ . Da  $0 = f(c) = (c - c)q(c) + r(c) = r(c) = a_0$  segue l'asserto.  $\square$

Il precedente risultato si generalizza nel seguente:

**6.6.6. Teorema di Ruffini generalizzato.** Sia  $(R, +, \cdot)$  un dominio d'integrità unitario e sia  $f(x) \in R[x]$  un polinomio non nullo. Se  $c_1, \dots, c_t$  sono elementi a due a due distinti di  $R$ , si ha che  $c_1, \dots, c_t$  sono radici di  $f(x)$  se e solo se il polinomio  $(x - c_1) \dots (x - c_t)$  divide  $f(x)$ .

*Dimostrazione.* La condizione sufficiente è ovvia. Si supponga ora che  $c_1, \dots, c_t$  siano radici di  $f(x)$ . Si ragioni per induzione su  $t$ . Per  $t = 1$ , l'asserto segue dal teorema di Ruffini. Supposto  $t > 1$ , ancora per il teorema di Ruffini si ha  $f(x) = (x - c_1)q(x)$ , e riesce  $0 = f(c_i) = (c_i - c_1)q(c_i)$ , con  $c_i - c_1 \neq 0$ , per ogni  $i = 2, \dots, t$ . Pertanto  $q(c_i) = 0$  per  $i = 2, \dots, t$ , cioè gli elementi  $c_2, \dots, c_t$  sono  $t - 1$  radici a due a due distinte del polinomio  $q(x)$ . L'ipotesi d'induzione assicura che  $q(x) = (x - c_2) \dots (x - c_t)l(x)$ , per un opportuno  $l(x) \in R[x]$ , da cui  $f(x) = (x - c_1) \dots (x - c_t)l(x)$ , come volevasi.  $\square$

Come conseguenza immediata si ha:

**6.6.7.** *Sia  $(R, +, \cdot)$  un dominio d'integrità unitario. Un polinomio di  $R[x]$  di grado  $n > 0$  ha al più  $n$  radici distinte.*

Si noti che (vedi Esercizio 6.6.2) nel risultato precedente è essenziale l'ipotesi che non esistano in  $R$  divisori dello 0.

Siano  $(R, +, \cdot)$  un anello commutativo unitario,  $f(x)$  un polinomio non nullo di  $R[x]$  e  $c \in R$  una radice di  $f(x)$ . Dal teorema di Ruffini segue che  $x - c$  divide  $f(x)$ . Si dice che  $c$  è **radice semplice** di  $f(x)$  se  $(x - c)^2$  non divide  $f(x)$ , in caso contrario  $c$  è detta **radice multipla**. Il massimo intero positivo  $k$  tale che  $(x - c)^k$  divide  $f(x)$  è detto la **moltelicità** della radice  $c$  di  $f(x)$ . Se  $k = 2$  ( $k = 3$ ),  $c$  è detta radice **doppia** (rispettivamente **tripla**) di  $f(x)$ .

**6.6.8. Esempio.** 2 è radice semplice del polinomio  $f(x) = x^2 - 5x + 6 \in \mathbb{R}[x]$ , è radice doppia del polinomio  $f_1(x) = x^2 - 4x + 4 \in \mathbb{R}[x]$ .

Si noti che, come evidenziato nel Capitolo 5, un polinomio  $f(x) \in \mathbb{C}[x]$  di grado  $n > 0$  ha sempre radici in  $\mathbb{C}$ , precisamente esistono numeri complessi  $c_1, \dots, c_n$ , non necessariamente distinti, tali che:

$$f(x) = b(x - c_1) \dots (x - c_n),$$

con  $b$  coefficiente direttivo di  $f(x)$ .

## Esercizi

**Esercizio 6.6.1.** *Si provi che  $(R[x], +, \cdot)$  è un anello commutativo unitario.*

**Esercizio 6.6.2.** *Si verifichi che il polinomio  $f(x) = \bar{1}x^2 - \bar{1} \in \mathbb{Z}_8[x]$  ha radici  $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ , e che, per esempio,  $(\bar{1}x - \bar{1})(\bar{1}x - \bar{3})$  non divide  $f(x)$ .*

**Esercizio 6.6.3.** *Considerati in  $\mathbb{Z}_7[x]$  i polinomi*

$$s(x) = x^7 + \bar{2}x^5 + \bar{4}x^3 + \bar{6}x + \bar{3}, \quad t(x) = \bar{3}x^3 + x + \bar{4},$$

*si determinino i polinomi  $s(x) + t(x)$  e  $s(x) \cdot t(x)$ .*

**Esercizio 6.6.4. Proprietà universale dell'anello dei polinomi.** Sia  $(R, +, \cdot)$  un anello commutativo unitario e si consideri l'anello dei polinomi  $(R[x], +, \cdot)$ . Si provi che, per ogni anello commutativo unitario  $(S, +, \cdot)$ , per ogni omomorfismo  $\varphi : R \rightarrow S$  tale che  $\varphi(1_R) = 1_S$  e per ogni  $c \in S$ , esiste uno e un solo omomorfismo  $\psi : R[x] \rightarrow S$  tale che  $\psi(a) = \varphi(a)$ , per ogni  $a \in R$ , e  $\psi(x) = c$ .

**Esercizio 6.6.5.** Sia  $(R, +, \cdot)$  un anello commutativo unitario. Per ogni polinomio  $f(x) = \sum_{i \in \mathbb{N}_0} a_i x^i \in R[x]$ , è detto **polinomio derivato** di  $f(x)$  il polinomio

$$f'(x) := \sum_{i \in \mathbb{N}} i a_i x^{i-1} \in R[x].$$

Si verifichi che il polinomio nullo e, più in generale, un qualunque polinomio costante, ha polinomio derivato nullo; e che, se  $f(x) = a_0 + a_1 x + \cdots + a_m x^m$  è un polinomio non nullo, si ha  $f'(x) = a_1 + 2a_2 x + \cdots + m a_m x^{m-1}$ . Si provi poi che, per ogni  $f(x), g(x) \in R[x]$ , si ha:

$$\begin{aligned} (f(x) + g(x))' &= f'(x) + g'(x), \\ (f(x)g(x))' &= f'(x)g(x) + f(x)g'(x). \end{aligned}$$

**Esercizio 6.6.6.** Siano  $(R, +, \cdot)$  un anello commutativo unitario,  $f(x) \in R[x]$  e  $c \in R$ . Si provi che  $c$  è radice multipla di  $f(x)$  se e solo se  $f'(c) = 0$ .

**Esercizio 6.6.7.** Si considerino i polinomi  $f(x) = x^4 - 2x^3 + 4x^2 - 6x + 3$  e  $g(x) = x^2 + x - 2 \in \mathbb{Q}[x]$ .

- (i) Si determinino i polinomi  $f(x) + g(x)$ ,  $f(x) \cdot g(x)$ ,  $(-5)f(x)$ ,  $f'(x)$ ,  $g'(x)$ .
- (ii) Si individuino il quoziente e il resto della divisione di  $f(x)$  per  $g(x)$ .
- (iii) Si verifichi se 1 è radice di  $f(x)$  o di  $g(x)$ , se è radice multipla e, in caso di risposta affermativa, si divida il polinomio per  $x - 1$ .

**Esercizio 6.6.8.** Considerato il polinomio  $h(x) = x^3 + x^2 - 8x - 12 \in \mathbb{Q}[x]$ , si determinino le sue radici e lo si decomponga nel prodotto di tre polinomi monici di primo grado.

**Esercizio 6.6.9.** Si consideri il polinomio  $f_{\bar{a}}(x) = x^4 + \bar{a}x + \bar{a} \in \mathbb{Z}_3[x]$ . Si determinino i valori di  $\bar{a} \in \mathbb{Z}_3$  per cui il polinomio  $f_{\bar{a}}(x)$  ammette radici in  $\mathbb{Z}_3$ .

**Esercizio 6.6.10.** Sia  $A$  un campo, e si considerino i polinomi  $g(x) = x^3 - 2$  e  $h(x) = x^2 + x + 1 \in A[x]$ . Si determinino quoziente e resto della divisione di  $g(x)$  per  $h(x)$ . Distinguendo i casi  $A = \mathbb{Q}$ ,  $A = \mathbb{Z}_3$ ,  $A = \mathbb{Z}_5$ ,  $A = \mathbb{Z}_7$ , si stabilisca poi se  $g(x)$  e  $h(x)$  hanno radici in  $A$ .

**Esercizio 6.6.11.** Si consideri il polinomio  $f_{\bar{a}}(x) = x^3 + \bar{a}x + \bar{1} \in \mathbb{Z}_3[x]$ . Si determinino i valori di  $\bar{a} \in \mathbb{Z}_3$  per cui il polinomio  $f_{\bar{a}}(x)$  ammette radici multiple in  $\mathbb{Z}_3$ .

**Esercizio 6.6.12.** Si determinino tutte le radici dei seguenti polinomi:

$$\begin{aligned} k(x) &= x^5 + x^4 + x^3 + x^2 + \bar{3}x + \bar{3} \in \mathbb{Z}_5[x], \\ l(x) &= x^5 + \bar{2}x \in \mathbb{Z}_3[x]. \end{aligned}$$

**Esercizio 6.6.13.** Si consideri il polinomio  $f(x) = x^2 - \bar{6}x + \bar{4} \in \mathbb{Z}_p[x]$ , con  $p$  primo.

- (i) Si provi che né  $\bar{1}$  né  $\bar{5}$  è radice di  $f(x)$ , qualunque sia  $p$ .
- (ii) Si determinino i valori di  $p$  per cui  $\bar{10}$  è radice di  $f(x)$ , e i valori di  $p$  per cui  $f(x)$  ha radici doppie.

**Esercizio 6.6.14.** Con  $p$  primo si ritrovi il teorema di Wilson (vedi 5.6.4), ragionando sul polinomio  $x^{p-1} - \bar{1} \in \mathbb{Z}_p[x]$  e utilizzando il piccolo teorema di Fermat (vedi 5.6.2) e il teorema di Ruffini generalizzato (vedi 6.6.6).

**Esercizio 6.6.15.** Siano  $F$  un campo,  $\lambda_1, \dots, \lambda_r$  elementi di  $F$  a due a due distinti ( $r \geq 2$ ) e si supponga

$$(x - \lambda_1)^{\mu_1} \dots (x - \lambda_r)^{\mu_r} = (x - \lambda_1)^{\nu_1} \dots (x - \lambda_r)^{\nu_r},$$

per opportuni  $\mu_1, \dots, \mu_r, \nu_1, \dots, \nu_r \geq 1$ . Si provi che  $\mu_1 = \nu_1, \dots, \mu_r = \nu_r$ .

*Svolgimento.* Si ragioni per induzione su  $r$ . Nel caso  $r = 2$  si supponga quindi  $(x - \lambda_1)^{\mu_1}(x - \lambda_2)^{\mu_2} = (x - \lambda_1)^{\nu_1}(x - \lambda_2)^{\nu_2}$  e, per assurdo, sia per esempio  $\mu_1 < \nu_1$ . Allora da  $F[x]$  dominio d'integrità segue che

$$(x - \lambda_2)^{\mu_2} = (x - \lambda_1)^{\nu_1 - \mu_1}(x - \lambda_2)^{\nu_2}$$

con  $\nu_1 - \mu_1 > 0$ , sicché per il teorema di Ruffini il polinomio  $(x - \lambda_2)^{\mu_2}$  ha per radice  $\lambda_1$ . Pertanto  $(\lambda_1 - \lambda_2)^{\mu_2} = 0$ , con  $\lambda_1 - \lambda_2 \neq 0$ , contro l'essere  $F$  un campo. La dimostrazione si completa poi facilmente.

## 6.7 Esercizi di riepilogo

**Esercizio 6.7.1.** Si consideri, nell'insieme  $\mathbb{Z}_5$ , l'operazione interna  $\star$  definita ponendo, con  $[x]_5, [y]_5 \in \mathbb{Z}_5$ ,

$$[x]_5 \star [y]_5 := [x + y + 3]_5.$$

Si verifichi che tale posizione ha senso, e si studi la struttura  $(\mathbb{Z}_5, \star)$ , scrivendone anche una tavola di moltiplicazione. Si dimostri che la posizione

$$f : [x]_5 \in \mathbb{Z}_5 \longmapsto [x + 2]_5 \in \mathbb{Z}_5$$

definisce un'applicazione e che tale applicazione è biettiva, se ne determini l'inversa, e si provi che  $f$  è un isomorfismo di  $(\mathbb{Z}_5, +)$  in  $(\mathbb{Z}_5, \star)$ .

**Esercizio 6.7.2.** Nel gruppo  $(G, \cdot) = (\mathrm{GL}(2, \mathbb{Z}_5), \cdot)$  delle matrici invertibili  $2 \times 2$  su  $\mathbb{Z}_5$ , con il prodotto righe per colonne, si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{b} \end{pmatrix} : \bar{a}, \bar{b} \in \mathbb{Z}_5^* \right\}.$$

- (i) Si provi che  $H$  è un sottogruppo abeliano di  $G$  e se ne determini l'ordine.
- (ii) Posto

$$X = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}, \quad Y = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{3} \end{pmatrix},$$

si determinino gli elementi di  $S = \langle X \rangle$  e di  $T = \langle Y \rangle$ .

- (iii) Si studi il gruppo quoziante  $H/S$ , determinandone l'ordine, gli elementi, i sottogruppi.
- (iv) Considerate infine

$$\begin{aligned} f : \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{b} \end{pmatrix} S \in H/S &\longmapsto \bar{a}\bar{b}^{-1} \in \mathbb{Z}_5^*, \\ g : \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{0} & \bar{b} \end{pmatrix} T \in H/T &\longmapsto \bar{a}\bar{b} \in \mathbb{Z}_5^*, \end{aligned}$$

si stabilisca se  $f$  e  $g$  sono ben poste e se sono omomorfismi di gruppi, e in tal caso se ne determinino il nucleo e l'immagine.

**Esercizio 6.7.3.** Nel gruppo  $(G, \cdot) = (\mathrm{GL}(2, \mathbb{Z}_6), \cdot)$  delle matrici invertibili  $2 \times 2$  su  $\mathbb{Z}_6$ , con il prodotto righe per colonne, si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{c} & \bar{a} \end{pmatrix} : \bar{a} \in \mathbb{Z}_6^*, \bar{c} \in \mathbb{Z}_6 \right\}.$$

- (i) Si provi che  $H$  è un sottogruppo abeliano di  $G$  e se ne determini l'ordine.
- (ii) Posto

$$N = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{2c} & \bar{1} \end{pmatrix} : \bar{c} \in \mathbb{Z}_6 \right\},$$

si provi che  $N$  è un sottogruppo di  $H$  e si studi il gruppo quoziante  $H/N$ , determinandone l'ordine, gli elementi e la struttura.

- (iii) Definita infine

$$f : \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{c} & \bar{a} \end{pmatrix} N \in H/N \longmapsto \bar{a} \in \mathbb{Z}_6^*$$

si provi che  $f$  è ben posta, che è un omomorfismo di gruppi e se ne determinino il nucleo e l'immagine.

**Esercizio 6.7.4.** Sia  $(\mathbb{Q}, +)$  il gruppo additivo dei numeri razionali. Si consideri l'anello  $(\mathbb{Q}, +, \star)$ , dove  $\star$  è l'operazione in  $\mathbb{Q}$  definita ponendo  $x \star y := \frac{5}{3}xy$ , per ogni  $x, y \in \mathbb{Q}$ .

- (i) Si provi che la struttura  $(\mathbb{Q}, +, \star)$  è un anello commutativo e unitario e se ne determini l'unità.
- (ii) Si calcoli la caratteristica di  $(\mathbb{Q}, +, \star)$  e se ne determini il sottoanello fondamentale.
- (iii) Considerate le parti  $\mathbb{N}_0$ ,  $\mathbb{Z}$  e  $T = \left\{ \frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$ , si stabilisca se esse sono sottoanelli o ideali di  $(\mathbb{Q}, +, \star)$ .
- (iv) Si provi che  $(\mathbb{Q}, +, \star)$  è isomorfo all'anello  $(\mathbb{Q}, +, \cdot)$  dei numeri razionali, dove  $\cdot$  denota l'ordinario prodotto di numeri razionali.

**Esercizio 6.7.5.** Si dimostri che l'insieme

$$A = \left\{ \frac{m}{2n+1} : m \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$$

è un sottoanello unitario dell'anello  $(\mathbb{Q}, +, \cdot)$  dei numeri razionali, e se ne determinino gli elementi invertibili e gli eventuali divisori dello zero. Posto poi  $H = \{a \in A : a \text{ non invertibile}\}$ , si verifichi che  $H$  è un ideale di  $A$ .

In generale, si dimostri che in un anello commutativo unitario  $R$  l'insieme costituito dagli elementi non invertibili costituisce un ideale di  $R$  se e solo se, per ogni  $x \in R$ , si ha  $x$  invertibile o  $1 - x$  invertibile.

**Esercizio 6.7.6.** Sia  $R \neq \{0\}$  un anello unitario, e si consideri l'anello  $M_2(R)$  delle matrici  $2 \times 2$  su  $R$ .

- (i) Posto

$$S = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} : x, y \in R \right\},$$

si provi che  $S$  è un sottoanello di  $M_2(R)$  e si stabilisca se  $S$  è unitario e se ha divisori dello zero.

- (ii) Si dimostri che l'applicazione

$$f : a \in R \longmapsto \begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix} \in S$$

è un monomorfismo di anelli e se ne determini l'immagine  $W$ , evidenziandone i legami con  $R$ .

- (iii) Si verifichi se  $W$  è un ideale destro, sinistro o bilatero di  $S$ .
- (iv) Infine, dopo aver provato che

$$L = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in R \right\}$$

è un ideale bilatero di  $S$ , si mostri che il quoziente  $S/L$  è isomorfo a  $W$  individuando un epimorfismo di  $S$  in  $W$  di nucleo  $L$ .

**Esercizio 6.7.7.** Si consideri la struttura  $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$  definita ponendo, per ogni  $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ ,

$$(a, b) + (c, d) := (a + c, b + d), \\ (a, b) \cdot (c, d) := (ad + bc, bd),$$

e si ponga  $A = \mathbb{Z} \times \mathbb{Z}$ .

- (i) Si provi che  $A$  è un anello commutativo e unitario.
- (ii) Si determinino la caratteristica di  $A$  e gli eventuali divisori dello zero in  $A$ , e si dica se  $A$  è un campo.
- (iii) Si verifichi che l'insieme degli elementi invertibili di  $A$  coincide con

$$U = \{(a, \epsilon) : a \in \mathbb{Z}, \epsilon \in \{1, -1\}\},$$

e si stabilisca se  $U \cup \{(0, 0)\}$  è un sottoanello o un ideale di  $A$ .

- (iv) Posto infine

$$f : (a, b) \in A \longmapsto a + b \in \mathbb{Z}$$

si stabilisca se  $f$  è iniettiva, suriettiva e se è un omomorfismo di anelli.

**Esercizio 6.7.8.** Si consideri la struttura  $(A, +, \cdot)$ , con  $A = \mathbb{Z} \times \mathbb{Z}$  e le operazioni  $+ e \cdot$  definite ponendo, per ogni  $(m, r), (n, s) \in A$ ,

$$(m, r) + (n, s) := (m + n, r + s), \\ (m, r) \cdot (n, s) := (mn, ms + nr + rs).$$

- (i) Si provi che  $(A, +, \cdot)$  è un anello commutativo e unitario, e se ne determinino la cardinalità, la caratteristica, gli eventuali divisori dello zero.
- (ii) Posto  $S = \{(n, -n) : n \in \mathbb{Z}\}$ , si provi che  $S$  è un ideale di  $A$  e che la posizione:

$$\psi : (m, r) + S \in A/S \longmapsto m + r \in \mathbb{Z}$$

definisce un'applicazione di  $A/S$  in  $\mathbb{Z}$  che è un isomorfismo di anelli.

- (iii) Posto infine  $T = \{(m, 0) : m \in \mathbb{Z}\}$  e  $V = \{(0, s) : s \in \mathbb{Z}\}$ , si stabilisca se  $T$  e  $V$  sono sottoanelli o ideali di  $A$ .

**Esercizio 6.7.9.** Si consideri il polinomio  $f_a(x) = x^4 + ax^3 + ax - a \in \mathbb{Z}_3[x]$ . Si determinino i valori di  $a \in \mathbb{Z}_3$  per cui il polinomio  $f_a(x)$  ammette radici in  $\mathbb{Z}_3$ .

**Esercizio 6.7.10.** Si consideri l'anello  $(M_2(\mathbb{Z}_4), +, \cdot)$  delle matrici  $2 \times 2$  su  $\mathbb{Z}_4$ .

- (i) Si dimostri che l'insieme

$$R = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{pmatrix} : \bar{a} \in \mathbb{Z}_4, \bar{b} \in 2\mathbb{Z}_4 \right\}$$

è un sottoanello commutativo dell'anello  $M_2(\mathbb{Z}_4)$ , e se ne determinino l'ordine e la caratteristica.

(ii) Considerati in  $(R, +)$  i sottogruppi

$$A = \left\langle \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \right\rangle, \quad B = \left\langle \begin{pmatrix} \bar{0} & \bar{2} \\ \frac{1}{2} & \bar{0} \end{pmatrix} \right\rangle, \quad C = \left\langle \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \right\rangle,$$

- si dimostri che  $A$  non è un ideale dell'anello  $R$ , che  $B$  e  $C$  sono ideali di  $R$ .  
 (iii) Si studi l'anello quoziante  $R/C$ ; in particolare se ne individui la caratteristica.  
 (iv) Si verifichi poi che ha senso l'applicazione

$$\varphi : \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{pmatrix} + B \in R/B \longmapsto \bar{a} \in \mathbb{Z}_4$$

e che tale applicazione è un isomorfismo di anelli.

- (v) Si studi infine se gli anelli  $R/C$  e  $R/B$  sono isomorfi.

**Esercizio 6.7.11.** Sia  $(A, +, \cdot)$  l'anello prodotto  $\mathbb{Z} \times \mathbb{Z}_{20}$ .

- (i) Si precisino la caratteristica e il sottoanello fondamentale di  $A$ .  
 (ii) Si individuino gli eventuali divisori dello zero in  $A$  e si precisi se  $A$  è un campo.  
 (iii) Si dimostri che la posizione

$$\phi((x, [y]_{20})) = [5xy]_{20}$$

definisce un'applicazione di  $A$  in  $\mathbb{Z}_{20}$ , che tale applicazione è un omomorfismo di  $(A, \cdot)$  in  $(\mathbb{Z}_{20}, \cdot)$ , non un omomorfismo di  $(A, +)$  in  $(\mathbb{Z}_{20}, +)$ .

**Esercizio 6.7.12.** Nel gruppo  $G = \mathbb{S}_5$  delle permutazioni su 5 oggetti si considerino gli elementi

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Si decompongano  $f$ ,  $g$  e  $h$  in prodotto di cicli disgiunti e se ne determini la parità. Posto poi  $N = \langle f \rangle$ , si provi che  $N$  non è normale in  $G$ .

**Esercizio 6.7.13.** Siano  $\mathbb{S}_3$  il gruppo delle permutazioni su 3 oggetti e  $C_3$  il gruppo ciclico di ordine 3. Sia  $(G, \cdot)$  il gruppo ottenuto considerando la struttura prodotto  $G = \mathbb{S}_3 \times C_3$ .

- (i) Si provi che il gruppo  $G$  non è abeliano.  
 (ii) Detto  $A$  l'unico sottogruppo di  $\mathbb{S}_3$  di ordine 3, si provi che le parti:

$$H = \{(a, b) : a \in A, b \in C_3\}, \quad K = \{(a, 1) : a \in A\}$$

sono sottogruppi di  $G$ , normali in  $G$ .

- (iii) Si studino i gruppi quoziante  $G/H$  e  $G/K$ , determinandone l'ordine e la struttura.

**Esercizio 6.7.14.** Sia  $\mathbb{R}$  l'insieme dei numeri reali e si considerino le applicazioni:

$$f : x \in \mathbb{R} \mapsto x + 1 \in \mathbb{R}, \quad g : x \in \mathbb{R} \mapsto 2 - x \in \mathbb{R}.$$

Si provi che  $f$  e  $g$  sono biettive e si determinino  $\langle f \rangle$  e  $\langle g \rangle$  nel gruppo simmetrico  $S_{\mathbb{R}}$ .

**Esercizio 6.7.15.** Nell'anello  $\mathbb{Z}_7[x]$  dei polinomi nell'indeterminata  $x$  a coefficienti in  $\mathbb{Z}_7$  si considerino gli elementi:

$$f(x) = x^3 + x, \quad g(x) = x^2 + 3x + 4, \quad h(x) = x^3 + x^2 + 4x + 4.$$

Si determinino le radici di  $f(x)$ ,  $g(x)$  e  $h(x)$  in  $\mathbb{Z}_7$ , e tutti i massimi comuni divisori tra  $f(x)$  e  $g(x)$ , e tra  $f(x)$  e  $h(x)$  in  $\mathbb{Z}_7[x]$ .

Si provi, più in generale, che se  $K$  è un campo e  $a(x)$  e  $b(x)$  sono polinomi a coefficienti in  $K$ , primi tra loro in  $K[x]$ , allora  $a(x)$  e  $b(x)$  non hanno radici in comune e  $a(x) + b(x)$  e  $a(x)$  sono primi tra loro.

**Esercizio 6.7.16.** Nell'anello  $(M_2(\mathbb{Z}), +, \cdot)$  delle matrici  $2 \times 2$  sull'anello degli interi, con le usuali operazioni di somma e di prodotto righe per colonne, si consideri la parte

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

- (i) Si provi che  $S$  è un sottoanello unitario di  $M_2(\mathbb{Z})$  e se ne determinino i divisori dello zero, il sottoanello fondamentale e la caratteristica.
- (ii) Posto

$$f : z \in \mathbb{Z} \mapsto \begin{pmatrix} 0 & 0 \\ 0 & z \end{pmatrix} \in M_2(\mathbb{Z}),$$

si provi che  $f$  è un omomorfismo di anelli e si stabilisca se  $J = \text{Im } f$  è un ideale bilatero di  $S$ . Si dica poi se i laterali

$$\begin{pmatrix} 4 & 0 \\ 8 & 4 \end{pmatrix} + J \quad e \quad \begin{pmatrix} 3 & 0 \\ 8 & 4 \end{pmatrix} + J$$

coincidono nel gruppo quoziante  $(S/J, +)$ .

- (iii) Posto

$$\varphi : \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + J \in S/J \mapsto a + c \in \mathbb{Z},$$

si stabilisca se  $\varphi$  è ben posta e se è un omomorfismo di anelli.

- (iv) Si provi che la matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix}$$

è un elemento invertibile in  $S$ , per ogni  $z \in \mathbb{Z}$ . Più in generale si mostri che se  $a$  è un elemento di un anello unitario  $R$  tale che  $a^2 = 0$ , allora gli elementi  $1 + a$  e  $1 - a$  sono invertibili in  $R$ .

# L'algebra delle matrici

---

*Questo capitolo è dedicato alle matrici, probabilmente già familiari al Lettore. Si introduciranno e si studieranno operazioni tra matrici e i fondamentali concetti di determinante di una matrice quadrata e di rango di una matrice qualsiasi. Ciò permetterà di illustrare notevoli applicazioni, quale per esempio lo studio dei sistemi di equazioni lineari.*

## 7.1 Generalità

Una **matrice**  $n \times m$  a coefficienti in un anello  $R$  è una tabella costituita da  $nm$  elementi di  $R$  disposti secondo  $n$  righe e  $m$  colonne. Per esempio la tabella

$$B = \begin{pmatrix} 0 & -1 & 3 & 5 \\ -4 & 22 & 7 & 15 \\ 0 & 0 & 32 & -17 \end{pmatrix}$$

è una matrice  $3 \times 4$  a coefficienti nell'anello  $\mathbb{Z}$  dei numeri interi.

Date una matrice  $A$  con  $n$  righe e  $m$  colonne su un anello  $R$  e una coppia  $(i, j)$  di numeri interi tali che  $i \in \{1, \dots, n\}$  e  $j \in \{1, \dots, m\}$ , si definisce **termine**, o anche **entrata**, di posto  $(i, j)$  di  $A$ , e si denota con  $a_{ij}$ , quell'unico elemento di  $R$  che appartiene alla riga  $i$ -esima e alla colonna  $j$ -esima della tabella considerata. Con questa notazione la matrice  $A$  viene indicata con

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

o, più brevemente, con  $A = (a_{ij})$ . Per esempio  $b_{22} = 22$  è il termine di posto  $(2, 2)$  della matrice  $B$  considerata prima; il termine di posto  $(3, 4)$  è  $b_{34} = -17$ .

Le  $n$  righe della matrice  $A$  vengono denotate con  $A^{(1)}, A^{(2)}, \dots, A^{(n)}$ ; per ogni  $i \in \{1, \dots, n\}$ , la  $i$ -esima riga della matrice  $A$  è quindi la matrice  $1 \times m$

$$A^{(i)} = ( a_{i1} \ a_{i2} \ \dots \ a_{im} ).$$

Così le  $m$  colonne della matrice  $A$  vengono denotate con  $A_{(1)}, A_{(2)}, \dots, A_{(m)}$ ; per ogni  $j \in \{1, \dots, m\}$ , la  $j$ -esima colonna della matrice  $A$  è quindi la matrice  $n \times 1$

$$A_{(j)} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}.$$

Se  $n = m$  la matrice è detta **quadrata** di ordine  $n$  e la  $n$ -upla  $(a_{11}, \dots, a_{nn})$  si chiama **diagonale principale** di  $A$ . La matrice quadrata  $A$  è detta **simmetrica** se  $a_{ij} = a_{ji}$  per ogni  $i, j \in \{1, \dots, n\}$ .

Data una matrice  $A$  con  $n$  righe e  $m$  colonne su un anello  $R$ , si definisce **trasposta** di  $A$ , e si denota con  $A^T$ , la matrice  $m \times n$  che si ottiene da  $A$  scambiando le righe con le colonne. Per esempio la trasposta della matrice

$$A = \begin{pmatrix} -5 & 7 & 3 \\ 0 & 0 & -1 \\ 2 & -2 & 4 \\ 3 & 0 & -2 \end{pmatrix}$$

è la matrice

$$A^T = \begin{pmatrix} -5 & 0 & 2 & 3 \\ 7 & 0 & -2 & 0 \\ 3 & -1 & 4 & -2 \end{pmatrix}.$$

È immediato osservare che una matrice quadrata è simmetrica se e solo se coincide con la sua trasposta.

Una matrice quadrata  $A = (a_{ij})$  è detta **triangolare superiore** (rispettivamente **inferiore**) se tutti i termini al di sotto (risp. al di sopra) della diagonale principale sono 0, cioè se  $a_{ij} = 0$  per ogni  $i > j$  ( $i < j$ ), ed è detta **diagonale** se tutti i termini che non appartengono alla diagonale principale sono 0, cioè se  $a_{ij} = 0$  per ogni  $i \neq j$ . Infine la matrice quadrata  $A = (a_{ij})$  è detta **scalare** se è diagonale e tutti i termini della diagonale principale sono uguali a uno stesso elemento  $\lambda \in R$ , cioè

$$a_{ij} = \begin{cases} \lambda & \text{se } i = j \\ 0 & \text{se } i \neq j. \end{cases}$$

### La matrice di una corrispondenza

Siano  $A = \{a_1, \dots, a_t\}$  e  $B = \{b_1, \dots, b_r\}$  insiemi finiti di ordini  $t$  e  $r$  rispettivamente e sia  $\mathcal{R}$  una corrispondenza tra  $A$  e  $B$ . Alla corrispondenza  $\mathcal{R}$  è possibile associare una matrice  $M_{\mathcal{R}}$  con  $t$  righe e  $r$  colonne a coefficienti interi definita ponendo

$$m_{ij} := \begin{cases} 1 & \text{se } (a_i, b_j) \in \mathcal{R} \\ 0 & \text{se } (a_i, b_j) \notin \mathcal{R}. \end{cases}$$

Tale matrice è detta appunto **matrice della corrispondenza**  $\mathcal{R}$ .

È immediato osservare che  $\mathcal{R}$  è un'applicazione se e solo se in ogni riga di  $M_{\mathcal{R}}$  vi è uno e un solo termine uguale a 1. In tal caso  $\mathcal{R}$  è iniettiva se e solo se in ogni colonna compare al più un termine uguale a 1 ed è suriettiva se e solo se in ogni colonna almeno un termine è uguale a 1. Pertanto un'applicazione tra insiemi finiti è biettiva se e solo se in ogni colonna dalla sua matrice vi è uno e un solo termine uguale a 1. In particolare, se ciò accade allora il numero delle righe è uguale a quello delle colonne, e quindi la matrice è quadrata.

Per esempio siano  $A = \{a_1, a_2, a_3, a_4, a_5\}$  e  $B = \{b_1, b_2, b_3, b_4\}$  e si consideri la corrispondenza  $\mathcal{R} = \{(a_1, b_2), (a_2, b_4), (a_3, b_3)\}$ . La matrice di tale corrispondenza è la seguente matrice  $5 \times 4$ :

$$M_{\mathcal{R}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$\mathcal{R}$  non è un'applicazione: nella quarta e nella quinta riga non ci sono termini uguali a 1 perché appunto  $a_4$  e  $a_5$  sono privi di corrispondenti.

Invece la corrispondenza  $\mathcal{R}_1$  tra  $A$  e  $B$  la cui matrice è

$$M_{\mathcal{R}_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

è un'applicazione perché in ogni riga vi è esattamente un termine uguale a 1. Tale applicazione è poi suriettiva perché in ogni colonna vi è almeno un termine uguale a 1, ma non è iniettiva perché nella terza colonna ci sono due termini uguali a 1. Infatti  $a_2$  e  $a_4$ , pur essendo distinti, hanno entrambi immagine  $b_3$ .

Le eventuali proprietà riflessiva, simmetrica, antisimmetrica e transitiva di una corrispondenza  $\mathcal{R}$  di un insieme finito  $A$  in sè, ovvero di una relazione binaria in  $A$ , possono essere facilmente dedotte dall'esame della matrice  $M_{\mathcal{R}}$ .

**7.1.1.** Sia  $\mathcal{R}$  una relazione binaria in un insieme finito  $A = \{a_1, \dots, a_n\}$ , e sia  $M_{\mathcal{R}} = (m_{ij})$  la matrice di  $\mathcal{R}$ . Allora si ha:

- (i)  $\mathcal{R}$  è riflessiva  $\iff M_{\mathcal{R}}$  è quadrata e ha tutti 1 sulla diagonale principale;
- (ii)  $\mathcal{R}$  è simmetrica  $\iff M_{\mathcal{R}}$  è simmetrica;
- (iii)  $\mathcal{R}$  è antisimmetrica  $\iff m_{ij} \cdot m_{ji} = 0$  per ogni  $i, j \in \{1, \dots, n\}$  tali che  $i \neq j$ ;
- (iv)  $\mathcal{R}$  è transitiva  $\iff m_{ih} \cdot m_{hj} \leq m_{ij}$  per ogni  $i, j, h \in \{1, \dots, n\}$ .

*Dimostrazione.* (i)  $\mathcal{R}$  è riflessiva se e solo se per ogni  $i \in \{1, \dots, n\}$  risulta  $a_i \mathcal{R} a_i$ , cioè  $m_{ii} = 1$  per ogni  $i$ , e quindi se e solo se tutti i termini della diagonale principale della matrice di  $\mathcal{R}$ , che è quadrata, sono uguali a 1.

(ii)  $\mathcal{R}$  è simmetrica se e solo se, per ogni  $i, j \in \{1, \dots, n\}$ , da  $a_i \mathcal{R} a_j$  segue  $a_j \mathcal{R} a_i$ , ovvero  $m_{ij} = 1$  se e solo se  $m_{ji} = 1$ , e quindi se e solo se  $M_{\mathcal{R}}$  è una matrice simmetrica.

(iii)  $\mathcal{R}$  è antisimmetrica se e solo se per ogni  $i, j \in \{1, \dots, n\}$  con  $i \neq j$ , se  $m_{ij} = 1$  cioè  $a_i \mathcal{R} a_j$  risulta  $a_j \not\mathcal{R} a_i$ , per cui  $m_{ji} = 0$ ; pertanto  $m_{ij} \cdot m_{ji} = 0$ .

(iv)  $\mathcal{R}$  è transitiva se e solo se per ogni  $i, j, h \in \{1, \dots, n\}$  da  $m_{ih} = 1$  e  $m_{hj} = 1$  segue  $m_{ij} = 1$ , ovvero se e solo se  $m_{ih} \cdot m_{hj} \leq m_{ij}$ .  $\square$

## Esercizi

**Esercizio 7.1.1.** Si determinino le trasposte delle seguenti matrici:

$$A = \begin{pmatrix} 1 & -4 & 3 \\ 0 & -7 & 8 \\ -5 & 1 & 2 \\ 4 & 4 & 7 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 32 & 1 \\ -7 & 21 \\ 0 & 0 \\ 15 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & -2 & 1 \\ -2 & 3 & -50 \\ 1 & -50 & 42 \end{pmatrix}.$$

**Esercizio 7.1.2.** Si considerino gli insiemi

$$S = \{0, 4, 6, 25\}, \quad T = \{-5, -2, 0, 2, 4\}.$$

Si determinino le matrici delle seguenti corrispondenze tra  $S$  e  $T$ :

$$x \mathcal{R}_1 y : \iff x \leq y^2, \quad x \mathcal{R}_2 y : \iff x > |y^3|,$$

con  $x \in S, y \in T$ , e delle seguenti relazioni binarie in  $S$ :

$$n \mathcal{R}_3 m : \iff |n - m| \leq 2, \quad n \mathcal{R}_4 m : \iff n^2 \geq 5m,$$

con  $n, m \in S$ .

**Esercizio 7.1.3.** Si considerino l'insieme  $S = \{x_1, x_2, x_3, x_4, x_5, x_6\}$  e le relazioni binarie  $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4$  in  $S$  le cui matrici sono rispettivamente

$$M_{\mathcal{R}_1} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_{\mathcal{R}_2} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$M_{\mathcal{R}_3} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad M_{\mathcal{R}_4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Si stabilisca quali tra queste sono relazioni d'ordine e quali d'equivalenza.

**Esercizio 7.1.4.** Tra gli insiemi  $A = \{a_1, a_2, a_3, a_4\}$  e  $B = \{b_1, b_2, b_3, b_4, b_5, b_6\}$ , si considerino le corrispondenze:

$$\begin{aligned}\mathcal{R}_1 &= \{(a_1, b_1), (a_1, b_4), (a_3, b_6)\}, \\ \mathcal{R}_2 &= \{(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)\}, \\ \mathcal{R}_3 &= \{(a_2, b_1), (a_3, b_1), (a_4, b_6)\}, \\ \mathcal{R}_4 &= \{(a_1, b_5), (a_2, b_6), (a_3, b_5), (a_4, b_2)\}.\end{aligned}$$

Dopo aver determinato le matrici delle corrispondenze considerate si dica quali di esse sono applicazioni, e di queste ultime si studi l'iniettività e la suriettività.

**Esercizio 7.1.5.** Siano  $S = \{x_1, x_2, x_3, x_4\}$ ,  $T = \{t_1, t_2, t_3, t_4, t_5\}$ , e  $\mathcal{R}$  la corrispondenza tra  $S$  e  $T$  la cui matrice è

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Si stabilisca se  $\mathcal{R}$  è un'applicazione e, in caso affermativo, se ne studino iniettività e suriettività. Si individui inoltre la corrispondenza tra  $T$  e  $S$  la cui matrice è la trasposta  $M^t$  di  $M$  e si stabilisca se essa è un'applicazione.

**Esercizio 7.1.6.** Siano  $S$  e  $T$  insiemi finiti e sia  $f$  un'applicazione biettiva di  $S$  in  $T$ . Indicata con  $A$  la matrice di  $f$  e con  $B$  quella di  $f^{-1}$ , si stabilisca che legame c'è tra le matrici  $A$  e  $B$ .

## 7.2 Operazioni con le matrici

Si denoti con  $M_{n,m}(R)$  l'insieme delle matrici  $n \times m$  su un anello  $R$ ; in tale insieme è possibile definire un'operazione interna e un'operazione esterna con dominio di operatori l'anello  $R$ . Per quanto riguarda l'operazione interna, ovvero l'addizione tra matrici, questa viene definita ponendo

$$\mathbf{A} + \mathbf{B} := (a_{ij} + b_{ij}), \text{ per ogni } A = (a_{ij}), B = (b_{ij}) \in M_{n,m}(R).$$

In altre parole, si definisce somma della matrice  $A$  e della matrice  $B$  quella matrice  $n \times m$  su  $R$  il cui termine di posto  $(i, j)$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ , è la somma, secondo l'addizione di  $R$ , dei termini di posto  $(i, j)$  di  $A$  e di  $B$ .

**7.2.1.** Rispetto alla somma di matrici  $M_{n,m}(R)$  è un gruppo abeliano.

*Dimostrazione.* Siano  $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in M_{n,m}(R)$ . La proprietà associativa dell'addizione in  $R$  comporta che  $(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij})$  per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ , pertanto  $(A + B) + C =$

$A + (B + C)$ . Inoltre la proprietà commutativa di cui gode l'addizione in  $R$  assicura che  $a_{ij} + b_{ij} = b_{ij} + a_{ij}$  per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ , dunque  $A + B = B + A$ . L'elemento neutro rispetto all'addizione, ovvero la matrice nulla, è, come è immediato verificare, la matrice  $n \times m$  che ha tutti i termini uguali allo 0 di  $R$ . Infine ogni matrice  $A = (a_{ij}) \in M_{n,m}(R)$  possiede opposto; basta infatti considerare la matrice  $-A := (-a_{ij})$ , ovvero la matrice  $n \times m$  su  $R$  il cui termine di posto  $(i, j)$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ , è l'opposto in  $R$  del termine di posto  $(i, j)$  di  $A$ .  $\square$

La legge esterna con dominio di operatori  $R$  si definisce ponendo

$$\lambda A := (\lambda a_{ij}), \text{ per ogni } A = (a_{ij}) \in M_{n,m}(R) \text{ e per ogni } \lambda \in R.$$

In altre parole, si definisce prodotto di  $\lambda \in R$  per la matrice  $A \in M_{n,m}(R)$  la matrice  $n \times m$  su  $R$  il cui termine di posto  $(i, j)$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ , è il prodotto, secondo la moltiplicazione di  $R$ , di  $\lambda$  per il termine di posto  $(i, j)$  di  $A$ .

**7.2.2.** *Sia  $R$  un anello commutativo unitario. Per ogni  $\lambda, \mu \in R$  e per ogni  $A = (a_{ij}), B = (b_{ij}) \in M_{n,m}(R)$  risulta:*

- (i)  $\lambda(A + B) = \lambda A + \lambda B$ ;
- (ii)  $(\lambda + \mu)A = \lambda A + \mu A$ ;
- (iii)  $(\lambda\mu)A = \lambda(\mu A)$ ;
- (iv)  $1A = A$ , dove 1 è l'unità di  $R$ .

*Dimostrazione.* (i) Per la proprietà distributiva della moltiplicazione rispetto all'addizione in  $R$  si ha  $\lambda(a_{ij} + b_{ij}) = \lambda a_{ij} + \lambda b_{ij}$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ .

(ii) Per la proprietà distributiva della moltiplicazione rispetto all'addizione in  $R$  risulta infatti  $(\lambda + \mu)a_{ij} = \lambda a_{ij} + \mu a_{ij}$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ .

(iii) Per la proprietà associativa della moltiplicazione in  $R$  risulta  $(\lambda\mu)a_{ij} = \lambda(\mu a_{ij})$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ .

(iv) Se 1 è l'unità di  $R$ , allora  $1a_{ij} = a_{ij}$ , per ogni  $i \in \{1, \dots, n\}$  e per ogni  $j \in \{1, \dots, m\}$ .  $\square$

Sia  $R$  un anello. Considerate una matrice  $A = (a_{ij}) \in M_{p,q}(R)$  e una matrice  $B = (b_{ij}) \in M_{q,n}(R)$ , ovvero matrici tali che il numero di colonne della prima coincida con il numero di righe della seconda, si definisce **prodotto righe per colonne** di  $A$  e  $B$  la matrice  $AB = (t_{ij})$  su  $R$ , con  $p$  righe e  $n$  colonne, il cui termine di posto  $(i, j)$  è la somma dei prodotti dei termini della riga  $i$ -esima di  $A$  per quelli della colonna  $j$ -esima di  $B$ , ovvero

$$t_{ij} := \sum_{h=1}^q a_{ih}b_{hj}, \text{ per ogni } i \in \{1, \dots, p\}, j \in \{1, \dots, n\}.$$

Per ogni  $n \in \mathbb{N}$  si denota con  $M_n(R)$  l'insieme delle matrici quadrate di ordine  $n$  sull'anello  $R$ . Siccome si può effettuare il prodotto righe per colonne di ogni coppia di matrici quadrate di ordine  $n$  ottenendo ancora una matrice quadrata di ordine  $n$ , il prodotto righe per colonne è un'operazione interna in  $M_n(R)$ .

**7.2.3.** Rispetto alla somma di matrici e al prodotto righe per colonne,  $M_n(R)$  è un anello. Inoltre se  $R$  è unitario, anche  $M_n(R)$  lo è.

*Dimostrazione.* Per 7.2.1,  $(M_n(R), +)$  è un gruppo abeliano.

Il prodotto righe per colonne in  $M_n(R)$  è associativo, in quanto per ogni  $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in M_n(R)$ , posto  $(AB)C = T = (t_{ij})$  e  $A(BC) = P = (p_{ij})$ , per ogni  $i, j \in \{1, \dots, n\}$  risulta

$$t_{ij} = \sum_{k=1}^n \left( \sum_{h=1}^n a_{ih} b_{hk} \right) c_{kj} = \sum_{k=1}^n \sum_{h=1}^n a_{ih} b_{hk} c_{kj} = \sum_{h=1}^n a_{ih} \left( \sum_{k=1}^n b_{hk} c_{kj} \right) = p_{ij},$$

e pertanto  $(AB)C = A(BC)$ .

Per ogni  $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in M_n(R)$ , posto  $(A+B)C = S = (s_{ij})$  e  $AC + BC = D = (d_{ij})$ , per ogni  $i, j \in \{1, \dots, n\}$  risulta

$$s_{ij} = \sum_{h=1}^n (a_{ih} + b_{ih}) c_{chj} = \sum_{h=1}^n (a_{ih} c_{chj} + b_{ih} c_{chj}) = \sum_{h=1}^n a_{ih} c_{chj} + \sum_{h=1}^n b_{ih} c_{chj} = d_{ij}.$$

Questo comporta che  $(A+B)C = AC + BC$ . Analogamente si verifica che  $A(B+C) = AB + AC$ .

Infine, se l'anello  $R$  è unitario, indicata con 1 l'unità di  $R$ , si definisce il **simbolo di Kronecker**  $\delta_{ij}$  ponendo

$$\delta_{ij} := \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j. \end{cases}$$

La matrice scalare  $I_n$  i cui termini della diagonale principale sono tutti 1, cioè  $I_n := (\delta_{ij})$ , è detta la **matrice identica** di ordine  $n$  su  $R$ , ed è elemento neutro rispetto al prodotto righe per colonne in  $M_n(R)$ . Per verificare ciò basta considerare una qualsiasi matrice  $A = (a_{ij}) \in M_n(R)$  e osservare che per ogni  $i, j \in \{1, \dots, n\}$  risulta

$$\sum_{h=1}^n a_{ih} \delta_{hj} = a_{ij} \delta_{jj} = a_{ij}$$

e

$$\sum_{k=1}^n \delta_{ik} a_{kj} = \delta_{ii} a_{ij} = a_{ij},$$

cioè  $AI_n = A = I_n A$ . □

**Osservazione.** In generale, se  $n > 1$ , l'anello  $M_n(R)$  non è commutativo neanche quando tale è  $R$ , perché il prodotto righe per colonne non è un'operazione commutativa. Per esempio, in  $M_2(\mathbb{Z})$  risulta

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Come già detto in 4.1, se  $R$  è un anello per ogni  $r \in \mathbb{N}$  si definisce la potenza  $r$ -esima di una matrice  $A \in M_n(R)$  ponendo:

$$A^r := \begin{cases} A, & \text{se } r = 1, \\ A^{r-1}A, & \text{se } r > 1. \end{cases}$$

Se  $R$  è unitario si pone anche  $A^0 := I_n$

### Esercizi

**Esercizio 7.2.1.** Si dimostri che per ogni  $A \in M_m(R)$  la matrice  $A + A^T$  è simmetrica.

**Esercizio 7.2.2.** Si considerino le seguenti matrici in  $M_{4,3}(\mathbb{Z})$ :

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 5 & 1 & 9 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 7 & 5 \\ 0 & 0 & 1 \\ 1 & 3 & 1 \\ 4 & 0 & 1 \end{pmatrix}.$$

Si determini la matrice  $2A^T + 3B^T \in M_{3,4}(\mathbb{Z})$ .

**Esercizio 7.2.3.** Si considerino le seguenti matrici su  $\mathbb{Z}$ :

$$A = \begin{pmatrix} 2 & -5 & 1 \\ 3 & 0 & -4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -2 & -3 \\ 0 & -1 & 5 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & -2 \\ 1 & -1 & -1 \end{pmatrix}.$$

Si determinino le matrici  $3A + 4B - 2C$  e  $A^T + 2B^T - C^T$ .

**Esercizio 7.2.4.** Siano

$$A = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \in M_2(\mathbb{Z}), \quad B = \begin{pmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{pmatrix} \in M_{2,3}(\mathbb{Z}).$$

Si calcoli il prodotto righe per colonne  $AB$ .

**Esercizio 7.2.5.** Siano

$$A = \begin{pmatrix} 2 & 1 \end{pmatrix} \in M_{1,2}(\mathbb{Q}), \quad B = \begin{pmatrix} 1 & -2 & 0 \\ 4 & 5 & -3 \end{pmatrix} \in M_{2,3}(\mathbb{Q}).$$

Si calcoli il prodotto righe per colonne  $AB$ .

**Esercizio 7.2.6.** Sia  $A$  una matrice  $m \times n$  su un campo  $F$ ; in quali ipotesi è definito il prodotto  $A^T A$ ?

**Esercizio 7.2.7.** Sia

$$A = \begin{pmatrix} 2 & 2 \\ 3 & -1 \end{pmatrix} \in M_2(\mathbb{Z}).$$

Si calcolino  $A^2$  e  $A^3$ .

**Esercizio 7.2.8.** Siano  $A$  e  $B$  matrici quadrate. Si dice che  $A$  e  $B$  sono **permutabili** se  $AB = BA$ . Si determinino tutte le matrici

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{R})$$

che sono permutabili con la matrice  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .

**Esercizio 7.2.9.** Sia

$$B = \begin{pmatrix} 1 & 3 \\ 5 & 3 \end{pmatrix} \in M_2(\mathbb{R});$$

si determini una matrice  $U \in M_{2,1}(\mathbb{R})$  tale che  $BU = 6U$ .

**Esercizio 7.2.10.** Siano

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 4 & 3 & 3 \\ -1 & 7 & -9 \\ 0 & 0 & 1 \end{pmatrix} \in M_{4,3}(\mathbb{Z}), \quad B = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -2 & 5 & 9 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in M_{3,4}(\mathbb{Z}).$$

Si calcolino i prodotti righe per colonne  $AB$  e  $BA$ .

**Esercizio 7.2.11.** Si considerino le seguenti matrici in  $M_{3,2}(\mathbb{R})$ :

$$A = \begin{pmatrix} 0 & -1 \\ 2 & 4 \\ -2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 0 \\ 3 & 1 \\ -7 & 5 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ 2 & 3 \\ 0 & 0 \end{pmatrix}.$$

- (i) Si calcolino le matrici  $3A$ ,  $A + B$ ,  $A - C$ ,  $2C - 5A$ ,  $-7A + 3B$  e  $A + C + B$ .
- (ii) Si determinino la matrice  $D \in M_{3,2}(\mathbb{R})$  tale che  $2A + B - D$  sia la matrice nulla, e la matrice  $E \in M_{3,2}(\mathbb{R})$  tale che  $A + 2B - 3C + E$  sia la matrice nulla.

**Esercizio 7.2.12.** Sia

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}).$$

*Si dimostri per induzione su n che*

$$A^n = \begin{pmatrix} 1 & 2n & 5n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

*per ogni n ≥ 0.*

**Esercizio 7.2.13.** *Sia*

$$A = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix} \in M_3(\mathbb{Z}).$$

*Si dimostri per induzione su n che*

$$A^n = \begin{pmatrix} 2^n & 3 \cdot 2^n - 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5^n \end{pmatrix}$$

*per ogni n ≥ 0.*

**Esercizio 7.2.14.** *Sia*

$$A = \begin{pmatrix} 3 & 0 & 1 \\ 0 & 10 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}).$$

*Si dimostri per induzione su n che*

$$A^n = \begin{pmatrix} 3^n & 0 & \sum_{i=0}^{n-1} 3^i \\ 0 & 10^n & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

*per ogni n ≥ 1.*

## 7.3 Matrici a scala

Siano  $F$  un campo,  $m, n \in \mathbb{N}$  interi positivi,  $M_{m,n}(F)$  l'insieme delle matrici  $m \times n$  su  $F$ . Una matrice  $A = (a_{ij}) \in M_{m,n}(F)$  è detta **a scala** se verifica le seguenti condizioni:

- per ogni  $i \in \{1, \dots, m\}$ , da  $a_{ij} = 0$  per ogni  $j \in \{1, \dots, n\}$  segue che anche  $a_{i+1,j} = 0$  per ogni  $j \in \{1, \dots, n\}$ ;
- se  $a_{ij} \neq 0$  e  $a_{ih} = 0$  per ogni  $h < j$ , allora  $a_{i+1,h} = 0$  per ogni  $h \leq j$ .

La prima condizione della definizione precedente comporta che se una riga di  $A$  è costituita da tutti 0 allora tutte le successive righe di  $A$  sono costituite da tutti 0. Il primo termine non nullo di ogni riga di una matrice a scala è detto *pivot*. Per la seconda condizione della definizione, l'elemento della riga  $(i+1)$ -esima che si trova esattamente sotto il pivot della riga  $i$ -esima è certamente 0. Inoltre l'eventuale pivot della riga  $(i+1)$ -esima si trova certamente "più a destra" di quello della riga  $i$ -esima. Per esempio, la matrice

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_{4,3}(\mathbb{Q})$$

è a scala; il pivot della prima riga è 1, il pivot della seconda riga è 3. Invece la matrice

$$B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_{4,3}(\mathbb{Q})$$

non è a scala, in quanto non verifica la seconda condizione della definizione.

Data una matrice  $A = (a_{ij}) \in M_{m,n}(F)$ , e denotate come di consueto con  $A^{(1)}, \dots, A^{(m)} \in M_{1,n}(F)$  le righe di  $A$ , si dirà che sulle righe di  $A$  è stata effettuata un'*operazione elementare* quando:

- si sono moltiplicati tutti i termini di una riga  $A^{(i)}$  di  $A$  per un elemento non nullo  $\lambda \in F$ ; per denotare questa circostanza si usa la notazione  $R^i \rightarrow \lambda R^i$ ;
- si sono scambiate di posto le due righe  $A^{(i)}$  e  $A^{(j)}$  di  $A$ ; in tal caso si utilizza la notazione  $R^i \leftrightarrow R^j$ ;
- si è sostituita la riga  $A^{(i)}$  con la riga  $A^{(i)} + \lambda A^{(j)} = (a_{i1} + \lambda a_{j1}, \dots, a_{in} + \lambda a_{jn})$  dove  $\lambda \in F$  e  $i \neq j$ ; questa circostanza si indica con  $R^i \rightarrow R^i + \lambda R^j$ .

Matrici  $A$  e  $B \in M_{m,n}(F)$  sono dette *equivalenti*, e si scrive  $A \sim B$ , se  $B$  si ottiene da  $A$  effettuando un numero finito di operazioni elementari sulle righe. In tal modo resta definita in  $M_{m,n}(F)$  una relazione binaria che, come è facile verificare, è d'equivalenza (vedi Esercizio 7.3.1). "Ridurre a scala" una matrice  $A$  significa determinare una matrice a scala  $T$  tale che  $A \sim T$ : ciò è sempre possibile, come prova il risultato che segue.

**7.3.1.** *Sia  $F$  un campo. Per ogni matrice  $A \in M_{m,n}(F)$  esiste una matrice a scala  $T \in M_{m,n}(F)$  tale che  $A \sim T$ .*

*Dimostrazione.* La matrice nulla è banalmente a scala, pertanto basterà prendere in considerazione matrici non nulle. L'asserto verrà provato per induzione sul numero  $m$  delle righe.

Se  $m = 1$ , allora  $M_{1,n}(F)$  è costituito da matrici a una riga che sono ovviamente a scala; sia quindi  $m > 1$  e si supponga per ipotesi induttiva che ogni matrice con  $h < m$  righe (ed un numero qualsiasi di colonne) sia equivalente a una matrice a scala. Data una matrice non nulla  $A \in M_{m,n}(F)$ , si può considerare il minimo indice  $j$  tale che la  $j$ -esima colonna di  $A$  non ha tutti i termini nulli e il minimo indice  $i$  tale che  $a_{ij} \neq 0$ . In altre parole si può considerare il primo termine diverso da 0 della prima colonna non nulla di  $A$ ; sia questo  $a_{ij}$ . Se  $i \neq 1$  si scambiano la prima riga e la riga  $i$ -esima, cioè si esegue l'operazione elementare  $R^i \leftrightarrow R^1$ , ottenendo la matrice equivalente

$$B = \begin{pmatrix} 0 & 0 & \dots & a_{ij} & * & \dots & * \\ 0 & 0 & \dots & * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & * & * & \dots & * \\ 0 & 0 & \dots & * & * & \dots & * \end{pmatrix}.$$

L'elemento  $a_{ij}$  è un elemento non nullo di  $F$  e quindi esiste  $a_{ij}^{-1} \in F$ ; posto  $\lambda_h = -(a_{ij}^{-1})b_{hj}$  per ogni  $h \in \{2, \dots, m\}$ , se si eseguono le  $m - 1$  operazioni elementari  $R^h \rightarrow R^h + \lambda_h R^1$  al variare di  $h \in \{2, \dots, m\}$ , si ottiene la matrice

$$C = \begin{pmatrix} 0 & 0 & \dots & a_{ij} & * & \dots & * \\ 0 & 0 & \dots & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & * & \dots & * \\ 0 & 0 & \dots & 0 & * & \dots & * \end{pmatrix}.$$

Si consideri la matrice  $D = (d_{hk}) \in M_{m-1,n-j}$  con  $d_{hk} = c_{h+1,k+j}$  per ogni  $h \in \{1, \dots, m-1\}$  e per ogni  $k \in \{1, \dots, n-j\}$ . Per ipotesi di induzione, eseguendo sulle righe di  $D$  un numero finito di operazioni elementari si ottiene una matrice a scala

$$S = \begin{pmatrix} s_{11} & \dots & s_{1,n-j} \\ s_{21} & \dots & s_{2,n-j} \\ \vdots & \ddots & \vdots \\ s_{m-1,1} & \dots & s_{m-1,n-j} \end{pmatrix}.$$

Se  $h_1, \dots, h_t$  sono gli indici delle righe di  $D$  coinvolte in tali operazioni allora eseguendo le stesse operazioni sulle righe di  $C$  di indici  $h_1 + 1, \dots, h_t + 1$  si ottiene la matrice a scala

$$T = \begin{pmatrix} 0 & 0 & \dots & a_{ij} & * & \dots & * \\ 0 & 0 & \dots & 0 & s_{11} & \dots & s_{1,n-j} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & s_{m-1,1} & \dots & s_{m-1,n-j} \end{pmatrix}$$

equivalente ad  $A$ . □

**7.3.2. Esempio.** Si voglia determinare una matrice a scala equivalente alla matrice

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & -5 & -3 \\ 0 & 1 & 1 \end{pmatrix} \in M_{4,3}(\mathbb{Q}).$$

Si noti che la prima colonna non nulla di  $A$  è la seconda e il primo elemento non nullo della prima colonna non nulla è quello di posto (3, 2). Occorre quindi scambiare la terza riga di  $A$  con la prima, cioè eseguire l'operazione elementare  $R^1 \leftrightarrow R^3$ , ottenendo:

$$B = \begin{pmatrix} 0 & -5 & -3 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

A questo punto occorre eseguire le tre operazioni elementari  $R^h \rightarrow R^h + \lambda_h R^1$  con  $\lambda_h = \frac{1}{5}b_{h2}$  per ogni  $h \in \{2, 3, 4\}$ . Poiché  $b_{22} = b_{32} = 0$  le corrispondenti operazioni elementari non hanno alcun effetto sulla matrice. Invece con l'operazione  $R^4 \rightarrow R^4 + \frac{1}{5}R^1$  si ottiene la matrice

$$C = \begin{pmatrix} 0 & -5 & -3 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 2/5 \end{pmatrix}.$$

Di qui, eseguendo le operazioni  $R^3 \rightarrow R^3 - \frac{1}{2}R^2$  e  $R^4 \rightarrow R^4 - \frac{1}{5}R^2$ , si ottiene la matrice a scala

$$T = \begin{pmatrix} 0 & -5 & -3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

che è equivalente ad  $A$  perché ottenuta da  $A$  con un numero finito di operazioni elementari sulle righe.

Siano  $F$  un campo,  $m \in \mathbb{N}$  un intero positivo, e  $I_m \in M_m(F)$  la matrice identica di ordine  $m$  su  $F$ . Le matrici che si ottengono applicando a  $I_m$  un'operazione elementare sulle righe si dicono **elementari**. La matrice elementare che si ottiene applicando a  $I_m$  l'operazione elementare  $R^h \rightarrow \lambda R^h$  con  $\lambda \in F \setminus \{0\}$ , ovvero la matrice diagonale i cui termini della diagonale principale sono tutti uguali a 1 tranne l' $h$ -esimo che è uguale a  $\lambda$ , si denota con  $E_h^\lambda$ . Si pone cioè  $E_h^\lambda := (e_{ij})$  con  $e_{hh} = \lambda$ ,  $e_{ii} = 1$  per ogni  $i \neq h$  e  $e_{ij} = 0$  per ogni  $i \neq j$ . La matrice elementare  $E_{hk}$  con  $h, k \in \{1, \dots, m\}$  è poi quella che si ottiene applicando a  $I_m$  l'operazione elementare  $R^h \leftrightarrow R^k$ , ovvero  $E_{hk} := (e_{ij})$  con  $e_{ii} = 1$  per ogni  $i \in \{1, \dots, m\} \setminus \{h, k\}$ ,  $e_{hh} = 0 = e_{kk}$ ,  $e_{hk} = 1 = e_{kh}$ , e  $e_{ij} = 0$  per ogni  $i \neq j$  con  $(i, j) \neq (h, k)$  e  $(i, j) \neq (k, h)$ . Infine si denota con  $E_{hk}^\lambda$  la matrice

elementare che si ottiene da  $I_m$  mediante l'operazione  $R^h \rightarrow R^h + \lambda R^k$ ; si pone cioè  $E_{hk}^\lambda := (e_{ij})$  con  $e_{ii} = 1$  per ogni  $i \in \{1, \dots, m\}$ ,  $e_{hk} = \lambda$ , e  $e_{ij} = 0$  per ogni  $i \neq j$  con  $(i, j) \neq (h, k)$ .

È possibile dimostrare che data una matrice  $A \in M_{m,n}(F)$ , se  $B \in M_{m,n}(F)$  si ottiene da  $A$  mediante un'operazione elementare allora  $B$  coincide con la matrice che si ottiene moltiplicando righe per colonne a sinistra  $A$  per la corrispondente matrice elementare. Si ha cioè che se  $B$  si ottiene da  $A$  mediante  $R^h \rightarrow \lambda R^h$ , allora  $B = E_h^\lambda A$ ; se  $B$  si ottiene da  $A$  mediante  $R^h \leftrightarrow R^k$  allora  $B = E_{hk} A$  e infine se  $B$  si ottiene da  $A$  mediante  $R^h \rightarrow R^h + \lambda R^k$ , allora  $B = E_{hk}^\lambda A$ . Ciò comporta che  $A \sim B$  se e solo se esiste una matrice  $E$  quadrata di ordine  $m$ , prodotto di un numero finito di matrici elementari, tale che  $B = EA$ .

**7.3.3. Esempio.** Con riferimento all'Esempio 7.3.2, risulta

$$E = E_{42}^{-\frac{1}{6}} E_{32}^{-\frac{1}{2}} E_{41}^{\frac{1}{5}} E_{13}.$$

Una matrice a scala si dice **ridotta** se i suoi pivot sono tutti 1, e tutti i termini sopra i pivot sono nulli.

**7.3.4. Sia  $F$  un campo. Per ogni matrice  $A \in M_{m,n}(F)$  esiste un'unica matrice a scala ridotta  $U \in M_{m,n}(F)$  tale che  $A \sim U$ .**

*Dimostrazione.* In primo luogo, in virtù di 7.3.1 si può assumere che  $A$  sia una matrice a scala. Detti  $a_{1j_1}, a_{2j_2}, \dots, a_{kj_k}$  i suoi pivot, mediante le operazioni elementari

$$\begin{aligned} R^1 &\rightarrow a_{1j_1}^{-1} R^1 \\ &\vdots \\ R^k &\rightarrow a_{kj_k}^{-1} R^k \end{aligned}$$

si ottiene una matrice  $B$  equivalente ad  $A$ , e i cui pivot sono

$$b_{1j_1} = b_{2j_2} = \dots = b_{kj_k} = 1.$$

A questo punto per annullare tutti i termini sopra i pivot basta eseguire le operazioni elementari seguenti:

$$\begin{aligned} R^1 &\rightarrow R^1 - b_{1j_2} R^2 \\ R^1 &\rightarrow R^1 - b_{1j_3} R^3 \\ R^2 &\rightarrow R^2 - b_{2j_3} R^3 \\ &\vdots \\ R^1 &\rightarrow R^1 - b_{1j_k} R^k \end{aligned}$$

$$\begin{aligned} R^2 &\rightarrow R^2 - b_{2j_k} R^k \\ &\vdots \\ R^{k-1} &\rightarrow R^{k-1} - b_{k-1j_k} R^k. \end{aligned}$$

Si tralascia per brevità la dimostrazione dell'unicità.  $\square$

**7.3.5. Corollario.** *Sia  $F$  un campo. Per ogni matrice  $A \in M_{m,n}(F)$  esistono una matrice a scala ridotta  $U \in M_{m,n}(F)$  e una matrice quadrata  $E \in M_m(F)$ , prodotto di un numero finito di matrici elementari, tali che  $U = EA$ .*

**7.3.6. Esempio.** Per ottenere la matrice a scala ridotta equivalente alla matrice a scala

$$T = \begin{pmatrix} 0 & -5 & -3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_{4,3}(\mathbb{Q})$$

dell'Esempio 7.3.2, occorre eseguire le operazioni elementari

$$\begin{aligned} R^1 &\rightarrow -\frac{1}{5}R^1 \\ R^2 &\rightarrow \frac{1}{2}R^2 \\ R^1 &\rightarrow R^1 - \frac{3}{5}R^2, \end{aligned}$$

ottenendo la matrice

$$U = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_{4,3}(\mathbb{Q}),$$

che è a scala ridotta ed equivalente a  $T$ . Posto

$$E = E_{12}^{-\frac{3}{5}} E_2^{\frac{1}{2}} E_1^{-\frac{1}{5}},$$

risulta ovviamente  $U = ET$ .

### Esercizi

**Esercizio 7.3.1.** *Sia  $F$  un campo. Si dimostri che ponendo  $A \sim B$  se e solo se  $B$  si ottiene da  $A$  effettuando un numero finito di operazioni elementari sulle righe, si definisce in  $M_{m,n}(F)$  una relazione d'equivalenza.*

**Esercizio 7.3.2.** Si riducano a scala le matrici

$$A = \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \\ 3 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 3 & 1 & 0 & 1 \end{pmatrix}.$$

**Esercizio 7.3.3.** Si riducano a scala le matrici

$$A = \begin{pmatrix} 1 & 2 & -3 & 0 \\ 2 & 4 & -2 & 2 \\ 3 & 6 & -4 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -2 & 3 & -1 \\ 2 & -1 & 2 & 2 \\ 3 & 1 & 2 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 6 & 3 & -4 \\ -4 & 1 & -6 \\ 1 & 2 & -5 \end{pmatrix}.$$

**Esercizio 7.3.4.** Si riducano a scala le matrici

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 5 \\ 2 & 7 & 8 \\ 0 & 9 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 3 & 0 & 0 & 4 \\ 1 & -4 & -2 & -2 \end{pmatrix}.$$

**Esercizio 7.3.5.** Si determinino le seguenti matrici elementari di ordine 3 su  $\mathbb{Q}$ :

$$E_{13}, \quad E_2^{\frac{1}{2}}, \quad E_{32}^{-5}, \quad E_{21}^3, \quad E_3^{-7}.$$

**Esercizio 7.3.6.** Dopo aver individuato una matrice a scala  $T$  equivalente alla matrice

$$A = \begin{pmatrix} 0 & 0 & -1 \\ -2 & 3 & 1 \\ 0 & 4 & -5 \\ 0 & 0 & -2 \end{pmatrix},$$

si determini la matrice  $E$  prodotto di un numero finito di matrici elementari tale che  $EA = T$ .

**Esercizio 7.3.7.** Si riducano a scala le seguenti matrici su  $\mathbb{Z}_7$ :

$$A = \begin{pmatrix} \bar{0} & \bar{5} & \bar{2} \\ \bar{3} & \bar{1} & \bar{4} \\ \bar{1} & \bar{2} & \bar{6} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{3} & \bar{0} & \bar{2} & \bar{1} \\ \bar{5} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{0} & \bar{0} & \bar{1} \end{pmatrix}.$$

**Esercizio 7.3.8.** Si determinino le matrici a scala ridotte equivalenti alle seguenti matrici su  $\mathbb{Z}_5$ :

$$A = \begin{pmatrix} \bar{3} & \bar{1} & \bar{2} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{2} & \bar{1} & \bar{2} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{3} & \bar{4} & \bar{3} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} & \bar{1} \end{pmatrix}.$$

**Esercizio 7.3.9.** Si determinino le matrici a scala ridotte equivalenti alle seguenti matrici su  $\mathbb{Q}$ :

$$A = \begin{pmatrix} 1 & 0 & -2 & 0 \\ -4 & 5 & 7 & 1 \\ 0 & 1 & 4 & 1 \\ 5 & 2 & 2 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1/3 & 1/5 & 0 \\ -2 & 1 & 2/3 \\ 3 & 2 & 2 \\ -1/6 & 0 & 0 \end{pmatrix}.$$

## 7.4 Determinante di una matrice quadrata

Sia  $A = (a_{ij}) \in M_{m,n}(R)$  una matrice  $m \times n$  su un anello commutativo  $R$ . Considerati un indice  $h \in \{1, \dots, m\}$  e un indice  $k \in \{1, \dots, n\}$ , si denota con  $A_{hk}$  la matrice  $(m-1) \times (n-1)$  che si ottiene da  $A$  eliminando la riga  $h$ -esima e la colonna  $k$ -esima. Tale matrice è detta **matrice complementare** dell'elemento  $a_{hk}$ .

Per esempio se si considera la matrice

$$A = \begin{pmatrix} 1 & 2 & 3 & 5 \\ 2 & 0 & 7 & 4 \\ 5 & 9 & 0 & 0 \end{pmatrix} \in M_{3,4}(\mathbb{Z}),$$

le matrici complementari degli elementi di posto (2, 3) e di posto (2, 4) sono rispettivamente le seguenti matrici di  $M_{2,3}(\mathbb{Z})$ :

$$A_{23} = \begin{pmatrix} 1 & 2 & 5 \\ 5 & 9 & 0 \end{pmatrix}, \quad A_{24} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 9 & 0 \end{pmatrix}.$$

Se  $A$  è una matrice quadrata di ordine  $n$ , allora per ogni  $i, j \in \{1, \dots, n\}$  la matrice  $A_{ij}$  è ancora quadrata e ha ordine  $n - 1$ .

Sia  $A \in M_n(R)$  una matrice quadrata di ordine  $n$  su un anello  $R$ . Si dice **determinante** di  $A$  lo scalare (cioè l'elemento di  $R$ ) che viene definito, per induzione su  $n$ , come segue:

$$\det A := \begin{cases} a_{11} & \text{se } n = 1, \\ \sum_{j=1}^n (-1)^{1+j} a_{1j} \det A_{1j} & \text{se } n > 1. \end{cases} \quad (7.4.1)$$

In particolare, se  $A$  è una matrice di ordine 2, posto

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

dalla (7.4.1) segue

$$\begin{aligned} \det A &= \sum_{j=1}^2 (-1)^{1+j} a_{1j} \det A_{1j} \\ &= (-1)^2 a_{11} \det(a_{22}) + (-1)^3 a_{12} \det(a_{21}) \\ &= a_{11}a_{22} - a_{12}a_{21}. \end{aligned}$$

Se invece  $A$  è una matrice di ordine 3, posto

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

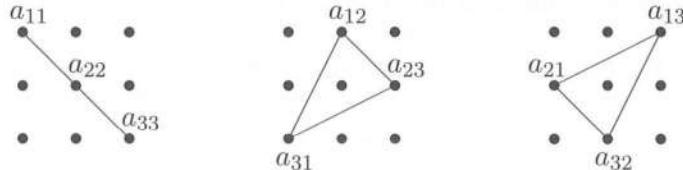
la (7.4.1) comporta che

$$\begin{aligned}\det A &= \sum_{j=1}^3 (-1)^{1+j} a_{1j} \det A_{1j} \\ &= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}).\end{aligned}$$

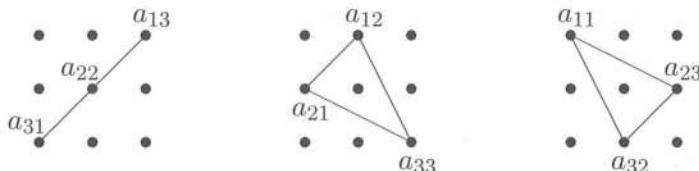
**Osservazione.** Un metodo spesso usato per il calcolo del determinante di una matrice di ordine 3 è la cosiddetta **regola di Sarrus**. In sostanza, se si vuole calcolare il determinante della matrice

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

basta eseguire la somma dei prodotti degli elementi situati sulla diagonale principale di  $A$  e di quelli situati ai vertici dei due triangoli *isosceli* che hanno un lato parallelo a tale diagonale, ossia  $a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13}$



e aggiungervi la somma degli opposti dei prodotti degli elementi situati sulla diagonale secondaria di  $A$  e di quelli situati ai vertici dei due triangoli *isosceli* che hanno un lato parallelo a quest'ultima, ossia  $-a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$



Si vede subito che così facendo si ottiene lo stesso risultato che si era ottenuto in precedenza sviluppando il determinante rispetto alla prima riga.

In alternativa, si può scrivere la matrice  $3 \times 5$  che si ottiene da  $A$  aggiungendovi una quarta colonna identica alla prima, e una quinta identica alla seconda:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{pmatrix},$$

ed eseguire la somma dei prodotti degli elementi situati sulle tre diagonali “principali” (quelle che, partendo dall’alto, vanno da sinistra a destra), e sottrarvi la

somma dei prodotti degli elementi situati sulle tre diagonali “secondarie” (quelle che, sempre partendo dall’alto, vanno da destra a sinistra): infatti così facendo si ottiene  $a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$ , che è ancora il medesimo risultato ottenuto in precedenza.

Ovviamente la regola di Sarrus è valida soltanto per i determinanti delle matrici di ordine 3.

Si può dimostrare che, per ogni matrice  $A \in M_n(R)$  e per ogni  $i \in \{1, \dots, n\}$ ,

$$\sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij} = \sum_{j=1}^n (-1)^{1+j} a_{1j} \det A_{1j} = \det A. \quad (7.4.2)$$

Se  $A$  è una matrice quadrata di ordine  $n$  su un anello  $R$  e  $i, j \in \{1, \dots, n\}$  si definisce **complemento algebrico** dell’elemento  $a_{ij}$  lo scalare

$$(-1)^{i+j} \det A_{ij}.$$

Per la (7.4.1), il determinante di  $A$  è la somma dei prodotti degli elementi della prima riga di  $A$  per i loro complementi algebrici. Per la (7.4.2), anziché la prima riga, è lecito scegliere una qualunque riga di  $A$ . Si può inoltre provare che la somma dei prodotti degli elementi di una qualsiasi colonna di  $A$  per i loro complementi algebrici uguaglia il determinante di  $A$ :

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij}, \text{ per ogni } j \in \{1, \dots, n\}. \quad (7.4.3)$$

In definitiva, quindi, il determinante di una matrice quadrata  $A$  è la somma dei prodotti degli elementi di una qualsiasi linea (cioè riga o colonna) per i loro complementi algebrici. Si potrebbe dimostrare quanto segue:

**7.4.1.** *Siano  $R$  un anello commutativo e  $A \in M_n(R)$ . Allora:*

- (i) *se  $A$  ha due righe oppure due colonne uguali allora  $\det A = 0$ ;*
- (ii) *se  $A$  possiede una riga o una colonna costituita da tutti 0 allora  $\det A = 0$ ;*
- (iii) *se  $A$  è triangolare superiore oppure triangolare inferiore allora risulta  $\det A = a_{11}a_{22} \dots a_{nn}$ ; in particolare  $\det I_n = 1$  per ogni  $n \in \mathbb{N}$ ;*
- (iv) *se  $B$  è la matrice che si ottiene da  $A$  scambiando di posto due righe o due colonne allora  $\det B = -\det A$ ;*
- (v) *se la matrice  $B$  si ottiene da  $A$  moltiplicando tutti gli elementi di una riga o di una colonna di  $A$  per uno scalare  $\lambda \in R$ , allora  $\det B = \lambda \det A$ ;*
- (vi) *se la matrice  $B$  si ottiene da  $A$  sommando a una riga (colonna) di  $A$  il prodotto di un’altra riga (colonna) di  $A$  per uno scalare  $\lambda \in R$ , allora  $\det B = \det A$ ;*
- (vii)  *$\det A = \det A^T$ .*

Sia  $R$  un anello unitario. Una matrice quadrata  $A \in M_n(R)$  è detta **non singolare** (o anche **non degenera**) se  $\det A$  è un elemento invertibile nell'anello  $R$ , **singolare** (o **degenera**) in caso contrario.

In particolare, se  $F$  è un campo, una matrice  $A \in M_n(F)$  è non singolare se e solo se  $\det A \neq 0$ . Per (iv), (v) e (vi) di 7.4.1, se  $A$  è non singolare allora ogni matrice che si ottiene da  $A$  eseguendo un'operazione elementare sulle righe di  $A$  è non singolare. Questo comporta che se  $A, B \in M_n(F)$  sono tali che  $A \sim B$ , allora  $\det A \neq 0$  se e solo se  $\det B \neq 0$  (vedi Esercizio 7.4.11).

Si può poi dimostrare il seguente:

**7.4.2. Teorema di Binet.** *Siano  $R$  un anello commutativo e  $A, B \in M_n(R)$ . Allora  $\det(AB) = (\det A)(\det B)$ .*

## Esercizi

**Esercizio 7.4.1.** *Siano  $F$  un campo,  $(\alpha_1, \alpha_2, \dots, \alpha_n) \in F^n$ . Il determinante*

$$V(\alpha_1, \alpha_2, \dots, \alpha_n) := \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}$$

*è detto determinante di Vandermonde di  $(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Si provi per induzione che per ogni  $n > 1$  risulta:*

$$V(\alpha_1, \alpha_2, \dots, \alpha_n) = \prod_{1 \leq h < k \leq n} (\alpha_k - \alpha_h).$$

**Esercizio 7.4.2.** *Si calcoli il determinante delle seguenti matrici su  $\mathbb{Z}$ :*

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & 3 \\ 2 & 3 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ -4 & 5 & 7 & 1 \\ 0 & 1 & 4 & 1 \\ 5 & 2 & 2 & 3 \end{pmatrix}.$$

**Esercizio 7.4.3.** *Considerata la matrice*

$$A = \begin{pmatrix} 1 & 7 & 3 & 5 & 0 \\ 2 & 4 & 1 & 0 & 3 \\ 3 & 1 & 0 & 2 & 1 \\ 1 & 0 & 7 & 4 & 4 \end{pmatrix} \in M_{4,5}(\mathbb{Z}),$$

*si determinino le matrici complementari  $A_{13}$ ,  $A_{24}$ ,  $A_{35}$  e  $A_{41}$ .*

**Esercizio 7.4.4.** Utilizzando la regola di Sarrus, si calcoli il determinante delle seguenti matrici di  $M_3(\mathbb{Z})$ :

$$A = \begin{pmatrix} 1 & 7 & 3 \\ 2 & 0 & 5 \\ 1 & 3 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 7 \\ 4 & 2 & 1 \end{pmatrix}.$$

**Esercizio 7.4.5.** Si calcoli il determinante della matrice

$$A = \begin{pmatrix} \bar{5} & \bar{4} & \bar{1} \\ \bar{0} & \bar{3} & \bar{0} \\ \bar{3} & \bar{5} & \bar{2} \end{pmatrix} \in M_3(\mathbb{Z}_6).$$

**Esercizio 7.4.6.** Si calcoli il determinante della matrice

$$B = \begin{pmatrix} \bar{3} & \bar{9} & \bar{5} \\ \bar{6} & \bar{0} & \bar{3} \\ \bar{4} & \bar{5} & \bar{2} \end{pmatrix} \in M_3(\mathbb{Z}_{10}).$$

**Esercizio 7.4.7.** Si calcoli il determinante delle seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 0 & 2 & 7 \\ 0 & 0 & \pi \\ 3 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 1 & -2 \\ 1 & -2 & 1 \\ -2 & 1 & -3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 4 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix}.$$

**Esercizio 7.4.8.** Utilizzando la regola di Sarrus, si calcoli il determinante della matrice

$$A = \begin{pmatrix} \bar{8} & \bar{1} & \bar{0} \\ \bar{5} & \bar{1} & \bar{4} \\ \bar{6} & \bar{6} & \bar{5} \end{pmatrix} \in M_3(\mathbb{Z}_9).$$

**Esercizio 7.4.9.** Considerata la matrice

$$A = \begin{pmatrix} -1/2 & 0 & 3 & 1/5 \\ 7 & -2 & 0 & 3 \\ 1 & 1 & -1 & 0 \\ 3/5 & -1/2 & 0 & 0 \end{pmatrix} \in M_4(\mathbb{Q}),$$

si determinino i complementi algebrici degli elementi di posto (2, 2), (1, 4), (3, 2), (2, 4).

**Esercizio 7.4.10.** Utilizzando la 7.4.1 si provi che

$$\det E_{hk} = -1, \quad \det E_h^\lambda = \lambda, \quad \det E_{hk}^\lambda = 1.$$

**Esercizio 7.4.11.** Utilizzando l'Esercizio 7.4.10 e il teorema di Binet (vedi 7.4.2) si provi che se  $A, B \in M_n(F)$  sono tali che  $A \sim B$ , allora  $A$  è non singolare se e solo se lo è  $B$ .

**Esercizio 7.4.12.** Utilizzando la 7.4.1 si calcoli rapidamente il determinante delle seguenti matrici di  $M_4(\mathbb{Q})$ :

$$A = \begin{pmatrix} 3 & 71 & 35 & -40 \\ 0 & -5 & 82 & 101 \\ 0 & 0 & 7 & 66 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 11 & 0 & 0 & 0 \\ 57 & 10 & 0 & 0 \\ 1/5 & -100 & 2 & 0 \\ 3/2 & -21 & 72 & -3 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & -14 & 6 \\ 1 & 37 & -43 & 103 \\ 0 & 0 & 0 & -5 \\ 0 & 2 & 15/4 & 73 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & 2 & 0 \\ -6 & 0 & 26 & 0 \\ 75 & 0 & -101 & -1 \\ -77 & 4 & -1/90 & 32 \end{pmatrix},$$

$$E = \begin{pmatrix} 5 & 1 & -3 & 7 \\ 21 & 76 & -32 & 28 \\ -5 & -1 & 3 & -7 \\ 54 & 65 & -99 & -89 \end{pmatrix}, \quad F = \begin{pmatrix} 201 & 7 & 21 & 14 \\ 78 & 1 & -15 & 2 \\ 1 & -15 & 17 & -30 \\ -6 & -6 & -6 & -12 \end{pmatrix},$$

$$G = \begin{pmatrix} -10 & 4 & 13 & 0 \\ 2 & -4 & 7 & 2 \\ -8 & 0 & 20 & 2 \\ 27 & 1 & 6 & -9 \end{pmatrix}, \quad H = \begin{pmatrix} -10 & -4 & -14 & 0 \\ 2 & -4 & -2 & 2 \\ -8 & 0 & -8 & 2 \\ 27 & 1 & 28 & -9 \end{pmatrix}.$$

## 7.5 Matrici invertibili

Sia  $R$  un anello unitario, e sia  $n$  un intero positivo. Come già provato in 7.2.3,  $M_n(R)$  è un anello unitario. Un elemento  $A \in M_n(R)$  si dice **matrice invertibile** se  $A$  è simmetrizzabile rispetto al prodotto righe per colonne in  $M_n(R)$ , e quindi se esiste una matrice  $B \in M_n(R)$  tale che  $AB = I_n = BA$ . Se  $A$  è invertibile una tale matrice  $B$  è unica (vedi 4.1.10); essa viene detta la **matrice inversa** di  $A$  e denotata col simbolo  $A^{-1}$ . Il risultato che segue fornisce un'utile caratterizzazione delle matrici invertibili.

**7.5.1.** Sia  $R$  un anello commutativo unitario. Una matrice  $A \in M_n(R)$  è invertibile se e solo se è non singolare. In tal caso  $A$  ha come inversa la matrice  $B = (b_{ij})$  dove

$$b_{ij} := (-1)^{i+j} \det A_{ji} (\det A)^{-1}$$

per ogni  $i, j \in \{1, \dots, n\}$ .

*Dimostrazione.* Sia  $A$  invertibile, e sia  $A^{-1}$  la sua inversa. Allora  $AA^{-1} = I_n$ , e per la (iii) di 7.4.1 risulta  $\det(AA^{-1}) = \det I_n = 1$ . Applicando il teorema di Binet (vedi 7.4.2) ne segue che  $(\det A)(\det A^{-1}) = 1$ . Dunque  $\det A$  è un elemento invertibile di  $R$ , e la matrice  $A$  è non singolare.

Viceversa, sia  $A$  non singolare. Poiché  $\det A$  è un elemento invertibile di  $R$ , si può considerare la matrice  $B$  di cui all'enunciato. Posto  $AB = P = (p_{ij})$ , per

ogni  $i, j \in \{1, \dots, n\}$  si ha

$$p_{ij} = \sum_{h=1}^n a_{ih} b_{hj} = \left( \sum_{h=1}^n a_{ih} (-1)^{h+j} \det A_{jh} \right) (\det A)^{-1}. \quad (7.5.1)$$

Se  $i = j$  allora

$$\sum_{h=1}^n a_{ih} (-1)^{h+i} \det A_{ih} = \det A$$

per (7.4.2), e quindi la (7.5.1) comporta  $p_{ii} = 1$ . Se invece  $i \neq j$ , si assuma  $i < j$  e si consideri la matrice  $C = (c_{ij})$  che si ottiene da  $A$  sostituendo la riga  $j$ -esima con la riga  $i$ -esima. Tale matrice  $C$  ha allora due righe uguali, la  $i$ -esima e la  $j$ -esima, dunque  $\det C = 0$  per la (i) di 7.4.1. Inoltre, per ogni  $h \in \{1, \dots, n\}$ , risulta banalmente  $c_{jh} = a_{ih}$  e  $C_{jh} = A_{jh}$ . Pertanto per la (7.4.3) si ha

$$0 = \det C = \sum_{h=1}^n c_{jh} (-1)^{h+j} \det C_{jh} = \sum_{h=1}^n a_{ih} (-1)^{h+j} \det A_{jh},$$

e dalla (7.5.1) segue che  $p_{ij} = 0$ . Pertanto  $P = I_n$ . Analogamente si prova che  $BA = I_n$ . Ne segue che  $A$  è invertibile, e  $B$  è la matrice inversa di  $A$ .  $\square$

Nel caso delle matrici non singolari di ordine 2, il calcolo della matrice inversa risulta particolarmente semplice.

**7.5.2. Corollario.** *Siano  $R$  un anello commutativo unitario e*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$$

*una matrice non singolare. Allora*

$$A^{-1} = \begin{pmatrix} d(\det A)^{-1} & -b(\det A)^{-1} \\ -c(\det A)^{-1} & a(\det A)^{-1} \end{pmatrix}.$$

*Dimostrazione.* Esercizio.  $\square$

Si noti che nella prima parte della dimostrazione di 7.5.1 si è in realtà provato quanto segue:

**7.5.3. Corollario.** *Sia  $R$  un anello commutativo unitario. Se  $A \in M_n(R)$  è invertibile allora  $\det A^{-1} = (\det A)^{-1}$ .*

Con  $R$  anello commutativo unitario, per ogni matrice  $A \in M_n(R)$  si definisca

$$A^* := ((-1)^{i+j} \det A_{ij}),$$

la matrice il cui termine di posto  $(i, j)$  è il complemento algebrico in  $A$  dell'elemento  $a_{ij}$ . La 7.5.1 assicura che, se  $A$  è non singolare, allora essa è invertibile e la sua inversa è la matrice

$$A^{-1} = (\det A)^{-1}(A^*)^T \quad (7.5.2)$$

che si ottiene moltiplicando la trasposta di  $A^*$  per lo scalare  $(\det A)^{-1} \in R$ .

**7.5.4. Esempio.** La matrice

$$A = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 0 & 1 \\ 4 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{Z}).$$

è non singolare, in quanto  $\det A = -1$  è un elemento invertibile in  $\mathbb{Z}$ . La 7.5.1 assicura allora che  $A$  è invertibile. Per calcolare l'inversa di  $A$  si determinerà in primo luogo la matrice  $A^*$  e, a tale scopo, i complementi algebrici dei termini di  $A$ . Si osservi che  $\det A_{11} = -1$ ,  $-\det A_{21} = -1$ ,  $\det A_{31} = 1$ ,  $-\det A_{12} = 2$ ,  $\det A_{22} = 3$ ,  $-\det A_{32} = -3$ ,  $\det A_{13} = 2$ ,  $-\det A_{23} = 1$ ,  $\det A_{33} = -2$ . Dunque

$$A^* = \begin{pmatrix} -1 & 2 & 2 \\ -1 & 3 & 1 \\ 1 & -3 & -2 \end{pmatrix},$$

e la (7.5.2) assicura che

$$A^{-1} = \begin{pmatrix} 1 & 1 & -1 \\ -2 & -3 & 3 \\ -2 & -1 & 2 \end{pmatrix}.$$

La proposizione che segue è spesso utile:

**7.5.5. Sia  $R$  un anello commutativo unitario. Con  $A, B \in M_n(R)$  risulta**

$$AB = I_n \iff BA = I_n.$$

*Dimostrazione.* Sia  $AB = I_n$ . Allora il teorema di Binet (vedi 7.4.2) e la (iii) di 7.4.1 assicurano che  $\det(AB) = (\det A)(\det B) = \det I_n = 1$ , ovvero  $\det A$  è un elemento invertibile di  $R$ , quindi  $A$  è non singolare. Allora  $A$  è invertibile per 7.5.1. Moltiplicando a sinistra per  $A^{-1}$  l'uguaglianza di partenza si ottiene  $A^{-1}(AB) = A^{-1}I_n$ , cioè  $(A^{-1}A)B = A^{-1}$  per l'associatività del prodotto righe per colonne (vedi 7.2.3). Essendo  $A^{-1}A = I_n$  si ottiene  $B = A^{-1}$ , quindi  $BA = I_n$  come volevasi.

L'implicazione opposta si dimostra in maniera analoga.  $\square$

**Osservazione.** Siano  $F$  un campo e  $A \in M_n(F)$  una matrice quadrata su  $F$  con  $\det A \neq 0$ . Allora  $A$  è non singolare, e 7.5.1 assicura che  $A$  è invertibile. Per il Corollario 7.3.5, esistono una matrice a scala ridotta  $U \in M_n(F)$  e una matrice  $E \in M_n(F)$ , prodotto di un numero finito di matrici elementari e quindi non singolare, tali che  $U = EA$ . Siccome in  $F$  non ci sono divisori dello 0 (vedi Paragrafo 6.5), il teorema di Binet (vedi 7.4.2) assicura che  $\det U \neq 0$ . Ciò comporta, in particolare, che  $U$  non può avere righe nulle (per la (ii) di 7.4.1). Dunque  $U$  ha esattamente  $n$  pivot, e pertanto  $U = I_n$  è la matrice identica. Ma allora  $EA = I_n$ , cioè  $E = A^{-1}$  in virtù di 7.5.5. Questo è quindi un metodo alternativo per determinare l'inversa di una matrice non singolare su un campo.

### 7.5.6. Esempio. La matrice

$$A = \begin{pmatrix} 3 & -1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & -2 \end{pmatrix} \in M_3(\mathbb{Q})$$

è non singolare, essendo  $\det A = -2$ . Le operazioni elementari mediante le quali si ottiene la matrice a scala ridotta equivalente ad  $A$  (che per l'osservazione precedente è  $I_3$ ) sono:

$$\begin{aligned} R^2 &\rightarrow R^2 - \frac{1}{3}R^1 \\ R^1 &\rightarrow \frac{1}{3}R^1 \\ R^2 &\rightarrow 3R^2 \\ R^3 &\rightarrow -\frac{1}{2}R^3 \\ R^1 &\rightarrow R^1 + \frac{1}{3}R^2 \\ R^1 &\rightarrow R^1 - R^3 \\ R^2 &\rightarrow R^2 - 3R^3. \end{aligned}$$

Dunque

$$A^{-1} = E_{23}^{-3} E_{13}^{-1} E_{12}^{\frac{1}{3}} E_3^{-\frac{1}{2}} E_2^3 E_1^{\frac{1}{3}} E_{21}^{-\frac{1}{3}} = \begin{pmatrix} 0 & 1 & 1/2 \\ -1 & 3 & 3/2 \\ 0 & 0 & -1/2 \end{pmatrix}.$$

## Esercizi

**Esercizio 7.5.1.** Si dimostri il Corollario 7.5.2.

**Esercizio 7.5.2.** Si stabilisca quali delle seguenti matrici su  $\mathbb{Q}$  sono invertibili, e di ciascuna di esse si determini la matrice inversa:

$$A = \begin{pmatrix} 2 & 4 & 6 \\ 4 & 5 & 6 \\ 3 & 1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 6 & 9 \\ 2 & 5 & 1 \\ 1 & 1 & 8 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -11 & 7 & 3 \\ 0 & 2 & -5 & 1 \\ 4 & -36 & 8 & 16 \\ 0 & -1 & 0 & -9 \end{pmatrix}.$$

**Esercizio 7.5.3.** Si stabilisca se la matrice

$$A = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{7} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{4} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{2} \end{pmatrix} \in M_4(\mathbb{Z}_9)$$

è invertibile e, in caso affermativo, si determini  $A^{-1}$  e si calcoli  $\det(A^{-1})$ .

**Esercizio 7.5.4.** Si stabilisca se la matrice

$$B = \begin{pmatrix} \bar{4} & \bar{3} & \bar{1} \\ \bar{5} & \bar{3} & \bar{2} \\ \bar{6} & \bar{6} & \bar{0} \end{pmatrix} \in M_3(\mathbb{Z}_7)$$

è invertibile e, in caso affermativo, si determini  $B^{-1}$  e si calcoli  $\det(B^{-1})$ .

**Esercizio 7.5.5.** Si stabilisca quali delle seguenti matrici su  $\mathbb{Z}_9$  sono invertibili, e di ciascuna di esse si determini la matrice inversa:

$$A = \begin{pmatrix} \bar{4} & \bar{0} \\ \bar{4} & \bar{4} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{3} & \bar{7} & \bar{0} \\ \bar{4} & \bar{4} & \bar{8} \\ \bar{7} & \bar{6} & \bar{5} \end{pmatrix}.$$

## 7.6 Rango di una matrice

Sia  $A = (a_{ij}) \in M_{m,n}(F)$  una matrice  $m \times n$  su di un campo  $F$ , e si denotino con  $A^{(1)}, \dots, A^{(m)}$  le sue righe e con  $A_{(1)}, \dots, A_{(n)}$  le sue colonne. Posto  $h := \min\{m, n\}$ , e fissato un intero positivo  $p \leq h$ , per ogni  $\{i_1, \dots, i_p\} \subseteq \{1, \dots, m\}$  con  $i_1 < i_2 < \dots < i_p$  e per ogni  $\{j_1, \dots, j_p\} \subseteq \{1, \dots, n\}$  con  $j_1 < j_2 < \dots < j_p$ , si dice **sottomatrice** quadrata di  $A$  di ordine  $p$  la matrice

$$A_{j_1, \dots, j_p}^{i_1, \dots, i_p} = \begin{pmatrix} a_{i_1 j_1} & \dots & a_{i_1 j_p} \\ \vdots & \ddots & \vdots \\ a_{i_p j_1} & \dots & a_{i_p j_p} \end{pmatrix}$$

i cui elementi sono tutti e soli gli elementi di  $A$  che appartengono simultaneamente a una delle righe  $A^{(i_1)}, \dots, A^{(i_p)}$  e a una delle colonne  $A_{(j_1)}, \dots, A_{(j_p)}$ . Il determinante di una tale sottomatrice di  $A$  è detto **minore** di ordine  $p$  della matrice considerata.

**7.6.1. Esempio.** Si consideri la matrice

$$A = \begin{pmatrix} 0 & -2 & 3 \\ 1 & 1 & -5 \\ 4 & 7 & 11 \\ -1 & 0 & 0 \end{pmatrix} \in M_{4,3}(\mathbb{Q}).$$

Le sottomatrici quadrate di ordine 3 di  $A$  sono:

$$\begin{aligned} A_{1,2,3}^{1,2,3} &= \begin{pmatrix} 0 & -2 & 3 \\ 1 & 1 & -5 \\ 4 & 7 & 11 \end{pmatrix}, & A_{1,2,3}^{1,2,4} &= \begin{pmatrix} 0 & -2 & 3 \\ 1 & 1 & -5 \\ -1 & 0 & 0 \end{pmatrix}, \\ A_{1,2,3}^{1,3,4} &= \begin{pmatrix} 0 & -2 & 3 \\ 4 & 7 & 11 \\ -1 & 0 & 0 \end{pmatrix}, & A_{1,2,3}^{2,3,4} &= \begin{pmatrix} 1 & 1 & -5 \\ 4 & 7 & 11 \\ -1 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Quindi i minori di ordine 3 di  $A$  sono:

$$\det A_{1,2,3}^{1,2,3} = 71, \quad \det A_{1,2,3}^{1,2,4} = -7, \quad \det A_{1,2,3}^{1,3,4} = 43, \quad \det A_{1,2,3}^{2,3,4} = -46.$$

Si osservi che se  $A$  è una matrice quadrata di ordine  $n$  allora  $\det A$  è l'unico minore di ordine  $n$  di  $A$ .

Considerata una matrice  $A \in M_{m,n}(F)$ , si dice **rango** di  $A$  il numero naturale non negativo  $\rho(A)$  definito come il massimo ordine di un minore non nullo di  $A$  se  $A$  non è la matrice nulla, 0 se  $A$  è la matrice nulla.

Dalla definizione segue immediatamente che  $\rho(A) \leq \min\{m, n\}$ ; inoltre se  $A$  è quadrata di ordine  $n$  allora  $\rho(A) = n$  se e solo se  $\det A \neq 0$ .

La matrice  $A$  di cui all'Esempio 7.6.1 ha rango 3. Infatti  $A$  possiede minori di ordine 3 non nulli, e ovviamente non possiede minori di ordine maggiore di 3.

**7.6.2.** Sia  $A \in M_{m,n}(F)$ , e sia  $0 < h < \min\{m, n\}$ . Allora  $\rho(A) = h$  se e solo se  $A$  possiede un minore non nullo di ordine  $h$  e tutti i minori di ordine  $h+1$  di  $A$  sono nulli.

*Dimostrazione.* Se  $\rho(A) = h$ , per definizione, tutti i minori di ordine  $h+1$  di  $A$  sono nulli. Viceversa, si assumano nulli tutti i minori di  $A$  di ordine  $h+1$ , e sia  $B$  una sottomatrice quadrata di  $A$  di ordine  $h+2$ . Allora  $\det B = 0$ , in quanto per (7.4.2)  $\det B$  è somma di prodotti in ciascuno dei quali compare come fattore un minore di  $A$  di ordine  $h+1$ , che è nullo per ipotesi. Dunque sono nulli tutti i minori di ordine  $h+2$  di  $A$ . Allo stesso modo si prova che sono allora nulli tutti i minori di ordine  $h+3$ . Iterando il ragionamento, tutti i minori di  $A$  di ordine maggiore di  $h$  risultano nulli, quindi  $\rho(A) = h$ .  $\square$

**Osservazione.** Si potrebbe dimostrare che se un minore  $\det A_{j_1, \dots, j_h}^{i_1, \dots, i_h}$  di  $A$  è non nullo, per poter dire che  $A$  ha rango  $h$  non è necessario verificare che sono nulli

tutti i minori di ordine  $h + 1$ , ma basta considerare solo alcuni di essi, e precisamente i cosiddetti **minori orlati** di  $\det A_{j_1, \dots, j_h}^{i_1, \dots, i_h}$ , ovvero i determinanti delle sottomatrici quadrate di ordine  $h + 1$  di  $A$  che possiedono  $\det A_{j_1, \dots, j_h}^{i_1, \dots, i_h}$  come minore di ordine  $h$ .

**7.6.3. Esempio.** Si consideri la matrice

$$A = \begin{pmatrix} -3 & 0 & 4 & 7 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in M_{5,4}(\mathbb{Q}).$$

Tale matrice ha rango 2. Per verificarlo basta osservare che  $A$  possiede un minore non nullo di ordine 2, per esempio

$$\det \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix} = -3,$$

e inoltre tutti i minori orlati di tale minore, e precisamente

$$\det \begin{pmatrix} -3 & 0 & 4 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \det \begin{pmatrix} -3 & 0 & 7 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

sono nulli.

Si potrebbe anche dimostrare che:

**7.6.4. Il rango di una matrice a scala coincide con il numero dei suoi pivot.**

E inoltre:

**7.6.5. Matrici equivalenti hanno lo stesso rango.**

Le 7.6.4 e 7.6.5 forniscono un ulteriore metodo per calcolare il rango di una matrice. Basta infatti individuare una matrice a scala equivalente alla matrice data e poi contarne i pivot.

## Esercizi

**Esercizio 7.6.1.** Si riducano a scala le seguenti matrici su  $\mathbb{Q}$ :

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 5 \\ 2 & 7 & 8 \\ 0 & 9 & 4 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 3 & 0 & 0 & 4 \\ 1 & -4 & -2 & -2 \end{pmatrix},$$

e se ne determini il rango.

**Esercizio 7.6.2.** Si riducano a scala le seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \\ 3 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 3 & 1 & 0 & 1 \end{pmatrix},$$

e se ne determini il rango.

**Esercizio 7.6.3.** Si calcoli il rango delle seguenti matrici su  $\mathbb{Q}$ :

$$C = \begin{pmatrix} 1 & 3 & 2 \\ 5 & 0 & 1 \\ 2 & 9 & 0 \\ 2 & 6 & 4 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 & 3 & 2 \\ 0 & 1 & 0 & 1 \\ 2 & 4 & 6 & 4 \end{pmatrix}.$$

**Esercizio 7.6.4.** Si determini, in funzione del parametro reale  $t$ , il rango della matrice

$$M = \begin{pmatrix} 1 & t & 2 \\ t & 1 & 2 \end{pmatrix} \in M_{2,3}(\mathbb{R}).$$

**Esercizio 7.6.5.** Si determini il rango della matrice

$$A = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in M_{5,4}(\mathbb{R}).$$

**Esercizio 7.6.6.** Sia  $F$  un campo, e si consideri la matrice

$$A = \begin{pmatrix} a & b & c \\ 1 & 1 & 1 \end{pmatrix} \in M_{2,3}(F).$$

Si stabiliscano le condizioni cui devono soddisfare  $a, b, c \in F$  affinché si abbia  $\rho(A) = 1$ , e affinché si abbia  $\rho(A) = 2$ .

## 7.7 Sistemi di equazioni lineari

Sia  $F$  un campo, e sia

$$\left\{ \begin{array}{l} a_{11}x_1 + \cdots + a_{1n}x_n = y_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = y_2 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = y_m \end{array} \right. \quad (7.7.1)$$

un sistema di  $m$  equazioni lineari in  $n$  incognite a coefficienti in  $F$ . Al sistema (7.7.1) restano associate la matrice

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in M_{m,n}(F),$$

detta **matrice incompleta** del sistema, e la matrice

$$A' = \begin{pmatrix} a_{11} & \dots & a_{1n} & y_1 \\ a_{21} & \dots & a_{2n} & y_2 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & y_m \end{pmatrix} \in M_{m,n+1}(F),$$

che prende invece il nome di **matrice completa** del sistema. Denotate con

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(F)$$

la matrice delle **incognite**, e con

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} \in M_{m,1}(F)$$

la matrice dei **termini noti**, per il sistema (7.7.1) si può utilizzare la notazione compatta

$$AX = Y,$$

dove il prodotto è, ovviamente, righe per colonne. Se  $Y$  è la matrice nulla allora il sistema è detto **omogeneo**. Il sistema lineare (7.7.1) è detto **compatibile** se ammette almeno una **soluzione**, cioè se esistono elementi  $c_1, \dots, c_n \in F$  tali che

$$\left\{ \begin{array}{l} a_{11}c_1 + \dots + a_{1n}c_n = y_1 \\ a_{21}c_1 + \dots + a_{2n}c_n = y_2 \\ \vdots \\ a_{m1}c_1 + \dots + a_{mn}c_n = y_m, \end{array} \right.$$

ovvero una matrice

$$C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in M_{n,1}(F)$$

tale che

$$AC = Y.$$

Un sistema lineare omogeneo è sempre compatibile perché ammette sempre almeno una soluzione, ovvero la matrice nulla. Un sistema lineare che non sia compatibile è detto *incompatibile*. Sistemi lineari che ammettono le stesse soluzioni sono detti *equivalenti*.

### Metodo di Cramer

In questa sezione si considerano sistemi di equazioni lineari in cui il numero delle equazioni coincide con quello delle incognite e quindi sistemi del tipo

$$AX = Y$$

dove la matrice incompleta  $A \in M_n(F)$  è quadrata di ordine  $n$ .

**7.7.1. Teorema di Cramer.** *Sia  $n = m$ . Allora  $\det A \neq 0$  se e solo se il sistema lineare (7.7.1) è compatibile e ammette un'unica soluzione, data da  $A^{-1}Y$ .*

*Dimostrazione.* Se  $\det A \neq 0$ , allora  $A$  è invertibile per cui si può considerare  $A^{-1}$  e quindi anche  $C := A^{-1}Y$ . Allora

$$AC = A(A^{-1}Y) = (AA^{-1})Y = I_n Y = Y,$$

dunque  $C$  è soluzione del sistema. Per verificare l'unicità si supponga che  $D \in M_{n,1}(F)$  sia soluzione del sistema, cioè risulti  $AD = Y$ . Allora

$$D = I_n D = (A^{-1}A)D = A^{-1}(AD) = A^{-1}Y = C,$$

come volevasi. L'altra implicazione verrà dimostrata nel Paragrafo 8.7 (vedi Esercizio 8.7.1).  $\square$

Nella pratica, l'unica soluzione del sistema lineare (7.7.1) con  $n = m$  e  $\det A \neq 0$  viene spesso determinata utilizzando la seguente:

**7.7.2. Regola di Cramer.** *Sia  $n = m$ . Se  $\det A \neq 0$  allora l'unica soluzione del sistema lineare (7.7.1) è la matrice*

$$C = \begin{pmatrix} \det B_1(\det A)^{-1} \\ \vdots \\ \det B_n(\det A)^{-1} \end{pmatrix},$$

*dove, per ogni  $i \in \{1, \dots, n\}$ ,  $B_i$  è la matrice che si ottiene da  $A$  sostituendo alla colonna  $i$ -esima la colonna  $Y$  dei termini noti.*

*Dimostrazione.* Sia

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

soluzione di (7.7.1). Per il teorema di Cramer (vedi 7.7.1) risulta  $C = A^{-1}Y$ , quindi da 7.5.1 segue che per ogni  $i \in \{1, \dots, n\}$  si ha

$$c_i = \sum_{h=1}^n (-1)^{i+h} \det A_{hi} (\det A)^{-1} y_h.$$

Da qui, applicando la (7.4.3), si ottiene subito

$$c_i = \det B_i (\det A)^{-1},$$

come volevasi.  $\square$

**7.7.3. Esempio.** Il sistema lineare di 3 equazioni in 3 incognite a coefficienti in  $\mathbb{Q}$

$$\begin{cases} 4x_1 + x_2 - 5x_3 = 0 \\ -2x_2 + 3x_3 = -4 \\ -6x_1 + 7x_3 = 5 \end{cases}$$

ha matrice incompleta

$$A = \begin{pmatrix} 4 & 1 & -5 \\ 0 & -2 & 3 \\ -6 & 0 & 7 \end{pmatrix}.$$

Poiché  $\det A = -14 \neq 0$ , per il teorema di Cramer (vedi 7.7.1) il sistema ammette un'unica soluzione, data da  $A^{-1}Y$ . L'inversa di  $A$  è la matrice

$$A^{-1} = \begin{pmatrix} 1 & 1/2 & 1/2 \\ 9/7 & 1/7 & 6/7 \\ 6/7 & 3/7 & 4/7 \end{pmatrix},$$

e quindi la soluzione del sistema è

$$C = A^{-1}Y = \begin{pmatrix} 1/2 \\ 26/7 \\ 8/7 \end{pmatrix}.$$

I tre termini  $c_1, c_2, c_3$  di  $C$  possono essere agevolmente calcolati utilizzando la regola di Cramer (vedi 7.7.2), ottenendo:

$$c_1 = \det \begin{pmatrix} 0 & 1 & -5 \\ -4 & -2 & 3 \\ 5 & 0 & 7 \end{pmatrix} (\det A)^{-1} = \frac{1}{2}$$

$$c_2 = \det \begin{pmatrix} 4 & 0 & -5 \\ 0 & -4 & 3 \\ -6 & 5 & 7 \end{pmatrix} (\det A)^{-1} = \frac{26}{7}$$

$$c_3 = \det \begin{pmatrix} 4 & 1 & 0 \\ 0 & -2 & -4 \\ -6 & 0 & 5 \end{pmatrix} (\det A)^{-1} = \frac{8}{7}.$$

### Metodo di Gauss-Jordan

In questa sezione si illustrerà un metodo per stabilire la compatibilità, e quindi risolvere, un sistema

$$AX = Y \quad (7.7.2)$$

di  $m$  equazioni lineari in  $n$  incognite a coefficienti in un campo  $F$ . Indicata con  $A'$  la matrice completa del sistema (7.7.2), la 7.3.1 assicura che esiste una matrice a scala  $Q \in M_{m,n+1}(F)$  tale che  $A' \sim Q$ . Denotata con  $P \in M_{m,n}(F)$  la matrice le cui colonne sono le prime  $n$  colonne di  $Q$ , e con

$$D = \begin{pmatrix} d_1 \\ \vdots \\ d_m \end{pmatrix} \in M_{m,1}(F)$$

l'ultima colonna di  $Q$ , ovviamente anche  $P$  è a scala, e si dimostra che il sistema

$$PX = D \quad (7.7.3)$$

è equivalente al sistema (7.7.2).

Denotati con  $\rho(P)$  e  $\rho(Q)$  il numero dei pivot di  $P$  e di  $Q$  rispettivamente, risulta  $\rho(Q) = \rho(P)$  oppure  $\rho(Q) = \rho(P) + 1$ .

Se  $\rho(Q) = \rho(P) + 1$ , allora nel sistema (7.7.3) vi è un'equazione del tipo  $0 = d_i$ , con  $d_i$  non nullo, che non ha soluzioni. Pertanto in tal caso il sistema (7.7.3) non ammette soluzioni, e quindi anche il sistema (7.7.2) è incompatibile.

Se invece  $\rho(Q) = \rho(P) = t$  allora si dimostra che il sistema (7.7.3) può essere riscritto nella forma

$$\left\{ \begin{array}{rcl} p_{1j_1}x_{j_1} + p_{1j_2}x_{j_2} + \cdots + p_{1j_t}x_{j_t} + p_{1j_{t+1}}x_{j_{t+1}} + \cdots + p_{1j_n}x_{j_n} & = & d_1 \\ p_{2j_2}x_{j_2} + \cdots + p_{2j_t}x_{j_t} + p_{2j_{t+1}}x_{j_{t+1}} + \cdots + p_{2j_n}x_{j_n} & = & d_2 \\ \vdots & & \vdots \\ p_{tj_t}x_{j_t} + p_{tj_{t+1}}x_{j_{t+1}} + \cdots + p_{tj_n}x_{j_n} & = & d_t \end{array} \right. \quad (7.7.4)$$

dove  $p_{1j_1}, p_{2j_2}, \dots, p_{tj_t}$  sono i pivot. Se si pone

$$x_{j_{t+1}} = k_{j_{t+1}}, \dots, x_{j_n} = k_{j_n},$$

dove  $k_{j_{t+1}}, \dots, k_{j_n}$  sono elementi di  $F$  arbitrariamente fissati, il sistema (7.7.4) diventa

$$\left\{ \begin{array}{rcl} p_{1j_1}x_{j_1} + p_{1j_2}x_{j_2} + \cdots + p_{1j_t}x_{j_t} & = & d_1 - p_{1j_{t+1}}k_{j_{t+1}} - \cdots - p_{1j_n}k_{j_n} \\ p_{2j_2}x_{j_2} + \cdots + p_{2j_t}x_{j_t} & = & d_2 - p_{2j_{t+1}}k_{j_{t+1}} - \cdots - p_{2j_n}k_{j_n} \\ \vdots \\ p_{tj_t}x_{j_t} & = & d_t - p_{tj_{t+1}}k_{j_{t+1}} - \cdots - p_{tj_n}k_{j_n}, \end{array} \right. \quad (7.7.5)$$

la cui matrice incompleta  $T$  è quadrata di ordine  $t$  e triangolare superiore, con tutti i termini della diagonale principale non nulli. Per la (iii) di 7.4.1, risulta  $\det T \neq 0$ . Per il teorema di Cramer (vedi 7.7.1), il sistema (7.7.5) ammette allora un'unica soluzione, che può essere facilmente determinata procedendo come segue. Dall'ultima equazione di (7.7.5) si ottiene subito

$$x_{j_t} = p_{tj_t}^{-1}(d_t - p_{tj_{t+1}}k_{j_{t+1}} - \cdots - p_{tj_n}k_{j_n}).$$

Sostituendo nella penultima equazione il valore così ottenuto per  $x_{j_t}$  si determina poi il valore di  $x_{j_{t-1}}$ . Risalendo in questo modo si determinano i valori di  $x_{j_{t-2}}, \dots, x_{j_1}$  che soddisfano il sistema (7.7.5). In tal modo si ottiene un'unica soluzione del sistema (7.7.2) per ogni scelta dei parametri  $k_{j_{t+1}}, \dots, k_{j_n} \in F$ .

**7.7.4. Esempio.** Il sistema di 3 equazioni lineari in 3 incognite su  $\mathbb{Q}$

$$\left\{ \begin{array}{l} x_1 + 3x_2 - x_3 = 0 \\ -6x_2 + 2x_3 = 1 \\ 2x_1 + 6x_2 - 2x_3 = -1 \end{array} \right. \quad (7.7.6)$$

ha matrice completa

$$A' = \begin{pmatrix} 1 & 3 & -1 & 0 \\ 0 & -6 & 2 & 1 \\ 2 & 6 & -2 & -1 \end{pmatrix},$$

che è equivalente alla matrice a scala

$$Q = \begin{pmatrix} 1 & 3 & -1 & 0 \\ 0 & -6 & 2 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Il sistema (7.7.6) è pertanto equivalente al sistema

$$\left\{ \begin{array}{l} x_1 + 3x_2 - x_3 = 0 \\ -6x_2 + 2x_3 = 1 \\ 0 = -1. \end{array} \right.$$

Quest'ultimo, contenendo l'equazione  $0 = -1$ , è incompatibile. Pertanto il sistema (7.7.6) è privo di soluzioni. Si noti che, posto

$$P = \begin{pmatrix} 1 & 3 & -1 \\ 0 & -6 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

risulta  $2 = \rho(P) < \rho(Q) = 3$ .

**7.7.5. Esempio.** Il sistema di 3 equazioni lineari in 4 incognite su  $\mathbb{Q}$

$$\begin{cases} x_1 + 2x_2 + x_4 = 2 \\ 2x_1 + 3x_2 + 4x_3 - x_4 = 1 \\ -x_1 + 5x_2 - x_3 + 2x_4 = 2 \end{cases} \quad (7.7.7)$$

ha matrice completa

$$A' = \begin{pmatrix} 1 & 2 & 0 & 1 & 2 \\ 2 & 3 & 4 & -1 & 1 \\ -1 & 5 & -1 & 2 & 2 \end{pmatrix},$$

che è equivalente alla matrice a scala

$$Q = \begin{pmatrix} 1 & 2 & 0 & 1 & 2 \\ 0 & -1 & 4 & -3 & -3 \\ 0 & 0 & 27 & -18 & -17 \end{pmatrix}.$$

Dunque il sistema (7.7.7) è equivalente al sistema

$$\begin{cases} x_1 + 2x_2 = -k_4 + 2 \\ -x_2 + 4x_3 = 3k_4 - 3 \\ 27x_3 = 18k_4 - 17. \end{cases} \quad (7.7.8)$$

Per ogni fissato  $k_4 = t \in \mathbb{Q}$ ,

$$c_3 = \frac{18t - 17}{27}$$

è soluzione dell'ultima equazione di (7.7.8). Sostituendo tale valore al posto di  $x_3$  nell'ultima equazione si ricava

$$c_2 = \frac{13 - 9t}{27},$$

e quindi dalla prima equazione si ottiene

$$c_1 = \frac{28 - 9t}{27}.$$

Per ogni  $t \in \mathbb{Q}$  il sistema (7.7.8), e quindi il sistema (7.7.7), ammette l'unica soluzione

$$C_t = \begin{pmatrix} (28 - 9t)/27 \\ (13 - 9t)/27 \\ (18t - 17)/27 \\ t \end{pmatrix}.$$

Per esempio, se si sceglie  $t = 1$ , l'unica soluzione di (7.7.7) è

$$C_1 = \begin{pmatrix} 19/27 \\ 4/27 \\ 1/27 \\ 1 \end{pmatrix}.$$

## Esercizi

**Esercizio 7.7.1.** Si risolva con la regola di Cramer il seguente sistema lineare su  $\mathbb{Q}$ :

$$\begin{cases} x - y + z = 1 \\ 2x + z = 0 \\ 3x + y = 2. \end{cases}$$

**Esercizio 7.7.2.** Si risolva con la regola di Cramer il seguente sistema lineare su  $\mathbb{Z}_{13}$ :

$$\begin{cases} x - y + z = \bar{0} \\ x + \bar{2}z = \bar{1} \\ \bar{2}x + \bar{3}y = \bar{1}. \end{cases}$$

**Esercizio 7.7.3.** Si risolvano con il metodo di Cramer i seguenti sistemi di equazioni lineari su  $\mathbb{Z}_{11}$ :

$$\begin{cases} \bar{6}x + \bar{5}y = \bar{4} \\ \bar{4}x + \bar{3}y = \bar{2}, \end{cases} \quad \begin{cases} \bar{5}x + \bar{6}y = \bar{2} \\ \bar{4}x + y = \bar{3}. \end{cases}$$

**Esercizio 7.7.4.** Si risolvano con il metodo di Cramer i seguenti sistemi di equazioni lineari su  $\mathbb{Z}_5$ :

$$\begin{cases} \bar{2}x + y = \bar{2} \\ y + \bar{2}z = \bar{3} \\ \bar{4}x + \bar{3}y + \bar{4}z = \bar{0}, \end{cases} \quad \begin{cases} \bar{2}x + \bar{2}y = \bar{0} \\ \bar{3}x + y = \bar{4}. \end{cases}$$

**Esercizio 7.7.5.** Considerati i seguenti sistemi di equazioni lineari su  $\mathbb{Q}$ , li si risolvano in più modi, una volta utilizzando il metodo di Cramer, l'altra il metodo di Gauss-Jordan:

$$\begin{cases} -2x + 3y - z = 1 \\ x + 2y - z = 4 \\ -2x - y + z = -3, \end{cases} \quad \begin{cases} 2x + 4y + 6z = 2 \\ x + 2z = 0 \\ 2x + 3y - z = -5. \end{cases}$$

**Esercizio 7.7.6.** Considerati i seguenti sistemi di equazioni lineari su  $\mathbb{Z}_5$ , li si risolvano in più modi, una volta utilizzando il metodo di Cramer, l'altra il metodo di Gauss-Jordan:

$$\begin{cases} \bar{2}x + \bar{3}y + z = \bar{1} \\ x + \bar{2}y + z = \bar{4} \\ \bar{2}x + y + z = \bar{3}, \end{cases} \quad \begin{cases} \bar{3}x + \bar{2}y + \bar{2}z = \bar{1} \\ x + \bar{4}z = \bar{2} \\ x + y + z = \bar{3}. \end{cases}$$

**Esercizio 7.7.7.** Si risolva con il metodo di Gauss-Jordan il seguente sistema lineare su  $\mathbb{Q}$ :

$$\begin{cases} 3x + 4y - z - 3t = 2 \\ x + y - z - 2t = 0 \\ x - y + z + 4t = 2 \\ x - y - z + t = 2. \end{cases}$$

**Esercizio 7.7.8.** Si stabilisca se i seguenti sistemi lineari omogenei su  $\mathbb{Q}$  ammettono o meno soluzioni non banali:

$$\begin{cases} x - z = 0 \\ 7x - 2y + 5z = 0 \\ 2x - 2y + 10z = 0, \end{cases} \quad \begin{cases} 7x - 2y + 5t = 0 \\ 4y + z = 0 \\ z + 2t = 0 \\ x + 3y + z = 0. \end{cases}$$

**Esercizio 7.7.9.** Si risolva il seguente sistema lineare su  $\mathbb{Q}$ :

$$\begin{cases} x + 2y - z + t = 2 \\ y + 3z + 2t = -1 \\ x - z + t = 0 \\ x + y + 2z + 3t = -1. \end{cases}$$

**Esercizio 7.7.10.** Si risolva con il metodo di Gauss-Jordan il seguente sistema lineare su  $\mathbb{Z}_{11}$ :

$$\begin{cases} x + \bar{3}y + z - w = \bar{1} \\ \bar{3}x + \bar{9}y + \bar{4}z + w = \bar{1} \\ \bar{2}x + y + \bar{5}z + \bar{2}w = \bar{0}. \end{cases}$$

**Esercizio 7.7.11.** Si risolvano con il metodo di Gauss-Jordan i seguenti sistemi di equazioni lineari su  $\mathbb{Q}$ :

$$\begin{cases} 2y - 4z + t = 1 \\ x - 3y - z + t = 0 \\ x - y + 4z - 2t = -1, \end{cases} \quad \begin{cases} 5x + 3y - 2z = 1 \\ y - 2z = -2 \\ y + 2z = 1. \end{cases}$$

**Esercizio 7.7.12.** Si stabilisca se il seguente sistema lineare su  $\mathbb{Z}_{13}$  è compatibile:

$$\begin{cases} \bar{2}x_1 - x_2 + \bar{4}x_3 + x_4 = -\bar{2} \\ -\bar{2}x_1 + x_2 - \bar{7}x_3 + x_4 = -\bar{1} \\ \bar{4}x_1 - \bar{2}x_2 + \bar{5}x_3 + \bar{4}x_4 = \bar{7}. \end{cases}$$

**Esercizio 7.7.13.** Si risolva il seguente sistema lineare su  $\mathbb{R}$ :

$$\begin{cases} x + y + z = 2 \\ 2x + 3y - z = 8 \\ x - y - z = -8. \end{cases}$$

**Esercizio 7.7.14.** Si stabilisca se il seguente sistema lineare su  $\mathbb{R}$  è compatibile:

$$\begin{cases} x + y - z + 2t = 10 \\ 3x - y + 7z - 4t = 1 \\ -5x + 3y - 15z - 6t = 9. \end{cases}$$

**Esercizio 7.7.15.** Si risolva il seguente sistema lineare su  $\mathbb{Q}$ :

$$\begin{cases} x + 2z = 1 \\ -x + 3y + z = 0 \\ x + 7z = 1. \end{cases}$$

**Esercizio 7.7.16.** Si risolva il seguente sistema lineare su  $\mathbb{Z}_{11}$ :

$$\begin{cases} \bar{2}y + \bar{3}z - \bar{4}t = -\bar{1} \\ \bar{2}z + \bar{3}t = \bar{4} \\ \bar{2}x + \bar{2}y - \bar{5}z + \bar{2}t = \bar{4} \\ \bar{2}x - \bar{6}z + \bar{9}t = \bar{7}. \end{cases}$$

**Esercizio 7.7.17.** Si risolva il seguente sistema lineare su  $\mathbb{Q}$ :

$$\begin{cases} x + 7y + 3z = 2 \\ -x + 2z = -1 \\ 3x + y + z = 1. \end{cases}$$

**Esercizio 7.7.18.** Si risolva il seguente sistema lineare su  $\mathbb{Z}_5$ :

$$\begin{cases} x + \bar{2}y + \bar{3}z = -\bar{1} \\ y + \bar{2}z = -\bar{2} \\ \bar{2}x + \bar{3}y + \bar{4}z = \bar{0}. \end{cases}$$

**Esercizio 7.7.19.** Si risolva il seguente sistema lineare su  $\mathbb{Z}_7$ :

$$\begin{cases} -\bar{3}x - \bar{3}y - \bar{3}z = -\bar{3} \\ -\bar{2}x + \bar{2}y + z = \bar{0} \\ x - \bar{3}y + \bar{3}z = \bar{0}. \end{cases}$$

## 7.8 Autovalori e autovettori di una matrice

Sia  $F$  un campo e sia  $A \in M_n(F)$  una matrice quadrata di ordine  $n$  su  $F$ . Uno scalare  $\lambda \in F$  è detto **autovalore** per  $A$  se esiste una  $n$ -upla  $(v_1, \dots, v_n) \in F^n$  di elementi di  $F$  non tutti nulli tale che, posto

$$V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(F),$$

risulta

$$AV = \lambda V.$$

Se ciò accade,  $V$  (o anche  $(v_1, \dots, v_n)$ ) è detto **autovettore** di  $A$  relativo all'autovalore  $\lambda$ . Si comincerà illustrando le proprietà elementari di autovalori e autovettori.

**7.8.1.** *Ogni autovettore di una matrice  $A \in M_n(F)$  è relativo a un unico autovalore di  $A$ .*

*Dimostrazione.* Sia  $V$  un autovettore di  $A$ . Se  $AV = \lambda V$  e  $AV = \mu V$  allora  $\lambda V = \mu V$ , da cui  $(\lambda - \mu)V = 0$ , cioè

$$\begin{pmatrix} (\lambda - \mu)v_1 \\ \vdots \\ (\lambda - \mu)v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

il che comporta che  $(\lambda - \mu)v_i = 0$  per ogni  $i \in \{1, \dots, n\}$ . Per ipotesi  $v_1, \dots, v_n$  non sono tutti nulli, ovvero esiste  $j \in \{1, \dots, n\}$  tale che  $v_j \neq 0$ . Allora da  $(\lambda - \mu)v_j = 0$  e  $v_j \neq 0$  segue  $(\lambda - \mu) = 0$ , cioè  $\lambda = \mu$ .  $\square$

**7.8.2.** *Siano  $F$  un campo e  $A \in M_n(F)$ . Un elemento  $\lambda \in F$  è autovalore per  $A$  se e solo se  $\det(A - \lambda I_n) = 0$ .*

*Dimostrazione.* Per definizione,  $\lambda$  è autovalore per  $A$  se e solo se esiste una matrice non nulla  $V \in M_{n,1}(F)$  tale che  $AV = \lambda V$ , cioè tale che  $AV = (\lambda I_n)V$ , ossia  $AV - (\lambda I_n)V = (A - \lambda I_n)V = 0$ . Pertanto  $\lambda$  è un autovalore per  $A$  se e solo se il sistema lineare omogeneo

$$(A - \lambda I_n)X = 0 \tag{7.8.1}$$

ammette una soluzione non banale  $V$ . Il sistema lineare (7.8.1) è omogeneo, quindi ammette certamente almeno la soluzione nulla. Essendo un sistema lineare di  $n$  equazioni in  $n$  incognite, per il teorema di Cramer (vedi 7.7.1) tale sistema

ammette un'unica soluzione (e quindi solo la soluzione nulla) se e solo se risulta  $\det(A - \lambda I_n) \neq 0$ . Ciò comporta che  $\lambda$  è un autovalore per  $A$  se e solo se  $\det(A - \lambda I_n) = 0$ .  $\square$

Lo sviluppo del determinante

$$\det(A - xI_n)$$

produce un polinomio  $p_A(x) \in F[x]$  di grado  $n$  (vedi Esercizio 7.8.1), detto **polinomio caratteristico** della matrice  $A$ . Pertanto:

**7.8.3. Corollario.** *Gli autovalori di  $A \in M_n(F)$  sono tutte e sole le radici in  $F$  del polinomio caratteristico  $p_A(x)$  di  $A$ .*

**7.8.4. Esempio.** La matrice

$$A = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & -2 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 8 & -4 & -1 \end{pmatrix} \in M_4(\mathbb{Q})$$

ha polinomio caratteristico

$$\begin{aligned} p_A(x) &= \det(A - xI_4) \\ &= \det \begin{pmatrix} 3-x & 0 & 0 & 0 \\ 0 & 3-x & -2 & 0 \\ 0 & 0 & -1-x & 0 \\ 0 & 8 & -4 & -1-x \end{pmatrix} \\ &= (3-x)^2(1+x)^2. \end{aligned}$$

Le radici di  $p_A(x)$  in  $\mathbb{Q}$ , e quindi gli autovalori di  $A$ , sono  $\lambda_1 = 3$  e  $\lambda_2 = -1$ .

Gli autovettori di  $A$  relativi all'autovalore  $\lambda_1 = 3$  sono le soluzioni non nulle  $(v_1, v_2, v_3, v_4) \in \mathbb{Q}^4$  del sistema lineare

$$\begin{cases} (3-3)x_1 + 0x_2 + 0x_3 + 0x_4 = 0 \\ 0x_1 + (3-3)x_2 - 2x_3 + 0x_4 = 0 \\ 0x_1 + 0x_2 - 4x_3 + 0x_4 = 0 \\ 0x_1 + 8x_2 - 4x_3 - 4x_4 = 0, \end{cases}$$

il quale, per ogni scelta dei parametri razionali  $r$  ed  $s$ , ammette l'unica soluzione  $(r, s, 0, 2s) \in \mathbb{Q}^4$ . Pertanto gli autovettori di  $A$  relativi all'autovalore  $\lambda_1 = 3$  costituiscono il sottoinsieme

$$V_3 = \left\{ \begin{pmatrix} r \\ s \\ 0 \\ 2s \end{pmatrix} : r, s \in \mathbb{Q} \right\}$$

di  $M_{4,1}(\mathbb{Q})$ . Ragionando in maniera analoga, si prova che gli autovettori di  $A$  relativi all'autovalore  $\lambda_2 = -1$  costituiscono il sottoinsieme

$$V_{-1} = \left\{ \begin{pmatrix} 0 \\ r \\ 2r \\ s \end{pmatrix} : r, s \in \mathbb{Q} \right\}$$

di  $M_{4,1}(\mathbb{Q})$ .

### Esercizi

**Esercizio 7.8.1.** Si provi, ragionando per induzione su  $n$ , che il polinomio caratteristico di una matrice  $A \in M_n(F)$  ha grado  $n$ , e che il suo coefficiente direttivo (ossia il coefficiente di  $x^n$ ) è  $(-1)^n$ .

**Esercizio 7.8.2.** Si determinino gli autovalori reali delle seguenti matrici:

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 4 & -2 & 0 \\ 0 & 3 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 0 & -2 & 0 \\ 0 & 2 & 0 & 5 \\ 3 & 0 & -1 & 0 \\ 0 & -1 & 0 & -2 \end{pmatrix}.$$

**Esercizio 7.8.3.** Si determinino i polinomi caratteristici e gli autovalori delle seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 3 & -2 & 0 \\ -2 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 4 & -17 & 8 \end{pmatrix}.$$

**Esercizio 7.8.4.** Si determinino gli autovalori delle seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & -2 \end{pmatrix}.$$

**Esercizio 7.8.5.** Si determinino il polinomio caratteristico e gli autovalori reali della matrice

$$A = \begin{pmatrix} 1 & -1 & 4 \\ 3 & 2 & -1 \\ 2 & 1 & -1 \end{pmatrix}.$$

**Esercizio 7.8.6.** Di ciascuna delle seguenti matrici su  $\mathbb{Q}$  si determinino il polinomio caratteristico, gli autovalori e i relativi autovettori:

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 3 & 0 \\ 3 & 2 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & -2 & 3 \\ 0 & 3 & -2 \\ 0 & -1 & 2 \end{pmatrix}.$$

**Esercizio 7.8.7.** Di ciascuna delle seguenti matrici su  $\mathbb{Q}$  si determinino il polinomio caratteristico, gli autovalori e i relativi autovettori:

$$A = \begin{pmatrix} 4 & 0 & -2 \\ 19 & -2 & 0 \\ 0 & -1 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & -17 & 0 \\ 0 & -3 & 1 \\ -2 & 0 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} -3 & 0 & 1 \\ 2 & 4 & 0 \\ 0 & 23 & -4 \end{pmatrix}.$$

**Esercizio 7.8.8.** Di ciascuna delle seguenti matrici su  $\mathbb{Z}_5$  si determinino il polinomio caratteristico, gli autovalori e i relativi autovettori:

$$A = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{1} & \bar{3} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{3} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}, \quad C = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{4} \end{pmatrix}, \quad D = \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{4} & \bar{2} \end{pmatrix}.$$

**Esercizio 7.8.9.** Di ciascuna delle seguenti matrici su  $\mathbb{Z}_7$  si determinino il polinomio caratteristico, gli autovalori e i relativi autovettori:

$$A = \begin{pmatrix} \bar{0} & \bar{6} \\ \bar{5} & \bar{0} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{3} & \bar{4} \\ \bar{4} & \bar{3} \end{pmatrix}, \quad C = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{4} & \bar{2} \end{pmatrix}, \quad D = \begin{pmatrix} \bar{4} & \bar{2} \\ \bar{3} & \bar{5} \end{pmatrix}.$$

**Esercizio 7.8.10.** Di ciascuna delle seguenti matrici su  $\mathbb{Z}_{11}$  si determinino il polinomio caratteristico, gli autovalori e i relativi autovettori:

$$A = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{7} & \bar{0} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{4} \end{pmatrix}, \quad C = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{5} & \bar{3} \end{pmatrix}, \quad D = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{7} & \bar{5} \end{pmatrix}.$$

## 7.9 Esercizi di riepilogo

**Esercizio 7.9.1.** Si effettuino i seguenti calcoli tra matrici a entrate in  $\mathbb{Z}_8$ :

$$\left( \begin{matrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{4} & \bar{5} & \bar{6} \end{matrix} \right) + \left( \begin{matrix} \bar{7} & \bar{6} & \bar{5} \\ \bar{4} & \bar{3} & \bar{2} \end{matrix} \right); \quad - \left( \begin{matrix} \bar{2} & \bar{1} & \bar{4} \\ \bar{5} & \bar{0} & \bar{3} \\ \bar{7} & \bar{2} & \bar{6} \end{matrix} \right);$$

$$\left( \begin{matrix} \bar{4} & \bar{1} \\ \bar{0} & \bar{3} \\ \bar{4} & \bar{6} \end{matrix} \right) \cdot \left( \begin{matrix} \bar{3} & \bar{2} & \bar{1} & \bar{0} \\ \bar{4} & \bar{2} & \bar{5} & \bar{7} \end{matrix} \right); \quad (\bar{4} \quad \bar{2} \quad \bar{0} \quad \bar{6}) \cdot \left( \begin{matrix} \bar{2} & \bar{1} \\ \bar{4} & \bar{2} \\ \bar{7} & \bar{3} \\ \bar{4} & \bar{0} \end{matrix} \right).$$

**Esercizio 7.9.2.** Di ciascuna delle seguenti matrici a entrate in  $\mathbb{Q}$  si calcoli il determinante e si determini, se esiste, la matrice inversa:

$$H = \begin{pmatrix} 1 & 2 & 0 & -3 \\ -2 & 0 & 1 & 0 \\ 0 & 3 & 4 & -2 \\ -7 & 0 & -3 & -5 \end{pmatrix}, \quad K = \begin{pmatrix} 2/5 & -1/3 & 0 \\ 2 & 4 & -10 \\ 0 & -1 & 2/3 \end{pmatrix}.$$

**Esercizio 7.9.3.** Di ciascuna delle seguenti matrici a entrate in  $\mathbb{Z}_5$  si scriva la trasposta, si calcoli il determinante e si determini, se esiste, la matrice inversa:

$$C = \begin{pmatrix} \bar{3} & \bar{4} \\ \bar{4} & \bar{2} \end{pmatrix}, \quad D = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{0} & \bar{3} & \bar{1} & \bar{2} \\ \bar{4} & \bar{1} & \bar{2} & \bar{4} \\ \bar{0} & \bar{3} & \bar{1} & \bar{3} \end{pmatrix}.$$

**Esercizio 7.9.4.** Di ciascuna delle seguenti matrici a entrate in  $\mathbb{Z}$  si scriva la trasposta, si calcoli il determinante e si dica se esiste la matrice inversa:

$$A = \begin{pmatrix} 2 & -4 & 7 \\ 5 & -3 & 6 \\ 1 & -9 & 15 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 5 & -3 & 7 \\ 8 & 2 & 5 \end{pmatrix}.$$

**Esercizio 7.9.5.** Sia  $R$  un anello commutativo unitario e si consideri la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R}).$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \in \mathbb{N}_0$  riesce:

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

**Esercizio 7.9.6.** Si risolvano i seguenti sistemi lineari, il primo in  $\mathbb{Q}$ , il secondo in  $\mathbb{Z}_{11}$ :

$$\left\{ \begin{array}{l} -3x_1 + 5x_2 = -4 \\ 7x_1 - 8x_3 = 3 \\ -2x_1 + 4x_2 - x_3 = 0, \end{array} \right. \quad \left\{ \begin{array}{l} \bar{9}x + \bar{2}y = \bar{10} \\ \bar{4}x + \bar{3}y = \bar{8}. \end{array} \right.$$

**Esercizio 7.9.7.** Si considerino le seguenti matrici a entrate in  $\mathbb{Q}$ :

$$A = \begin{pmatrix} 8 & 1 \\ 0 & -8 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 6 & -5 \\ -2 & -1 & 7 \end{pmatrix}, \quad C = \begin{pmatrix} 7 & -1 & -6 \\ -3 & 4 & 5 \\ 3 & -2 & 0 \end{pmatrix}.$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \geq 2$  riesce

$$A^n = \begin{pmatrix} 8^n & 8^{n-2}(4 + (-1)^{n-1}4) \\ 0 & (-8)^n \end{pmatrix}.$$

Infine si calcoli:  $AB$ ,  $BC$ ,  $A^{-1}$ ,  $\det C$ .

**Esercizio 7.9.8.** Sia  $K$  un campo. Nel gruppo  $\mathrm{GL}(3, K)$  delle matrici  $3 \times 3$  non singolari su  $K$ , con il prodotto righe per colonne, si considerino il sottogruppo

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in K \right\},$$

e le parti:

$$S = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in K \right\}, \quad T = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in K \right\},$$

$$V = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : c \in K \right\}.$$

- (i) Si determini l'inverso di ogni elemento di  $G$ . Si provi che  $S$ ,  $T$  e  $V$  sono sottogruppi di  $G$  e si stabilisca se essi sono normali in  $G$ .
- (ii) Posto

$$g : \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} T \in G/T \longmapsto a + c \in K,$$

- si provi che l'applicazione  $g$  è ben posta ed è un omomorfismo di  $(G/T, \cdot)$  in  $(K, +)$ . Infine si stabilisca se  $g$  è iniettiva o suriettiva.
- (iii) Nel caso  $K = \mathbb{Z}_2$ , si determini l'ordine di  $G$  e si stabilisca se il gruppo  $G$  è abeliano.

**Esercizio 7.9.9.** Si consideri la matrice

$$A = \begin{pmatrix} 2 & 3 \\ 2 & -3 \end{pmatrix} \in M_2(\mathbb{Z}).$$

Utilizzando il teorema di Binet, si dimostri per induzione su  $n$  che

$$\det A^n = (-1)^n 12^n,$$

per ogni  $n \geq 1$ .

**Esercizio 7.9.10.** Si consideri la matrice

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{Z}).$$

Utilizzando il teorema di Binet, si dimostri per induzione su  $n$  che

$$\det A^n = (-1)^n 5^n,$$

per ogni  $n \geq 1$ .

**Esercizio 7.9.11.** Si consideri la matrice

$$A = \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} \in M_2(\mathbb{R}).$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \geq 1$  riesce

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} A^n = \begin{pmatrix} 8^n & 8^n \\ 8^n & -8^n \end{pmatrix}.$$

**Esercizio 7.9.12.** Si consideri la matrice

$$A = \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Q}).$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \geq 1$  riesce

$$A^{2n} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

**Esercizio 7.9.13.** Si consideri la matrice

$$A = \begin{pmatrix} 1 & 0 \\ 1/3 & 1 \end{pmatrix}.$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \geq 1$  riesce

$$A^{3n} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.$$

**Esercizio 7.9.14.** Si consideri la matrice

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} \in M_2(\mathbb{Q}).$$

Si dimostri, per induzione su  $n$ , che per ogni  $n \geq 1$  riesce

$$A^n = \begin{pmatrix} 1 & 0 \\ \frac{3^n-1}{2} & 3^n \end{pmatrix}.$$

**Esercizio 7.9.15.** Di ciascuna delle seguenti matrici su  $\mathbb{Z}$  si scriva la trasposta, si calcoli il determinante, e si determini, se esiste, la matrice inversa:

$$A = \begin{pmatrix} 2 & -4 & 7 \\ 5 & -3 & 6 \\ 1 & -9 & 15 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 5 & -3 & 7 \\ 8 & 2 & 5 \end{pmatrix}.$$

**Esercizio 7.9.16.** Di ciascuna delle seguenti matrici su  $\mathbb{Z}_5$  si scriva la trasposta, si calcoli il determinante, e si determini, se esiste, la matrice inversa:

$$A = \begin{pmatrix} \bar{3} & \bar{2} \\ \bar{4} & \bar{2} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{0} & \bar{3} & \bar{1} & \bar{2} \\ \bar{4} & \bar{1} & \bar{2} & \bar{4} \\ \bar{0} & \bar{3} & \bar{1} & \bar{3} \end{pmatrix}.$$

**Esercizio 7.9.17.** Di ciascuna delle seguenti matrici su  $\mathbb{Q}$  si scriva la trasposta, si calcoli il determinante, e si determini, se esiste, la matrice inversa:

$$A = \begin{pmatrix} 1 & 2 & 0 & -3 \\ -2 & 0 & 1 & 0 \\ 0 & 3 & 4 & -2 \\ -7 & 0 & -3 & -5 \end{pmatrix}, \quad B = \begin{pmatrix} 2/5 & -1/3 & 0 \\ 7/2 & 5 & -10 \\ 0 & -1 & 2/3 \end{pmatrix}.$$

**Esercizio 7.9.18.** Si considerino le seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 0 & -3 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & -3 \\ 0 & 1 & 2 & -2 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & -1 & 2 & 0 & 4 \\ 8 & 6 & 10 & 0 & 0 \\ -2 & 0 & -2 & 2 & 2 \\ 4 & -9 & 2 & 6 & 4 \end{pmatrix}.$$

Posto  $C = A_{54}$  e  $D = B_{42}$ , si determini la matrice  $H = \frac{1}{2}DC$ .

- (i) Si calcolino il determinante e il rango di  $H$ . Si stabilisca se tale matrice è invertibile e, in caso affermativo, se ne determini l'inversa.
- (ii) Si risolva il sistema lineare

$$H \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

- (iii) Siano

$$K = \begin{pmatrix} 0 & -1 & 5 \\ 3 & -12 & 8 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(\mathbb{R}),$$

e  $T = H - K$ . Si determinino il polinomio caratteristico e gli autovalori della matrice  $T$ .

**Esercizio 7.9.19.** Si considerino le matrici

$$A_n = \begin{pmatrix} \bar{1} & \bar{0} & \bar{4} \\ \bar{3} & \bar{1} & \bar{n} \\ \bar{0} & \bar{10} & \bar{2} \end{pmatrix} \in M_3(\mathbb{Z}_{11}), \quad B_n = \begin{pmatrix} \bar{n} & \bar{2} & \bar{3} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{3} & \bar{12} & \bar{0} \end{pmatrix} \in M_3(\mathbb{Z}_{13}),$$

al variare di  $n \in \mathbb{N}$ . Si determinino tutti i valori positivi di  $n < 500$  in corrispondenza dei quali  $A_n$  e  $B_n$  risultano simultaneamente non invertibili.

**Esercizio 7.9.20.** Si considerino le seguenti matrici su  $\mathbb{Q}$ :

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 \\ -1 & -1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 2 & 2 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Posto  $C = A_{14}$  e  $D = B_{21}$ , si determini la matrice  $H = C \cdot 2D$ . Si calcoli il determinante e il rango di  $H$ , si stabilisca se essa è invertibile e, in caso affermativo, se ne determini l'inversa.

**Esercizio 7.9.21.** Si considerino le seguenti matrici su  $\mathbb{Q}$ :

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 \\ -1 & -1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 2 & 2 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Posto  $C = A_{14}$  e  $D = B_{21}$ , si determini la matrice  $H = C \cdot 2D$ . Si calcoli il determinante e il rango di  $H$ , si stabilisca se essa è invertibile e, in caso affermativo, se ne determini l'inversa.

**Esercizio 7.9.22.** Si considerino le seguenti matrici su  $\mathbb{Z}_7$ :

$$A = \begin{pmatrix} \bar{3} & \bar{0} & \bar{1} & \bar{2} \\ \bar{4} & \bar{0} & \bar{3} & \bar{5} \\ \bar{1} & \bar{2} & \bar{0} & \bar{0} \\ \bar{2} & \bar{0} & \bar{0} & \bar{1} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{4} & \bar{1} & \bar{0} \\ \bar{1} & \bar{3} & \bar{1} \\ \bar{6} & \bar{2} & \bar{0} \end{pmatrix}.$$

Posto  $C = A_{11}^T$  e  $H = CB$ . Si calcoli il determinante e il rango di  $H$ , si stabilisca se essa è invertibile e, in caso affermativo, se ne determini l'inversa.

**Esercizio 7.9.23.** Si considerino le seguenti matrici su  $\mathbb{R}$ :

$$B = \begin{pmatrix} 5 & 0 & -35 & 0 \\ 0 & 25 & -5 & 5 \\ 0 & 0 & 10 & 55 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -2 & 6 & 0 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 1 & -4 \\ 11 & -3 & 4 & 5 \end{pmatrix}.$$

Posto  $A = C + \frac{1}{5}B$  e  $H = A_{24}$ , si calcolino il determinante e il rango di  $H$ . Si stabilisca se  $H$  è invertibile e, in caso affermativo, si determini  $H^{-1}$ . Si risolva il sistema

$$H \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

**Esercizio 7.9.24.** Si considerino le seguenti matrici su  $\mathbb{R}$ :

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 2 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & -7 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 8 & 12 \\ 8 & 10 & 12 \\ 6 & 2 & -4 \end{pmatrix}.$$

Posto  $C = A_{24}^T$  e  $H = C \cdot \frac{1}{2}B$ , si calcolino il determinante e il rango di  $H$ . Si stabilisca se  $H$  è invertibile e, in caso affermativo, si determini  $H^{-1}$ . Infine si risolva il sistema lineare

$$H \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 18 \\ 24 \\ 4 \end{pmatrix}.$$

**Esercizio 7.9.25.** Si consideri la seguente matrice su  $\mathbb{R}$ :

$$B_t = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 2 & 3 & 4 \\ 2 & 4 & 7 & 2t+6 \\ 2 & 2 & 6-t & t \end{pmatrix}.$$

- (i) Si stabilisca per quali valori di  $t$  la matrice  $B_t$  è invertibile.
- (ii) Si calcoli il rango di  $B_t$  per  $t = 2$ .
- (iii) Posto  $H = B_4$ , si provi che  $H$  è invertibile e si determini  $H^{-1}$ .
- (iv) Utilizzando il metodo di Cramer, si risolva il sistema lineare

$$B_0 \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}.$$

**Esercizio 7.9.26.** Si consideri la seguente matrice su  $\mathbb{R}$ :

$$B_t = \begin{pmatrix} t-2 & -7 & 11 & 2 \\ 0 & 2-t & -2t & -6 \\ 0 & 0 & t & 3 \\ 0 & 3 & 3 & t \end{pmatrix}.$$

- (i) Si stabilisca per quali valori di  $t$  la matrice  $B_t$  è invertibile.
- (ii) Si calcoli il rango di  $B_t$  per  $t = 2$ .
- (iii) Posto  $K = B_0$  e  $H = K_{31}$ , si provi che  $H$  è invertibile e si determini  $H^{-1}$ .
- (iv) Utilizzando il metodo di Cramer, si risolva il sistema lineare

$$B_0 \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

# 8

## Spazi vettoriali

Uno spazio vettoriale è essenzialmente un insieme di oggetti chiamati vettori, che, seguendo determinate regole, è possibile sia sommare tra loro che moltiplicare per gli elementi di un fissato corpo. L'importanza degli spazi vettoriali deriva dal fatto che questa struttura algebrica compare in numerose branche della matematica e della fisica, così come in molte applicazioni. In particolare, la teoria degli spazi vettoriali consente di studiare al meglio le soluzioni dei sistemi di equazioni lineari. Per evitare complicazioni qui non essenziali, si tratteranno esclusivamente spazi vettoriali su un campo, e quest'ultimo verrà in genere denotato con la lettera  $F$  (dall'inglese "field"). Per la più generale definizione di spazio vettoriale su un corpo si veda il Capitolo 4.

### 8.1 Generalità

Sia  $F$  un campo. Una struttura algebrica  $(V, +, \cdot)$ , dove

$$\begin{aligned}+ : V \times V &\longrightarrow V \\(x, y) &\longmapsto x + y\end{aligned}$$

è un'operazione interna in  $V$  e

$$\begin{aligned}\cdot : F \times V &\longrightarrow V \\(\alpha, x) &\longmapsto \alpha x\end{aligned}$$

un'operazione esterna con dominio di operatori  $F$ , viene detta uno **spazio vettoriale** su  $F$  (o anche un  $F$ -spazio vettoriale) se valgono le seguenti proprietà:

- (i)  $x + (y + z) = (x + y) + z$ , per ogni  $x, y, z \in V$ ,
- (ii)  $x + y = y + x$ , per ogni  $x, y \in V$ ,
- (iii)  $\exists 0 \in V : x + 0 = x$ , per ogni  $x \in V$ ,
- (iv)  $\forall x \in V, \exists -x \in V : x + (-x) = 0$ ,
- (v)  $(\alpha\beta)x = \alpha(\beta x)$ , per ogni  $\alpha, \beta \in F, x \in V$ ,
- (vi)  $\alpha(x + y) = \alpha x + \alpha y$ , per ogni  $\alpha \in F, x, y \in V$ ,
- (vii)  $(\alpha + \beta)x = \alpha x + \beta x$ , per ogni  $\alpha, \beta \in F, x \in V$ ,
- (viii)  $1x = x$ , per ogni  $x \in V$ ,

dove ovviamente 1 denota l'unità del campo  $F$ . Con la terminologia introdotta nel Capitolo 4, le proprietà (i) – (iv) esprimono il fatto che  $(V, +)$  è un gruppo abeliano. Gli elementi di  $V$  sono detti **vettori** e denotati con lettere dell'alfabeto latino, quelli di  $F$  vengono detti **scalar**i e denotati usualmente con lettere dell'alfabeto greco. L'elemento neutro del gruppo abeliano  $(V, +)$ , denotato al solito con 0, è detto il **vettore nullo**.

**8.1.1. Esempio.** Siano  $F$  un campo e  $\{0\}$  il gruppo identico. Ponendo  $\alpha \cdot 0 = 0$  per ogni  $\alpha \in F$  si ottiene un'operazione esterna  $\cdot : F \times \{0\} \longrightarrow \{0\}$ , e si verifica subito che valgono le proprietà (i) – (viii). Pertanto il gruppo identico è uno spazio vettoriale su qualunque campo  $F$  (il cosiddetto *F-spazio vettoriale nullo*).

**8.1.2. Esempio.** Siano  $F$  un campo ed  $n \in \mathbb{N}$ . Si consideri l'insieme

$$F^n = \{(\lambda_1, \lambda_2, \dots, \lambda_n) : \lambda_1, \lambda_2, \dots, \lambda_n \in F\}$$

delle  $n$ -uple ordinate di elementi di  $F$ . Le posizioni

$$\begin{aligned} (\lambda_1, \lambda_2, \dots, \lambda_n) + (\mu_1, \mu_2, \dots, \mu_n) &:= (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \dots, \lambda_n + \mu_n), \\ \alpha(\lambda_1, \lambda_2, \dots, \lambda_n) &:= (\alpha\lambda_1, \alpha\lambda_2, \dots, \alpha\lambda_n) \end{aligned}$$

definiscono rispettivamente un'operazione interna in  $F^n$  e un'operazione esterna in  $F^n$  con dominio di operatori  $F$ , ed è molto agevole verificare (vedi Esercizio 8.1.1) che valgono le proprietà (i) – (viii). Pertanto  $(F^n, +, \cdot)$  è uno spazio vettoriale su  $F$ . In particolare, per  $n = 1$ , ogni campo può essere strutturato a spazio vettoriale su se stesso.

**8.1.3. Esempio.** Sia  $M_{n,m}(F)$  l'insieme delle matrici  $n \times m$  su un campo  $F$ . Si ponga, come già fatto nel Capitolo 7:

$$\begin{aligned} A + B &:= (a_{ij} + b_{ij}), \\ \lambda A &:= (\lambda a_{ij}), \end{aligned}$$

per ogni  $A = (a_{ij})$ ,  $B = (b_{ij}) \in M_{n,m}(F)$ , e per ogni  $\lambda \in F$ . Allora 7.2.1 e 7.2.2 assicurano che  $(M_{n,m}(F), +, \cdot)$  è uno spazio vettoriale su  $F$ .

**8.1.4. Esempio.** Sia  $F[x]$  l'insieme dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$ . Nel Paragrafo 6.6 è stata definita una somma tra polinomi, e  $(F[x], +)$  è un gruppo abeliano (vedi Esercizio 6.6.1). Se per ogni  $\alpha \in F$  e per ogni  $a_0 + a_1x + \cdots + a_nx^n \in F[x]$  si pone

$$\alpha(a_0 + a_1x + \cdots + a_nx^n) := \alpha a_0 + \alpha a_1x + \cdots + \alpha a_nx^n,$$

si definisce un'operazione esterna in  $F[x]$  con dominio di operatori  $F$ . Si può provare facilmente che  $(F[x], +, \cdot)$  è uno spazio vettoriale su  $F$  (vedi Esercizio 8.1.3).

**8.1.5. Esempio.** Siano  $F$  un campo ed  $S$  un insieme non vuoto, e si denoti al solito con  $F^S$  l'insieme di tutte le applicazioni di  $S$  in  $F$ . Si definisca in  $F^S$  un'operazione interna  $+$  ponendo, per ogni  $f, g \in F^S$  e per ogni  $x \in S$ :

$$(f + g)(x) := f(x) + g(x),$$

dove l'operazione  $+$  che compare a destra nella precedente uguaglianza è ovviamente la somma del campo  $F$ . Si vede facilmente che la struttura  $(F^S, +)$  è un gruppo abeliano. Si definisca poi in  $F^S$  un'operazione esterna con operatori in  $F$ , ponendo, per ogni  $\alpha \in F$ , per ogni  $f \in F^S$  e per ogni  $x \in S$ :

$$(\alpha f)(x) := \alpha f(x),$$

dove il prodotto che compare a destra nella precedente uguaglianza è il prodotto nel campo  $F$ . È agevole verificare che in tal modo  $F^S$  resta strutturato a spazio vettoriale su  $F$  (vedi Esercizio 8.1.4).

**8.1.6. Esempio.** Siano  $V$  uno spazio vettoriale su un campo  $F$  ed  $S$  un insieme non vuoto, e si denoti al solito con  $V^S$  l'insieme di tutte le applicazioni di  $S$  in  $V$ . Si definisca in  $V^S$  un'operazione interna  $+$  ponendo, per ogni  $f, g \in V^S$  e per ogni  $x \in S$ :

$$(f + g)(x) := f(x) + g(x),$$

dove l'operazione  $+$  che compare a destra nella precedente uguaglianza è ovviamente la somma di vettori di  $V$ . Si vede facilmente che la struttura  $(V^S, +)$  è un gruppo abeliano. Si definisca poi in  $V^S$  un'operazione esterna con operatori in  $F$ , ponendo, per ogni  $\alpha \in F$ , per ogni  $f \in V^S$  e per ogni  $x \in S$ :

$$(\alpha f)(x) := \alpha f(x),$$

dove il prodotto che compare a destra nella precedente uguaglianza è il prodotto di uno scalare di  $F$  per un vettore di  $V$ . Si prova agevolmente che  $(V^S, +, \cdot)$  è uno spazio vettoriale su  $F$  (vedi Esercizio 8.1.5).

Le principali regole di calcolo valide negli spazi vettoriali sono sintetizzate nella proposizione che segue:

**8.1.7.** *Sia  $V$  uno spazio vettoriale su un campo  $F$ . Per ogni  $\alpha, \beta \in F$  e per ogni  $x, y \in V$  si ha:*

- (i)  $\alpha 0 = 0 = 0x$ ;
- (ii)  $\alpha(-x) = -(\alpha x) = (-\alpha)x$ ;
- (iii)  $\alpha(x - y) = \alpha x - \alpha y$ ;
- (iv)  $(\alpha - \beta)x = \alpha x - \beta x$ ;
- (v)  $\alpha x = 0 \iff \alpha = 0$  oppure  $x = 0$ .

*Dimostrazione.* (i) Utilizzando la (vi) della definizione di spazio vettoriale, risulta  $0 + \alpha 0 = \alpha 0 = \alpha(0 + 0) = \alpha 0 + \alpha 0$ , e la cancellabilità nel gruppo abeliano  $(V, +)$  implica che  $0 = \alpha 0$ . Analogamente, facendo uso della (vii) della definizione di spazio vettoriale, da  $0 + 0x = 0x = (0 + 0)x = 0x + 0x$  segue che  $0 = 0x$ .

(ii) Da quanto provato nella (i) si ottiene  $0 = \alpha 0 = \alpha(x + (-x)) = \alpha x + \alpha(-x)$ , quindi  $\alpha(-x) = -(\alpha x)$ ; poi  $0 = 0x = (\alpha + (-\alpha))x = \alpha x + (-\alpha)x$ , da cui  $(-\alpha)x = -(\alpha x)$ .

(iii) Risulta  $\alpha(x - y) = \alpha(x + (-y)) = \alpha x + \alpha(-y) = \alpha x - \alpha y$  per la (vi) della definizione di spazio vettoriale e per quanto provato nella (ii).

(iv) Risulta  $(\alpha - \beta)x = (\alpha + (-\beta))x = \alpha x + (-\beta)x = \alpha x - \beta x$  per la (vii) della definizione di spazio vettoriale e per quanto provato nella (ii).

(v) Se  $\alpha = 0$  oppure  $x = 0$  il risultato è stato già provato nella (i). Viceversa, sia  $\alpha x = 0$  con  $\alpha \neq 0$ . Allora esiste  $\alpha^{-1} \in F$ , e  $0 = \alpha^{-1}0 = \alpha^{-1}(\alpha x) = (\alpha^{-1}\alpha)x = 1x = x$  per quanto provato nella (i) e per la (v) e la (viii) della definizione di spazio vettoriale.  $\square$

## Esercizi

**Esercizio 8.1.1.** Si provi 8.1.2.

**Esercizio 8.1.2.** Come generalizzazione dell'Esempio 8.1.2, si provi che se  $A$  è un anello e  $n$  un intero positivo, l'insieme

$$A^n = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in A\}$$

delle  $n$ -uple ordinate di elementi di  $A$  può essere strutturato in maniera naturale a spazio vettoriale su un qualunque sottoanello  $F$  di  $A$  che sia un campo. In tale modo, per esempio,  $\mathbb{R}^n$  può essere visto come spazio vettoriale su  $\mathbb{Q}$ ,  $\mathbb{C}^n$  come spazio vettoriale su  $\mathbb{R}$  o su  $\mathbb{Q}$ .

**Esercizio 8.1.3.** Si provi 8.1.4.

**Esercizio 8.1.4.** Si provi 8.1.5.

**Esercizio 8.1.5.** Si provi 8.1.6.

**Esercizio 8.1.6.** Sia  $R$  il gruppo additivo di un anello di caratteristica prima  $p$ . Si dimostri che  $R$  può essere strutturato a spazio vettoriale sul campo  $\mathbb{Z}_p$ .

*Suggerimento.* L'applicazione

$$\begin{aligned} \cdot : \mathbb{Z}_p \times R &\longrightarrow R \\ ([n]_p, x) &\longmapsto nx \end{aligned}$$

è ben posta, in quanto da  $[n]_p = [m]_p$  segue  $p|n - m$ , dunque  $nx - mx = (n - m)x = 0$  essendo  $p$  la caratteristica di  $R$  (vedi (iii) di 6.5.22); ne segue che  $nx = mx$ . Allora  $\cdot$  è un'operazione esterna in  $R$  con dominio di operatori  $\mathbb{Z}_p$ . Ora  $(R, +)$  è un gruppo abeliano, e le leggi di calcolo nell'anello  $R$ , tenendo conto del fatto che la caratteristica di  $R$  è  $p$ , consentono di verificare agevolmente le proprietà (v) – (viii) della definizione di spazio vettoriale.

**Esercizio 8.1.7.** Si consideri il gruppo abeliano  $(\mathbb{R}^2, +)$ , dove l'operazione  $+$  è definita nel modo usuale. Si provi che la posizione  $\alpha \star (a, b) := (\alpha^2 a, \alpha^2 b)$  definisce un'operazione esterna in  $\mathbb{R}^2$  con dominio di operatori  $\mathbb{R}$ , ma che  $(\mathbb{R}^2, +, \star)$  non è uno spazio vettoriale su  $\mathbb{R}$ .

## 8.2 Sottospazi e generatori

Sia  $V$  un  $F$ -spazio vettoriale. Un sottoinsieme  $W$  di  $V$  è detto un **sottospazio** di  $V$  se è stabile rispetto alle due operazioni di  $V$  (ossia, se  $x + y \in W$  e  $\alpha x \in W$ , per ogni  $x, y \in W$  e per ogni  $\alpha \in F$ ), e se  $W$  stesso, con le operazioni indotte da quelle di  $V$ , è un  $F$ -spazio vettoriale. Ciò ovviamente equivale a richiedere che  $(W, +)$  sia un sottogruppo di  $(V, +)$ , e che  $W$  sia stabile rispetto all'operazione esterna.

**8.2.1.** Sia  $V$  uno spazio vettoriale su un campo  $F$ . Un sottoinsieme non vuoto  $W$  di  $V$  è un sottospazio di  $V$  se e solo se  $x - y \in W$  e  $\alpha x \in W$ , per ogni  $x, y \in W$  e per ogni  $\alpha \in F$ .

*Dimostrazione.* Basta utilizzare la caratterizzazione dei sottogruppi in 6.3.7.  $\square$

**8.2.2.** Sia  $V$  uno spazio vettoriale su un campo  $F$ . Un sottoinsieme non vuoto  $W$  di  $V$  è un sottospazio di  $V$  se e solo se  $\alpha x + \beta y \in W$ , per ogni  $x, y \in W$  e per ogni  $\alpha, \beta \in F$ .

*Dimostrazione.* Esercizio.  $\square$

Ogni spazio vettoriale  $V$  possiede almeno i **sottospazi banali**, ossia  $V$  stesso e il sottospazio nullo  $\{0\}$ . Ogni sottospazio  $W$  di  $V$  con  $W \neq V$  è detto un **sottospazio proprio**.

**8.2.3. Esempio.** Sia  $F$  un campo. I sottospazi di  $F$  visto come  $F$ -spazio vettoriale (vedi Esempio 8.1.2 con  $n = 1$ ) sono solo quelli banali. Infatti se  $W \neq \{0\}$  è un sottospazio di  $F$ , allora esiste  $x \in W$  con  $x \neq 0$ . Ciò significa che  $x^{-1} \in F$ , pertanto  $1 = x^{-1}x \in W$ . Di qui, per ogni  $\alpha \in F$  risulta  $\alpha = \alpha 1 \in W$ , e  $W = F$ .

**8.2.4. Esempio.** Sia  $F$  un campo. Nello  $F$ -spazio vettoriale  $F^n$  (vedi Esempio 8.1.2) il sottoinsieme  $D = \{(x, x, \dots, x) : x \in F\}$  è un sottospazio, detto il **sottospazio diagonale**. Infatti  $D \neq \emptyset$ , e da  $(x, x, \dots, x), (y, y, \dots, y) \in D$  segue  $(x, x, \dots, x) - (y, y, \dots, y) = (x - y, x - y, \dots, x - y) \in D$ . Inoltre, per ogni  $\alpha \in F$  risulta ovviamente  $\alpha(x, x, \dots, x) = (\alpha x, \alpha x, \dots, \alpha x) \in D$ .

**8.2.5. Esempio.** Sia  $F[x]$  lo spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$  (vedi Esempio 8.1.4). Con  $n \in \mathbb{N}_0$ , sia  $F[x; n]$  l'insieme costituito dal polinomio nullo e da tutti i polinomi di  $F[x]$  aventi grado al

più  $n$ . Ovviamente  $F[x; n] \neq \emptyset$  in quanto il polinomio nullo appartiene a  $F[x; n]$ . Per ogni  $f(x), g(x) \in F[x; n]$  il polinomio  $f(x) - g(x)$  o è nullo oppure ha grado che non supera il massimo tra il grado di  $f(x)$  e quello di  $g(x)$ , e quindi al più  $n$ . Inoltre, per ogni  $\alpha \in F$  e per ogni polinomio  $f(x) \in F[x; n]$ , il polinomio  $\alpha f(x)$  o è nullo oppure ha lo stesso grado di  $f(x)$ , quindi ancora al più  $n$ . Pertanto 8.2.1 assicura che  $F[x; n]$  è un sottospazio di  $F[x]$ , per ogni  $n \in \mathbb{N}_0$ .

**8.2.6. Esempio.** Sia  $M_2(\mathbb{Q})$  lo spazio vettoriale su  $\mathbb{Q}$  costituito dalle matrici quadrate di ordine 2 su  $\mathbb{Q}$  (vedi Esempio 8.1.3). È immediato verificare che il sottoinsieme

$$W = \left\{ \begin{pmatrix} 0 & \alpha \\ \beta & \gamma \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Q} \right\}$$

è un sottospazio di  $M_2(\mathbb{Q})$  (vedi Esercizio 8.2.9).

Siccome l'unione di sottogruppi non è in generale un sottogruppo (vedi Esercizio 6.3.6), l'unione di sottospazi non è in generale un sottospazio.

**8.2.7. Sia  $V$  uno spazio vettoriale su un campo  $F$ , e siano  $W_1$  e  $W_2$  sottospazi di  $V$ . Allora  $W_1 \cap W_2$  è un sottospazio di  $V$ .**

*Dimostrazione.* Ovviamente  $0 \in W_1 \cap W_2$ , quindi  $W_1 \cap W_2 \neq \emptyset$ . Inoltre la 8.2.2 assicura che  $\alpha x + \beta y \in W_1 \cap W_2$ , per ogni  $x, y \in W_1 \cap W_2$  e per ogni  $\alpha, \beta \in F$ . Pertanto  $W_1 \cap W_2$  è un sottospazio di  $V$ , ancora per 8.2.2.  $\square$

Più in generale si può provare che:

**8.2.8. Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $\{W_i : i \in I\}$  un insieme non vuoto di sottospazi di  $V$ . Allora**

$$\bigcap_{i \in I} W_i$$

è un sottospazio di  $V$ .

*Dimostrazione.* Esercizio.  $\square$

Sia  $X$  un sottoinsieme di uno spazio vettoriale  $V$  su un campo  $F$ . Per la 8.2.8, l'intersezione di tutti i sottospazi di  $V$  che contengono  $X$  è un sottospazio di  $V$ , detto il sottospazio di  $V$  **generato** da  $X$ , e denotato con il simbolo  $\langle X \rangle$ . Per definizione,  $\langle X \rangle$  è quindi il più piccolo (rispetto all'inclusione) tra i sottospazi di  $V$  contenenti  $X$ . Per esempio, è chiaro che  $\langle \emptyset \rangle = \langle \{0\} \rangle$  è il sottospazio nullo, e che  $\langle V \rangle = V$ . Più in generale, se  $W$  è un sottospazio di  $V$ , si ha banalmente  $\langle W \rangle = W$ .

Sia  $W$  un sottospazio di uno spazio vettoriale  $V$ . Se risulta  $W = \langle X \rangle$  per qualche sottoinsieme  $X$  di  $V$  si dice che  $X$  è un *insieme di generatori* di  $W$ , o anche che  $X$  *genera*  $W$ .

**8.2.9.** *Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $X = \{x_1, x_2, \dots, x_n\}$  un insieme non vuoto di vettori di  $V$ , con  $|X| = n$ . Allora risulta:*

$$\langle X \rangle = \{\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n : \alpha_1, \alpha_2, \dots, \alpha_n \in F\}.$$

*Dimostrazione.* Si ponga

$$W = \{\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n : \alpha_1, \alpha_2, \dots, \alpha_n \in F\}.$$

Si mostrerà che  $W = \langle X \rangle$ , ossia che  $W$  è, rispetto all'inclusione, il più piccolo tra i sottospazi di  $V$  contenenti  $X$ . Innanzitutto  $W$  è un sottospazio di  $V$ . Infatti  $W \neq \emptyset$  in quanto certamente  $0 = 0x_1 + 0x_2 + \dots + 0x_n \in W$ . Siano poi  $x = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$  e  $y = \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n$  arbitrari elementi di  $W$ , e  $\alpha \in F$ . Allora, utilizzando le proprietà (ii), (iv) e (vii) della definizione di spazio vettoriale si ottiene:

$$\begin{aligned} x - y &= (\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n) - (\beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n) \\ &= (\alpha_1 - \beta_1)x_1 + (\alpha_2 - \beta_2)x_2 + \dots + (\alpha_n - \beta_n)x_n \in W; \end{aligned}$$

utilizzando invece le proprietà (vi) e (v) si ha:

$$\begin{aligned} \alpha x &= \alpha(\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n) \\ &= (\alpha\alpha_1)x_1 + (\alpha\alpha_2)x_2 + \dots + (\alpha\alpha_n)x_n \in W. \end{aligned}$$

Pertanto 8.2.1 assicura che  $W$  è un sottospazio di  $V$ . È poi chiaro che  $X \subseteq W$ , in quanto per ogni  $i = 1, 2, \dots, n$  risulta

$$x_i = 0x_1 + \dots + 0x_{i-1} + 1x_i + 0x_{i+1} + \dots + 0x_n \in W.$$

Infine, un qualunque sottospazio di  $V$  contenente  $X$  contiene necessariamente ogni elemento  $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$  di  $W$ . Pertanto  $W$  è il più piccolo tra i sottospazi di  $V$  contenenti  $X$ , quindi  $W = \langle X \rangle$ .  $\square$

Se  $X = \{x_1, x_2, \dots, x_n\}$  è un insieme finito di vettori di  $V$  avente ordine  $n$ , si utilizza spesso la notazione  $\langle x_1, x_2, \dots, x_n \rangle$  in luogo di  $\langle X \rangle$ . Così, per ogni  $x \in V$ , dalla 8.2.9 segue subito  $\langle x \rangle = \{\alpha x : \alpha \in F\}$ . Un sottoinsieme  $X$  di  $V$  è detto un *insieme minimale di generatori* di  $V$  se  $V = \langle X \rangle$  e  $V \neq \langle Y \rangle$  per ogni  $Y \subset X$ . In altre parole, se  $X$ , rispetto all'inclusione, è un elemento minimale nell'insieme dei sottoinsiemi di  $V$  che generano  $V$ . Uno spazio vettoriale  $V$  è detto *finitamente generato* se esiste un insieme finito  $X$  di vettori di  $V$  tale che  $V = \langle X \rangle$ . Un facile esempio di spazio vettoriale non finitamente generato è quello dei polinomi su un campo (vedi Esercizio 8.2.14).

**8.2.10. Esempio.** Sia  $F$  un campo. Nello  $F$ -spazio vettoriale  $F$  (vedi Esempio 8.1.2 con  $n = 1$ ) il singleton  $\{x\}$  di ogni elemento  $x \neq 0$  è un insieme minimale di generatori. Più in generale, se  $n \geq 1$ , nello  $F$ -spazio vettoriale  $F^n$  si ponga  $e_1 = (1, 0, 0, \dots, 0)$ ,  $e_2 = (0, 1, 0, \dots, 0)$ , ...,  $e_n = (0, 0, \dots, 0, 1)$ . Si vede facilmente che  $\{e_1, e_2, \dots, e_n\}$  è un insieme minimale di generatori di  $F^n$  (vedi Esercizio 8.2.11).

**8.2.11. Esempio.** Sia  $F[x]$  lo spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$ . Si verifica facilmente che, per ogni  $n \in \mathbb{N}_0$ , risulta  $\langle 1, x, x^2, \dots, x^n \rangle = F[x; n]$ , il sottospazio costituito dal polinomio nullo e da tutti i polinomi di  $F[x]$  aventi grado al più  $n$  (vedi Esempio 8.2.5). Inoltre  $\{1, x, x^2, \dots, x^n\}$  è un insieme minimale di generatori per  $F[x; n]$  (vedi Esercizio 8.2.12).

**8.2.12.** Siano  $W_1, \dots, W_n$  sottospazi di uno spazio vettoriale  $V$ . L'insieme

$$W_1 + \dots + W_n := \{w_1 + \dots + w_n : w_1 \in W_1, \dots, w_n \in W_n\}$$

è un sottospazio di  $V$ , detto il **sottospazio somma** di  $W_1, \dots, W_n$ . Più precisamente, esso coincide con il sottospazio di  $V$  generato da  $W_1, \dots, W_n$ .

*Dimostrazione.* Esercizio. □

## Esercizi

**Esercizio 8.2.1.** Si provi 8.2.2.

**Esercizio 8.2.2.** Sia  $V$  uno spazio vettoriale su un campo  $F$ . Si provi che un sottoinsieme  $W$  di  $V$  è un sottospazio di  $V$  se e solo se  $0 \in W$  e  $\alpha x + \beta y \in W$ , per ogni  $x, y \in W$  e per ogni  $\alpha, \beta \in F$ .

**Esercizio 8.2.3.** Si provi che un sottogruppo additivo di uno spazio vettoriale non ne è necessariamente un sottospazio.

*Suggerimento.* Si utilizzi l'Esempio 8.2.3.

**Esercizio 8.2.4.** Si consideri  $M_2(\mathbb{R})$  strutturato a  $\mathbb{R}$ -spazio vettoriale nel modo usuale. Si stabilisca se i sottoinsiemi  $W_1$  e  $W_2$  costituiti rispettivamente dalle matrici singolari e da quelle non singolari sono sottospazi di  $M_2(\mathbb{R})$ .

**Esercizio 8.2.5.** Per ciascuno dei sottoinsiemi seguenti si stabilisca se esso è un sottospazio di  $\mathbb{Q}^2$ , strutturato a spazio vettoriale su  $\mathbb{Q}$  nel modo usuale:

$$\begin{aligned} W_1 &= \{(x, y) : x = y\}, \\ W_2 &= \{(x, y) : x = 2y\}, \\ W_3 &= \{(x, y) : x + y = 1\}, \\ W_4 &= \{(x, y) : x = 0\}. \end{aligned}$$

**Esercizio 8.2.6.** Per ciascuno dei sottoinsiemi seguenti si stabilisca se esso è un sottospazio di  $\mathbb{R}^3$ , strutturato a spazio vettoriale su  $\mathbb{R}$  nel modo usuale:

$$\begin{aligned} W_1 &= \{(x, y, z) : x^2 + y^2 + z^2 = 0\}, \\ W_2 &= \{(x, y, z) : x = y = z\}, \\ W_3 &= \{(x, y, z) : x = 5y, y = 5x + 1\}, \\ W_4 &= \{(x, y, z) : x^2 + y^2 = 1\}, \\ W_5 &= \{(x, y, z) : x - 3z = 0\}. \end{aligned}$$

**Esercizio 8.2.7.** Per ciascuno dei sottoinsiemi seguenti si stabilisca se esso è un sottospazio di  $\mathbb{Q}^3$ , strutturato a spazio vettoriale su  $\mathbb{Q}$  nel modo usuale:

$$\begin{aligned} W_1 &= \{(x, y, z) : y^2 - z^2 = 0\}, \\ W_2 &= \{(x, y, z) : x + y + z = 0\}, \\ W_3 &= \{(x, y, z) : x + y - z = 0\}, \\ W_4 &= \{(x, y, z) : x + y = 0\}. \end{aligned}$$

**Esercizio 8.2.8.** Per ciascuno dei sottoinsiemi seguenti si stabilisca se esso è un sottospazio di  $(\mathbb{Z}_7)^4$ , strutturato a spazio vettoriale su  $\mathbb{Z}_7$  nel modo usuale:

$$\begin{aligned} W_1 &= \{(a, b, c, d) : a + b + c + d = \bar{0}\}, \\ W_2 &= \{(a, b, c, d) : a + b + c = \bar{0}\}, \\ W_3 &= \{(a, b, c, d) : a + b = \bar{0}\}, \\ W_4 &= \{(a, b, c, d) : a = \bar{0}\}. \end{aligned}$$

**Esercizio 8.2.9.** Si provi 8.2.6.

**Esercizio 8.2.10.** Si provi 8.2.8.

**Esercizio 8.2.11.** Si provi 8.2.10.

**Esercizio 8.2.12.** Si provi 8.2.11.

**Esercizio 8.2.13.** Si consideri l'insieme  $V = \{(2, 0, 0), (0, -3, 0)\}$  nello spazio vettoriale reale  $\mathbb{R}^3$  e, dopo aver descritto  $\langle V \rangle$ , si stabilisca se il vettore  $(5, -2, 0)$  ne è un elemento.

**Esercizio 8.2.14.** Sia  $F[x]$  lo spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$ . Si dimostri che  $F[x]$  non è finitamente generato.

**Esercizio 8.2.15.** Sia  $F[x]$  lo spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$ . Si dimostri che l'insieme infinito  $\{x^n : n \in \mathbb{N}_0\}$  è un insieme minimale di generatori per  $F[x]$ .

**Esercizio 8.2.16.** Si provi 8.2.12.

### 8.3 Dipendenza lineare, basi e dimensione

In questo paragrafo si introdurrà il concetto di dimensione di uno spazio vettoriale, un fondamentale invariante che misura qual è il minimo numero di vettori necessario per generare uno spazio vettoriale. Nel seguito, per semplicità, si tratteranno esclusivamente spazi vettoriali di dimensione finita. In realtà la quasi totalità dei risultati provati restano validi anche per spazi vettoriali di dimensione infinita, sebbene in tale situazione essi necessitino di un approccio dimostrativo differente, che spesso richiede concetti più sofisticati di teoria degli insiemi e della cardinalità.

Sia  $V$  un  $F$ -spazio vettoriale, e sia  $X = \{x_1, x_2, \dots, x_n\}$  un insieme costituito da  $n$  vettori di  $V$ . Si dice **combinazione lineare** dei vettori di  $X$  un qualunque vettore

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$$

con  $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ . Per esempio, nello  $\mathbb{Q}$ -spazio vettoriale  $\mathbb{Q}^2$ , avendosi  $(3, 4) = 3(1, 0) + 4(0, 1) = 2(2, 5) - 1(1, 6)$ , il vettore  $(3, 4)$  è combinazione lineare sia dei vettori di  $\{(1, 0), (0, 1)\}$  che dei vettori di  $\{(2, 5), (1, 6)\}$ .

Dalla 8.2.9 segue subito che:

**8.3.1.** Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $X$  un insieme finito non vuoto di vettori di  $V$ . Allora il sottospazio di  $V$  generato da  $X$  è l'insieme di tutte le combinazioni lineari dei vettori di  $X$  con scalari in  $F$ .

Si dice che l'insieme  $X = \{x_1, x_2, \dots, x_n\}$  di vettori di  $V$ , con  $|X| = n$ , è **linearmente indipendente** se

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0 \iff \alpha_i = 0, \forall i = 1, 2, \dots, n,$$

cioè se l'unica combinazione lineare dei vettori di  $X$  che risulti uguale al vettore nullo è quella con scalari tutti nulli. Talvolta tale circostanza si esprime anche dicendo che gli  $n$  vettori  $x_1, x_2, \dots, x_n$  di  $V$  sono linearmente indipendenti. Per convenzione, l'insieme vuoto è sempre linearmente indipendente. L'insieme di vettori  $X = \{x_1, x_2, \dots, x_n\}$ , con  $|X| = n$ , si dice **linearmente dipendente** se non è linearmente indipendente, cioè se esiste una combinazione lineare dei vettori di  $X$  con scalari non tutti nulli che risulti uguale al vettore nullo. In tal caso si dice anche che gli  $n$  vettori  $x_1, x_2, \dots, x_n$  sono linearmente dipendenti.

**8.3.2. Esempio.** Sia  $V$  uno spazio vettoriale su un campo  $F$ . Allora per ogni  $x \in V \setminus \{0\}$  il singleton  $\{x\}$  è linearmente indipendente, come si ottiene subito applicando (v) di 8.1.7.

**8.3.3. Esempio.** Sia  $F$  un campo. Per ogni  $n \geq 1$ , il sottoinsieme  $\{e_1, \dots, e_n\}$  di  $F^n$  (vedi Esempio 8.2.10) è linearmente indipendente: da  $\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n = 0$  segue  $(\alpha_1, 0, 0, \dots, 0) + (0, \alpha_2, 0, \dots, 0) + \cdots + (0, 0, \dots, 0, \alpha_n) = (\alpha_1, \alpha_2, \dots, \alpha_n) = (0, 0, \dots, 0)$ , cioè  $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ .

**8.3.4. Esempio.** In  $\mathbb{Q}^3$ , strutturato a  $\mathbb{Q}$ -spazio vettoriale nel modo usuale, i vettori  $(1, 2, 0)$ ,  $(\frac{1}{3}, 0, \frac{1}{3})$ ,  $(4, 4, 2)$  sono linearmente dipendenti. Infatti si ha:  $1(1, 2, 0) + 3(\frac{1}{3}, 0, \frac{1}{3}) - \frac{1}{2}(4, 4, 2) = 0$ .

**8.3.5. Esempio.** Siano  $F$  un campo ed  $F[x]$  lo spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in  $F$ . Per ogni  $n \in \mathbb{N}_0$ , i polinomi  $1 = x^0$ ,  $x$ ,  $x^2, \dots, x^n$  sono linearmente indipendenti: se  $f(x) = \alpha_0 + \alpha_1 x^1 + \dots + \alpha_n x^n = 0$  allora  $f(x)$  è il polinomio nullo, pertanto  $\alpha_0 = \alpha_1 = \dots = \alpha_n = 0$ .

Si dice che un vettore  $v \in V$  **dipende linearmente** dagli  $n$  vettori  $x_1, x_2, \dots, x_n$  di  $V$  (o dall'insieme  $X = \{x_1, x_2, \dots, x_n\}$  di vettori di  $V$ ) se  $v \in \langle X \rangle$ , ossia se esistono scalari  $\alpha_1, \alpha_2, \dots, \alpha_n \in F$  tali che  $v = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ .

**8.3.6. Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $X = \{x_1, x_2, \dots, x_n\}$  un insieme non vuoto di vettori di  $V$ , con  $|X| = n$ . Allora:**

- (i) il vettore nullo dipende linearmente da  $X$ ;
- (ii) ogni  $x_i \in X$  dipende linearmente da  $X$ ;
- (iii)  $X$  è un insieme di generatori di  $V$  se e solo se ogni vettore di  $V$  dipende linearmente da  $X$ ;
- (iv) se  $v \in V$  dipende linearmente da  $X$ , e ogni vettore di  $X$  dipende linearmente da  $Y = \{y_1, y_2, \dots, y_m\}$ , allora  $v$  dipende linearmente da  $Y$ .

*Dimostrazione.* (i) e (ii) sono del tutto ovvie, essendo  $0 = 0x_1 + 0x_2 + \dots + 0x_n$  e  $x_i = 0x_1 + \dots + 0x_{i-1} + 1x_i + 0x_{i+1} + \dots + 0x_n$ . La (iii) è una immediata conseguenza di 8.3.1. Per provare la (iv), sia  $v = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ , e si abbia  $x_i = \beta_{i1} y_1 + \beta_{i2} y_2 + \dots + \beta_{im} y_m$  per ogni  $i = 1, 2, \dots, n$ . Allora risulta:

$$\begin{aligned} v &= \sum_{i=1}^n \alpha_i x_i \\ &= \sum_{i=1}^n \alpha_i \left( \sum_{j=1}^m \beta_{ij} y_j \right) \\ &= \sum_{j=1}^m \left( \sum_{i=1}^n \alpha_i \beta_{ij} \right) y_j, \end{aligned}$$

e  $v$  dipende linearmente da  $Y$ . □

**8.3.7. Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $X = \{x_1, x_2, \dots, x_n\}$  un insieme non vuoto di vettori di  $V$ , con  $|X| = n$ . Le seguenti condizioni sono equivalenti:**

- (i) ogni sottoinsieme di  $X$  è linearmente indipendente;
- (ii)  $X$  è linearmente indipendente;
- (iii)  $x_i$  non dipende linearmente da  $X \setminus \{x_i\}$ , per ogni  $i = 1, 2, \dots, n$ .

*Dimostrazione.* (i)  $\Rightarrow$  (ii). Ovvio.

(ii)  $\Rightarrow$  (i). Per assurdo, sia  $Y \subseteq X$  un sottoinsieme di  $X$  linearmente dipendente. Allora  $Y \neq \emptyset$ , e deve esistere una combinazione lineare

$$0 = \sum_{y \in Y} \alpha_y y$$

con scalari  $\alpha_y$  non tutti nulli. Ma da ciò segue subito che

$$0 = \sum_{y \in Y} \alpha_y y + \sum_{x \in X \setminus Y} 0x$$

è una combinazione lineare dei vettori di  $X$  uguale al vettore nullo, e con scalari non tutti nulli. Questo è impossibile in quanto  $X$  è linearmente indipendente per ipotesi.

(ii)  $\Rightarrow$  (iii). Per assurdo, esista un  $j \in \{1, 2, \dots, n\}$  tale che  $x_j$  dipende linearmente da  $X \setminus \{x_j\}$ . Allora risulta

$$x_j = \sum_{i \neq j} \alpha_i x_i,$$

da cui

$$0 = -x_j + \sum_{i \neq j} \alpha_i x_i,$$

una combinazione lineare dei vettori di  $X$  in cui almeno uno scalare (il primo) è non nullo (essendo uguale a  $-1$ ). Ciò è assurdo in quanto  $X$  è linearmente indipendente.

(iii)  $\Rightarrow$  (ii): Per assurdo, sia  $X$  linearmente dipendente. Allora esiste una combinazione lineare del tipo

$$0 = \alpha_1 x_1 + \cdots + \alpha_{i-1} x_{i-1} + \alpha_i x_i + \alpha_{i+1} x_{i+1} + \cdots + \alpha_n x_n, \quad (8.3.1)$$

con  $\alpha_i \neq 0$ . Essendo  $F$  un campo, esiste  $\alpha_i^{-1} \in F$ , e da (8.3.1) segue subito, moltiplicando per  $\alpha_i^{-1}$ ,

$$x_i = -\alpha_1 \alpha_i^{-1} x_1 - \cdots - \alpha_{i-1} \alpha_i^{-1} x_{i-1} - \alpha_{i+1} \alpha_i^{-1} x_{i+1} - \cdots - \alpha_n \alpha_i^{-1} x_n.$$

Ma allora  $x_i$  dipende linearmente da  $X \setminus \{x_i\}$ , una contraddizione.  $\square$

**8.3.8. Corollario.** *Un insieme di vettori che contenga il vettore nullo è sempre linearmente dipendente.*

*Dimostrazione.* Segue subito da (i) di 8.3.6 e da 8.3.7.  $\square$

Il risultato che segue è fondamentale per gli sviluppi successivi.

**8.3.9. Lemma di Steinitz.** *Sia  $V$  uno spazio vettoriale su un campo  $F$ . Se  $x_1, \dots, x_n$  sono  $n$  vettori linearmente indipendenti di  $V$ , e se ciascuno di essi dipende linearmente da  $Y = \{y_1, \dots, y_m\}$  con  $|Y| = m$ , allora  $n \leq m$ .*

*Dimostrazione.* Si ponga  $X = \{x_1, \dots, x_n\}$ , e per assurdo sia  $n \geq m + 1$ . Siccome per ipotesi i vettori  $x_1, \dots, x_{m+1}$  dipendono linearmente da  $Y$ , esistono scalari  $\alpha_{ij} \in F$  tali che

$$\begin{aligned} x_1 &= \alpha_{11}y_1 + \cdots + \alpha_{1m}y_m \\ x_2 &= \alpha_{21}y_1 + \cdots + \alpha_{2m}y_m \\ &\vdots \\ x_{m+1} &= \alpha_{m+1,1}y_1 + \cdots + \alpha_{m+1,m}y_m. \end{aligned} \tag{8.3.2}$$

Se fosse  $\alpha_{11} = \cdots = \alpha_{1m} = 0$  dalla prima equazione di (8.3.2) seguirebbe  $x_1 = 0$ , assurdo per il Corollario 8.3.8 essendo  $X$  linearmente indipendente per ipotesi. Pertanto almeno uno tra gli scalari  $\alpha_{11}, \dots, \alpha_{1m}$  è non nullo, e senza ledere la generalità si può assumere che sia  $\alpha_{11} \neq 0$ . Allora esiste  $\alpha_{11}^{-1} \in F$ , e dalla prima equazione di (8.3.2) segue

$$y_1 = \alpha_{11}^{-1}x_1 - \alpha_{11}^{-1}\alpha_{12}y_2 - \cdots - \alpha_{11}^{-1}\alpha_{1m}y_m.$$

Sostituendo l'espressione appena ottenuta per  $y_1$  nelle rimanenti equazioni di (8.3.2) si ottengono relazioni del tipo

$$\begin{aligned} x_2 &= \beta_{21}x_1 + \beta_{22}y_2 + \cdots + \beta_{2m}y_m \\ x_3 &= \beta_{31}x_1 + \beta_{32}y_2 + \cdots + \beta_{3m}y_m \\ &\vdots \\ x_{m+1} &= \beta_{m+1,1}x_1 + \beta_{m+1,2}y_2 + \cdots + \beta_{m+1,m}y_m, \end{aligned} \tag{8.3.3}$$

con gli scalari  $\beta_{ij}$  in  $F$ . Se fosse  $\beta_{22} = \cdots = \beta_{2m} = 0$  dalla prima equazione di (8.3.3) seguirebbe  $x_2 = \beta_{21}x_1$ , quindi  $x_2$  dipende linearmente da  $X \setminus \{x_2\}$ , assurdo per 8.3.7 essendo  $X$  linearmente indipendente per ipotesi. Pertanto, come prima, almeno uno tra gli scalari  $\beta_{22}, \dots, \beta_{2m}$  è non nullo, e senza ledere la generalità si può assumere che sia  $\beta_{22} \neq 0$ . Dalla prima equazione di (8.3.3) si può allora ricavare  $y_2$ , che risulta combinazione lineare di  $x_1, x_2, y_3, \dots, y_m$ . Sostituendo l'espressione così ottenuta per  $y_2$  nelle rimanenti equazioni di (8.3.3) si ottengono relazioni del tipo

$$\begin{aligned} x_3 &= \gamma_{31}x_1 + \gamma_{32}x_2 + \gamma_{33}y_3 + \cdots + \gamma_{3m}y_m \\ x_4 &= \gamma_{41}x_1 + \gamma_{42}x_2 + \gamma_{43}y_3 + \cdots + \gamma_{4m}y_m \\ &\vdots \\ x_{m+1} &= \gamma_{m+1,1}x_1 + \gamma_{m+1,2}x_2 + \gamma_{m+1,3}y_3 + \cdots + \gamma_{m+1,m}y_m, \end{aligned} \tag{8.3.4}$$

con gli scalari  $\gamma_{ij}$  in  $F$ . Il procedimento indicato consente di eliminare progressivamente tutti gli  $y_i$  e produce, dopo  $m$  passi, una relazione del tipo

$$x_{m+1} = \delta_1 x_1 + \cdots + \delta_m x_m,$$

con gli scalari  $\delta_i$  in  $F$ . Dunque  $x_{m+1}$  dipende linearmente da  $X \setminus \{x_{m+1}\}$  e quindi  $X$  è linearmente dipendente per 8.3.7, la contraddizione voluta. Pertanto  $n \leq m$  e l'asserto è provato.  $\square$

**8.3.10. Corollario.** *Se uno spazio vettoriale  $V$  può essere generato da  $n$  elementi, allora ogni sottoinsieme di  $V$  che contenga più di  $n$  elementi è linearmente dipendente.*

Un sottoinsieme  $X$  di uno spazio vettoriale  $V$  è detto un **insieme linearmente indipendente massimale** se  $X$  è linearmente indipendente, e se non è contenuto propriamente in nessun insieme linearmente indipendente di  $V$ . Ossia se  $X$  è linearmente indipendente, ma  $X \cup \{v\}$  è linearmente dipendente, per ogni vettore  $v \in V \setminus X$ . In altre parole, se  $X$  è un elemento massimale nell'insieme dei sottoinsiemi linearmente indipendenti di  $V$ , ordinato per inclusione.

**8.3.11. Esempio.** Nello  $F$ -spazio vettoriale  $F$ , per ogni  $x \in F \setminus \{0\}$  il singleton  $\{x\}$  è un insieme linearmente indipendente massimale. Infatti innanzitutto  $\{x\}$  è linearmente indipendente (vedi Esempio 8.3.2). Se poi  $X \supset \{x\}$  allora  $X$  non può essere linearmente indipendente. Per rendersi conto di ciò, sia  $y \in X \setminus \{x\}$ . Se  $y = 0$  allora certamente  $X$  è linearmente dipendente per il Corollario 8.3.8. Se invece  $y \neq 0$  allora  $(x^{-1})x + (-y^{-1})y = 0$ , quindi  $\{x, y\}$  è linearmente dipendente, e anche  $X$  lo è per 8.3.7.

Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ . Un sottoinsieme finito  $B$  di  $V$  è detto una **base** di  $V$  se  $B$  è linearmente indipendente e genera  $V$ .

**8.3.12. Esempio.** L'insieme vuoto è una base per lo spazio vettoriale nullo (vedi Esercizio 8.3.3).

**8.3.13. Esempio.** Sia  $F$  un campo. Per ogni  $x \in F \setminus \{0\}$ , il singleton  $\{x\}$  è una base dello  $F$ -spazio vettoriale  $F$ , come si ottiene subito dagli Esempi 8.2.10 e 8.3.2.

**8.3.14. Esempio.** Sia  $F$  un campo. Per ogni  $n \geq 1$ , l'insieme  $\{e_1, e_2, \dots, e_n\}$  (vedi Esempio 8.2.10) è una base di  $F^n$ , come si ottiene subito dagli Esempi 8.2.10 e da 8.3.3. Tale base è detta la **base canonica** di  $F^n$ .

**8.3.15. Esempio.** Sia  $F[x]$  lo  $F$ -spazio vettoriale dei polinomi nell'indeterminata  $x$  a coefficienti in un campo  $F$ . Per ogni numero intero non negativo  $n$ , l'insieme  $\{1 = x^0, x, x^2, \dots, x^n\}$  è una base del sottospazio  $F[x; n]$  costituito dal polinomio nullo e dai polinomi di grado al più  $n$  (vedi Esempio 8.2.5 ed Esercizio 8.3.4).

**8.3.16. Esempio.** Sia  $F$  un campo, e si denoti con  $M_{n,m}(F)$  lo spazio vettoriale su  $F$  costituito dalle matrici  $n \times m$  a entrate in  $F$  (vedi Esempio 8.1.3). Per ogni  $i = 1, 2, \dots, n$  e per ogni  $j = 1, 2, \dots, m$  si denoti con  $E_{ij}$  la matrice  $n \times m$  avente 1 al posto  $(i, j)$  e 0 altrove. Si osservi innanzitutto che per ogni  $\alpha_{ij} \in F$  (con  $i \in \{1, 2, \dots, n\}$  e  $j \in \{1, 2, \dots, m\}$ ) risulta

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_{ij} E_{ij} = (\alpha_{ij}), \quad (8.3.5)$$

ossia la matrice di  $M_{n,m}(F)$  che ha al posto  $(i, j)$  esattamente l'elemento  $\alpha_{ij}$ . Quindi l'insieme  $B = \{E_{ij} : 1 \leq i \leq n, 1 \leq j \leq m\}$  genera  $M_{n,m}(F)$ . Inoltre  $B$  è linearmente indipendente, in quanto da

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_{ij} E_{ij} = 0$$

segue subito per (8.3.5) che  $(\alpha_{ij})$  è la matrice nulla, ossia  $\alpha_{ij} = 0$  per ogni  $i = 1, 2, \dots, n$  e per ogni  $j = 1, 2, \dots, m$ . Pertanto  $B$  è una base per  $M_{n,m}(F)$ . Tale base è detta la **base canonica** di  $M_{n,m}(F)$ .

Il risultato che segue assicura che ogni spazio vettoriale finitamente generato possiede una base, che può essere “estratta” da un qualunque insieme finito di generatori dello spazio.

**8.3.17.** *Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ . Allora ogni insieme finito di generatori di  $V$  contiene una base di  $V$ .*

*Dimostrazione.* Sia  $X$  un insieme finito di generatori di  $V$ , e si ragioni per induzione sull'ordine  $|X|$  di  $X$ . Se  $|X| = 0$ , allora  $X = \emptyset$  è linearmente indipendente, quindi è una base di  $V$ . Sia ora  $|X| = n > 0$ . Ovviamente si può assumere che  $X$  non sia una base di  $V$ . Allora  $X$  è linearmente dipendente. Pertanto 8.3.7 assicura che esiste un vettore  $x_i \in X$  che dipende linearmente da  $Y = X \setminus \{x_i\}$ . Ne segue che ogni vettore di  $X$  dipende linearmente da  $Y$ . Da ciò, ricordando che ogni vettore  $x \in V$  dipende linearmente da  $X$  (in quanto  $\langle X \rangle = V$ ), e applicando la (iv) di 8.3.6, si ottiene subito che  $\langle Y \rangle = V$ , ossia  $Y$  è un insieme finito di generatori di  $V$ . Siccome  $|Y| = n - 1$ , l'ipotesi induttiva garantisce che  $Y$ , e quindi anche  $X$ , contiene una base di  $V$ , come volevasi.  $\square$

Quella che segue è la proprietà fondamentale delle basi di uno spazio vettoriale.

**8.3.18.** *Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $B$  un sottoinsieme finito di  $V$ . Allora  $B$  è una base di  $V$  se e solo se ogni vettore di  $V$  si esprime in unico modo come combinazione lineare dei vettori di  $B$ .*

*Dimostrazione.* Esercizio. □

Le seguenti caratterizzazioni delle basi sono spesso molto utili.

**8.3.19.** Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ , e sia  $B$  un sottoinsieme finito di  $V$ . Le seguenti condizioni sono equivalenti:

- (i)  $B$  è una base di  $V$ ;
- (ii)  $B$  è un insieme minimale di generatori di  $V$ ;
- (iii)  $B$  è un insieme linearmente indipendente massimale di  $V$ .

*Dimostrazione.* (i)  $\Rightarrow$  (ii). Per ipotesi  $B$  è una base, quindi è un insieme di generatori di  $V$ . Bisogna perciò solo provarne la minimalità (rispetto all'inclusione) tra gli insiemi di generatori di  $V$ . In altre parole, bisogna dimostrare che se  $Y \subset B$  allora  $\langle Y \rangle \neq V$ . Sia per assurdo  $\langle Y \rangle = V$ . Certamente esiste  $b \in B \setminus Y$ . Allora  $b$  dipende linearmente dai vettori di  $Y$ , quindi per 8.3.7 l'insieme  $Y \cup \{b\}$  è linearmente dipendente. Ma quest'ultimo è un sottoinsieme di  $B$ , che è linearmente indipendente per ipotesi: un assurdo ancora per 8.3.7.

(ii)  $\Rightarrow$  (i). Siccome  $B$  è un insieme minimale di generatori di  $V$ , allora 8.3.17 assicura che  $B$  contiene una base  $B_1$  di  $V$ . Per la minimalità di  $B$  tra gli insiemi di generatori di  $V$  si ha  $B_1 = B$ , cioè  $B$  è una base di  $V$ .

(i)  $\Rightarrow$  (iii). Per ipotesi  $B$  è linearmente indipendente. Se poi  $X$  è un sottoinsieme di  $V$  che contiene propriamente  $B$  allora ogni elemento  $x \in X \setminus B$  dipende linearmente da  $B$ , in quanto  $\langle B \rangle = V$ . Pertanto  $B \cup \{x\}$  è linearmente dipendente per 8.3.7, e anche  $X$ , contenendo  $B \cup \{x\}$ , risulta linearmente dipendente. Ciò significa che  $B$  è un insieme linearmente indipendente massimale di  $V$ .

(iii)  $\Rightarrow$  (i). Sia  $B = \{x_1, x_2, \dots, x_n\}$ , con  $|B| = n$ . Occorre provare che  $\langle B \rangle = V$ . Sia  $x \in V$ . Se  $x \in B$  allora  $x \in \langle B \rangle$  per la (ii) di 8.3.6. Se invece  $x \notin B$  allora  $B \cup \{x\}$  contiene propriamente  $B$ . Siccome  $B$  è massimale come insieme linearmente indipendente di  $V$ , necessariamente  $B \cup \{x\}$  è linearmente dipendente. Ne segue che esistono scalari  $\alpha, \alpha_1, \dots, \alpha_n \in F$  non tutti nulli tali che

$$\alpha x + \alpha_1 x_1 + \cdots + \alpha_n x_n = 0. \quad (8.3.6)$$

Se fosse  $\alpha = 0$  dalla (8.3.6) seguirebbe  $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$ , e ciò è assurdo perché gli  $\alpha_i$  non possono essere tutti nulli e  $B$  è linearmente indipendente. Pertanto  $\alpha \neq 0$ , quindi esiste  $\alpha^{-1} \in F$ . Allora dalla (8.3.6) si ottiene

$$x = (-\alpha^{-1} \alpha_1)x_1 + \cdots + (-\alpha^{-1} \alpha_n)x_n,$$

cioè  $x \in \langle B \rangle$ , come volevasi. □

In uno spazio vettoriale finitamente generato ogni insieme di vettori linearmente indipendente può essere ampliato fino a ottenere una base.

**8.3.20.** Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ . Allora ogni insieme finito  $X$  di vettori linearmente indipendenti di  $V$  è contenuto in una base di  $V$ .

*Dimostrazione.* Sia  $B$  un base di  $V$ , e sia  $|B| = n$ . Allora il Corollario 8.3.10 assicura che ogni sottoinsieme di  $V$  che contenga più di  $n$  elementi è linearmente dipendente. Sia  $|X| = m$ . Se  $m = n$  allora  $X$  è un insieme linearmente indipendente massimale, quindi una base di  $V$  per 8.3.19, e non c'è nulla da provare. Sia ora  $m < n$ . Si scelga un vettore  $y_1 \in V \setminus \langle X \rangle$ . Allora  $X_1 = X \cup \{y_1\}$  è linearmente indipendente (vedi Esercizio 8.3.2) e ha ordine  $m + 1$ . Si scelga poi un vettore  $y_2 \in V \setminus \langle X_1 \rangle$ , e si prosegua nella maniera indicata. Dopo  $n - m$  passi si ottiene il sistema linearmente indipendente massimale  $X \cup \{y_1, \dots, y_{n-m}\}$  che contiene  $X$ , come volevasi.  $\square$

**8.3.21.** *Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ . Allora tutte le basi di  $V$  hanno lo stesso ordine.*

*Dimostrazione.* Siano  $B_1$  e  $B_2$  basi di  $V$ . Siccome  $B_1$  è un insieme linearmente indipendente, e ogni vettore di  $B_1$  dipende linearmente da  $B_2$ , il lemma di Steinitz (vedi 8.3.9) assicura che  $|B_1| \leq |B_2|$ . Invertendo i ruoli di  $B_1$  e  $B_2$  nel ragionamento precedente si ottiene anche  $|B_2| \leq |B_1|$ , da cui  $|B_1| = |B_2|$ .  $\square$

La 8.3.21 consente di definire la **dimensione** su  $F$  di un  $F$ -spazio vettoriale finitamente generato  $V$  come l'ordine di una sua base. Tale intero non negativo viene denotato con  $\dim_F V$ .

**8.3.22. Esempio.** Lo spazio vettoriale nullo ha dimensione 0 su qualsiasi campo (vedi Esempio 8.3.12). Un qualunque spazio vettoriale finitamente generato e non nullo ha dimensione positiva. Dall'Esempio 8.3.14 si ricava subito che  $\dim_F F^n = n$ . Ancora, se  $F[x; n]$  è il sottospazio di  $F[x]$  costituito dal polinomio nullo e dai polinomi di grado al più  $n$  risulta  $\dim_F F[x; n] = n + 1$  (vedi Esempio 8.3.15). Dall'Esempio 8.3.16 si ricava poi  $\dim_F M_{n,m}(F) = nm$ .

**8.3.23.** *Sia  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ . Allora ogni sottospazio  $W$  di  $V$  è finitamente generato, e risulta  $\dim_F W \leq \dim_F V$ .*

*Dimostrazione.* Per il Corollario 8.3.10 l'ordine dei sottoinsiemi linearmente indipendenti di  $W$  non supera  $\dim_F V$ . Sia  $B$  un sottoinsieme linearmente indipendente massimale di  $W$ . Per (iii) di 8.3.19,  $B$  è una base di  $W$ . Pertanto  $W$  è finitamente generato e  $\dim_F W \leq \dim_F V$ .  $\square$

Sia  $V$  uno spazio vettoriale di dimensione  $n$  su un campo  $F$ . Data una base  $B = \{x_1, \dots, x_n\}$  di  $V$ , per ogni vettore  $x \in V$  esistono, e sono univocamente determinati, scalari  $\alpha_1, \dots, \alpha_n \in F$  tali che  $x = \alpha_1 x_1 + \dots + \alpha_n x_n$  (vedi 8.3.18). Gli scalari  $\alpha_1, \dots, \alpha_n$  sono detti le **componenti** di  $x$  nella base  $B$ .

**Osservazione.** Una qualunque  $n$ -upla  $(x_1, \dots, x_n) \in V^n$  tale che  $\{x_1, \dots, x_n\}$  sia una base di  $V$  è detta una **base ordinata** di  $V$ . L'esigenza di fissare un ordine tra gli elementi di una base  $B$  scaturisce dalla frequente necessità di rappresentare le componenti in  $B$  di ogni vettore  $x$  di  $V$  mediante un vettore di  $F^n$ , il cosiddetto **vettore coordinato** di  $x$  relativo alla base  $B$ . Per evitare di appesantire la trattazione, nel seguito del presente capitolo e in tutto il Capitolo 9, ogni volta che si parlerà del vettore  $(\alpha_1, \dots, \alpha_n)$  delle componenti di un vettore  $x$  di  $V$  nella base  $B = \{x_1, \dots, x_n\}$  si supporrà tacitamente che i vettori di  $B$  siano ordinati nel modo in cui appaiono scritti, cioè si continuerà a denotare con  $B = \{x_1, \dots, x_n\}$  la base ordinata  $(x_1, \dots, x_n)$ .

## Esercizi

**Esercizio 8.3.1.** Siano  $x, y, z$  vettori linearmente indipendenti in uno spazio vettoriale  $V$ . Si dimostri che l'insieme  $\{x+y, x-y, x-2y+z\}$  è ancora linearmente indipendente.

**Esercizio 8.3.2.** Sia  $X = \{x_1, \dots, x_n\}$  un insieme linearmente indipendente in uno spazio vettoriale  $V$ . Si provi che se  $x \in V \setminus \langle X \rangle$  allora  $X \cup \{x\}$  è linearmente indipendente.

*Suggerimento.* Si ragioni come in (iii)  $\implies$  (i) della dimostrazione di 8.3.19.

**Esercizio 8.3.3.** Si dimostri 8.3.12.

**Esercizio 8.3.4.** Si dimostri 8.3.15.

**Esercizio 8.3.5.** Si dimostri 8.3.18.

**Esercizio 8.3.6.** Sia  $V$  uno spazio vettoriale di dimensione  $n$  su un campo  $F$ . Si dimostri che ogni insieme di generatori di  $V$  di ordine  $n$  è una base di  $V$ .

**Esercizio 8.3.7.** Sia  $V$  uno spazio vettoriale di dimensione  $n$  su un campo  $F$ . Si dimostri che ogni insieme linearmente indipendente di ordine  $n$  è una base di  $V$ .

**Esercizio 8.3.8.** Nell'insieme  $\mathbb{R}^3$  strutturato a spazio vettoriale su  $\mathbb{R}$ , si stabilisca quali dei seguenti insiemi di vettori sono linearmente indipendenti:

$$\begin{aligned} A &= \{(1, 0, 0), (2, 1, 0)\}, \\ B &= \{(0, 2, 3), (0, -4, -6)\}, \\ C &= \{(1, 0, 0), (3, 2, 0), (0, 1, 0)\}, \\ D &= \{(2, 0, 0), (1, -5, 0), (0, -2, 1)\}. \end{aligned}$$

**Esercizio 8.3.9.** Nell'insieme  $\mathbb{R}^2$  strutturato a spazio vettoriale su  $\mathbb{R}$ , si stabilisca quali dei seguenti insiemi di vettori sono linearmente indipendenti, quali sono un

sistema di generatori dello spazio, e quali costituiscono una base:

$$\begin{aligned} A &= \{(2, 12), (-\pi, -\pi)\}, \\ B &= \{(2, -1/3), (-1, 1/6)\}, \\ C &= \{(2/3, 3/2), (2, 3)\}, \\ D &= \{(1, 2), (3, -2\sqrt{2}), (-2, 2)\}. \end{aligned}$$

**Esercizio 8.3.10.** Si determini una base e la dimensione dei seguenti sottospazi di  $\mathbb{R}^4$ , strutturato a spazio vettoriale su  $\mathbb{R}$  nel modo usuale:

$$\begin{aligned} V &= \{(a, b, c, d) : a - c + d = 0\}; \\ W &= \{(a, b, c, d) : a = c, b = 2d\}. \end{aligned}$$

**Esercizio 8.3.11.** Si determini una base per il sottospazio di  $\mathbb{Q}^4$  (strutturato a spazio vettoriale su  $\mathbb{Q}$ ) generato dai vettori seguenti:

$$x_1 = (1, 1, 2, 3), x_2 = (3, 2, 1, 0), x_3 = (-1, 0, 3, 6), x_4 = (2, 2, 2, 2).$$

**Esercizio 8.3.12.** Nello  $\mathbb{Q}$ -spazio vettoriale  $\mathbb{Q}[x]$  si considerino i vettori

$$\begin{aligned} v_1 &= x^3 - 2x^2 + 4x + 1, & v_2 &= x^3 + 6x - 5, \\ v_3 &= 2x^3 - 3x^2 + 9x - 1, & v_4 &= 2x^3 - 5x^2 + 7x + 5. \end{aligned}$$

Si determinino una base e la dimensione del sottospazio  $W = \langle v_1, v_2, v_3, v_4 \rangle$ .

**Esercizio 8.3.13.** Si determinino tre basi distinte per ciascuno dei seguenti sottospazi di  $(\mathbb{Z}_{11})^3$  (strutturato a spazio vettoriale su  $\mathbb{Z}_{11}$ ):

$$\begin{aligned} W_1 &= \{(x, y, x - 2y) : x, y \in \mathbb{Z}_{11}\}, \\ W_2 &= \{(x, y + z, x + z) : x, y, z \in \mathbb{Z}_{11}\}, \\ W_3 &= \{(x, x + y, z) : x, y, z \in \mathbb{Z}_{11}\}. \end{aligned}$$

**Esercizio 8.3.14.** Nell'insieme  $M_{2,3}(\mathbb{Q})$  strutturato a spazio vettoriale su  $\mathbb{Q}$ , si stabilisca se le matrici

$$\left( \begin{array}{ccc} 1 & 1 & 1 \\ 2 & 0 & 1 \end{array} \right), \quad \left( \begin{array}{ccc} 2 & -2 & 1 \\ 1 & 0 & 0 \end{array} \right), \quad \left( \begin{array}{ccc} 1 & 1 & 0 \\ -1 & 0 & 1 \end{array} \right)$$

sono linearmente indipendenti, e se costituiscono una base.

**Esercizio 8.3.15.** Dopo aver provato che l'insieme

$$B = \{(-1, -1, -1), (1, -1, 0), (-1, 0, 0)\}$$

è una base dell'usuale spazio vettoriale reale  $\mathbb{R}^3$ , si determinino le componenti in tale base dei vettori  $v = (-3, 1, 2)$  e  $w = (0, 1, 1)$ .

**Esercizio 8.3.16.** Sia  $F$  un campo e sia  $A = (a_{ij}) \in M_n(F)$  una matrice quadrata. Si definisce **traccia** di  $A$  l'elemento  $\text{tr}(A) := a_{11} + a_{22} + \dots + a_{nn} \in F$ . Si dimostri che il sottoinsieme  $\{A \in M_n(F) : \text{tr}(A) = 0\}$  è un sottospazio dello  $F$ -spazio vettoriale  $M_n(F)$ , e se ne determini la dimensione.

## 8.4 Applicazioni lineari

Siano  $V_1$  e  $V_2$  spazi vettoriali su uno stesso campo  $F$ . Un'applicazione

$$f : V_1 \longrightarrow V_2$$

è detta un'*applicazione lineare* (o un *omomorfismo di spazi vettoriali*, o anche un  *$F$ -omomorfismo*) di  $V_1$  in  $V_2$  se per ogni  $x, y \in V_1$  e per ogni  $\alpha \in F$  si ha:

$$\begin{cases} f(x+y) = f(x) + f(y), \\ f(\alpha x) = \alpha f(x). \end{cases} \quad (8.4.1)$$

Dalla definizione segue subito che un'applicazione lineare  $f : V_1 \longrightarrow V_2$  è in particolare un omomorfismo di gruppi abeliani tra le strutture additive  $(V_1, +)$  e  $(V_2, +)$ . Utilizzando la terminologia ormai consueta, anche tra spazi vettoriali un omomorfismo iniettivo (rispettivamente suriettivo, biettivo) viene detto un *monomorfismo* (risp. *epimorfismo, isomorfismo*). Un omomorfismo di uno spazio vettoriale in se stesso viene detto un *endomorfismo (automorfismo)* se esso è biettivo). Spazi vettoriali  $V_1$  e  $V_2$  su uno stesso campo si dicono *isomorfi* (e si scrive  $V_1 \simeq V_2$ ) se esiste un isomorfismo  $f : V_1 \longrightarrow V_2$ .

### 8.4.1. Esempi.

$$\begin{aligned} x \in V &\longmapsto 0 \in V \\ x \in V &\longmapsto x \in V \end{aligned}$$

sono lineari (vedi Esercizio 8.4.2), e sono dette rispettivamente l'*endomorfismo nullo* di  $V$  e l'*automorfismo identico* di  $V$ .

Con  $V_1$  e  $V_2$  spazi vettoriali su un campo  $F$ , l'applicazione

$$x \in V_1 \longmapsto 0 \in V_2$$

è lineare (ed è detta l'*omomorfismo nullo* di  $V_1$  in  $V_2$ ).

Per ogni sottospazio  $W$  di uno spazio vettoriale  $V$ , l'applicazione

$$x \in W \longmapsto x \in V$$

è un monomorfismo (ed è detto l'*immersione* di  $W$  in  $V$ ).

Siano  $V$  uno spazio vettoriale su un campo  $F$ , e  $W$  un sottospazio di  $V$ . In  $V$  si definisca una relazione  $\mathcal{R}_W$  ponendo

$$x \mathcal{R}_W y : \iff x - y \in W.$$

La relazione  $\mathcal{R}_W$  è riflessiva, in quanto per ogni  $x \in V$  risulta  $x - x = 0 \in W$ , quindi  $x \mathcal{R}_W x$ . Inoltre essa è simmetrica, perché da  $x, y \in V$  e  $x \mathcal{R}_W y$  segue  $x - y \in W$ , quindi  $y - x = -(x - y) \in W$ , pertanto  $y \mathcal{R}_W x$ . Infine  $\mathcal{R}_W$  è transitiva, infatti da  $x, y, z \in V$  e  $x \mathcal{R}_W y$ ,  $y \mathcal{R}_W z$  segue  $x - y, y - z \in W$ ,

quindi  $x - z = (x - y) + (y - z) \in W$ , cioè  $x \mathcal{R}_W z$ . Pertanto  $\mathcal{R}_W$  è una relazione d'equivalenza in  $V$ .

Per ogni  $x \in V$  si denoti con il simbolo  $x + W$  la classe d'equivalenza di  $x$  rispetto a  $\mathcal{R}_W$ :

$$x + W := [x]_{\mathcal{R}_W} = \{y \in V : x - y \in W\} = \{x + w : w \in W\}.$$

Si denoti poi con  $V/W$  l'insieme quoziante di  $V$  rispetto a  $\mathcal{R}_W$ :

$$V/W := V/\mathcal{R}_W = \{x + W : x \in V\}.$$

Si osservi che in  $V/W$  risulta:

$$x + W = y + W \iff x - y \in W. \quad (8.4.2)$$

La relazione d'equivalenza  $\mathcal{R}_W$  è compatibile rispetto all'operazione  $+$  in  $V$ : infatti da  $x \mathcal{R}_W y$  e  $z \mathcal{R}_W t$  segue  $x - y, z - t \in W$ , cioè  $x + z - (y + t) \in W$ , dunque  $(x + z) + W = (y + t) + W$ . Ciò consente, come fatto nel Paragrafo 4.2, di definire l'operazione quoziante

$$+ : (x + W, y + W) \in V/W \times V/W \longmapsto (x + y) + W \in V/W.$$

Siccome  $(V, +)$  è un gruppo abeliano, 4.2.10 assicura che anche  $(V/W, +)$  è un gruppo abeliano. In particolare, l'elemento neutro di  $(V/W, +)$  è

$$0 + W = [0]_{\mathcal{R}_W} = \{0 + w : w \in W\} = W, \quad (8.4.3)$$

e l'opposto di un elemento  $x + W$  è

$$-(x + W) = (-x) + W. \quad (8.4.4)$$

La relazione d'equivalenza  $\mathcal{R}_W$  è compatibile anche rispetto al prodotto per uno scalare di  $F$ : infatti da  $x \mathcal{R}_W y$  e  $\alpha \in F$  segue  $\alpha(x - y) = \alpha x - \alpha y \in W$ , dunque  $\alpha x + W = \alpha y + W$ . Ciò consente di definire l'operazione quoziante

$$\cdot : (\alpha, x + W) \in F \times V/W \longmapsto \alpha x + W \in V/W.$$

Si verifica agevolmente che la struttura algebrica  $(V/W, +, \cdot)$  è uno spazio vettoriale su  $F$  (detto lo **spazio vettoriale quoziante** di  $V$  rispetto a  $W$ ). Infatti le proprietà (i) – (iv) della definizione di spazio vettoriale valgono in quanto, come ricordato,  $(V/W, +)$  è un gruppo abeliano, mentre le proprietà (v) – (viii) si possono verificare in maniera diretta, utilizzando essenzialmente le analoghe proprietà di  $V$ .

**8.4.2. Esempio.** Sia  $V$  uno spazio vettoriale, e si considerino i sottospazi banali  $\{0\}$  e  $V$  di  $V$ . Lo spazio vettoriale quoziante  $V/\{0\}$  ha come elementi i laterali  $x + \{0\}$  con  $x \in V$ , e ovviamente l'applicazione  $x \in V \longmapsto x + \{0\} \in V/\{0\}$  è un isomorfismo. Quindi  $V/\{0\} \simeq V$ . Invece lo spazio vettoriale quoziante  $V/V$  contiene un unico elemento,  $0 + V$ , e pertanto è lo spazio vettoriale nullo.

Se  $f : V_1 \rightarrow V_2$  è un'applicazione lineare, il sottoinsieme di  $V_1$

$$\text{Ker } f := \{x \in V_1 : f(x) = 0\}$$

è detto il **nucleo** di  $f$ , mentre il sottoinsieme di  $V_2$

$$\text{Im } f := f(V_1)$$

è detto l'**immagine** di  $f$ . Il risultato che segue, di importanza fondamentale, è ovviamente un caso particolare di 4.3.10.

**8.4.3. Teorema di omomorfismo (negli spazi vettoriali).** *Sia  $f : V_1 \rightarrow V_2$  un'applicazione lineare. Allora:*

- (i) *Ker  $f$  è un sottospazio di  $V_1$ ;*
- (ii) *Im  $f$  è un sottospazio di  $V_2$ ;*
- (iii) *gli spazi vettoriali  $V_1 / \text{Ker } f$  e  $\text{Im } f$  sono isomorfi;*
- (iv) *per ogni sottospazio  $W$  di  $V_1$ , l'applicazione*

$$\pi_W : x \in V_1 \longmapsto x + W \in V_1/W$$

*è un epimorfismo (detto l'**epimorfismo canonico** di  $V_1$  in  $V_1/W$ ); inoltre risulta  $\text{Ker } \pi_W = W$ .*

*Dimostrazione.* (i) Siccome  $f$  è in particolare un omomorfismo di gruppi, dal Teorema 6.3.24 segue che  $(\text{Ker } f, +)$  è un sottogruppo di  $(V_1, +)$ . Siano poi  $\alpha \in F$  e  $x \in \text{Ker } f$ . Allora  $f(\alpha x) = \alpha f(x) = \alpha 0 = 0$  per (i) di 8.1.7, quindi  $\alpha x \in \text{Ker } f$ , e  $\text{Ker } f$  è un sottospazio di  $V_1$ .

(ii) Siccome  $f$  è in particolare un omomorfismo di gruppi, ancora dal Teorema 6.3.24 segue che  $(\text{Im } f, +)$  è un sottogruppo di  $(V_2, +)$ . Siano poi  $\alpha \in F$  e  $y \in \text{Im } f$ . Allora esiste un vettore  $x \in V_1$  tale che  $f(x) = y$ . Poiché ovviamente  $\alpha x \in V_1$ , da  $\alpha y = \alpha f(x) = f(\alpha x)$  segue che  $\alpha y \in \text{Im } f$ , e  $\text{Im } f$  è un sottospazio di  $V_2$ .

(iii) Si osservi innanzitutto che, in virtù di (8.4.2),  $x + \text{Ker } f = y + \text{Ker } f$  equivale a  $x - y \in \text{Ker } f$ , quindi a  $f(x - y) = 0$ , cioè  $f(x) = f(y)$  per la linearità di  $f$ . Ciò assicura che l'assegnazione

$$\begin{aligned} \varphi : V_1 / \text{Ker } f &\longrightarrow \text{Im } f \\ x + \text{Ker } f &\longmapsto f(x) \end{aligned}$$

definisce un'applicazione iniettiva. Tale applicazione è anche evidentemente suriettiva, in quanto per ogni elemento  $f(x) \in \text{Im } f$  si ha  $x + \text{Ker } f \in V_1 / \text{Ker } f$  e  $\varphi(x + \text{Ker } f) = f(x)$ . Inoltre l'applicazione  $\varphi$  è lineare, giacché per ogni  $\alpha \in F$  e per ogni  $x, y \in V_1$  risulta

$$\begin{aligned} \varphi((x + \text{Ker } f) + (y + \text{Ker } f)) &= \varphi((x + y) + \text{Ker } f) \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= \varphi(x + \text{Ker } f) + \varphi(y + \text{Ker } f) \end{aligned}$$

e

$$\begin{aligned}\varphi(\alpha(x + \text{Ker } f)) &= \varphi((\alpha x) + \text{Ker } f) \\ &= f(\alpha x) \\ &= \alpha f(x) \\ &= \alpha \varphi(x + \text{Ker } f).\end{aligned}$$

Pertanto  $\varphi$  è un isomorfismo di spazi vettoriali e l'asserto è provato.

(iv) L'applicazione  $\pi_W$  è banalmente suriettiva. Inoltre essa è lineare, in quanto per ogni  $\alpha \in F$  e per ogni  $x, y \in V_1$  risulta

$$\begin{aligned}\pi_W(x + y) &= (x + y) + W = (x + W) + (y + W) = \pi_W(x) + \pi_W(y), \\ \pi_W(\alpha x) &= (\alpha x) + W = \alpha(x + W) = \alpha \pi_W(x).\end{aligned}$$

Infine  $x \in \text{Ker } \pi_W$  se e solo se  $\pi_W(x) = W$ , che per (8.4.3) è lo zero additivo di  $V_1/W$ .  $\square$

**8.4.4. Corollario.** *Un'applicazione lineare  $f : V_1 \rightarrow V_2$  è un monomorfismo se e solo se  $\text{Ker } f = \{0\}$ .*

*Dimostrazione.* Se  $f$  è iniettiva e  $x \in \text{Ker } f$  allora  $f(x) = 0 = f(0)$  perché  $f$  è in particolare omomorfismo di gruppi, quindi  $x = 0$ ; ne segue che  $\text{Ker } f = \{0\}$ . Viceversa, da  $\text{Ker } f = \{0\}$  e  $f(x) = f(y)$  segue  $f(x - y) = 0$ , e ciò implica  $x - y \in \text{Ker } f$ , dunque  $x - y = 0$  e  $x = y$ ; pertanto  $f$  è iniettiva.  $\square$

Negli spazi vettoriali di dimensione finita le dimensioni di nucleo e immagine di un'applicazione lineare sono legate tra loro, come mostra il risultato che segue.

**8.4.5.** *Siano  $V_1$  e  $V_2$  spazi vettoriali finitamente generati su un campo  $F$ , e sia  $f : V_1 \rightarrow V_2$  un'applicazione lineare. Allora:*

$$\dim_F \text{Ker } f + \dim_F \text{Im } f = \dim_F V_1.$$

*Dimostrazione.* L'asserto è banalmente vero se  $V_1$  è lo spazio nullo; si assuma quindi  $V_1 \neq \{0\}$ . Sia  $\dim_F \text{Ker } f = r$ , e sia  $\{x_1, \dots, x_r\}$  una base di  $\text{Ker } f$ . Per 8.3.20, posto  $\dim_F V_1 = n \geq r$ , esistono vettori  $x_{r+1}, \dots, x_n \in V_1$  tali che  $\{x_1, \dots, x_n\}$  è una base di  $V_1$ . Si proverà che i vettori  $f(x_{r+1}), \dots, f(x_n) \in V_2$  costituiscono una base di  $\text{Im } f$ . Se  $0 = \alpha_{r+1}f(x_{r+1}) + \dots + \alpha_nf(x_n)$  con scalari  $\alpha_{r+1}, \dots, \alpha_n \in F$ , allora  $f(\alpha_{r+1}x_{r+1} + \dots + \alpha_nx_n) = 0$  per la linearità di  $f$ , dunque  $\alpha_{r+1}x_{r+1} + \dots + \alpha_nx_n \in \text{Ker } f$ . Ciò implica, essendo  $\{x_1, \dots, x_r\}$  una base di  $\text{Ker } f$ , che esistono scalari  $\alpha_1, \dots, \alpha_r \in F$  tali che  $\alpha_1x_1 + \dots + \alpha_rx_r = \alpha_{r+1}x_{r+1} + \dots + \alpha_nx_n$ . Di qui ovviamente segue che  $\alpha_1x_1 + \dots + \alpha_rx_r - \alpha_{r+1}x_{r+1} - \dots - \alpha_nx_n = 0$ . Essendo  $\{x_1, \dots, x_n\}$  una base di  $V_1$ , da ciò si ottiene  $\alpha_1 = \dots = \alpha_n = 0$ . Si è così provato che i vettori  $f(x_{r+1}), \dots, f(x_n)$

sono linearmente indipendenti. Inoltre essi generano  $\text{Im } f$ , in quanto per ogni  $y \in \text{Im } f$  risulta  $y = f(x)$  con  $x = \beta_1 x_1 + \cdots + \beta_n x_n \in V_1$ , da cui

$$\begin{aligned} y &= f(\beta_1 x_1 + \cdots + \beta_n x_n) \\ &= \beta_1 f(x_1) + \cdots + \beta_r f(x_r) + \beta_{r+1} f(x_{r+1}) + \cdots + \beta_n f(x_n) \\ &= \beta_{r+1} f(x_{r+1}) + \cdots + \beta_n f(x_n) \end{aligned}$$

in quanto  $f(x_1) = \cdots = f(x_r) = 0$  essendo  $x_1, \dots, x_r \in \text{Ker } f$ . Dunque  $\{f(x_{r+1}), \dots, f(x_n)\}$  è una base di  $\text{Im } f$ , e l'asserto segue subito.  $\square$

**8.4.6.** *Sia  $f : V_1 \rightarrow V_2$  un'applicazione lineare. Allora:*

- (i) *se  $f$  è iniettiva e  $x_1, \dots, x_n$  sono vettori linearmente indipendenti di  $V_1$ , allora  $f(x_1), \dots, f(x_n)$  sono vettori linearmente indipendenti di  $V_2$ ;*
- (ii) *se  $f$  è suriettiva e  $\langle x_1, \dots, x_n \rangle = V_1$ , allora  $\langle f(x_1), \dots, f(x_n) \rangle = V_2$ .*

*Dimostrazione.* (i) Siano  $f$  iniettiva e  $X = \{x_1, \dots, x_n\}$  un sottoinsieme linearmente indipendente di  $V_1$ . Da  $\alpha_1 f(x_1) + \cdots + \alpha_n f(x_n) = 0$  segue subito  $f(\alpha_1 x_1 + \cdots + \alpha_n x_n) = 0$  per la linearità di  $f$ , e poi  $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$  per l'iniettività di  $f$ . Siccome  $X$  è linearmente indipendente, si ha  $\alpha_1 = \cdots = \alpha_n = 0$ , ed  $f(X)$  è linearmente indipendente.

(ii) Siano  $f$  suriettiva e  $\langle x_1, \dots, x_n \rangle = V_1$ . Per ogni  $y \in V_2$ , la suriettività di  $f$  implica l'esistenza di un vettore  $x \in V_1$  tale che  $f(x) = y$ . Allora esistono  $\alpha_1, \dots, \alpha_n \in F$  tali che  $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$ . Pertanto

$$y = f(x) = f(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \alpha_1 f(x_1) + \cdots + \alpha_n f(x_n)$$

per la linearità di  $f$ . Ciò significa che  $\langle f(x_1), \dots, f(x_n) \rangle = V_2$ .  $\square$

Di qui segue subito che:

**8.4.7. Corollario.** *Ogni isomorfismo di spazi vettoriali trasforma basi in basi.*

Si osservi che nella dimostrazione di 8.4.6 (ii) si è in realtà provato che:

**8.4.8.** *Sia  $f : V_1 \rightarrow V_2$  un'applicazione lineare. Se  $\langle x_1, \dots, x_n \rangle = V_1$ , allora  $\langle f(x_1), \dots, f(x_n) \rangle = \text{Im } f$ .*

**8.4.9. Teorema.** *Siano  $V_1$  e  $V_2$  spazi vettoriali su un campo  $F$ ,  $B = \{x_1, \dots, x_n\}$  una base di  $V_1$ ,  $y_1, \dots, y_n$  vettori di  $V_2$ . Allora esiste un'unica applicazione lineare  $f : V_1 \rightarrow V_2$  tale che  $f(x_i) = y_i$  per ogni  $i = 1, \dots, n$ .*

*Dimostrazione.* In virtù di 8.3.18, ogni vettore  $x \in V_1$  si esprime in unico modo nella forma  $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$ . Ciò consente di definire un'applicazione  $f : V_1 \rightarrow V_2$  ponendo  $f(\alpha_1 x_1 + \cdots + \alpha_n x_n) := \alpha_1 y_1 + \cdots + \alpha_n y_n$ . Se  $x$  e  $x'$  sono elementi di  $V_1$ , e  $\alpha \in F$ , posto  $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$  e  $x' = \alpha'_1 x_1 + \cdots + \alpha'_n x_n$ , risulta:

$$\begin{aligned} f(x + x') &= f((\alpha_1 + \alpha'_1)x_1 + \cdots + (\alpha_n + \alpha'_n)x_n) \\ &= (\alpha_1 + \alpha'_1)y_1 + \cdots + (\alpha_n + \alpha'_n)y_n \\ &= (\alpha_1 y_1 + \cdots + \alpha_n y_n) + (\alpha'_1 y_1 + \cdots + \alpha'_n y_n) \\ &= f(x) + f(x'), \end{aligned}$$

$$\begin{aligned} f(\alpha x) &= f(\alpha \alpha_1 x_1 + \cdots + \alpha \alpha_n x_n) \\ &= \alpha \alpha_1 y_1 + \cdots + \alpha \alpha_n y_n \\ &= \alpha(\alpha_1 y_1 + \cdots + \alpha_n y_n) \\ &= \alpha f(x). \end{aligned}$$

Ciò assicura che  $f$  è lineare. Inoltre per ogni  $i = 1, \dots, n$  risulta banalmente  $x_i = 0x_1 + \cdots + 0x_{i-1} + 1x_i + 0x_{i+1} + \cdots + 0x_n$ , quindi  $f(x_i) = y_i$ . Infine si proverà che  $f$  è l'unica applicazione lineare di  $V_1$  in  $V_2$  con tale proprietà. Sia infatti  $g : V_1 \rightarrow V_2$  un'applicazione lineare tale che  $g(x_i) = y_i$  per ogni  $i = 1, \dots, n$ . Allora per ogni  $x \in V_1$  risulta  $g(x) = g(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \alpha_1 g(x_1) + \cdots + \alpha_n g(x_n) = \alpha_1 y_1 + \cdots + \alpha_n y_n = f(x)$ , cioè  $g = f$ .  $\square$

Si suole dire che l'applicazione lineare costruita nel Teorema 8.4.9 è ottenuta “estendendo per linearità” l'applicazione  $x_i \in B \mapsto y_i \in V_2$ . Se si scelgono i vettori  $y_1, \dots, y_n$  di  $V_2$  in maniera opportuna, l'omomorfismo che si ottiene verifica ulteriori proprietà.

**8.4.10.** Siano  $V_1$  e  $V_2$  spazi vettoriali su un campo  $F$ ,  $B = \{x_1, \dots, x_n\}$  una base di  $V_1$ ,  $y_1, \dots, y_n$  vettori di  $V_2$ ,  $f : V_1 \rightarrow V_2$  l'omomorfismo che si ottiene estendendo per linearità l'applicazione  $x_i \in B \mapsto y_i \in V_2$ . Si ha:

- (i) se l'insieme  $\{y_1, \dots, y_n\}$  ha ordine  $n$  ed è linearmente indipendente allora  $f$  è un monomorfismo;
- (ii) se l'insieme  $\{y_1, \dots, y_n\}$  genera  $V_2$  allora  $f$  è un epimorfismo;
- (iii) se l'insieme  $\{y_1, \dots, y_n\}$  ha ordine  $n$  ed è una base di  $V_2$  allora  $f$  è un isomorfismo.

*Dimostrazione.* Nelle ipotesi (i), sia  $f(x) = f(y)$ . Allora  $f(x - y) = 0$  per la linearità di  $f$ . Siccome i vettori  $y_1, \dots, y_n$  sono a due a due distinti e linearmente indipendenti, la loro unica combinazione lineare uguale al vettore nullo è quella con scalari tutti nulli. Pertanto  $f(x - y) = 0y_1 + \cdots + 0y_n$ . Ma allora  $x - y = 0x_1 + \cdots + 0x_n = 0$ . Così  $x = y$  e  $f$  è iniettiva.

Nell'ipotesi (ii), sia  $y \in V_2$ . Siccome  $y \in \langle y_1, \dots, y_n \rangle$ , esistono scalari  $\beta_1, \dots, \beta_n \in F$  tali che  $y = \beta_1 y_1 + \cdots + \beta_n y_n$ . Considerato allora il vettore

$x = \beta_1 x_1 + \cdots + \beta_n x_n \in V_1$ , risulta  $f(x) = y$ . L'arbitrarietà di  $y$  in  $V_2$  assicura che  $f$  è suriettiva.

Infine, nelle ipotesi (iii),  $f$  è biettiva per (i) e (ii).  $\square$

Ora si può provare facilmente che spazi vettoriali finitamente generati su uno stesso campo sono isomorfi se e solo se hanno la stessa dimensione.

**8.4.11.** Siano  $V_1$  e  $V_2$  spazi vettoriali finitamente generati su un campo  $F$ . Allora:

$$V_1 \simeq V_2 \iff \dim_F V_1 = \dim_F V_2.$$

*Dimostrazione.* Sia  $V_1 \simeq V_2$ . Allora esiste un isomorfismo  $f : V_1 \longrightarrow V_2$ . Sia  $B_1$  una base di  $V_1$ . Per il Corollario 8.4.7 l'insieme  $f(B_1)$  è una base di  $V_2$ . Siccome la biettività di  $f$  assicura che  $B_1$  e  $f(B_1)$  hanno lo stesso numero di elementi, ne segue che  $\dim_F V_1 = \dim_F V_2$ .

Viceversa, sia  $\dim_F V_1 = \dim_F V_2$ . Allora le basi di  $V_1$  e quelle di  $V_2$  hanno lo stesso ordine. Siano  $B_1 = \{x_1, \dots, x_n\}$  una base di  $V_1$ ,  $B_2 = \{y_1, \dots, y_n\}$  una base di  $V_2$ . Si consideri poi l'applicazione  $\sigma : x_i \in B_1 \longmapsto y_i \in B_2$ . La (iii) di 8.4.10 garantisce che l'applicazione che si ottiene estendendo  $\sigma$  per linearità è un isomorfismo. Pertanto  $V_1 \simeq V_2$ , come volevasi.  $\square$

## Esercizi

**Esercizio 8.4.1.** Si dimostri che per ogni intero positivo  $n$  gli  $F$ -spazi vettoriali  $F^n$ ,  $M_{1,n}(F)$  e  $M_{n,1}(F)$  sono a due a due isomorfi. In virtù di ciò, nel seguito si parlerà indifferentemente di vettori di  $F^n$ , o di vettori riga, o di vettori colonna.

**Esercizio 8.4.2.** Si provi 8.4.1.

**Esercizio 8.4.3.** Siano  $V_1$ ,  $V_2$  e  $V_3$  spazi vettoriali su uno stesso campo  $F$ , e siano  $f : V_1 \longrightarrow V_2$  e  $g : V_2 \longrightarrow V_3$  applicazioni lineari. Si provi che l'applicazione composta  $g \circ f : V_1 \longrightarrow V_3$  è lineare.

**Esercizio 8.4.4.** Sia  $f : V_1 \longrightarrow V_2$  un'applicazione lineare. Si provi che  $f(nx) = nf(x)$ , per ogni  $x \in V_1$  e per ogni  $n \in \mathbb{Z}$ .

**Esercizio 8.4.5.** Sia  $f : V_1 \longrightarrow V_2$  un isomorfismo di  $F$ -spazi vettoriali. Si dimostri che l'applicazione inversa  $f^{-1} : V_2 \longrightarrow V_1$  è lineare.

**Esercizio 8.4.6.** Si consideri  $\mathbb{R}^2$  strutturato a spazio vettoriale reale nel modo usuale. Si stabilisca se l'applicazione  $f : (x, y) \in \mathbb{R}^2 \longmapsto (x+1, y+1) \in \mathbb{R}^2$  è lineare.

**Esercizio 8.4.7.** Con  $\mathbb{R}^3$  strutturato a spazio vettoriale reale nel modo usuale, si stabilisca quali tra le seguenti applicazioni  $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$  sono lineari:

$$\begin{aligned} f(x, y, z) &= (3, x - z, y); \\ f(x, y, z) &= (x, y - z, z^2); \\ f(x, y, z) &= (2y - z, x + 4z, 0). \end{aligned}$$

**Esercizio 8.4.8.** Si dimostri, con particolare riguardo alle proprietà (v) – (viii) della definizione di spazio vettoriale, che se  $V$  è uno spazio vettoriale sul campo  $F$  e  $W$  un sottospazio di  $V$ , allora il quoziente  $V/W$ , con le operazioni quoziante, è uno spazio vettoriale su  $F$ .

**Esercizio 8.4.9.** Siano  $V$  uno spazio vettoriale su un campo  $F$ , e  $W$  un sottospazio di  $V$ . Si dia una condizione necessaria e sufficiente su  $W$  affinché l'epimorfismo canonico di  $V$  in  $V/W$  (vedi Teorema 8.4.3 (iv)) sia un isomorfismo.

**Esercizio 8.4.10.** Siano  $V$  uno spazio vettoriale di dimensione finita  $n$  su un campo  $F$ , e  $B = \{x_1, \dots, x_n\}$  una base di  $V$ . Si dimostri che l'applicazione

$$\Phi : x \in V \longmapsto (\alpha_1, \dots, \alpha_n) \in F^n$$

che a ogni vettore di  $V$  associa la  $n$ -upla delle sue componenti nella base  $B$  è un isomorfismo di spazi vettoriali, detto **isomorfismo coordinato** rispetto alla base  $B$ .

**Esercizio 8.4.11.** Sia  $f : V_1 \rightarrow V_2$  un'applicazione lineare, e sia  $B_1$  una base di  $V_1$ . Si provi che  $f$  è un isomorfismo se e solo se  $f(B_1)$  è una base di  $V_2$ .

**Esercizio 8.4.12.** Considerati gli insiemi  $\mathbb{R}^3$  e  $\mathbb{R}^4$ , strutturati a spazio vettoriale su  $\mathbb{R}$ , si stabilisca quali delle seguenti applicazioni sono lineari, e per ciascuna di queste si determinino il nucleo, l'immagine e le rispettive dimensioni:

$$\begin{aligned} f_1 &: (x, y, z) \longmapsto (x + y, x + z, x, y), \\ f_2 &: (x, y, z) \longmapsto (x + 1, x, 2x + 3y, x - y), \\ f_3 &: (x, y, z) \longmapsto (1, 1, 0, y), \\ f_4 &: (x, y, z) \longmapsto (x, z, 2, y), \\ f_5 &: (x, y, z) \longmapsto (x^2, y^2, z^2, 1). \end{aligned}$$

**Esercizio 8.4.13.** Si stabilisca per quali valori del parametro razionale  $k$  l'applicazione  $f : (x, y) \in \mathbb{Q}^2 \longmapsto (x + ky, 1 - k^2, (2 + k)y) \in \mathbb{Q}^3$  è un isomorfismo di  $\mathbb{Q}$ -spazi vettoriali.

**Esercizio 8.4.14.** Si consideri l'applicazione  $f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$  definita ponendo  $f(x, y, z, t) = (t - 2z, y + z, x - 3t)$ , per ogni  $(x, y, z, t) \in \mathbb{R}^4$ . Si dimostri che  $f$  è lineare. Si determinino poi il nucleo e l'immagine di  $f$ , e le rispettive dimensioni.

**Esercizio 8.4.15.** Si determini in forma esplicita un omomorfismo di  $\mathbb{Q}$ -spazi vettoriali  $f : \mathbb{Q}^3 \rightarrow \mathbb{Q}^2$  tale che  $f((1, 2, 3)) = (2, 1)$  e  $f((1, 0, 1)) = (1, 2)$ . Si calcoli poi la dimensione di  $\text{Im } f$ .

**Esercizio 8.4.16.** Sia  $f : \mathbb{R}^4 \rightarrow \mathbb{R}^3$  l'applicazione lineare definita ponendo

$$f(x, y, z, w) = (x - 2y + 3z, x - y + (k + 3)z + 2w, 2x - 3y + (k + 6)z + (k + 1)w)$$

per ogni  $(x, y, z, w) \in \mathbb{R}^4$ , con  $k$  parametro reale. Si stabilisca se esistono valori di  $k$  per cui  $f$  è un monomorfismo, e se esistono valori di  $k$  per cui è un epimorfismo.

## 8.5 Somma diretta di sottospazi

Sia  $V$  uno spazio vettoriale su un campo  $F$ , e siano  $W_1$  e  $W_2$  sottospazi di  $V$ . In virtù di 8.2.12, l'insieme  $W_1 + W_2 := \{w_1 + w_2 : w_1 \in W_1, w_2 \in W_2\}$  coincide con il sottospazio di  $V$  generato da  $W_1$  e  $W_2$ . Quando è finita, la dimensione di  $W_1 + W_2$  può essere calcolata a partire dalle dimensioni di  $W_1$ ,  $W_2$  e  $W_1 \cap W_2$ .

**8.5.1. Formula di Grassmann.** *Sia  $V$  uno spazio vettoriale su un campo  $F$ , e siano  $W_1$  e  $W_2$  sottospazi di dimensione finita di  $V$ . Allora anche  $W_1 \cap W_2$  e  $W_1 + W_2$  hanno dimensione finita, e risulta:*

$$\dim_F W_1 + \dim_F W_2 = \dim_F(W_1 + W_2) + \dim_F(W_1 \cap W_2).$$

*Dimostrazione.* Essendo un sottospazio di  $W_1$ , anche  $W_1 \cap W_2$  ha dimensione finita per 8.3.23. Sia  $\dim_F(W_1 \cap W_2) = n$ , e si fissi una base  $\{x_1, \dots, x_n\}$  di  $W_1 \cap W_2$ . Per 8.3.20, l'insieme linearmente indipendente  $\{x_1, \dots, x_n\}$  è contenuto in una base  $\{x_1, \dots, x_n, y_1, \dots, y_r\}$  di  $W_1$ ; dunque  $\dim_F W_1 = n + r$ . Per lo stesso motivo,  $\{x_1, \dots, x_n\}$  è contenuto in una base  $\{x_1, \dots, x_n, z_1, \dots, z_s\}$  di  $W_2$ ; di qui,  $\dim_F W_2 = n + s$ . Pertanto bisogna provare che  $\dim_F(W_1 + W_2) = n + r + s$ : lo si farà dimostrando che  $B = \{x_1, \dots, x_n, y_1, \dots, y_r, z_1, \dots, z_s\}$  è una base di  $W_1 + W_2$ .

Per provare che  $B$  è linearmente indipendente, si abbia

$$0 = \alpha_1 x_1 + \dots + \alpha_n x_n + \beta_1 y_1 + \dots + \beta_r y_r + \gamma_1 z_1 + \dots + \gamma_s z_s, \quad (8.5.1)$$

con  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_r, \gamma_1, \dots, \gamma_s \in F$ . Allora risulta

$$\alpha_1 x_1 + \dots + \alpha_n x_n + \beta_1 y_1 + \dots + \beta_r y_r = -\gamma_1 z_1 - \dots - \gamma_s z_s \in W_1 \cap W_2,$$

quindi  $-\gamma_1 z_1 - \dots - \gamma_s z_s = \delta_1 x_1 + \dots + \delta_n x_n$  dove  $\delta_1, \dots, \delta_n \in F$ , in quanto  $\{x_1, \dots, x_n\}$  è una base di  $W_1 \cap W_2$ . Da qui si ottiene subito

$$\gamma_1 z_1 + \dots + \gamma_s z_s + \delta_1 x_1 + \dots + \delta_n x_n = 0;$$

essendo  $\{x_1, \dots, x_n, z_1, \dots, z_s\}$  linearmente indipendente in quanto base di  $W_2$ , se ne ricava  $\gamma_1 = \dots = \gamma_s = 0$ . Ora da (8.5.1) si ottiene

$$\alpha_1 x_1 + \dots + \alpha_n x_n + \beta_1 y_1 + \dots + \beta_r y_r = 0,$$

il che ovviamente comporta  $\alpha_1 = \dots = \alpha_n = \beta_1 = \dots = \beta_r = 0$  in quanto  $\{x_1, \dots, x_n, y_1, \dots, y_r\}$  è una base di  $W_1$ . In definitiva

$$\alpha_1 = \dots = \alpha_n = \beta_1 = \dots = \beta_r = \gamma_1 = \dots = \gamma_s = 0,$$

quindi  $B$  è linearmente indipendente.

Per provare infine che  $B$  genera  $W_1 + W_2$ , si osservi che da  $B \subseteq W_1 + W_2$  segue subito  $\langle B \rangle \subseteq W_1 + W_2$ . Per provare l'inclusione opposta, siano  $w_1 \in W_1$

e  $w_2 \in W_2$ . Siccome  $\{x_1, \dots, x_n, y_1, \dots, y_r\}$  è una base di  $W_1$ , esistono scalari  $\eta_1, \dots, \eta_n, \theta_1, \dots, \theta_r \in F$  tali che

$$w_1 = \eta_1 x_1 + \cdots + \eta_n x_n + \theta_1 y_1 + \cdots + \theta_r y_r.$$

Analogamente, siccome  $\{x_1, \dots, x_n, z_1, \dots, z_s\}$  è una base di  $W_2$ , esistono scalari  $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_s \in F$  tali che

$$w_2 = \lambda_1 x_1 + \cdots + \lambda_n x_n + \mu_1 z_1 + \cdots + \mu_s z_s.$$

Di conseguenza

$$w_1 + w_2 = (\eta_1 + \lambda_1)x_1 + \cdots + (\eta_n + \lambda_n)x_n + \theta_1 y_1 + \cdots + \theta_r y_r + \mu_1 z_1 + \cdots + \mu_s z_s$$

è un elemento di  $\langle B \rangle$ . Pertanto  $B$  è una base di  $W_1 + W_2$ , come volevasi.  $\square$

Si dice che lo spazio vettoriale  $V$  è **somma diretta** dei sottospazi  $W_1$  e  $W_2$  (e si scrive  $V = W_1 \oplus W_2$ ) se  $V = W_1 + W_2$  e  $W_1 \cap W_2 = \{0\}$ .

**8.5.2. Esempi.** Qualunque sia  $V$ , si può sempre scrivere  $V = V \oplus \{0\}$  (la cosiddetta **decomposizione diretta banale**).

Decomposizioni dirette non banali dello  $\mathbb{Q}$ -spazio vettoriale  $\mathbb{Q}^2$  sono per esempio  $\mathbb{Q}^2 = \langle(1, 0)\rangle \oplus \langle(0, 1)\rangle$  e  $\mathbb{Q}^2 = \langle(1, 0)\rangle \oplus \langle(1, 1)\rangle$ .

**8.5.3.** Sia  $V$  uno spazio vettoriale su un campo  $F$ , e siano  $W_1$  e  $W_2$  sottospazi di  $V$ . Allora  $V = W_1 \oplus W_2$  se e solo se ogni  $x \in V$  si può scrivere in unico modo nella forma  $x = x_1 + x_2$ , con  $x_1 \in W_1$  e  $x_2 \in W_2$ .

*Dimostrazione.* Se  $V = W_1 \oplus W_2$  allora innanzitutto  $V = W_1 + W_2$ , quindi per ogni  $x \in V$  si ha  $x = x_1 + x_2$ , con  $x_1 \in W_1$  e  $x_2 \in W_2$ . Se si avesse anche  $x = y_1 + y_2$ , con  $y_1 \in W_1$  e  $y_2 \in W_2$  allora risulterebbe  $0 = (x_1 - y_1) + (x_2 - y_2)$ , quindi  $x_1 - y_1 = y_2 - x_2 \in W_1 \cap W_2 = \{0\}$ , da cui  $x_1 = y_1$  e  $x_2 = y_2$ .

Viceversa, se ogni  $x \in V$  si scrive in unico modo nella forma  $x = x_1 + x_2$  con  $x_1 \in W_1$  e  $x_2 \in W_2$ , allora innanzitutto  $x \in W_1 + W_2$ , quindi  $V = W_1 + W_2$ . Se poi  $x \in W_1 \cap W_2$  allora  $x = x + 0 = 0 + x$  sono due scritture distinte di  $x$  come somma di un elemento di  $W_1$  e di uno di  $W_2$ , e dunque esse coincidono per ipotesi. Pertanto  $x = 0$  e  $W_1 \cap W_2 = \{0\}$ , da cui  $V = W_1 \oplus W_2$ .  $\square$

Sia  $V$  uno spazio vettoriale su un campo  $F$ , e sia  $W_1$  un sottospazio di  $V$ . Un sottospazio  $W_2$  di  $V$  è detto un **supplementare** di  $W_1$  se risulta  $V = W_1 \oplus W_2$ . Come si evince da 8.5.2, un sottospazio di  $V$  può ammettere più supplementari. Se  $V$  è finitamente generato, l'esistenza di supplementari è garantita, per ogni sottospazio di  $V$ , dal risultato seguente.

**8.5.4. Teorema.** Ogni sottospazio di uno spazio vettoriale finitamente generato ammette un supplementare.

*Dimostrazione.* Siano  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ , e sia  $W_1$  un sottospazio di  $V$ . Per 8.3.23,  $W_1$  ha una base  $B_1 = \{x_1, \dots, x_n\}$ . Allora  $B_1$  è un sottoinsieme linearmente indipendente di  $V$ , pertanto per 8.3.20 esso è contenuto in una base  $B = \{x_1, \dots, x_n, x_{n+1}, \dots, x_m\}$  di  $V$ . Si ponga  $W_2 := \langle x_{n+1}, \dots, x_m \rangle$ . Si osservi che  $B_2 = \{x_{n+1}, \dots, x_m\}$  è un insieme linearmente indipendente di generatori di  $W_2$ , quindi ne è una base. Si proverà che  $W_2$  è un supplementare di  $W_1$ , ossia che  $V = W_1 \oplus W_2$ . Il fatto che  $B$  sia una base di  $V$  garantisce che, per ogni  $x \in V$ , esistano scalari  $\alpha_1, \dots, \alpha_m \in F$  tali che  $x = \alpha_1 x_1 + \dots + \alpha_n x_n + \alpha_{n+1} x_{n+1} + \dots + \alpha_m x_m$ . Pertanto  $x = w_1 + w_2$  con  $w_1 = \alpha_1 x_1 + \dots + \alpha_n x_n \in W_1$  e  $w_2 = \alpha_{n+1} x_{n+1} + \dots + \alpha_m x_m \in W_2$ . Ciò dimostra che  $V = W_1 + W_2$ . Sia ora  $x \in W_1 \cap W_2$ . Allora, siccome  $B_1$  è una base di  $W_1$  e  $B_2$  una base di  $W_2$ , esistono scalari  $\beta_1, \dots, \beta_n, \beta_{n+1}, \dots, \beta_m \in F$  tali che  $x = \beta_1 x_1 + \dots + \beta_n x_n = \beta_{n+1} x_{n+1} + \dots + \beta_m x_m$ . Da ciò si ottiene  $\beta_1 x_1 + \dots + \beta_n x_n - \beta_{n+1} x_{n+1} - \dots - \beta_m x_m = 0$ . Poiché  $B$  è linearmente indipendente, ciò comporta che  $\beta_1 = \dots = \beta_n = \beta_{n+1} = \dots = \beta_m = 0$ , quindi  $x = 0$ . Pertanto  $W_1 \cap W_2 = \{0\}$ , e l'asserto è provato.  $\square$

**8.5.5.** *Siano  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ ,  $W_1$  un sottospazio di  $V$ ,  $W_2$  un supplementare di  $W_1$ ,  $B_1$  una base di  $W_1$  e  $B_2$  una base di  $W_2$ . Allora  $B_1 \cap B_2 = \emptyset$ , e l'insieme  $B := B_1 \cup B_2$  è una base di  $V$ .*

*Dimostrazione.* Per 8.3.23 i sottospazi  $W_1$  e  $W_2$  sono finitamente generati, quindi si può assumere  $B_1 = \{x_1, \dots, x_n\}$  e  $B_2 = \{y_1, \dots, y_m\}$ . Si osservi innanzitutto che  $B_1 \cap B_2 \subseteq W_1 \cap W_2 = \{0\}$ , quindi  $B_1 \cap B_2 = \emptyset$  per il Corollario 8.3.8. Ne segue che  $|B_1 \cup B_2| = n + m$ . Per ogni  $x \in V$  esistono  $w_1 \in W_1$  e  $w_2 \in W_2$  tali che  $x = w_1 + w_2$ . Inoltre per le ipotesi risulta  $w_1 \in \langle B_1 \rangle$ ,  $w_2 \in \langle B_2 \rangle$ . Quindi  $x \in \langle B \rangle$ . Pertanto  $V = \langle B \rangle$ . Resta da provare che  $B$  è linearmente indipendente. Ciò segue subito dal fatto che se risulta  $0 = \alpha_1 x_1 + \dots + \alpha_n x_n + \beta_1 y_1 + \dots + \beta_m y_m$  per certi scalari  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in F$ , allora

$$\alpha_1 x_1 + \dots + \alpha_n x_n = -\beta_1 y_1 - \dots - \beta_m y_m \in W_1 \cap W_2 = \{0\},$$

e la lineare indipendenza di  $B_1$  e  $B_2$  assicura che

$$\alpha_1 = \dots = \alpha_n = \beta_1 = \dots = \beta_m = 0.$$

L'asserto è dunque provato.  $\square$

**8.5.6. Teorema.** *Siano  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ ,  $W_1$  un sottospazio di  $V$ ,  $W_2$  un supplementare di  $W_1$ . Allora risulta:*

- (i)  $\dim_F V = \dim_F W_1 + \dim_F W_2$ ,
- (ii)  $\dim_F V/W_1 = \dim_F V - \dim_F W_1$ .

*Dimostrazione.* La (i) segue subito dalla formula di Grassmann (vedi 8.5.1). Per l'Esercizio 8.5.3 le ipotesi implicano  $V/W_1 \simeq W_2$ . Allora per 8.4.11 e per la (i) già provata si ha  $\dim_F V/W_1 = \dim_F W_2 = \dim_F V - \dim_F W_1$ , cioè la (ii).  $\square$

## Esercizi

**Esercizio 8.5.1.** Nello spazio vettoriale reale  $\mathbb{R}^3$ , si considerino i sottospazi

$$U = \{(a, b, 0) : a, b \in \mathbb{R}\}, \quad W = \{(0, b, c) : b, c \in \mathbb{R}\}.$$

Si dimostri che  $\mathbb{R}^3 = U + W$ , e che la somma non è diretta.

**Esercizio 8.5.2.** Siano  $U$  e  $W$  sottospazi dello spazio vettoriale reale  $\mathbb{R}^3$ , di dimensioni 1 e 2 rispettivamente. Si provi che se  $U \not\subset W$  allora  $\mathbb{R}^3 = U \oplus W$ .

**Esercizio 8.5.3.** Siano  $V$  uno spazio vettoriale finitamente generato su un campo  $F$ ,  $W_1$  un sottospazio di  $V$ ,  $W_2$  un supplementare di  $W_1$ . Si dimostri che allora  $V/W_1 \simeq W_2$ .

**Esercizio 8.5.4.** Nell'insieme  $\mathbb{Q}^4$  strutturato a spazio vettoriale su  $\mathbb{Q}$ , si considerino i vettori  $x_1 = (1, 2, 1, 0)$ ,  $x_2 = (1/2, 0, 0, -1)$ ,  $x_3 = (0, 1, 1, -1)$ ,  $x_4 = (1, 1, 2, 2)$ . Siano poi  $W$  il sottospazio generato da  $x_1$  e da  $x_2$ ,  $U$  il sottospazio generato da  $x_3$  e da  $x_4$ . Si determini la dimensione e una base di  $W$ ,  $U$ ,  $W + U$  e  $W \cap U$ , e un supplementare di  $W$ .

**Esercizio 8.5.5.** Nell'insieme  $\mathbb{R}^4$  strutturato a spazio vettoriale su  $\mathbb{R}$ , si considerino i sottoinsiemi

$$\begin{aligned} W_1 &= \{(a, b, c, d) : a + b = 0, c = 2d\}, \\ W_2 &= \{(x, y, z, t) : x - 4y = 0, 3z - 6y = 0\}. \end{aligned}$$

Si provi che  $W_1$  e  $W_2$  sono sottospazi di  $\mathbb{R}^4$ , e di ciascuno si determini la dimensione, una base e un supplementare.

**Esercizio 8.5.6.** Si provi la (i) del Teorema 8.5.6 senza utilizzare la formula di Grassmann (vedi 8.5.1).

*Svolgimento.* Con  $B_1$  base di  $W_1$  e  $B_2$  base di  $W_2$ , si ponga  $B := B_1 \cup B_2$ . Per 8.5.5 risulta  $B_1 \cap B_2 = \emptyset$ , e  $B$  è una base di  $V$ . Per il principio di inclusione-esclusione (vedi 3.1.3) si ottiene subito  $|B| = |B_1| + |B_2|$ , e ciò prova l'asserto.

**Esercizio 8.5.7.** Siano  $V$  uno spazio vettoriale e  $\sigma$  un endomorfismo di  $V$  tale che  $\sigma \circ \sigma = \sigma$ . Si provi che  $V = \text{Ker } \sigma \oplus \text{Im } \sigma$ .

**Esercizio 8.5.8.** Nello  $\mathbb{Z}_7$ -spazio vettoriale  $\mathbb{Z}_7[x; 3]$  si determini la dimensione e un supplementare del sottospazio  $W$  generato dai vettori  $x^3 + \bar{4}x^2 - x + \bar{3}$  e  $x^3 + \bar{5}x^2 + \bar{5}$ .

**Esercizio 8.5.9.** Nell'usuale spazio vettoriale reale  $M_2(\mathbb{R})$  si consideri il sottospazio

$$W = \left\langle \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

Si determini un supplementare di  $W$ .

**Esercizio 8.5.10.** Nell'usuale spazio vettoriale reale  $M_3(\mathbb{R})$  si considerino i sottospazi:

$$T = \{(a_{ij}) \in M_3(\mathbb{R}) : a_{11} = a_{22} = a_{33} = 0\},$$

$$K = \{(a_{ij}) \in M_3(\mathbb{R}) : a_{21} = a_{22} = a_{23} = 0\}.$$

Si determini una base e un supplementare del sottospazio  $T \cap K$ .

**Esercizio 8.5.11.** La definizione di somma diretta si generalizza facilmente a un numero arbitrario di sottospazi. Se infatti  $W_1, \dots, W_n$  sono sottospazi di uno spazio vettoriale  $V$ , si dice che  $V$  è somma diretta dei sottospazi  $W_1, \dots, W_n$  (e si scrive  $V = W_1 \oplus \dots \oplus W_n$ ) se accade che:

$$(1) \quad V = W_1 + \dots + W_n,$$

$$(2) \quad W_i \cap \langle W_j : j \neq i \rangle = \{0\}, \text{ per ogni } i = 1, \dots, n.$$

Si dimostri che  $V = W_1 \oplus \dots \oplus W_n$  se e solo se ogni vettore di  $x \in V$  si scrive in unico modo nella forma  $x = x_1 + \dots + x_n$  con  $x_1 \in W_1, \dots, x_n \in W_n$ .

## 8.6 Matrice associata a un'applicazione lineare

Siano  $V_1$  e  $V_2$  spazi vettoriali finitamente generati su un campo  $F$ , e  $f : V_1 \longrightarrow V_2$  un'applicazione lineare. Se  $B_1 = \{x_1, \dots, x_n\}$  e  $B_2 = \{y_1, \dots, y_m\}$  sono basi rispettivamente di  $V_1$  e  $V_2$ , allora per ogni  $j = 1, \dots, n$  esistono scalari  $\alpha_{ij} \in F$  (univocamente determinati per 8.3.18) tali che

$$f(x_j) = \sum_{i=1}^m \alpha_{ij} y_i. \tag{8.6.1}$$

La matrice  $(\alpha_{ij}) \in M_{m,n}(F)$  viene detta la **matrice associata** a  $f$  rispetto alle basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$ . Ovviamente qui, come del resto verrà fatto nel seguito senza ulteriori annotazioni, si intende che  $B_1$  e  $B_2$  siano basi ordinate (si tenga ben presente l'osservazione che conclude il Paragrafo 8.3). Viceversa, ogni matrice  $(\alpha_{ij}) \in M_{m,n}(F)$  dà luogo, mediante le (8.6.1), a un'applicazione  $B_1 \longrightarrow V_2$  che, in virtù del Teorema 8.4.9, si estende per linearità a un unico omomorfismo  $f : V_1 \longrightarrow V_2$ . Quest'ultimo ammette ovviamente proprio  $(\alpha_{ij})$  come matrice associata rispetto alle basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$ .

Siano ora  $V_3$  uno spazio vettoriale di dimensione  $r$  su  $F$ , e  $g : V_2 \longrightarrow V_3$  un'applicazione lineare. Fissata una base  $B_3 = \{z_1, \dots, z_r\}$  di  $V_3$ , la matrice

associata a  $g$  rispetto alle basi  $B_2$  di  $V_2$  e  $B_3$  di  $V_3$  è data da  $\beta_{hi} \in M_{r,m}(F)$ , con

$g(y_i) = \sum_{h=1}^r \beta_{hi} z_h$ . Per ogni  $j = 1, \dots, n$  risulta allora:

$$(g \circ f)(x_j) = \sum_{i=1}^m \alpha_{ij} g(y_i) = \sum_{i=1}^m \sum_{h=1}^r \beta_{hi} \alpha_{ij} z_h. \quad (8.6.2)$$

Dalla (8.6.2), posto  $\gamma_{hj} := \sum_{i=1}^m \beta_{hi} \alpha_{ij}$ , si ottiene subito

$$(g \circ f)(x_j) = \sum_{h=1}^r \gamma_{hj} z_h. \quad (8.6.3)$$

La (8.6.3) assicura che la matrice associata all'applicazione lineare  $g \circ f$  (vedi Esercizio 8.4.3) rispetto alle basi  $B_1$  di  $V_1$  e  $B_3$  di  $V_3$  è  $(\gamma_{hj}) \in M_{r,n}(F)$ , ossia proprio la matrice che si ottiene mediante prodotto righe per colonne (vedi 7.2) dalle matrici  $(\beta_{hi}) \in M_{r,m}(F)$  e  $(\alpha_{ij}) \in M_{m,n}(F)$ . Si è così provato che:

**8.6.1. Teorema.** *Sia  $F$  un campo, e siano  $V_1$  e  $V_2$  spazi vettoriali su  $F$  di dimensioni  $n$  e  $m$  rispettivamente. Per ogni scelta di basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$  esiste una corrispondenza biunivoca tra  $M_{m,n}(F)$  e l'insieme delle applicazioni lineari di  $V_1$  in  $V_2$ . Se  $V_3$  è uno spazio vettoriale su  $F$  di dimensione  $r$ , scelta una sua base  $B_3$ , la matrice associata all'applicazione lineare  $g \circ f$  rispetto alle basi  $B_1$  di  $V_1$  e  $B_3$  di  $V_3$  è il prodotto righe per colonne delle matrici associate rispettivamente a  $g$  rispetto a  $B_2$  e  $B_3$  e a  $f$  rispetto a  $B_1$  e  $B_2$ .*

Con  $F$ ,  $V_1$  e  $V_2$  come nel Teorema 8.6.1, si denoti con  $\text{Hom}_F(V_1, V_2)$  l'insieme delle applicazioni lineari di  $V_1$  in  $V_2$ . Si ponga, per ogni  $f, g \in \text{Hom}_F(V_1, V_2)$ ,  $x \in V_1$ ,  $\alpha \in F$ :

$$\begin{aligned} (f + g)(x) &:= f(x) + g(x), \\ (\alpha \cdot f)(x) &:= \alpha(f(x)). \end{aligned}$$

Si verifica facilmente che  $f + g, \alpha \cdot f \in \text{Hom}_F(V_1, V_2)$ , e che quindi restano definite in  $\text{Hom}_F(V_1, V_2)$  un'operazione interna  $+$  e un'operazione esterna  $\cdot$  con dominio di operatori  $F$ . Con tali operazioni,  $\text{Hom}_F(V_1, V_2)$  resta strutturato a spazio vettoriale su  $F$ .

**8.6.2.** *Per ogni scelta di basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$ , la corrispondenza biunivoca tra  $M_{m,n}(F)$  e  $\text{Hom}_F(V_1, V_2)$  stabilita nel Teorema 8.6.1 è un isomorfismo di  $F$ -spazi vettoriali.*

*Dimostrazione.* Esercizio. □

**Osservazione.** La matrice  $(\alpha_{ij}) \in M_{m,n}(F)$  associata a un'applicazione lineare  $f : V_1 \rightarrow V_2$  rispetto alle basi  $B_1 = \{x_1, \dots, x_n\}$  di  $V_1$  e  $B_2 = \{y_1, \dots, y_m\}$  di  $V_2$  ha dunque, come colonna  $j$ -esima, le componenti del vettore  $f(x_j) \in V_2$  nella base  $B_2$ . Mediante tale matrice è possibile calcolare l'immagine di qualsiasi vettore  $x \in V_1$ . Infatti, posto  $x = \sum_{j=1}^n \beta_j x_j$ , per la linearità della  $f$  risulta:

$$\begin{aligned} f(x) &= f\left(\sum_{j=1}^n \beta_j x_j\right) = \sum_{j=1}^n \beta_j f(x_j) = \sum_{j=1}^n \beta_j \sum_{i=1}^m \alpha_{ij} y_i \\ &= \sum_{i=1}^m \sum_{j=1}^n \beta_j \alpha_{ij} y_i = \sum_{i=1}^m \left( \sum_{j=1}^n \beta_j \alpha_{ij} \right) y_i. \end{aligned}$$

Pertanto se  $x \in V_1$  ha componenti  $(\beta_1, \dots, \beta_n)$  nella base  $B_1$ , il vettore  $y = f(x)$  ha componenti

$$\left( \sum_{j=1}^n \beta_j \alpha_{1j}, \dots, \sum_{j=1}^n \beta_j \alpha_{mj} \right)$$

nella base  $B_2$ . Ciò si può scrivere più efficacemente in termini di matrici. Se infatti si pone

$$X := \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \in M_{n,1}(F), \quad Y := \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} \in M_{m,1}(F),$$

con  $\gamma_i = \sum_{j=1}^n \beta_j \alpha_{ij}$  per ogni  $i = 1, \dots, m$ , si ottiene

$$AX = Y. \tag{8.6.4}$$

Ciò significa che, moltiplicando righe per colonne la matrice  $A$  associata a  $f$  rispetto a basi  $B_1$  e  $B_2$  per la matrice  $X \in M_{n,1}(F)$  costituita dalle componenti nella base  $B_1$  di un arbitrario vettore  $x \in V_1$  si ottiene una matrice  $Y \in M_{m,1}(F)$  i cui elementi sono esattamente le componenti nella base  $B_2$  del vettore  $f(x) \in V_2$ .

Se  $f : V \rightarrow V$  è un endomorfismo di uno spazio vettoriale  $V$  di dimensione finita su un campo  $F$ , nel considerare la matrice associata a  $f$  è possibile utilizzare la medesima base  $B$  sia per il dominio che per il codominio. In tal caso la matrice ottenuta è detta associata a  $f$  rispetto alla base  $B$  di  $V$ .

**8.6.3. Esempio.** Sia  $V$  uno spazio vettoriale di dimensione  $n$  sul campo  $F$ , e sia  $X = \{x_1, \dots, x_n\}$  una base di  $V$ . Denotata con  $\text{id}_V$  l'applicazione identica di  $V$ , la matrice associata a  $\text{id}_V$  rispetto alla base  $X$  di  $V$  è la matrice  $(\alpha_{ij}) \in M_n(F)$

dove, per (8.6.1), per ogni  $j = 1, \dots, n$  si ha:  $x_j = \text{id}_V(x_j) = \sum_{i=1}^n \alpha_{ij}x_i$ .

Per 8.3.18 da ciò segue subito che per ogni  $i, j = 1, \dots, n$  risulta

$$\alpha_{ij} = \delta_{ij} = \begin{cases} 1 & \text{se } i = j, \\ 0 & \text{se } i \neq j. \end{cases}$$

Pertanto la matrice  $(\alpha_{ij})$  è la matrice identica  $I_n$ . Viceversa, il Teorema 8.6.1 assicura che l'unica applicazione lineare  $V \rightarrow V$  associata alla matrice identica  $I_n$  rispetto alla base  $X$  è l'applicazione identica  $\text{id}_V$ .

**8.6.4. Teorema.** *Siano  $F$  un campo,  $V_1$  e  $V_2$  spazi vettoriali su  $F$  della stessa dimensione  $n$ ,  $f : V_1 \rightarrow V_2$  un'applicazione lineare,  $A = (\alpha_{ij}) \in M_n(F)$  la matrice associata a  $f$  rispetto alle basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$ . Allora  $A$  è invertibile se e solo se  $f$  è un isomorfismo. In tal caso, la matrice associata all'inversa di  $f$  rispetto a  $B_2$  e  $B_1$  è l'inversa della matrice associata a  $f$  rispetto a  $B_1$  e  $B_2$ .*

*Dimostrazione.* Sia  $f$  invertibile, sia  $f^{-1} : V_2 \rightarrow V_1$  l'inversa di  $f$ , e sia  $B = (\beta_{ij}) \in M_n(F)$  la matrice associata a  $f^{-1}$  rispetto alle basi  $B_2$  e  $B_1$ . Da  $f \circ f^{-1} = \text{id}_{V_2}$  e  $f^{-1} \circ f = \text{id}_{V_1}$  segue subito, per il Teorema 8.6.1 e l'Esempio 8.6.3, che  $AB = I_n = BA$ . Dunque  $A$  è invertibile e  $B = A^{-1}$ .

Viceversa, sia  $A$  invertibile e sia  $A^{-1}$  la sua inversa. Per il Teorema 8.6.1 esiste un'unica applicazione lineare  $g : V_2 \rightarrow V_1$  la cui matrice associata rispetto a  $B_2$  e  $B_1$  è  $A^{-1}$ . Ancora per il Teorema 8.6.1 l'unica matrice associata all'applicazione  $f \circ g$  è  $AA^{-1} = I_n$ , l'unica matrice associata all'applicazione  $g \circ f$  è  $A^{-1}A = I_n$ . Per l'Esempio 8.6.3 risulta  $g \circ f = \text{id}_{V_1}$  e  $f \circ g = \text{id}_{V_2}$ , cioè  $f$  è invertibile.  $\square$

La matrice associata a un'applicazione lineare dipende dalla scelta delle basi. Il teorema seguente chiarisce come un eventuale cambiamento delle basi si riflette sulla matrice associata.

**8.6.5. Formula di cambiamento delle basi.** *Siano  $F$  un campo,  $V_1$  e  $V_2$  spazi vettoriali su  $F$  di dimensioni  $n$  e  $m$  rispettivamente,  $f : V_1 \rightarrow V_2$  un'applicazione lineare, e  $A = (\alpha_{ij}) \in M_{m,n}(F)$  la matrice associata a  $f$  rispetto alle basi  $B_1$  di  $V_1$  e  $B_2$  di  $V_2$ . Se  $B'_1$  e  $B'_2$  sono altre basi di  $V_1$  e  $V_2$  rispettivamente, si denoti con  $A'$  la matrice associata a  $f$  rispetto alle basi  $B'_1$  di  $V_1$  e  $B'_2$  di  $V_2$ . Allora risulta:*

$$A' = BAC,$$

where  $B$  è la matrice associata all'identità di  $V_2$  rispetto alle basi  $B_2$  e  $B'_2$ , e  $C$  è la matrice associata all'identità di  $V_1$  rispetto alle basi  $B'_1$  e  $B_1$ .

*Dimostrazione.* Si denotino con  $\text{id}_{V_1}$  e  $\text{id}_{V_2}$  le applicazioni identiche rispettivamente di  $V_1$  e  $V_2$ . Per il Teorema 8.6.1,  $AC$  è la matrice associata a  $f = f \circ \text{id}_{V_1}$  rispetto alle basi  $B'_1$  di  $V_1$  e  $B_2$  di  $V_2$ . Di conseguenza  $B(AC) = BAC$  è la matrice associata a  $f = \text{id}_{V_2} \circ f$  rispetto alle basi  $B'_1$  di  $V_1$  e  $B'_2$  di  $V_2$ . Pertanto  $A' = BAC$ .  $\square$

**8.6.6. Corollario.** *Siano  $F$  un campo,  $V$  uno spazio vettoriale di dimensione finita  $n$  su  $F$ ,  $B = \{x_1, \dots, x_n\}$  e  $B' = \{x'_1, \dots, x'_n\}$  basi di  $V$ . Allora esiste una matrice invertibile  $C \in M_n(F)$  tale che, denotate con  $X, X' \in M_{n,1}(F)$  le componenti di un arbitrario vettore  $x \in V$  rispettivamente nella base  $B$  e nella base  $B'$ , risulta  $X' = CX$ . La matrice  $C$  è detta la matrice del cambiamento di base da  $B$  a  $B'$ .*

*Dimostrazione.* Si denoti con  $\text{id}_V$  l'applicazione identica di  $V$ , e sia  $C \in M_n(F)$  la matrice associata a  $\text{id}_V$  rispetto alle basi  $B$  e  $B'$ . Per quanto osservato in precedenza il prodotto righe per colonne di  $C$  per la matrice colonna  $X$  costituita dalle componenti di un qualunque vettore  $x \in V$  nella base  $B$  dà luogo a una matrice colonna  $X'$  costituita dalle componenti del vettore  $x$  nella base  $B'$ . Tale matrice  $C$  è invertibile per il Teorema 8.6.4, e la sua inversa  $C^{-1}$  è la matrice associata a  $\text{id}_V$  rispetto alle basi  $B'$  e  $B$ . È poi ovvio che  $X' = CX$ .  $\square$

Si osservi che la dimostrazione del corollario precedente illustra anche come costruire la matrice  $C$  del cambiamento di base da  $B$  a  $B'$ : le colonne di  $C$  sono ordinatamente le componenti dei vettori di  $B'$  nella base  $B$ .

Nello scrivere la matrice associata a un endomorfismo, come osservato in precedenza, è possibile scegliere la stessa base sia per il dominio che per il codominio. Sebbene ovviamente anche in questo caso la matrice associata dipenda dalla base scelta, la formula di cambiamento delle basi 8.6.5 consente di stabilire un legame particolare tra matrici associate rispetto a basi diverse. Matrici  $A$  e  $A' \in M_n(F)$  si dicono *simili* se esiste una matrice invertibile  $C \in M_n(F)$  tale che  $A' = C^{-1}AC$ . Si ha:

**8.6.7. Siano  $F$  un campo,  $V$  uno spazio vettoriale di dimensione finita  $n$  su  $F$ ,  $f : V \rightarrow V$  un endomorfismo,  $A = (\alpha_{ij}) \in M_n(F)$  la matrice associata a  $f$  rispetto a una base  $B$  di  $V$ , e  $A' = (\alpha'_{ij}) \in M_n(F)$  la matrice associata a  $f$  rispetto a un'altra base  $B'$  di  $V$ . Allora  $A$  e  $A'$  sono simili.**

*Dimostrazione.* Siano  $B = \{x_1, \dots, x_n\}$ ,  $B' = \{x'_1, \dots, x'_n\}$ . Per la formula di cambiamento delle basi 8.6.5 risulta  $A' = DAC$ , dove  $D$  è la matrice associata a  $\text{id}_V$  rispetto alla base  $B'$  e  $C$  è la matrice associata a  $\text{id}_V$  rispetto alla base  $B$ . Per il Teorema 8.6.4 risulta che  $C$  è invertibile, e inoltre  $D = C^{-1}$ . Pertanto  $A' = C^{-1}AC$ .  $\square$

Come verrà evidenziato anche nel seguito (vedi 8.8.3 ed Esercizio 8.8.7), matrici simili hanno molte caratteristiche in comune. In particolare, esse hanno lo stesso determinante.

**8.6.8.** *Siano  $A$  e  $A' \in M_n(F)$  matrici simili. Allora  $\det A = \det A'$ .*

*Dimostrazione.* Per ipotesi, esiste una matrice invertibile  $C \in M_n(F)$  tale che  $A' = C^{-1}AC$ . Allora il teorema di Binet (vedi 7.4.2), insieme con 7.5.3, assicura che  $\det A' = \det C^{-1} \det A \det C = (\det C)^{-1} \det A \det C = \det A$ , come richiesto.  $\square$

### Rango di una matrice o di un'applicazione lineare

Sia  $F$  un campo. Nel Paragrafo 7.6 è stato definito il rango  $\rho(A)$  di una matrice non nulla  $A \in M_{m,n}(F)$  come il massimo ordine di un minore non nullo della matrice  $A$ . Considerate le righe  $A^{(1)}, A^{(2)}, \dots, A^{(m)}$  di  $A$  come vettori dello  $F$ -spazio vettoriale  $F^n$ , si dimostrerà che  $\rho(A)$  coincide con la dimensione del sottospazio di  $F^n$  generato da  $\{A^{(1)}, A^{(2)}, \dots, A^{(m)}\}$ .

**8.6.9. Lemma.** *Siano  $A, B \in M_{m,n}(F)$  matrici equivalenti. Allora il sottospazio generato dalle righe di  $A$  coincide col sottospazio generato dalle righe di  $B$ .*

*Dimostrazione.* Sia  $E \in M_m(F)$  una matrice elementare (vedi 7.3), e si ponga  $B = EA$ . Tenendo presente la definizione di prodotto righe per colonne, è facile convincersi che ogni riga di  $B$  è combinazione lineare dei vettori di  $\{A^{(1)}, A^{(2)}, \dots, A^{(n)}\}$  con scalari in  $F$ . Il sottospazio  $\langle B^{(1)}, B^{(2)}, \dots, B^{(n)} \rangle$  generato dalle righe di  $B$  è quindi contenuto nel sottospazio  $\langle A^{(1)}, A^{(2)}, \dots, A^{(n)} \rangle$  generato dalle righe di  $A$ . Siccome le matrici elementari sono invertibili (come segue immediatamente dall'Esercizio 7.4.10), esiste la matrice  $E^{-1} \in M_m(F)$ , e risulta  $A = E^{-1}B$ . Allora lo stesso argomento appena utilizzato assicura che  $\langle A^{(1)}, A^{(2)}, \dots, A^{(n)} \rangle$  è contenuto in  $\langle B^{(1)}, B^{(2)}, \dots, B^{(n)} \rangle$ , e l'asserto è provato.  $\square$

**8.6.10. Teorema.** *Per ogni matrice  $A \in M_{m,n}(F)$ , il rango di  $A$  coincide col massimo numero di righe di  $A$  linearmente indipendenti come vettori di  $F^n$ .*

*Dimostrazione.* Per 7.3.1 esiste una matrice a scala  $B \in M_{m,n}(F)$  equivalente alla matrice  $A$ . È immediato convincersi che, scartate quelle costituite da tutti 0, le rimanenti righe di  $B$  costituiscono una base per il sottospazio generato dalle righe di  $A$ . Infatti, per il Lemma 8.6.9, esse generano il medesimo sottospazio generato dalle righe di  $A$ ; sono poi ovviamente linearmente indipendenti perché  $B$  è una matrice a scala. Chiaramente il numero dei pivot di  $B$  coincide col numero

di righe linearmente indipendenti di  $B$ , e quindi, per quanto appena provato, di  $A$ . Ma per 7.6.4 il numero dei pivot di  $B$  è proprio il rango di  $B$ . Infine si ha  $\rho(B) = \rho(A)$  per 7.6.5. L'asserto è così provato.  $\square$

Allo stesso modo, se si considerano le colonne  $A_{(1)}, A_{(2)}, \dots, A_{(n)}$  di  $A$  come vettori dello  $F$ -spazio vettoriale  $F^m$ , si può dimostrare che  $\rho(A)$  coincide con la dimensione del sottospazio di  $F^m$  generato da  $\{A_{(1)}, A_{(2)}, \dots, A_{(n)}\}$ . Sussiste cioè il seguente risultato, analogo al Teorema 8.6.10, e la cui dimostrazione si omette.

**8.6.11. Teorema.** *Per ogni matrice  $A \in M_{m,n}(F)$ , il rango di  $A$  coincide col massimo numero di colonne di  $A$  linearmente indipendenti come vettori di  $F^m$ .*

Il Teorema 8.6.10 consente in particolare di calcolare la dimensione di un sottospazio a partire da un suo insieme di generatori.

**8.6.12.** *Siano  $V$  uno spazio vettoriale di dimensione finita  $n$  su un campo  $F$ ,  $B = \{x_1, \dots, x_n\}$  una base di  $V$ ,  $W = \langle w_1, \dots, w_m \rangle$  un sottospazio di  $V$ . Della  $A \in M_{m,n}(F)$  la matrice le cui righe sono le componenti dei generatori di  $W$  nella base  $B$ , risulta  $\dim_F W = \rho(A)$ .*

*Dimostrazione.* Sia  $\Psi : V \longrightarrow F^n$  l'isomorfismo coordinato rispetto alla base  $B$  (vedi Esercizio 8.4.10). La restrizione  $\Psi|_W$  di  $\Psi$  a  $W$  (vedi Esercizio 2.2.15) è ancora iniettiva, pertanto  $W \simeq \Psi(W)$ , quindi  $\dim_F W = \dim_F \Psi(W)$  per 8.4.11. Inoltre, per 8.4.8,  $\Psi(W)$  è generato dai vettori  $\Psi(w_1), \dots, \Psi(w_m) \in F^n$ . In virtù di 8.3.17 e 8.3.19, una base di  $\Psi(W)$  è un insieme massimale di vettori linearmente indipendenti in  $\{\Psi(w_1), \dots, \Psi(w_m)\}$ . Siccome le righe della matrice  $A$  sono precisamente  $\Psi(w_1), \dots, \Psi(w_m)$ , l'asserto segue subito dal Teorema 8.6.10.  $\square$

**8.6.13. Esempio.** Sia  $\mathbb{Q}[x; 3]$  il sottospazio di  $\mathbb{Q}[x]$  costituito dal polinomio nullo e da tutti i polinomi a coefficienti razionali nell'indeterminata  $x$  aventi grado al più 3. Si consideri poi il seguente sottospazio  $W$  di  $\mathbb{Q}[x; 3]$ :

$$W = \langle 1 - x - 2x^3, 1 + x^3, 1 + x + 4x^3, x^2 \rangle.$$

La matrice le cui righe sono le componenti dei generatori di  $W$  nella base canonica  $B = \{1, x, x^2, x^3\}$  di  $\mathbb{Q}[x; 3]$  è

$$A = \begin{pmatrix} 1 & -1 & 0 & -2 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 4 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in M_{4,4}(\mathbb{Q}).$$

Per 8.6.12 risulta  $\dim_{\mathbb{Q}} W = \rho(A)$ . La matrice a scala ridotta equivalente ad  $A$  è

$$C = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in M_{4,4}(\mathbb{Q}).$$

Per 7.6.5 si ha subito  $\dim_{\mathbb{Q}} W = 3$ . Inoltre, ragionando come nella dimostrazione del Teorema 8.6.10, si prova che una base per il sottospazio generato dalle righe di  $A$  è  $\{(1, 0, 0, 1), (0, 1, 0, 3), (0, 0, 1, 0)\}$ . L'isomorfismo coordinato rispetto alla base  $B$  (vedi Esercizio 8.4.10) garantisce allora che  $\{1 + x^3, x + 3x^3, x^2\}$  è una base di  $W$  (vedi Corollario 8.4.7).

**8.6.14. Teorema.** *Siano  $V_1$  e  $V_2$  spazi vettoriali di dimensione finita su uno stesso campo  $F$ ,  $f : V_1 \rightarrow V_2$  un'applicazione lineare,  $A$  la matrice associata a  $f$  rispetto a una base  $B_1$  di  $V_1$  e a una base  $B_2$  di  $V_2$ . Allora risulta:*

$$\rho(A) = \dim_F \text{Im } f.$$

*Dimostrazione.* Siano  $A = (\alpha_{ij})$ ,  $B_1 = \{x_1, \dots, x_n\}$ ,  $B_2 = \{y_1, \dots, y_m\}$ . Allora per (8.6.1) risulta

$$f(x_j) = \sum_{i=1}^m \alpha_{ij} y_i,$$

per ogni  $j = 1, \dots, n$ . Sia poi  $B = \{e_1, \dots, e_m\}$ , con

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad e_m = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

la base canonica di  $M_{m,1}(F)$  (vedi Esempio 8.3.14). Per il Teorema 8.4.9 esiste un'unica applicazione lineare  $\sigma : M_{m,1}(F) \rightarrow V_2$  tale che  $\sigma(e_i) = y_i$  per ogni  $i = 1, \dots, m$ . Siccome  $B_2$  è una base di  $V_2$ ,  $\sigma$  è un isomorfismo (vedi Esercizio 8.4.11). Indicate con  $A_{(1)}, \dots, A_{(n)}$  le colonne di  $A$ , risulta

$$A_{(j)} = \sum_{i=1}^m \alpha_{ij} e_i$$

per ogni  $j = 1, \dots, n$ , da cui

$$\sigma(A_{(j)}) = \sigma \left( \sum_{i=1}^m \alpha_{ij} e_i \right) = \sum_{i=1}^m \alpha_{ij} \sigma(e_i) = \sum_{i=1}^m \alpha_{ij} y_i = f(x_j). \quad (8.6.5)$$

La restrizione  $\langle A_{(1)}, \dots, A_{(n)} \rangle \longrightarrow \langle f(x_1), \dots, f(x_n) \rangle$  di  $\sigma$  è iniettiva in quanto tale è  $\sigma$ , ed è suriettiva per la linearità di  $\sigma$  e per (8.6.5). Pertanto essa è un isomorfismo, e 8.4.11 assicura che  $\dim_F \langle A_{(1)}, \dots, A_{(n)} \rangle = \dim_F \langle f(x_1), \dots, f(x_n) \rangle$ . Inoltre per il Teorema 8.6.11 si ha  $\rho(A) = \dim_F \langle A_{(1)}, \dots, A_{(n)} \rangle$ , mentre da 8.4.8 segue  $\langle f(x_1), \dots, f(x_n) \rangle = \text{Im } f$ . L'asserto è dunque provato.  $\square$

A causa del Teorema 8.6.14, la dimensione dell'immagine di  $f$  viene spesso detta il **rango** dell'applicazione lineare  $f$ , e denotata con  $\rho(f)$ .

## Esercizi

**Esercizio 8.6.1.** Si provi 8.6.2.

**Esercizio 8.6.2.** Siano  $F$  un campo,  $n$  ed  $m$  interi positivi, e si considerino gli insiemi  $F^n$  ed  $F^m$  strutturati a spazi vettoriali su  $F$  nel modo usuale. Si provi che, fissati elementi  $\alpha_{ij} \in F$  per ogni  $i = 1, \dots, m$  e per ogni  $j = 1, \dots, n$ , la posizione

$$f(x_1, x_2, \dots, x_n) = \\ = (\alpha_{11}x_1 + \dots + \alpha_{1n}x_n, \alpha_{21}x_1 + \dots + \alpha_{2n}x_n, \dots, \alpha_{m1}x_1 + \dots + \alpha_{mn}x_n)$$

definisce un'applicazione lineare di  $F^n$  in  $F^m$ , la cui matrice associata rispetto alle basi canoniche di  $F^n$  ed  $F^m$  è  $(\alpha_{ij}) \in M_{m,n}(F)$ .

**Esercizio 8.6.3.** Si dimostri che, ponendo  $A \mathcal{R} B$  se e solo se  $A$  e  $B$  sono matrici simili, si definisce una relazione d'equivalenza in  $M_n(F)$ .

**Esercizio 8.6.4.** Si provi che l'applicazione

$$f : (x, y, z) \in \mathbb{Q}^3 \longmapsto (x + 2y, x - z, y + z, x - y - z) \in \mathbb{Q}^4$$

è un omomorfismo di  $\mathbb{Q}$ -spazi vettoriali, e si scrivano le matrici associate a  $f$  rispetto alle basi canoniche di  $\mathbb{Q}^3$  e di  $\mathbb{Q}^4$  e rispetto alla base canonica di  $\mathbb{Q}^3$  e alla base  $\{(1, \frac{1}{2}, 1, \frac{1}{3}), (0, 1, 0, 2), (1, \frac{1}{3}, \frac{2}{3}, 0), (0, 0, 2, 1)\}$  di  $\mathbb{Q}^4$ .

**Esercizio 8.6.5.** Nell'insieme  $\mathbb{R}^3$ , strutturato a spazio vettoriale su  $\mathbb{R}$  nella maniera usuale, si consideri la base  $B = \{(1, 2, 0), (0, 1, 1), (1, 0, 1)\}$ . Si determini l'automorfismo  $f$  di  $\mathbb{R}^3$  che trasforma ordinatamente i vettori della base canonica di  $\mathbb{R}^3$  nei vettori di  $B$ . Si scriva poi la matrice associata a  $f$  rispetto alla base  $B$ .

**Esercizio 8.6.6.** Si provi che l'applicazione

$$f : (x, y, z) \in (\mathbb{Z}_5)^3 \longmapsto (x + y - z, x - y + z) \in (\mathbb{Z}_5)^2$$

è un omomorfismo di  $\mathbb{Z}_5$ -spazi vettoriali, e si scrivano le matrici associate a  $f$  rispetto alle basi canoniche di  $(\mathbb{Z}_5)^3$  e di  $(\mathbb{Z}_5)^2$  e rispetto alla base canonica di  $(\mathbb{Z}_5)^3$  e alla base  $\{(\bar{2}, \bar{3}), (\bar{1}, \bar{3})\}$  di  $(\mathbb{Z}_5)^2$ .

**Esercizio 8.6.7.** Si determini la matrice associata all'omomorfismo di  $\mathbb{Q}$ -spazi vettoriali

$$f : (x, y) \in \mathbb{Q}^2 \longmapsto (x - y, x + y, 0) \in \mathbb{Q}^3$$

rispetto alla base canonica di  $\mathbb{Q}^2$  e alla base  $\left\{ \left( \frac{1}{2}, 0, 1 \right), \left( 2, \frac{1}{2}, 0 \right), \left( \frac{1}{3}, -1, 1 \right) \right\}$  di  $\mathbb{Q}^3$ .

**Esercizio 8.6.8.** Si consideri l'insieme  $(\mathbb{Z}_{13})^3$  strutturato a spazio vettoriale su  $\mathbb{Z}_{13}$  nel modo usuale.

- (i) Si determini l'endomorfismo  $\varphi$  di  $(\mathbb{Z}_{13})^3$  che trasforma ordinatamente i vettori della base canonica nei vettori  $(2, 3, 4)$ ,  $(3, 4, 5)$ ,  $(5, 7, 10)$ .
- (ii) Si scriva la matrice associata a  $\varphi$  rispetto alla base naturale di  $(\mathbb{Z}_{13})^3$ .
- (iii) Si stabilisca se  $\varphi$  è iniettiva, suriettiva, biettiva.

**Esercizio 8.6.9.** Assegnate le basi  $B_1 = \{(2, 3), (4, 2)\}$  e  $B_2 = \{(1, 1), (0, 4)\}$  dello  $\mathbb{Z}_5$ -spazio vettoriale  $(\mathbb{Z}_5)^2$ , si determini la matrice del cambiamento di base da  $B_1$  a  $B_2$ .

**Esercizio 8.6.10.** Si considerino le basi  $B_1 = \{1, x, x^2\}$  e  $B_2 = \{2, 3x, x^2 + 1\}$  dello  $\mathbb{R}$ -spazio vettoriale  $\mathbb{R}[x; 2]$  (vedi Esempio 8.2.5). Si determini la matrice del cambiamento di base da  $B_1$  a  $B_2$ .

**Esercizio 8.6.11.** Si considerino lo  $\mathbb{Z}_7$ -spazio vettoriale  $\mathbb{Z}_7[x]$ , e il suo sottospazio  $\mathbb{Z}_7[x; 3]$  (vedi Esempio 8.2.5). Si dimostri che gli insiemi

$$\begin{aligned} B_1 &= \{2, x, 3x^2, x^3\} \\ B_2 &= \{1, x, x^2 + x, x^3 + 2x^2 + 1\} \end{aligned}$$

sono basi di  $\mathbb{Z}_7[x; 3]$ , e si determini la matrice del cambiamento di base da  $B_1$  a  $B_2$ .

## 8.7 Ancora sui sistemi di equazioni lineari

Le definizioni fondamentali concernenti i sistemi di equazioni lineari sono già state introdotte nel Paragrafo 7.7. Sono anche già stati discussi due metodi per risolvere i sistemi lineari, quello di Cramer e quello di Gauss-Jordan. Qui si utilizzeranno la teoria degli spazi vettoriali e il concetto di dipendenza lineare per mettere in luce ulteriori proprietà dell'insieme delle soluzioni di un sistema di equazioni lineari.

Con le notazioni del Paragrafo 7.7, si consideri il sistema di equazioni lineari

$$AX = Y, \tag{8.7.1}$$

e si denotino con  $A \in M_{m,n}(F)$  e con  $A' \in M_{m,n+1}(F)$  rispettivamente le matrici incompleta e completa di (8.7.1).

**8.7.1. Teorema di Rouché-Capelli.** Il sistema lineare (8.7.1) ammette almeno una soluzione se e solo se  $\rho(A) = \rho(A')$ .

*Dimostrazione.* Siano  $A_{(1)}, \dots, A_{(n)}$  le colonne di  $A$ . Il sistema (8.7.1) ammette almeno una soluzione se e solo se esistono  $x_1, \dots, x_n \in F$  tali che

$$Y = x_1 A_{(1)} + \cdots + x_n A_{(n)},$$

ossia se e solo se la  $(n+1)$ -esima colonna di  $A'$  dipende linearmente dall'insieme costituito dalle rimanenti, cioè se e solo se  $\rho(A) = \rho(A')$  (per il Teorema 8.6.11).  $\square$

Il teorema di Cramer (vedi 7.7.1) assicura che se  $n = m$  allora il sistema (8.7.1) ha un'unica soluzione se e solo se  $\rho(A) = n$ . Si consideri ora il **sistema lineare omogeneo associato**

$$AX = 0, \quad (8.7.2)$$

dove 0 è la matrice nulla di  $M_{n,1}(F)$ . È evidente che (8.7.2) ammette almeno la soluzione nulla  $X = 0$ , dove ancora 0 è la matrice nulla di  $M_{n,1}(F)$ .

**8.7.2.** Se  $n = m$ , il sistema lineare omogeneo (8.7.2) ammette soltanto la soluzione nulla  $X = 0$  se e solo se  $\rho(A) = n$ .

*Dimostrazione.* Segue subito dal teorema di Cramer (vedi 7.7.1).  $\square$

**8.7.3. Teorema.** Con  $A \in M_{m,n}(F)$  si considerino il sistema lineare (8.7.1) e il sistema lineare omogeneo associato  $AX = 0$ . L'insieme  $S$  delle soluzioni del sistema lineare omogeneo associato è un sottospazio di  $M_{n,1}(F)$  avente dimensione  $n - \rho(A)$ . Se  $X \in M_{n,1}(F)$  è una qualunque soluzione del sistema lineare (8.7.1), l'insieme di tutte le soluzioni di (8.7.1) è dato da  $T = \{X + Z : Z \in S\}$ .

*Dimostrazione.* Fissate una base  $B_1$  di  $M_{n,1}(F)$  e una base  $B_2$  di  $M_{m,1}(F)$ , per il Teorema 8.6.1 la matrice  $A$  è associata rispetto a  $B_1$  e  $B_2$  a un'unica applicazione lineare  $f : M_{n,1}(F) \longrightarrow M_{m,1}(F)$ . In virtù della (8.6.1), una matrice colonna  $X \in M_{n,1}(F)$  è soluzione del sistema lineare omogeneo associato se e solo se  $f(X) = 0$ . Ne segue che  $S = \text{Ker } f$  è un sottospazio di  $M_{n,1}(F)$  per la (i) del teorema di omomorfismo (vedi 8.4.3). Inoltre 8.4.5 e 8.6.14 comportano che  $\dim_F S = \dim_F M_{n,1}(F) - \dim_F \text{Im } f = n - \rho(f) = n - \rho(A)$ .

Infine, sia  $X \in M_{n,1}(F)$  una fissata soluzione del sistema lineare (8.7.1). Allora per la (8.6.1) risulta  $f(X) = Y$ . Ancora,  $X_1 \in M_{n,1}(F)$  è un elemento di  $T$  se e solo se  $f(X_1) = Y$ , cioè se e solo se  $f(X_1 - X) = 0$ , ossia se e solo se  $X_1 - X \in S = \text{Ker } f$ .  $\square$

In definitiva si ha:

#### 8.7.4. Teorema. Sia

$$\left\{ \begin{array}{l} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n = y_1 \\ \alpha_{21}x_1 + \cdots + \alpha_{2n}x_n = y_2 \\ \vdots \\ \alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n = y_m \end{array} \right. \quad (8.7.3)$$

un sistema di  $m$  equazioni lineari in  $n$  incognite su un campo  $F$ , e siano  $A$  e  $A'$  rispettivamente le sue matrici incompleta e completa. Allora il sistema (8.7.3) ammette almeno una soluzione se e solo se  $\rho(A) = \rho(A')$ . In tal caso, posto  $k = \rho(A) = \rho(A')$ , se  $k = n$  la soluzione del sistema è unica. Se invece  $k < n$  si ottiene un'unica soluzione per ogni possibile scelta di  $n - k$  parametri in  $F$ .

*Dimostrazione.* Per il teorema di Rouché-Capelli (vedi 8.7.1) il sistema lineare (8.7.3) ha soluzioni se e solo se  $\rho(A) = \rho(A') = k$ . In tal caso  $k$  è il massimo numero di righe linearmente indipendenti di  $A$  (vedi Teorema 8.6.10); senza perdita di generalità si può supporre che le prime  $k$  righe di  $A$  costituiscano un insieme linearmente indipendente di vettori di  $F^n$ . Allora il sistema (8.7.3) è equivalente al sistema lineare

$$\left\{ \begin{array}{l} \alpha_{11}x_1 + \cdots + \alpha_{1k}x_k + \alpha_{1,k+1}x_{k+1} + \cdots + \alpha_{1n}x_n = y_1 \\ \alpha_{21}x_1 + \cdots + \alpha_{2k}x_k + \alpha_{2,k+1}x_{k+1} + \cdots + \alpha_{2n}x_n = y_2 \\ \vdots \\ \alpha_{k1}x_1 + \cdots + \alpha_{kk}x_k + \alpha_{k,k+1}x_{k+1} + \cdots + \alpha_{kn}x_n = y_k. \end{array} \right. \quad (8.7.4)$$

La matrice incompleta di (8.7.4) ha rango  $k$ , quindi possiede un minore non nullo di ordine  $k$ ; senza perdita di generalità si può supporre che quest'ultimo sia il determinante della sottomatrice

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kk} \end{pmatrix}.$$

Se  $k = n$  allora (8.7.4) ammette un'unica soluzione per il teorema di Cramer (vedi 7.7.1), e quest'ultima coincide con l'unica soluzione di (8.7.3), e può essere determinata mediante la regola di Cramer (vedi 7.7.2).

Se invece  $k < n$ , fissati  $n - k$  elementi  $\bar{x}_{k+1}, \bar{x}_{k+2}, \dots, \bar{x}_n$  di  $F$ , il sistema

lineare

$$\left\{ \begin{array}{l} \alpha_{11}x_1 + \cdots + \alpha_{1k}x_k + \alpha_{1,k+1}\bar{x}_{k+1} + \cdots + \alpha_{1n}\bar{x}_n = y_1 \\ \alpha_{21}x_1 + \cdots + \alpha_{2k}x_k + \alpha_{2,k+1}\bar{x}_{k+1} + \cdots + \alpha_{2n}\bar{x}_n = y_2 \\ \vdots \\ \alpha_{k1}x_1 + \cdots + \alpha_{kk}x_k + \alpha_{k,k+1}\bar{x}_{k+1} + \cdots + \alpha_{kn}\bar{x}_n = y_k \end{array} \right.$$

ovvero

$$\left\{ \begin{array}{l} \alpha_{11}x_1 + \cdots + \alpha_{1k}x_k = y_1 - \alpha_{1,k+1}\bar{x}_{k+1} - \cdots - \alpha_{1n}\bar{x}_n \\ \alpha_{21}x_1 + \cdots + \alpha_{2k}x_k = y_2 - \alpha_{2,k+1}\bar{x}_{k+1} - \cdots - \alpha_{2n}\bar{x}_n \\ \vdots \\ \alpha_{k1}x_1 + \cdots + \alpha_{kk}x_k = y_k - \alpha_{k,k+1}\bar{x}_{k+1} - \cdots - \alpha_{kn}\bar{x}_n \end{array} \right. \quad (8.7.5)$$

ammette un'unica soluzione ancora per il teorema di Cramer (vedi 7.7.1), e quest'ultima può essere determinata mediante la regola di Cramer (vedi 7.7.2). Se

$$\begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_k \end{pmatrix} \in M_{k,1}(F)$$

è la soluzione di (8.7.5) allora chiaramente

$$\begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_k \\ \bar{x}_{k+1} \\ \vdots \\ \bar{x}_n \end{pmatrix} \in M_{n,1}(F)$$

è soluzione di (8.7.4) e quindi di (8.7.3).  $\square$

Se  $k < n$  e  $|F| = t$ , il Teorema 8.7.4 assicura che il sistema (8.7.3) ammette esattamente  $t^{n-k}$  soluzioni, corrispondenti a ogni possibile scelta di  $n-k$  elementi tra  $t$  (vedi 3.5.5). Se il campo  $F$  è infinito (per esempio  $\mathbb{Q}, \mathbb{R}$  oppure  $\mathbb{C}$ ), si dice talvolta che “il sistema (8.7.3) ammette  $\infty^{n-k}$  soluzioni”.

## Esercizi

**Esercizio 8.7.1.** Si completi la dimostrazione del teorema di Cramer (vedi 7.7.1), provando che se  $n = m$  e  $\det A = 0$  allora il sistema lineare (8.7.1) è incompatibile oppure ammette più soluzioni.

*Svolgimento.* Sia  $\det A = 0$ . Allora  $\rho(A) < n$ . Fissata una base di  $F^n$ , il Teorema 8.6.1 assicura che la matrice  $A$  è associata, rispetto alla base fissata, a un unico endomorfismo  $f$  di  $F^n$ . Inoltre per il Teorema 8.6.14 risulta  $\rho(f) = \rho(A) < n$ , cosicché 8.4.5 garantisce che  $\text{Ker } f \neq \{0\}$ . Per la (8.6.4) si ha poi che un elemento  $X \in F^n$  è soluzione di (8.7.1) se e solo se  $f(X) = Y$ . Pertanto certamente se  $Y \notin f(F^n)$  il sistema (8.7.1) non ammette soluzioni. Se invece  $Y \in f(F^n)$  il sistema (8.7.1) ammette almeno una soluzione  $X \in F^n$ . Inoltre in tal caso per ogni  $X' \in \text{Ker } f$  risulta  $X + X'$  ancora soluzione di (8.7.1), in quanto  $f(X + X') = f(X) + f(X') = Y + 0 = Y$ , dove 0 è la matrice nulla di  $M_{n,1}(F)$ . L'asserto segue quindi dall'essere  $\text{Ker } f \neq \{0\}$ .

**Esercizio 8.7.2.** Utilizzando il teorema di Rouché-Capelli (vedi 8.7.1), si stabilisca se il seguente sistema di equazioni lineari su  $\mathbb{R}$  è compatibile:

$$\begin{cases} x + 3z = 1 \\ 2x + y = 2 \\ x + y + z = 0 \\ 3y + z = 1. \end{cases}$$

**Esercizio 8.7.3.** Si risolva il seguente sistema lineare su  $\mathbb{R}$ :

$$\begin{cases} x + 2y + 3z = 1 \\ 2x + y + 4z = 2 \\ 3x - 3y + z = 1. \end{cases}$$

**Esercizio 8.7.4.** Utilizzando il Teorema 8.7.3 si determini la dimensione dello spazio vettoriale delle soluzioni del seguente sistema di equazioni lineari su  $\mathbb{Q}$ :

$$\begin{cases} x - y - z + t = 2 \\ x - y + t = 0 \\ 3x - 2y + z + t = 3. \end{cases}$$

Si risolva poi il sistema lineare assegnato.

**Esercizio 8.7.5.** Utilizzando il Teorema 8.7.3 si determini la dimensione dello spazio vettoriale delle soluzioni del seguente sistema di equazioni lineari su  $\mathbb{Z}_7$ :

$$\begin{cases} \bar{3}x - \bar{2}y + \bar{2}t = \bar{0} \\ x - \bar{2}t = \bar{0} \\ y + z + t = \bar{3}. \end{cases}$$

Si risolva poi il sistema lineare assegnato.

**Esercizio 8.7.6.** Si risolva il seguente sistema lineare su  $\mathbb{R}$ :

$$\begin{cases} x + 2y + 3z = 1 \\ 2x + y + 4z = 2 \\ 3x - 3y + z = 1. \end{cases}$$

**Esercizio 8.7.7.** Si risolva il seguente sistema lineare su  $\mathbb{R}$ :

$$\begin{cases} z + 2t = 3 \\ 2x + 4y - 2z = 4 \\ 2x + 4y - z + 2t = 7. \end{cases}$$

**Esercizio 8.7.8.** Si risolva il seguente sistema lineare su  $\mathbb{R}$ :

$$\begin{cases} y - z = -1 \\ x + z = 1 \\ 2x + y + z = 2. \end{cases}$$

**Esercizio 8.7.9.** Si determinino i valori del parametro reale  $k$  per i quali il sistema di equazioni lineari

$$\begin{cases} kx + y + z = 1 \\ x + ky + z = 1 \\ x + y + kz = 1 \end{cases}$$

ammette un'unica soluzione, nessuna soluzione, più soluzioni.

**Esercizio 8.7.10.** Si determinino i valori del parametro razionale  $k$  per i quali il sistema di equazioni lineari

$$\begin{cases} x + 2y + kz = 1 \\ 2x + ky + 8z = 3 \end{cases}$$

ammette un'unica soluzione, nessuna soluzione, più soluzioni.

**Esercizio 8.7.11.** Si determini la condizione per  $a, b, c \in \mathbb{R}$  per la quale il sistema di equazioni lineari

$$\begin{cases} x - 2y + z = a \\ 2x + 3y - z = b \\ 3x + y + 2z = c \end{cases}$$

risulti compatibile.

**Esercizio 8.7.12.** Si risolva il seguente sistema lineare omogeneo su  $\mathbb{Q}$ :

$$\begin{cases} x_1 - 2x_2 + 3x_3 + 4x_4 + 5x_5 = 0 \\ x_1 + 4x_2 + 7x_4 + 2x_5 = 0 \\ 2x_1 + 8x_2 + 14x_4 + 4x_5 = 0 \\ 2x_1 + 2x_2 + 3x_3 + 11x_4 + 7x_5 = 0 \\ 3x_1 + 6x_2 + 3x_3 + 18x_4 + 9x_5 = 0. \end{cases}$$

## 8.8 Diagonalizzazione di una matrice

In questo paragrafo si esamina la possibilità di determinare una matrice diagonale simile a un'assegnata matrice quadrata. Il motivo di ciò risiede essenzialmente nel fatto che operare con matrici diagonali è computazionalmente molto più agevole che operare con matrici generiche. Per esempio, se  $D \in M_n(F)$  è una matrice diagonale, allora la potenza  $m$ -esima  $D^m$  è semplicemente la matrice diagonale le cui entrate sono ciascuna la potenza  $m$ -esima della corrispondente entrata di  $D$ .

Sia  $A \in M_n(F)$  una matrice quadrata su un campo  $F$ . Per le definizioni di autovalore e autovettore di  $A$  si rimanda al Paragrafo 7.8. Nel seguito, un autovettore di  $A$  sarà considerato talvolta come un vettore colonna in  $M_{n,1}(F)$ , talaltra come un vettore di  $F^n$ . Ciò è giustificato dal fatto che gli  $F$ -spazi vettoriali  $M_{n,1}(F)$  e  $F^n$  sono isomorfi (vedi Esercizio 8.4.1).

**8.8.1.** Sia  $\lambda$  un autovalore di una matrice  $A \in M_n(F)$ . Allora l'insieme  $W_\lambda$  costituito dal vettore nullo di  $M_{n,1}(F)$  e dagli autovettori di  $A$  relativi all'autovalore  $\lambda$  è un sottospazio di  $M_{n,1}(F)$ , detto l'autospazio di  $A$  relativo all'autovalore  $\lambda$ .

*Dimostrazione.* Esercizio. □

Ovviamente se  $W_\lambda$  è l'autospazio di  $A$  relativo all'autovalore  $\lambda$  allora gli autovettori di  $A$  relativi all'autovalore  $\lambda$  sono tutti e soli i vettori non nulli in  $W_\lambda$ . Nel Paragrafo 7.8 si è definito il polinomio caratteristico  $p_A(x) \in F[x]$  di una matrice  $A \in M_n(F)$  ponendo  $p_A(x) = \det(A - xI_n)$ , e si è osservato che gli autovalori di  $A$  sono tutte e sole le radici in  $F$  del polinomio caratteristico  $p_A(x)$  (vedi Corollario 7.8.3). Sia  $\lambda \in F$  un autovalore della matrice  $A$ . Si dice **molteplicità algebrica** di  $\lambda$  la sua molteplicità  $\nu_\lambda$  come radice di  $p_A(x)$ . Pertanto dire che  $\lambda$  ha molteplicità algebrica  $t$  equivale a dire che, in  $F[x]$ , il polinomio  $(x - \lambda)^t$  divide  $p_A(x)$  ma  $(x - \lambda)^{t+1}$  non divide  $p_A(x)$  (vedi Paragrafo 6.6). La dimensione dell'autospazio  $W_\lambda$  di  $A$  relativo all'autovalore  $\lambda$  viene spesso detta la **molteplicità geometrica** di  $\lambda$ , qui denotata col simbolo  $\mu_\lambda$ . In generale questi due interi, sempre compresi tra 1 e  $n$  per la definizione di autovalore, sono distinti. Si potrebbe dimostrare che riesce sempre  $1 \leq \mu_\lambda \leq \nu_\lambda \leq n$ .

**8.8.2. Esempio.** Il polinomio caratteristico della matrice

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$$

è  $p_A(x) = x^2 - 2x + 1 = (x - 1)^2$ , che ha 1 come radice doppia. Pertanto l'unico autovalore di  $A$  è 1, e si ha  $\nu_1 = 2$ . L'autospazio di  $A$  relativo all'autovettore 1 è  $W_1 = \{(a, -a) : a \in \mathbb{R}\}$ . Siccome  $W_1$  ha come base  $\{(1, -1)\}$ , risulta  $\mu_1 = 1$ .

Si prova facilmente che matrici simili hanno lo stesso polinomio caratteristico, e quindi gli stessi autovalori, con la stessa molteplicità algebrica.

**8.8.3.** *Siano  $A$  e  $A' \in M_n(F)$  matrici simili. Allora  $p_A(x) = p_{A'}(x)$ .*

*Dimostrazione.* Per ipotesi esiste una matrice invertibile  $C \in M_n(F)$  tale che  $A' = C^{-1}AC$ . Allora  $A' - xI_n = C^{-1}AC - xC^{-1}I_nC = C^{-1}(A - xI_n)C$ , quindi  $\det(A' - xI_n) = (\det C)^{-1}\det(A - xI_n)\det C = \det(A - xI_n)$  per il teorema di Binet (vedi 7.4.2) e per 7.5.3. Ne segue l'asserto.  $\square$

È interessante osservare che il risultato in 8.8.3 non si inverte: esistono matrici che, pur avendo lo stesso polinomio caratteristico, non sono simili (vedi Esempio 8.8.12).

Autovettori relativi ad autovalori distinti sono linearmente indipendenti, come assicura la proposizione seguente.

**8.8.4.** *Siano  $\lambda_1, \dots, \lambda_r \in F$  autovalori distinti di una matrice  $A \in M_n(F)$ , e per ogni  $i = 1, \dots, r$  sia  $V_i \in M_{n,1}(F)$  un autovettore di  $A$  relativo all'autovalore  $\lambda_i$ . Allora  $\{V_1, \dots, V_r\}$  è un sottoinsieme linearmente indipendente di  $M_{n,1}(F)$  avente ordine  $r$ .*

*Dimostrazione.* Si osservi innanzitutto che  $|\{V_1, \dots, V_r\}| = r$  per 7.8.1.

Per assurdo, sia  $\{V_1, \dots, V_r\}$  linearmente dipendente. Siccome  $V_1$  è un autovettore di  $A$ , e quindi non è il vettore nullo di  $F^n$ , il singleton  $\{V_1\}$  è linearmente indipendente. Allora esiste un intero positivo  $i < r$  tale che l'insieme  $\{V_1, \dots, V_i\}$  è linearmente indipendente, ma  $\{V_1, \dots, V_i, V_{i+1}\}$  è linearmente dipendente. Ciò significa che esistono scalari  $\beta_1, \dots, \beta_i, \beta_{i+1} \in F$ , non tutti nulli, tali che

$$\beta_1 V_1 + \cdots + \beta_i V_i + \beta_{i+1} V_{i+1} = 0, \quad (8.8.1)$$

dove ovviamente 0 è la matrice nulla di  $M_{n,1}(F)$ . Moltiplicando (righe per colonne) entrambi i membri di tale uguaglianza per la matrice  $A$ , e utilizzando le uguaglianze  $AV_j = \lambda_j V_j$  valide per ogni  $j = 1, \dots, n$  in quanto  $V_j$  è autovettore di  $A$  relativo all'autovalore  $\lambda_j$ , si ottiene

$$\lambda_1 \beta_1 V_1 + \cdots + \lambda_i \beta_i V_i + \lambda_{i+1} \beta_{i+1} V_{i+1} = 0. \quad (8.8.2)$$

Moltiplicando (8.8.1) per  $\lambda_{i+1}$  e sottraendo il risultato da (8.8.2), si ottiene

$$(\lambda_1 - \lambda_{i+1}) \beta_1 V_1 + \cdots + (\lambda_i - \lambda_{i+1}) \beta_i V_i = 0. \quad (8.8.3)$$

Siccome  $\{V_1, \dots, V_i\}$  è linearmente indipendente, da (8.8.3) segue subito che  $(\lambda_j - \lambda_{i+1}) \beta_j = 0$  per ogni  $j = 1, \dots, i$ . Essendo per ipotesi  $\lambda_j \neq \lambda_{i+1}$ , ciò implica  $\beta_j = 0$  per ogni  $j = 1, \dots, i$ . Ma allora da (8.8.1) segue  $\beta_{i+1} = 0$ , una contraddizione in quanto  $\beta_1, \dots, \beta_i, \beta_{i+1}$  non possono essere tutti nulli.  $\square$

**8.8.5. Corollario.** Siano  $\lambda_1, \dots, \lambda_r \in F$  gli autovalori distinti di una matrice  $A \in M_n(F)$ . Denotato con  $W_{\lambda_i}$  l'autospazio di  $A$  relativo all'autovalore  $\lambda_i$ , per ogni  $i = 1, \dots, r$ , risulta allora  $W_{\lambda_1} + \dots + W_{\lambda_r} = W_{\lambda_1} \oplus \dots \oplus W_{\lambda_r}$ .

*Dimostrazione.* Esercizio. □

Una matrice  $A \in M_n(F)$  si dice **diagonalizzabile** su  $F$  se essa è simile a una matrice diagonale, ossia se esistono una matrice diagonale  $D \in M_n(F)$  e una matrice invertibile  $C \in M_n(F)$  tali che  $A = C^{-1}DC$ . In tal caso si dice anche che la matrice  $C$  **diagonalizza**  $A$ . Il risultato che segue evidenzia il legame tra matrici diagonalizzabili e autovalori.

**8.8.6.** Sia  $A \in M_n(F)$  una matrice diagonalizzabile su  $F$ . Allora  $A$  è simile a una matrice diagonale  $D \in M_n(F)$  che ha sulla diagonale principale gli autovalori di  $A$ . Inoltre ciascun autovalore  $\lambda$  di  $A$  compare esattamente  $\nu_\lambda$  volte sulla diagonale principale di  $D$ .

*Dimostrazione.* L'asserto segue immediatamente dalla definizione, dall'Esercizio 8.8.3 e da 8.8.3. □

Da 8.8.6 segue subito che il polinomio caratteristico di una matrice diagonalizzabile  $A \in M_n(F)$  ha tutte le sue radici in  $F$ .

**8.8.7. Corollario.** Sia  $A \in M_n(F)$  una matrice diagonalizzabile su  $F$ . Allora la somma delle molteplicità algebriche degli autovalori distinti di  $A$  è  $n$ .

Da 8.8.4 segue un importante criterio di diagonalizzabilità.

**8.8.8. Teorema.** Una matrice  $A \in M_n(F)$  è diagonalizzabile su  $F$  se e solo se essa ammette  $n$  autovettori linearmente indipendenti in  $M_{n,1}(F)$ .

*Dimostrazione.* Si assuma che  $A$  ammette  $n$  autovettori  $V_1, \dots, V_n$  linearmente indipendenti in  $M_{n,1}(F)$ , e siano rispettivamente  $\lambda_1, \dots, \lambda_n \in F$  i relativi autovalori. Sia  $C \in M_n(F)$  la matrice la cui colonna  $i$ -esima è  $V_i$ , per ogni  $i = 1, \dots, n$ . Si osservi che dal Teorema 8.6.11 e da 7.5.1 segue subito che  $C$  è invertibile. Le colonne della matrice  $AC$  (prodotto righe per colonne) sono ordinatamente  $AV_1, \dots, AV_n$ . Si consideri ora la matrice diagonale

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

È immediato verificare che il prodotto  $CD$  è la matrice le cui colonne sono ordinatamente  $\lambda_1 V_1, \dots, \lambda_n V_n$ . Avendosi  $AV_i = \lambda_i V_i$  per ogni  $i = 1, \dots, n$ , risulta quindi  $AC = CD$ , cioè  $C^{-1}AC = D$ . Pertanto  $A$  è diagonalizzabile su  $F$ .

Viceversa, sia  $A$  diagonalizzabile su  $F$ . Allora esistono una matrice invertibile  $C \in M_n(F)$  e una matrice diagonale

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix} \in M_n(F)$$

tale che  $C^{-1}AC = D$ , cioè  $AC = CD$ . Da ciò segue che, per ogni  $i = 1, \dots, n$ , se  $C_{(i)}$  è la  $i$ -esima colonna di  $C$ , allora  $AC_{(i)}$  coincide con la  $i$ -esima colonna di  $CD$ , che è  $d_i C_{(i)}$ . Inoltre  $C_{(i)}$  non è il vettore nullo di  $M_{n,1}(F)$  in quanto  $C$  è invertibile. Pertanto  $C_{(1)}, \dots, C_{(n)}$  sono autovettori di  $A$  relativi rispettivamente agli autovalori  $d_1, \dots, d_n$ . Infine,  $C_{(1)}, \dots, C_{(n)}$  sono linearmente indipendenti in  $M_{n,1}(F)$  per il Teorema 8.6.11 e per 7.5.1, in quanto colonne di una matrice invertibile.  $\square$

**Osservazione.** Il risultato appena provato assicura che una matrice  $A \in M_n(F)$  è diagonalizzabile su  $F$  se e solo se esiste una base  $B$  di  $M_{n,1}(F)$  costituita da autovettori di  $A$ . Se  $A$  è diagonalizzabile su  $F$ , la dimostrazione del Teorema 8.8.8 fornisce di fatto un modo per determinare una matrice invertibile  $C$  che diagonalizza  $A$ : le colonne di  $C$  sono costituite dagli  $n$  vettori della base  $B$ . È anche importante evidenziare che la matrice  $A$  risulta simile alla matrice diagonale  $D \in M_n(F)$  che ha sulla diagonale principale gli autovalori corrispondenti agli autovettori di  $A$  che costituiscono la base  $B$ .

In particolare:

**8.8.9. Corollario.** Una matrice  $A \in M_n(F)$  che possiede  $n$  autovalori distinti in  $F$  è diagonalizzabile su  $F$ .

*Dimostrazione.* Segue subito da 8.8.4 e dal Teorema 8.8.8.  $\square$

Esistono, ovviamente, matrici non diagonalizzabili.

**8.8.10. Esempio.** Si consideri la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{C}).$$

Gli autovalori di  $A$  sono  $\lambda_1 = \lambda_2 = 1$  (vedi Esercizio 8.8.3), pertanto, se fosse diagonalizzabile,  $A$  risulterebbe simile alla matrice identica  $I_2$  (vedi 8.8.6). Ma allora esiste una matrice invertibile  $C \in M_2(\mathbb{C})$  tale che  $C^{-1}AC = I_2$ , e ciò implica  $I_2 = CI_2C^{-1} = A$ , una contraddizione.

Se  $A \in M_n(F)$  possiede  $n$  autovalori distinti  $\lambda_1, \dots, \lambda_n$ , allora 8.8.4 assicura che ogni autospazio  $W_{\lambda_i}$  ha dimensione 1, e  $M_{n,1}(F) = W_{\lambda_1} \oplus \dots \oplus W_{\lambda_n}$ . Più in generale si ha:

**8.8.11. Teorema.** Una matrice  $A \in M_n(F)$  è diagonalizzabile su  $F$  se e solo se la somma delle molteplicità geometriche degli autovalori distinti di  $A$  è  $n$ .

*Dimostrazione.* Siano  $\lambda_1, \dots, \lambda_r$  gli autovalori distinti di  $A$ , e si assuma dapprima  $\dim_F W_{\lambda_1} + \dots + \dim_F W_{\lambda_r} = n$ . Utilizzando il Corollario 8.8.5 e il Teorema 8.5.6, si ottiene facilmente  $M_{n,1}(F) = W_{\lambda_1} \oplus \dots \oplus W_{\lambda_r}$ . Allora 8.5.5 assicura che, se  $B_i$  è una base di  $W_{\lambda_i}$  per ogni  $i = 1, \dots, r$ , l'insieme  $B = B_1 \cup \dots \cup B_r$  è una base di  $M_{n,1}(F)$ . Di conseguenza  $A$  è diagonalizzabile su  $F$  per il Teorema 8.8.8.

Viceversa, sia  $A$  diagonalizzabile su  $F$ , e quindi esista per il Teorema 8.8.8 una base  $B$  di  $M_{n,1}(F)$  costituita da autovettori di  $A$ . Se  $\lambda_1, \dots, \lambda_r$  sono gli autovalori distinti di  $A$ , il Corollario 8.8.5 garantisce che

$$W_{\lambda_1} + \dots + W_{\lambda_r} = W_{\lambda_1} \oplus \dots \oplus W_{\lambda_r}.$$

Per ogni  $i = 1, \dots, r$ , siano  $V_{i1}, \dots, V_{is_i}$  gli elementi di  $B$  che appartengono all'autospazio  $W_{\lambda_i}$ . Allora ovviamente  $s_1 + \dots + s_r = n$ . Inoltre, essendo  $B$  una base, risulta  $\dim_F W_{\lambda_i} \geq s_i$ , per ogni  $i = 1, \dots, r$ . Da ciò segue facilmente che  $\dim_F W_{\lambda_1} + \dots + \dim_F W_{\lambda_r} = n$ , come volevasi.  $\square$

**8.8.12. Esempio.** In  $M_3(\mathbb{Q})$ , si considerino le matrici

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}, \quad A' = \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & -2 \end{pmatrix}.$$

Si verifica facilmente (vedi Esercizio 8.8.14) che

$$p_A(x) = p_{A'}(x) = -x^3 + 12x + 16 = -(x+2)^2(x-4).$$

Pertanto  $A$  e  $A'$  hanno lo stesso polinomio caratteristico; gli autovalori distinti, sia di  $A$  che di  $A'$ , sono dunque  $\lambda_1 = -2$  e  $\lambda_2 = 4$ . Eseguendo i calcoli, si trova che una base dell'autospazio  $W_{-2}$  di  $A$  relativo all'autovalore  $-2$  è  $\{(1, 1, 0), (1, 0, -1)\}$ , e che una base di  $W_4$  è  $\{(1, 1, 2)\}$ . Pertanto il Teorema 8.8.11 assicura che  $A$  è diagonalizzabile su  $\mathbb{Q}$ . Più precisamente, il Teorema 8.8.8 mostra che una matrice che diagonalizza  $A$  è

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix},$$

e che  $A$  è simile alla matrice diagonale

$$D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Svolgendo i calcoli si trova inoltre che una base dell'autospazio  $W'_{-2}$  di  $A'$  relativo all'autovalore  $-2$  è  $\{(1, 1, 0)\}$ , e che una base di  $W'_4$  è  $\{(0, 1, 1)\}$ . Pertanto, per il Teorema 8.8.11, la matrice  $A'$  non è diagonalizzabile su  $\mathbb{Q}$ . Per l'Esercizio 8.6.3, da ciò si deduce facilmente che  $A$  e  $A'$  non sono simili. Pertanto 8.8.3 non si inverte.

Nella pratica, risulta spesso comodo utilizzare il criterio di diagonalizzabilità fornito dal teorema che segue.

**8.8.13. Teorema.** *Una matrice  $A \in M_n(F)$  è diagonalizzabile su  $F$  se e solo se sono verificate le due condizioni seguenti:*

- (i) *tutte le radici del polinomio caratteristico di  $A$  appartengono a  $F$ ;*
- (ii) *ogni autovalore di  $A$  ha molteplicità algebrica e geometrica coincidenti.*

*Dimostrazione.* Si assuma dapprima che valgano (i) e (ii). A causa di (i), la somma delle molteplicità algebriche degli autovalori distinti di  $A$  vale  $n$ . Ne segue, per (ii), che vale  $n$  anche la somma delle molteplicità geometriche degli autovalori distinti di  $A$ . Pertanto  $A$  è diagonalizzabile su  $F$  per il Teorema 8.8.11.

Sia ora  $A$  diagonalizzabile su  $F$ . Allora vale la (i) per 8.8.6. Inoltre, per il Teorema 8.8.8 (e la successiva osservazione), la matrice  $A$  è simile a una matrice diagonale  $D \in M_n(F)$  che ha sulla diagonale principale gli autovalori di  $A$  corrispondenti ad autovettori che formano una base di  $M_{n,1}(F)$ . Siano  $\lambda_1, \dots, \lambda_r$  gli autovalori distinti di  $A$  che si trovano sulla diagonale principale di  $D$ . Allora, per il Teorema 8.8.11, dette  $\mu_1, \dots, \mu_r$  le molteplicità geometriche di  $\lambda_1, \dots, \lambda_r$  rispettivamente, risulta  $\mu_1 + \dots + \mu_r = n$ . Inoltre ciascuno dei  $\lambda_i$  ( $i = 1, \dots, r$ ) compare sulla diagonale principale di  $D$  esattamente  $\mu_i$  volte. Ne segue, per il Corollario 8.8.5, che  $\lambda_1, \dots, \lambda_r$  sono tutti gli autovalori distinti di  $A$ . Allora 8.8.6 assicura che  $A$  è anche simile a una matrice diagonale  $D' \in M_n(F)$  avente sulla diagonale principale gli autovalori  $\lambda_1, \dots, \lambda_r$ ; ciascuno dei  $\lambda_i$  ( $i = 1, \dots, r$ ) compare sulla diagonale principale di  $D'$  esattamente  $\nu_i$  volte, dove  $\nu_i$  è la molteplicità algebrica di  $\lambda_i$ . Siccome  $D$  e  $D'$  sono simili (vedi Esercizio 8.6.3), per 8.8.3 esse hanno lo stesso polinomio caratteristico. Pertanto risulta

$$\begin{aligned} p_D(x) &= (-1)^n (x - \lambda_1)^{\mu_1} (x - \lambda_2)^{\mu_2} \dots (x - \lambda_r)^{\mu_r} \\ &= (-1)^n (x - \lambda_1)^{\nu_1} (x - \lambda_2)^{\nu_2} \dots (x - \lambda_r)^{\nu_r} = p_{D'}(x). \end{aligned} \quad (8.8.4)$$

Essendo  $\lambda_1, \dots, \lambda_r$  a due a due distinti, da (8.8.4) segue che  $\mu_i = \nu_i$  per ogni  $i = 1, \dots, r$  (vedi Esercizio 6.6.15), quindi vale la (ii).  $\square$

Siano  $F$  un campo e  $V$  uno spazio vettoriale su  $F$  di dimensione finita  $n$ , e sia  $f : V \rightarrow V$  un endomorfismo di  $V$ . Uno scalare  $\lambda \in F$  è detto **autovalore** di  $f$  se esiste un vettore non nullo  $v \in V$  tale che  $f(v) = \lambda v$ . Se ciò accade  $v$  è detto **autovettore** di  $f$  relativo all'autovalore  $\lambda$ .

Sia ora  $B$  una base di  $V$ , e  $A = (a_{ij}) \in M_n(F)$  la matrice associata all'endomorfismo  $f$  rispetto alla base  $B$ . Sia

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(F)$$

il vettore colonna delle componenti nella base  $B$  del generico vettore  $v \in V$ , univocamente determinate per 8.3.18. Allora le componenti di  $f(v)$  nella base  $B$  sono date dal prodotto righe per colonne

$$A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(F)$$

(vedi osservazione in 8.6). Pertanto uno scalare  $\lambda \in F$  è autovalore di  $f$  se e solo se esiste un vettore non nullo  $v \in V$  tale che

$$A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \lambda \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

ossia se e solo se  $\lambda$  è autovalore della matrice  $A$  associata a  $f$  rispetto alla base  $B$ , secondo la definizione data nel Paragrafo 7.8. Se  $A'$  è la matrice associata a  $f$  rispetto a un'altra base  $B'$  di  $V$ , allora per 8.6.7 le matrici  $A$  e  $A'$  sono simili. Sussistendo 8.8.3, è lecito definire **polinomio caratteristico** dell'endomorfismo  $f$  di  $V$  il polinomio caratteristico di una qualunque matrice associata all'endomorfismo  $f$  rispetto a una qualunque base di  $V$ . Per quanto osservato finora, il Corollario 7.8.3 assicura che:

**8.8.14.** *Gli autovalori (ed i relativi autovettori) di un endomorfismo  $f$  di uno spazio vettoriale  $V$  sono tutti e soli quelli della matrice associata a  $f$  rispetto a una qualunque base di  $V$ , e quindi tutte e sole le radici del polinomio caratteristico dell'endomorfismo  $f$ .*

In virtù del Teorema 8.6.1 e di 8.8.14, parlare di autovalori (e autovettori) di una matrice o di un endomorfismo è perfettamente equivalente.

Un endomorfismo  $f$  di uno spazio vettoriale  $V$  è detto **diagonizzabile** se esiste una base  $B$  di  $V$  tale che la matrice associata a  $f$  rispetto a  $B$  è diagonale.

Tutti i risultati dimostrati in questo paragrafo con riferimento alle matrici possono essere riformulati con riferimento agli endomorfismi, e permane la loro validità. I dettagli dimostrativi sono lasciati al Lettore.

Si conclude questo capitolo enunciando uno dei risultati più importanti dell’algebra lineare, per la cui dimostrazione si rimanda a testi più specialistici (per esempio [12]). Siano  $F$  un campo, e sia

$$p(x) = \alpha_t x^t + \cdots + \alpha_1 x + \alpha_0$$

un polinomio a coefficienti in  $F$  nell’indeterminata  $x$ . Assegnata una matrice  $A \in M_n(F)$ , si pone

$$p(A) := \alpha_t A^t + \cdots + \alpha_1 A + \alpha_0 I_n \in M_n(F),$$

dove  $I_n \in M_n(F)$  è la matrice identica. Se  $p(A)$  è la matrice nulla, si dice che  $A$  è *radice* di  $p(x)$  in  $M_n(F)$ .

**8.8.15. Teorema di Cayley-Hamilton.** *Ogni matrice  $A \in M_n(F)$  è radice del suo polinomio caratteristico  $p_A(x)$ .*

**8.8.16. Esempio.** Il polinomio caratteristico della matrice

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \in M_2(\mathbb{R})$$

è  $p_A(x) = x^2 - 3x - 4$ . Si ha:

$$A^2 - 3A - 4 = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}^2 - 3 \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} - 4 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

quindi  $A$  è radice del suo polinomio caratteristico, come garantito dal teorema di Cayley-Hamilton (vedi 8.8.15).

Una semplice applicazione del teorema di Cayley-Hamilton (vedi 8.8.15) è il risultato che segue, spesso utilizzato soprattutto in Informatica.

**8.8.17.** *Sia  $A \in M_n(F)$  una matrice quadrata su un campo  $F$ . Allora per ogni intero  $m \geq 0$  la potenza  $m$ -esima  $A^m$  è combinazione lineare, con coefficienti in  $F$ , degli elementi  $I_n, A, A^2, \dots, A^{n-1}$  di  $M_n(F)$ .*

*Dimostrazione.* Esercizio. □

## Esercizi

**Esercizio 8.8.1.** *Si provi 8.8.1.*

**Esercizio 8.8.2.** *Si dimostri il Corollario 8.8.5.*

**Esercizio 8.8.3.** Sia  $A \in M_n(F)$  una matrice triangolare (superiore o inferiore). Si dimostri che gli autovalori di  $A$  sono tutti e soli gli elementi della diagonale principale di  $A$ .

**Esercizio 8.8.4.** Siano  $A$  e  $B$  matrici quadrate su un campo  $F$ . Si dimostri che  $AB$  e  $BA$  hanno gli stessi autovalori.

*Suggerimento.* Si osservi innanzitutto che  $0$  è autovalore di  $AB$  se e solo se lo è di  $BA$ . Si provi poi che ogni autovalore non nullo di  $AB$  è autovalore di  $BA$ , e viceversa.

**Esercizio 8.8.5.** Sia  $A \in M_n(F)$ , e sia  $C \in M_n(F)$  una matrice invertibile. Si dimostri che  $V \in M_{n,1}(F)$  è autovettore di  $C^{-1}AC$  relativo all'autovalore  $\lambda \in F$  se e solo se  $CV$  è autovettore di  $A$  relativo all'autovalore  $\lambda$ . Se ne deduca che l'insieme degli autovettori di una matrice non è invariante per similitudine.

**Esercizio 8.8.6.** Sia  $A \in M_n(F)$ , e sia  $p_A(x)$  il polinomio caratteristico di  $A$ . Si dimostri che il termine noto di  $p_A(x)$  coincide con  $\det A$ .

**Esercizio 8.8.7.** Sia  $A \in M_n(F)$ , e sia  $p_A(x)$  il polinomio caratteristico di  $A$ . Si dimostri, per induzione su  $n$ , che il coefficiente di grado  $n-1$  di  $p_A(x)$  è  $(-1)^{n-1} \operatorname{tr}(A)$ , dove  $\operatorname{tr}(A)$  è la traccia di  $A$  (vedi Esercizio 8.3.16). Se ne deduca che matrici simili hanno la stessa traccia.

**Esercizio 8.8.8.** Si provi che una matrice  $A \in M_n(\mathbb{C})$ , il cui polinomio caratteristico non abbia radici multiple, è diagonalizzabile. Si osservi, esibendo un controesempio, che la conclusione non è in generale vera in presenza di radici multiple.

**Esercizio 8.8.9.** Si stabilisca se la matrice

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}$$

è diagonalizzabile su  $\mathbb{Q}$ , ed in caso affermativo la si diagonalizzi.

**Esercizio 8.8.10.** Si stabilisca se le matrici

$$A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$$

sono diagonalizzabili su  $\mathbb{Q}$ , su  $\mathbb{R}$ , su  $\mathbb{C}$ , e in caso affermativo le si diagonalizzzi.

**Esercizio 8.8.11.** Si stabilisca se le matrici

$$A = \begin{pmatrix} \bar{1} & \bar{2} \\ \frac{1}{3} & \frac{1}{4} \end{pmatrix}, \quad B = \begin{pmatrix} \bar{1} & \bar{0} \\ \frac{1}{2} & \frac{1}{3} \end{pmatrix}$$

sono diagonalizzabili su  $\mathbb{Z}_5$ , su  $\mathbb{Z}_7$  e su  $\mathbb{Z}_{11}$ , e in caso affermativo le si diagonalizzzi.

**Esercizio 8.8.12.** Si stabilisca se la matrice

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

è diagonalizzabile su  $\mathbb{R}$ , e in caso affermativo la si diagonalizzi.

**Esercizio 8.8.13.** Si stabilisca se la matrice

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

è diagonalizzabile su  $\mathbb{Q}$ , e in caso affermativo la si diagonalizzi.

**Esercizio 8.8.14.** Si eseguano nei dettagli i calcoli e le verifiche necessarie nell'Esempio 8.8.12.

**Esercizio 8.8.15.** Si dimostri 8.8.17.

*Suggerimento.* Per  $m = 0, 1, \dots, n-1$  il risultato è ovvio. Si utilizzi il teorema di Cayley-Hamilton (vedi 8.8.15) per provare che esso vale per  $m = n$ . Si proceda poi per induzione su  $m - n > 0$ .

## 8.9 Esercizi di riepilogo

**Esercizio 8.9.1.** Si provi che gli insiemi

$$\begin{aligned} V &= \{(1, 0, -1), (-2, 4, 1), (0, 0, 5)\}, \\ W &= \{(0, 3, 0), (1, -1, 0), (-1, 2, 1)\} \end{aligned}$$

sono basi dello spazio vettoriale reale usuale  $\mathbb{R}^3$ , e si determinino le matrici del cambiamento di base da  $V$  a  $W$  e da  $W$  alla base canonica di  $\mathbb{R}^3$ . Considerata poi l'applicazione lineare  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  definita ponendo

$$\begin{aligned} f(1, 0, -1) &= (1, 0, -1), \\ f(-2, 4, 1) &= (2, -4, -1), \\ f(0, 0, 5) &= (0, 0, 15), \end{aligned}$$

si determini  $f(x, y, z)$  per ogni  $(x, y, z) \in \mathbb{R}^3$ .

**Esercizio 8.9.2.** Si considerino  $\mathbb{R}^3$  ed  $\mathbb{R}^4$  strutturati a spazio vettoriale su  $\mathbb{R}$  nel modo usuale.

(i) Si dimostri che  $B = \{(1, 0, 1), (0, 0, 2), (3, -1, 0)\}$  è una base di  $\mathbb{R}^3$ .

(ii) Considerata l'applicazione lineare  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$  definita dalle posizioni

$$\begin{aligned} f(1, 0, 1) &= (1, 0, 0, 0), \\ f(0, 0, 2) &= (-1, 1, k-1, 0), \\ f(3, -1, 0) &= (1, 1, k, 0), \end{aligned}$$

dove  $k$  è un parametro reale, si determini  $f(x, y, z)$  per ogni  $(x, y, z) \in \mathbb{R}^3$ .  
(iii) Si stabilisca per quali valori di  $k$  l'applicazione  $f$  è iniettiva.

**Esercizio 8.9.3.** Nell'usuale spazio vettoriale reale  $\mathbb{R}^4$ , si considerino i sottospazi

$$\begin{aligned} V &= \{(x, y, z, t) : x + 3y - z = 0\}, \\ W &= \langle(1, 0, 0, 1), (0, 1, 1, 0), (1, 2, 2, 1)\rangle. \end{aligned}$$

- (i) Si determinino una base e la dimensione di  $V$ ,  $W$ ,  $V \cap W$  e  $V + W$ .  
(ii) Si stabilisca se la somma  $V + W$  è diretta.

**Esercizio 8.9.4.** Si considerino gli usuali spazi vettoriali reali  $\mathbb{R}^2$  e  $\mathbb{R}^3$ , e l'applicazione  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$  definita da  $f(x, y) = (2x - y, x + y, x)$ .

- (i) Si dimostri che  $f$  è lineare.  
(ii) Si determini la matrice che rappresenta  $f$  rispetto alle basi canoniche di  $\mathbb{R}^2$  e di  $\mathbb{R}^3$ .  
(iii) Si determini la matrice che rappresenta  $f$  rispetto alle basi  $\{(1, 1), (2, 0)\}$  di  $\mathbb{R}^2$  e  $\{(-1, -1, -1), (0, -1, -1), (0, 0, -1)\}$  di  $\mathbb{R}^3$ .  
(iv) Si determini la dimensione di  $\text{Ker } f$  e di  $\text{Im } f$ .

**Esercizio 8.9.5.** Sia  $F$  un campo e si consideri l'usuale spazio vettoriale  $F^4$ .

- (i) Si verifichi che l'applicazione

$$\varphi : (a, b, c, d) \in F^4 \mapsto (a + 3c, 4b + d) \in F^2$$

è un epimorfismo di  $F$ -spazi vettoriali.

- (ii) Si determinino il nucleo  $\text{Ker } \varphi$  e un suo supplementare.  
(iii) Si discuta la dimensione del sottospazio

$$W = \langle(6, 2, 0, 3), (-4, 0, 1, 6), (0, -6, -2, 0), (3, 4, 1, 0)\rangle$$

di  $F^4$  in funzione della caratteristica di  $F$ , determinandone poi una base.

**Esercizio 8.9.6.** Siano  $F$  un campo e  $V$  uno spazio vettoriale su  $F$  di dimensione 4 e di base  $\{x_1, x_2, x_3, x_4\}$ .

- (i) Strutturato  $F$  come spazio vettoriale su se stesso, si provi che l'applicazione

$$\psi : \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4 \in V \mapsto \alpha + \beta + \gamma + \delta \in F$$

è lineare, e se ne determinino nucleo e immagine, precisandone la dimensione e una base.

(ii) Si considerino i sottospazi

$$W = \langle 2x_1 + x_3, x_2, 3x_3 \rangle, \quad U = \langle x_3 - x_1, 5x_4 \rangle$$

di  $V$ , e se ne precisi una base e la dimensione in funzione della caratteristica di  $F$ . Si determini il valore di  $\text{car } F$  per cui  $W$  e  $U$  sono supplementari.

(iii) Considerato lo spazio vettoriale canonico  $F^2$  su  $F$ , si dimostri che la posizione

$$\mu(\alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4 + U) = (\alpha + \gamma, \beta)$$

definisce un'applicazione  $\mu$  di  $V/U$  in  $F^2$ , che tale applicazione è un epimorfismo di spazi vettoriali, e di essa si descriva il nucleo.

**Esercizio 8.9.7.** Siano  $F$  un campo e si consideri l'usuale  $F$ -spazio vettoriale  $F^3$ . Con  $h \in F$  si considerino i vettori

$$\begin{aligned} v_1 &= (1, h+1, 5), \\ v_2 &= (4, 3, 0), \\ v_3 &= (5h, 10h-5, 5h) \end{aligned}$$

e il sottospazio  $W = \langle v_1, v_2, v_3 \rangle$  di  $F^3$ .

- (i) Si discuta la dimensione di  $W$  in funzione di  $h$  e della caratteristica di  $F$ .  
(ii) Sempre in funzione di  $h$  e della caratteristica di  $F$ , si precisi quando esiste un  $F$ -omomorfismo  $\phi$  di  $F^3$  in  $F$  tale che

$$\phi(v_1) = 0, \quad \phi(v_2) = 1, \quad \phi(v_3) = 1.$$

(iii) Supposto infine  $h = 2$  e posto  $U = \langle v_1, v_3 \rangle = \langle (1, 3, 5), (10, 15, 10) \rangle$ , si provi che la posizione

$$\psi((a, b, c) + U) = 9a - 8b + 3c$$

definisce un'applicazione  $\psi$  di  $F^3/U$  in  $F$  e che tale applicazione è un epimorfismo di  $F$ -spazi vettoriali. Si discuta poi quando  $\psi$  è iniettiva e, in tal caso, se ne determini l'inversa.

**Esercizio 8.9.8.** Siano  $F$  un campo e si consideri l'usuale  $F$ -spazio vettoriale  $F^4$ . Si considerino i vettori

$$\begin{aligned} v_1 &= (-2, 4, 0, 4), \\ v_2 &= (0, -2, 6, 6), \\ v_3 &= (1, -1, 2, 4) \end{aligned}$$

e il sottospazio  $W = \langle v_1, v_2, v_3 \rangle$  di  $F^4$ .

- (i) Si discuta la dimensione di  $W$  in funzione della caratteristica di  $F$ .  
(ii) Si determinino, sempre in funzione della caratteristica di  $F$ , un sottospazio  $V$  e un sottospazio  $L$  tali che:

$$F^4 = W \oplus V, \quad F^4 = W + L.$$

(iii) Posto  $U = \langle v_3 \rangle$ , si provi che la posizione

$$\psi((a, b, c, d) + U) = a + b + 2c - d$$

definisce un'applicazione  $\psi$  di  $F^4/U$  in  $F$  e che tale applicazione è lineare. Si determini infine  $\text{Ker } \psi$ .

**Esercizio 8.9.9.** Siano  $F$  un campo e si consideri l'usuale  $F$ -spazio vettoriale  $F^3$ . Si considerino i vettori

$$v_1 = (2, 6, 10),$$

$$v_2 = (3, 4, 5),$$

$$v_3 = (7, 8, 15)$$

e il sottospazio  $W = \langle v_1, v_2, v_3 \rangle$  di  $F^3$ .

- (i) In funzione della caratteristica di  $F$  si discuta la dimensione di  $W$  e se ne determinino, se esistono, due basi e due supplementari.
- (ii) Posto  $U = \langle v_3 \rangle$ , si provi che la posizione

$$\psi((a, b, c) + U) = a + b - c$$

definisce un'applicazione  $\psi$  di  $F^3/U$  in  $F$  e che tale applicazione è un epimorfismo di  $F$ -spazi vettoriali. Si precisi infine se  $\psi$  è iniettiva.

**Esercizio 8.9.10.** Sia  $F$  un campo e si consideri l'usuale spazio vettoriale  $F^4$ .

- (i) Si verifichi che l'applicazione

$$\varphi : (a, b, c, d) \in F^4 \longmapsto (a - 3c, 2b - 4d, 10a, 6b) \in F^4$$

è lineare.

- (ii) Si determinino, in funzione della caratteristica di  $F$ , il nucleo  $\text{Ker } \varphi$  e l'immagine  $\text{Im } \varphi$ , precisando di ciascuno la dimensione, due basi (se esistono), un supplementare.
- (iii) Si provi poi che la posizione

$$\psi((a, b, c, d) + \text{Ker } \varphi) = a - 2b - 3c + 4d$$

definisce un'applicazione di  $F^4/\text{Ker } \varphi$  in  $F$  e che tale applicazione è un epimorfismo di  $F$ -spazi vettoriali, precisando se esiste qualche valore della caratteristica di  $F$  per cui  $\psi$  risulti un isomorfismo.

**Esercizio 8.9.11.** Sia  $F$  un campo, e si consideri l'applicazione

$$\psi : \sum_{n \in \mathbb{N}_0} b_n x^n \in F[x] \longmapsto 6b_0 + 6b_1 x \in F[x].$$

- (i) Si dimostri che  $\psi$  è un endomorfismo dello spazio vettoriale  $F[x]$  su  $F$ , e si determinino  $\text{Ker } \psi$  e  $\text{Im } \psi$ , precisandone una base e la dimensione.
- (ii) Si verifichi che  $F[x] = \text{Ker } \psi \oplus \text{Im } \psi$ .

- (iii) Si determinino i valori della caratteristica di  $F$  per cui  $\psi$  è un endomorfismo dell'anello  $F[x]$ .
- (iv) Si verifichi che, in ogni caso,  $\text{Ker } \psi$  è un ideale dell'anello  $F[x]$ , e se ne determini un generatore.
- (v) Supposto  $\psi \neq 0$ , si osservi che  $\text{Im } \psi$  non è un sottoanello dell'anello  $F[x]$ , e si determini l'ideale di  $F[x]$  generato da  $\text{Im } \psi$ .
- (vi) Si provi che la posizione

$$\mu \left( \sum_{n \in \mathbb{N}_0} b_n x^n + \text{Ker } \psi \right) = b_1$$

definisce un'applicazione  $\mu$  di  $F[x]/\text{Ker } \psi$  in  $F$ , e che  $\mu$  è suriettiva ma non iniettiva.

**Esercizio 8.9.12.** Sia  $F$  un campo e si consideri l'usuale  $F$ -spazio vettoriale  $F^4$ .

- (i) Si verifichi che l'applicazione

$$\psi : (a, b, c, d) \in F^4 \longmapsto (2a - b, a + 7b, c + d, 7c + 2d) \in F^4$$

è un  $F$ -endomorfismo dello spazio vettoriale  $F^4$  e si determinino, in funzione della caratteristica di  $F$ , il nucleo  $\text{Ker } \psi$  e l'immagine  $\text{Im } \psi$ , precisando la dimensione e una base.

- (ii) Con  $F = \mathbb{Z}_5$ , si determinino un supplementare di  $\text{Ker } \psi$  e uno di  $\text{Im } \psi$ , precisando se ne esiste uno comune, e se  $\text{Ker } \psi$  e  $\text{Im } \psi$  sono tra loro supplementari.
- (iii) Con  $F = \mathbb{Z}_3$ , si verifichi che la posizione

$$\varphi((a, b, c, d) + \text{Ker } \psi) = (a + b, c, 2d)$$

definisce un'applicazione  $\varphi$  di  $F^4/\text{Ker } \psi$  in  $F^3$ , e che tale applicazione è un isomorfismo di  $F$ -spazi vettoriali.

**Esercizio 8.9.13.** Sia  $F$  un campo e si consideri l'insieme  $F^2$  strutturato ad anello e a  $F$ -spazio vettoriale nel modo usuale. Sia

$$\varphi : (a, b) \in F^2 \longmapsto a^3 + b^3 \in F.$$

- (i) Si provi che  $\varphi$  è un omomorfismo di  $(F^2, +)$  in  $(F, +)$  se e solo se  $F$  ha caratteristica 3 oppure  $|F| = 2$ .
- (ii) Si dimostri che  $\varphi$  è un'applicazione lineare se e solo se  $|F| = 2$  o  $|F| = 3$ . Distinguendo allora i casi  $F = \mathbb{Z}_2$  e  $F = \mathbb{Z}_3$ , si determinino  $\text{Ker } \varphi$  e tutti i suoi supplementari.
- (iii) Si provi che  $\varphi$  non è mai un omomorfismo di  $(F^2, \cdot)$  in  $(F, \cdot)$ .

**Esercizio 8.9.14.** Sia  $F$  un campo e si consideri l'insieme  $F^2$  strutturato ad anello e a  $F$ -spazio vettoriale nel modo usuale. Si provi che l'applicazione

$$\varphi : (a, b) \in F^2 \longmapsto 2a + 3b \in F$$

è un epimorfismo di  $F$ -spazi vettoriali, e che il sottospazio  $D = \{(c, c) : c \in F\}$  è un supplementare di  $\text{Ker } \varphi$  se e solo se  $\text{car } F \neq 5$ . Si dimostri poi che  $\varphi$  è un omomorfismo di anelli se e solo se  $\text{car } F = 2$ .

**Esercizio 8.9.15.** Sia  $F$  un campo e si consideri l'usuale  $F$ -spazio vettoriale  $F^3$ . Siano  $V$  e  $W$  i sottospazi di dimensione 1 di  $F^3$  generati da  $\{(0, 1, 2)\}$  e da  $\{(2, 0, 1)\}$  rispettivamente. Distinguendo i casi  $F = \mathbb{R}$  e  $F = \mathbb{Z}_3$ :

- (i) si descrivano  $V$  e  $W$  e si precisi se l'elemento  $(2, 1, 0)$  appartiene a  $V + W$ ;
- (ii) posto

$$f : (a, b, c) + V \in F^3/V \longmapsto (a, 2b - c, a) \in F^3,$$

si stabilisca se  $f$  è ben posta, se è iniettiva o suriettiva, e se è un omomorfismo di spazi vettoriali.

**Esercizio 8.9.16.** Si consideri l'usuale spazio vettoriale  $\mathbb{R}^4$  sul campo  $\mathbb{R}$  dei numeri reali e si ponga

$$W = \{(a, b, c, d) : a, b, c, d \in \mathbb{R}, a + b = 0, a - b + c = 0\}.$$

- (i) Si provi che  $W$  è un sottospazio di  $\mathbb{R}^4$  e se ne determini una base.
- (ii) Si provi che ponendo

$$\varphi : (a, b, c, d) + W \in \mathbb{R}^4/W \longmapsto (2a + c, a + b) \in \mathbb{R}^2$$

si definisce un'applicazione di  $\mathbb{R}^4/W$  in  $\mathbb{R}^2$ , e si stabilisca se  $\varphi$  è iniettiva o suriettiva e se è un omomorfismo di spazi vettoriali.

- (iii) Si determinino la dimensione e una base di  $\mathbb{R}^4/W$ .

**Esercizio 8.9.17.** Sia  $K$  un campo. Si considerino  $K[x]$  e  $M_2(K)$ , muniti delle consuete strutture di  $K$ -spazio vettoriale, e l'applicazione

$$\varphi : \sum_{n \in \mathbb{N}_0} a_n x^n \in K[x] \longmapsto \begin{pmatrix} a_1 & 2a_5 \\ a_2 - a_3 & 8a_4 \end{pmatrix} \in M_2(K).$$

- (i) Si verifichi che  $\varphi$  è un omomorfismo di spazi vettoriali.
- (ii) Nei casi  $K = \mathbb{Q}$  e  $K = \mathbb{Z}_2$ , si determinino il nucleo  $\text{Ker } \varphi$  e l'immagine  $\text{Im } \varphi$  di  $\varphi$ , si precisino le dimensioni di  $\text{Ker } \varphi$  e di  $\text{Im } \varphi$  e si individuino una base di  $\text{Ker } \varphi$  e una base di  $\text{Im } \varphi$ .
- (iii) Nei casi  $K = \mathbb{Q}$  e  $K = \mathbb{Z}_2$ , si stabilisca se  $\text{Ker } \varphi$  è un sottoanello dell'anello  $(K[x], +, \cdot)$  e se ne è un ideale.

**Esercizio 8.9.18.** Sia  $k$  un fissato numero reale e sia  $f_k : \mathbb{R}^4 \longrightarrow \mathbb{R}^3$  l'applicazione dell' $\mathbb{R}$ -spazio vettoriale  $\mathbb{R}^4$  nell'  $\mathbb{R}$ -spazio vettoriale  $\mathbb{R}^3$  definita da

$$f_k(x, y, z, t) := (x, z - 3t, t + y + (k - 5)).$$

- (i) Dopo aver individuato il valore  $\bar{k}$  di  $k$  per il quale  $f_{\bar{k}}$  è un  $\mathbb{R}$ -omomorfismo, si determinino il nucleo e l'immagine di  $f_{\bar{k}}$  e di tali sottospazi si individui una base e la dimensione.
- (ii) Si stabilisca se  $f_{\bar{k}}$  è un  $\mathbb{R}$ -monomorfismo e se è un  $\mathbb{R}$ -epimorfismo.
- (iii) Infine, indicato con  $V$  il sottospazio di  $\mathbb{R}^4$  generato da

$$\{(0, 0, 2, 2), (0, 1, 2, -3), (0, 0, 0, 1)\},$$

si provi che il nucleo  $\text{Ker } f_{\bar{k}}$  è contenuto in  $V$  e si determini lo spazio quoziante  $V / \text{Ker } f_{\bar{k}}$ .

**Esercizio 8.9.19.** Siano  $V$  uno spazio vettoriale sul campo  $\mathbb{R}$  dei numeri reali ed  $f : V \longrightarrow V$  un endomorfismo di spazi vettoriali tale che  $f^2 = 1$ .

- (i) Si provi che  $f$  è biettiva;
- (ii) Posto

$$W = \{w \in V : f(w) = w\}, \quad U = \{u \in V : f(u) = -u\},$$

si verifichi che  $U$  e  $W$  sono sottospazi di  $V$ .

- (iii) Si provi che  $V = W \oplus U$ .
- (iv) Si dimostri che  $v - f(v) \in U$ , per ogni  $v \in V$ , e che, posto

$$g : v + W \in V/W \longmapsto v - f(v) \in U,$$

$g$  è un'applicazione. Si provi infine che  $g$  è un isomorfismo tra gli spazi vettoriali  $V/W$  e  $U$ .

**Esercizio 8.9.20.** Si consideri  $\mathbb{R}^3$ , strutturato in modo naturale come  $\mathbb{R}$ -spazio vettoriale.

- (i) Si stabilisca se le parti

$$H = \{(a, b, c) : a + b - 3c = 0\}, \quad K = \{(a, b, c) : a - b + c = 1\}$$

sono sottospazi di  $\mathbb{R}^3$  ed, in tal caso, se ne determinino la dimensione ed una base.

- (ii) Si descrivano gli elementi del sottospazio  $V$  generato da  $(1, 1, 0)$ .
- (iii) Con  $\lambda \in \mathbb{R}$ , posto

$$f_\lambda : (a, b, c) + V \in \mathbb{R}^3/V \longmapsto (a - \lambda^2 b + \lambda c, c) \in \mathbb{R}^2,$$

si stabilisca per quali valori di  $\lambda$  l'applicazione  $f_\lambda$  è ben posta, per quali  $f_\lambda$  è un  $\mathbb{R}$ -omomorfismo, per quali è un  $\mathbb{R}$ -monomorfismo, per quali è un  $\mathbb{R}$ -isomorfismo.

## Elementi di geometria analitica

In questo capitolo verranno presentati alcuni dei concetti fondamentali della geometria analitica nel piano e nello spazio. La trattazione è volutamente di carattere molto intuitivo, talvolta anche a discapito della rigorosità. Inoltre il Lettore è tenuto senz'altro in possesso delle conoscenze elementari di geometria euclidea fornite abitualmente dalle scuole medie superiori, che nel seguito verranno utilizzate spesso senza ulteriori riferimenti. Durante l'intero capitolo, diversamente da quanto fatto finora, si adopererà per i vettori la notazione con la sottolineatura.

### 9.1 Riferimenti affini nel piano e nello spazio

Sia  $\pi$  un piano euclideo e si denoti con  $\mathcal{E}^2$  l'insieme dei suoi punti; fissato un punto  $O \in \mathcal{E}^2$ , si definisce **vettore applicato** in  $O$  ogni segmento orientato  $\overrightarrow{OA}$  avente come primo estremo il punto  $O$  e come secondo estremo un altro punto  $A \in \mathcal{E}^2$ :

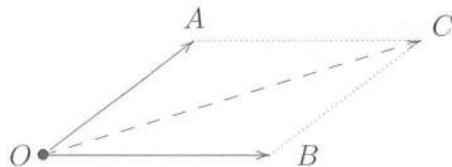


L'insieme dei vettori di  $\pi$  applicati in  $O$  si denota con  $\mathcal{V}_O^2$ , si pone cioè

$$\mathcal{V}_O^2 := \left\{ \overrightarrow{OA} : A \in \mathcal{E}^2 \right\}.$$

Come si vedrà, tale insieme può essere dotato di struttura di spazio vettoriale sul campo  $\mathbb{R}$  dei numeri reali. Vettori  $\overrightarrow{OA}$  e  $\overrightarrow{O'B}$ , applicati in  $O$  e in  $O'$  rispettivamente, si dicono **congruenti** se i segmenti  $\overline{OA}$  e  $\overline{O'B}$  hanno la stessa lunghezza. Nel seguito la lunghezza di un segmento  $\overline{OA}$  sarà spesso indicata con il simbolo  $|OA|$ . Considerati ora  $\overrightarrow{OA}, \overrightarrow{OB} \in \mathcal{V}_O^2$ , si pone  $\overrightarrow{OA} + \overrightarrow{OB} := \overrightarrow{OC}$  dove  $C$  è il quarto vertice del parallelogramma individuato dai punti  $O, A$  e  $B$ , ovvero il secondo estremo del vettore applicato in  $A$  parallelo, congruente e con lo stesso

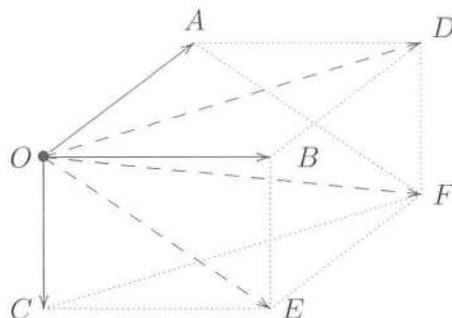
verso del vettore  $\overrightarrow{OB}$ :



Questa posizione definisce un'operazione interna in  $\mathcal{V}_O^2$  e si ha che:

**9.1.1.** *La struttura algebrica  $(\mathcal{V}_O^2, +)$  è un gruppo abeliano.*

*Dimostrazione.* Per dimostrare che l'addizione è associativa occorre distinguere vari casi. Per esempio nel caso in cui i punti  $O, A, B, C$  sono a tre a tre non allineati, si considerano  $\overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC} \in \mathcal{V}_O^2$  e si pone  $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OD}$  e  $\overrightarrow{OB} + \overrightarrow{OC} = \overrightarrow{OE}$ :



Occorre dimostrare che  $\overrightarrow{OD} + \overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OE}$  e a tale scopo, posto

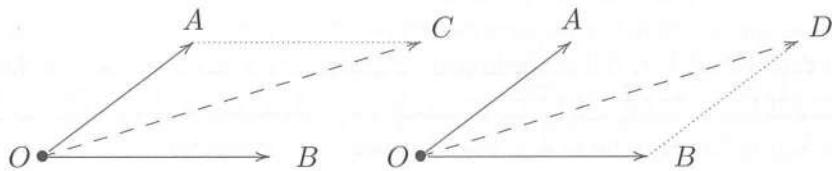
$$\overrightarrow{OD} + \overrightarrow{OC} = \overrightarrow{OF},$$

basterà osservare che  $OAFE$  è un parallelogramma e quindi per esempio che  $|OA| = |EF|$  e  $|AF| = |OE|$ . Si considerino i triangoli  $OBD$  e  $CFE$ ; tali triangoli sono uguali perché hanno ordinatamente uguali due lati ( $|CE| = |OB|$  e  $|CF| = |OD|$ ) e l'angolo compreso ( $\widehat{FC}E = \widehat{D}OB$  perché sono parallele le rette  $OD$  e  $CF$  e le rette  $OB$  e  $CE$ ), quindi  $|EF| = |BD| = |OA|$ . Analogamente si prova l'uguaglianza dei triangoli  $ADF$  e  $OBE$  da cui segue che  $|AF| = |OE|$ .

Analoghe argomentazioni provano l'asserto anche negli altri casi (vedi Esercizio 9.1.1).

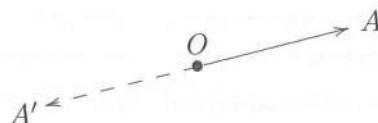
Per provare che l'addizione è commutativa è sufficiente osservare che dati  $\overrightarrow{OA}, \overrightarrow{OB} \in \mathcal{V}_O^2$  il secondo estremo  $C$  del vettore applicato in  $A$  parallelo, congruente e con lo stesso verso di  $\overrightarrow{OB}$  coincide con il secondo estremo  $D$  del vettore

applicato in  $B$  parallelo, congruente e con lo stesso verso di  $\overrightarrow{OA}$ :



Pertanto  $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OC} = \overrightarrow{OD} = \overrightarrow{OB} + \overrightarrow{OA}$ .

È immediato osservare che il vettore  $\overrightarrow{OO}$  (vettore nullo) è elemento neutro rispetto all'addizione ed è altrettanto facile osservare che per ogni  $\overrightarrow{OA} \in \mathcal{V}_O^2$  l'opposto  $-\overrightarrow{OA}$ , cioè il simmetrico di  $\overrightarrow{OA}$  rispetto all'addizione, è il vettore applicato in  $O$  parallelo, congruente e avente verso opposto rispetto a  $\overrightarrow{OA}$ , ovvero il vettore applicato in  $O$  il cui secondo estremo  $A'$  è il simmetrico di  $A$  rispetto a  $O$ :

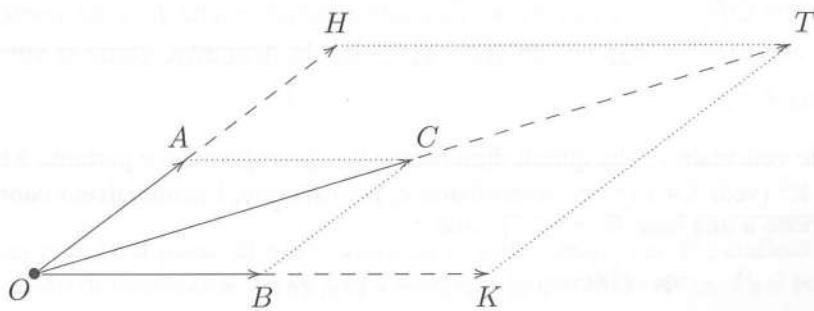


□

Per ogni  $t \in \mathbb{R}$  e per ogni vettore applicato  $\overrightarrow{OA} \in \mathcal{V}_O^2$ , si pone  $t\overrightarrow{OA} := \overrightarrow{OC}$ , dove  $C$  è il punto della retta  $OA$  tale che il rapporto tra le lunghezze  $|OC|$  e  $|OA|$  dei segmenti  $\overline{OC}$  e  $\overline{OA}$  sia il valore assoluto  $|t|$  di  $t$ , e che si trova sulla semiretta orientata  $OA$  se  $t > 0$ , su quella opposta se  $t < 0$ . In questo modo si definisce un'operazione esterna in  $\mathcal{V}_O^2$  con dominio di operatori il campo  $\mathbb{R}$  dei numeri reali, e si può verificare che:

### 9.1.2. La struttura algebrica $(\mathcal{V}_O^2, +, \cdot)$ è uno spazio vettoriale su $\mathbb{R}$ .

*Dimostrazione.* Per provare per esempio che per ogni  $\overrightarrow{OA}, \overrightarrow{OB} \in \mathcal{V}_O^2$  e per ogni  $\lambda \in \mathbb{R}$  con  $\lambda \geq 0$  riesce  $\lambda(\overrightarrow{OA} + \overrightarrow{OB}) = \lambda\overrightarrow{OA} + \lambda\overrightarrow{OB}$ , si ponga  $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OC}$ ,  $\lambda\overrightarrow{OA} = \overrightarrow{OH}$ ,  $\lambda\overrightarrow{OB} = \overrightarrow{OK}$  e  $\overrightarrow{OH} + \overrightarrow{OK} = \overrightarrow{OT}$ .



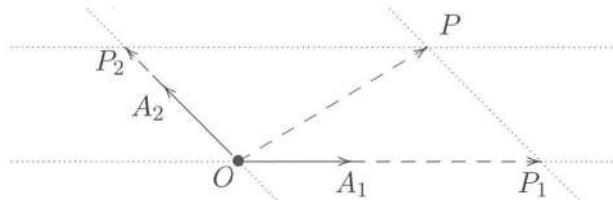
È immediato osservare che i triangoli  $OAC$  e  $OHT$  sono simili perché hanno due lati proporzionali (precisamente  $|\lambda||OA| = |OH|$ ,  $|\lambda||AC| = |HT|$ ) e uguale l'angolo compreso. Questo comporta che  $|OT| = |\lambda||OC|$ , da cui  $\overrightarrow{OT} = \lambda \overrightarrow{OC}$ .

Nel caso in cui  $\lambda < 0$  il procedimento è analogo. La facile verifica del fatto che  $(\lambda + \mu)\overrightarrow{OA} = \lambda \overrightarrow{OA} + \mu \overrightarrow{OA}$ , che  $(\lambda\mu)\overrightarrow{OA} = \lambda(\mu \overrightarrow{OA})$  e che  $1\overrightarrow{OA} = \overrightarrow{OA}$  per ogni  $\lambda, \mu \in \mathbb{R}$  e per ogni  $\overrightarrow{OA} \in \mathcal{V}_O^2$  è lasciata come esercizio.  $\square$

### 9.1.3. Lo spazio vettoriale $(\mathcal{V}_O^2, +, \cdot)$ ha dimensione 2.

*Dimostrazione.* Per provare l'asserto basta osservare che se  $\underline{i} = \overrightarrow{OA_1}$  e  $\underline{j} = \overrightarrow{OA_2}$  sono vettori di  $\mathcal{V}_O^2$  non appartenenti a una stessa retta, allora  $\{\underline{i}, \underline{j}\}$  è una base di  $\mathcal{V}_O^2$ .

A tale scopo si noti che dalla definizione dell'operazione esterna segue immediatamente che se  $\underline{i} = \overrightarrow{OA_1}$  è un vettore non nullo di  $\mathcal{V}_O^2$  allora, detta  $r_1$  la retta  $OA_1$ , i vettori di  $\mathcal{V}_O^2$  appartenenti a  $r_1$ , ovvero i vettori applicati in  $O$  il cui secondo estremo sia un punto di  $r_1$ , sono tutti e soli i vettori del tipo  $\lambda \overrightarrow{OA_1}$  con  $\lambda \in \mathbb{R}$ . Ciò comporta che richiedere che  $\underline{i}$  e  $\underline{j}$  non appartengano alla stessa retta equivale a richiedere che  $\underline{i}$  e  $\underline{j}$  non siano proporzionali, ovvero che siano linearmente indipendenti. Dunque, per dimostrare che  $\{\underline{i}, \underline{j}\}$  è una base di  $\mathcal{V}_O^2$  occorre e basta provare che per ogni  $\overrightarrow{OP} \in \mathcal{V}_O^2$  esistono  $x_1, x_2 \in \mathbb{R}$  tali che  $\overrightarrow{OP} = x_1\underline{i} + x_2\underline{j}$  ossia che  $\{\underline{i}, \underline{j}\}$  è un sistema di generatori di  $\mathcal{V}_O^2$ . Sia dunque  $\overrightarrow{OP} \in \mathcal{V}_O^2$ , e siano  $r_1$  la retta  $OA_1$  e  $r_2$  la retta  $OA_2$ .



Indicati con  $P_1$  e  $P_2$  i punti di intersezione di  $r_1$  con la retta per  $P$  parallela a  $r_2$  e di  $r_2$  con la retta per  $P$  parallela a  $r_1$  rispettivamente, si ha che  $OP_1PP_2$  è un parallelogramma e quindi  $\overrightarrow{OP} = \overrightarrow{OP_1} + \overrightarrow{OP_2}$ . Poiché  $P_1$  è un punto di  $r_1$  si ha che  $\overrightarrow{OP_1} = x_1\underline{i}$  con  $x_1 \in \mathbb{R}$ ; analogamente poiché  $P_2$  è un punto di  $r_2$  si ha che  $\overrightarrow{OP_2} = x_2\underline{j}$  per un certo  $x_2 \in \mathbb{R}$ . In definitiva, come si voleva,  $\overrightarrow{OP} = x_1\underline{i} + x_2\underline{j}$ .  $\square$

Lo spazio vettoriale  $\mathcal{V}_O^2$  ha quindi dimensione 2 sul campo reale e pertanto è isomorfo a  $\mathbb{R}^2$  (vedi 8.4.11); un isomorfismo è, per esempio, l'**isomorfismo coordinato** rispetto a una base  $B = \{\underline{i}, \underline{j}\}$ , cioè

$$\Phi : \overrightarrow{OP} = x_1\underline{i} + x_2\underline{j} \longmapsto (x_1, x_2) \in \mathbb{R}^2.$$

La terna costituita da un punto  $O \in \mathcal{E}^2$  e da due vettori  $\underline{i} = \overrightarrow{OA_1}$ ,  $\underline{j} = \overrightarrow{OA_2}$  non proporzionali applicati in  $O$  (ovvero linearmente indipendenti e cioè non appartenenti alla stessa retta) è detta **riferimento affine del piano** e si denota con  $\mathcal{RA}(O, \underline{i}, \underline{j})$  o anche con  $\mathcal{RA}(O, A_1, A_2)$ . Il punto  $O$  è detto **origine** del riferimento affine; le rette  $OA_1$  e  $OA_2$ , generate rispettivamente dai vettori  $\underline{i}$  e  $\underline{j}$ , sono dette gli **assi** del riferimento. Se  $P$  è un punto del piano allora le sue **coordinate cartesiane** rispetto al riferimento affine considerato sono le componenti  $(x_1, x_2)$  di  $\overrightarrow{OP}$  rispetto alla base  $B = \{\underline{i}, \underline{j}\}$ .

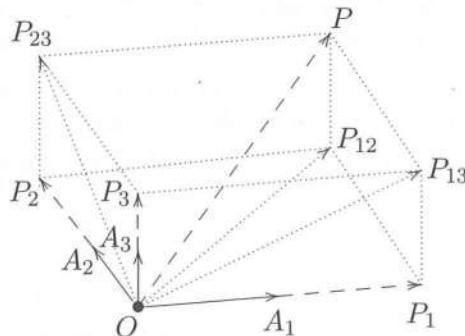
Analogamente a quanto fatto per  $(\mathcal{V}_O^2, +, \cdot)$ , si può introdurre l'insieme  $\mathcal{V}_O^3$  costituito dai vettori applicati in un punto  $O$  dello spazio euclideo  $\mathcal{E}^3$ . E si prova agevolmente (vedi anche Esercizio 9.1.3) che  $(\mathcal{V}_O^3, +, \cdot)$  è uno spazio vettoriale.

#### 9.1.4. Lo spazio vettoriale $(\mathcal{V}_O^3, +, \cdot)$ ha dimensione 3.

*Dimostrazione.* Siano  $\underline{i} = \overrightarrow{OA_1}$ ,  $\underline{j} = \overrightarrow{OA_2}$ ,  $\underline{k} = \overrightarrow{OA_3}$  tre vettori non complanari di  $\mathcal{V}_O^3$ . Si noti che il sottospazio generato da due vettori  $\overrightarrow{OA_h}$  e  $\overrightarrow{OA_k}$ , non appartenenti a una stessa retta, è costituito da tutti e soli i vettori applicati in  $O$  che appartengono al piano individuato dai punti  $O, A_h, A_k$ . Quindi richiedere che  $\underline{i}$ ,  $\underline{j}$ ,  $\underline{k}$  non siano complanari equivale a richiedere che nessuno dei tre vettori appartenga al sottospazio generato dagli altri due, e cioè che nessuno dei tre dipenda linearmente dai rimanenti, ovvero che  $B = \{\underline{i}, \underline{j}, \underline{k}\}$  sia un insieme linearmente indipendente (vedi 8.3.7).

Si proverà che  $B$  è una base di  $\mathcal{V}_O^3$  e a tale scopo occorre e basta dimostrare che  $B$  è un sistema di generatori di  $\mathcal{V}_O^3$  e quindi che per ogni  $\overrightarrow{OP} \in \mathcal{V}_O^3$  esistono  $x_1, x_2, x_3 \in \mathbb{R}$  tali che  $\overrightarrow{OP} = x_1\underline{i} + x_2\underline{j} + x_3\underline{k}$ .

Siano  $r_1, r_2, r_3$  le rette  $OA_1, OA_2, OA_3$  rispettivamente; siano poi  $\pi_{12}$  il piano individuato da  $r_1$  e  $r_2$  (cioè generato da  $\underline{i}$  e  $\underline{j}$ ),  $\pi_{23}$  quello individuato da  $r_2$  e  $r_3$ , e  $\pi_{13}$  quello determinato da  $r_1$  e  $r_3$ .



Indicati con  $P_1$  il punto di intersezione di  $r_1$  con il piano per  $P$  parallelo a  $\pi_{23}$ ,  $P_2$  il punto di intersezione di  $r_2$  con il piano per  $P$  parallelo a  $\pi_{13}$ ,  $P_3$  il punto di

intersezione di  $r_3$  con il piano per  $P$  parallelo a  $\pi_{12}$ , si ha che

$$\overrightarrow{OP} = \overrightarrow{OP_1} + \overrightarrow{OP_2} + \overrightarrow{OP_3}.$$

Infatti se  $P_{12}$  è il punto di intersezione di  $\pi_{12}$  con la retta per  $P$  parallela a  $r_3$ , allora  $\overrightarrow{OP_{12}} = \overrightarrow{OP_1} + \overrightarrow{OP_2}$  e poiché  $\overrightarrow{OP} = \overrightarrow{OP_{12}} + \overrightarrow{OP_3}$ , si ha l'asserto. Ora, siccome  $P_1 \in r_1$ ,  $P_2 \in r_2$  e  $P_3 \in r_3$ , esistono  $x_1, x_2, x_3 \in \mathbb{R}$  tali che  $\overrightarrow{OP_1} = x_1\underline{i}$ ,  $\overrightarrow{OP_2} = x_2\underline{j}$  e  $\overrightarrow{OP_3} = x_3\underline{k}$ . Pertanto  $\overrightarrow{OP} = x_1\underline{i} + x_2\underline{j} + x_3\underline{k}$  come volevasi.  $\square$

Lo spazio vettoriale  $\mathcal{V}_O^3$ , avendo dimensione 3 su  $\mathbb{R}$ , è isomorfo a  $\mathbb{R}^3$  (vedi 8.4.11); un isomorfismo è quello coordinato (rispetto a una base  $B = \{\underline{i}, \underline{j}, \underline{k}\}$ ):

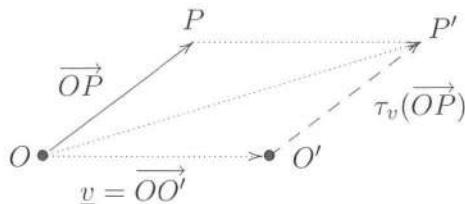
$$\Phi : \overrightarrow{OP} = x_1\underline{i} + x_2\underline{j} + x_3\underline{k} \longmapsto (x_1, x_2, x_3) \in \mathbb{R}^3.$$

La quaterna  $(O, \underline{i}, \underline{j}, \underline{k})$ , che si denota con  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  (oppure, posto  $\underline{i} = \overrightarrow{OA_1}$ ,  $\underline{j} = \overrightarrow{OA_2}$  e  $\underline{k} = \overrightarrow{OA_3}$ , con  $\mathcal{RA}(O, A_1, A_2, A_3)$ ) è detta **riferimento affine** di  $\mathcal{E}^3$ . Il punto  $O$  è detto **origine** del riferimento affine; le rette  $OA_1$ ,  $OA_2$  e  $OA_3$ , generate rispettivamente dai vettori  $\underline{i}$ ,  $\underline{j}$  e  $\underline{k}$ , sono dette gli **assi** del riferimento. Le **coordinate cartesiane** di un punto  $P \in \mathcal{E}^3$  in tale riferimento sono le componenti di  $\overrightarrow{OP}$  nella base  $B = \{\underline{i}, \underline{j}, \underline{k}\}$ .

## Traslazioni

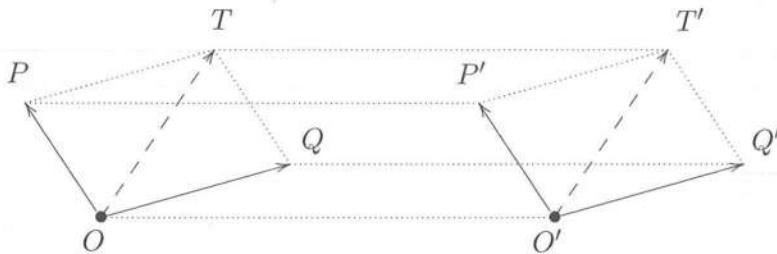
Nel costruire lo spazio vettoriale  $\mathcal{V}_O^2$  (rispettivamente  $\mathcal{V}_O^3$ ) è stato privilegiato un punto  $O$  di  $\mathcal{E}^2$  (risp. di  $\mathcal{E}^3$ ). Fissando un diverso punto  $O'$ , si ottiene lo spazio vettoriale  $\mathcal{V}_{O'}^2$  (risp.  $\mathcal{V}_{O'}^3$ ) che è diverso da  $\mathcal{V}_O^2$  (risp.  $\mathcal{V}_O^3$ ), ma isomorfo a tale spazio vettoriale perché ancora spazio vettoriale di dimensione 2 (risp. 3) sul campo  $\mathbb{R}$  dei numeri reali (vedi 8.4.11).

Sia  $\mathcal{V}_O$  lo spazio  $\mathcal{V}_O^2$  oppure  $\mathcal{V}_O^3$  e sia  $\mathcal{V}_{O'}$  lo spazio che si ottiene scegliendo un diverso punto  $O'$  di  $\mathcal{E}^2$  nel primo caso e di  $\mathcal{E}^3$  nel secondo. Denotato con  $\underline{v}$  il vettore  $\overrightarrow{OO'} \in \mathcal{V}_O$ , si definisce **traslazione** relativa al vettore  $\underline{v} = \overrightarrow{OO'}$  l'applicazione  $\tau_v : \mathcal{V}_O \longrightarrow \mathcal{V}_{O'}$  che a ogni vettore  $\overrightarrow{OP}$  applicato in  $O$  associa il vettore  $\overrightarrow{O'P'}$  applicato in  $O'$  parallelo e concorde a  $\overrightarrow{OP}$ , e tale che i segmenti  $\overrightarrow{OP}$  e  $\overrightarrow{O'P'}$  siano congruenti. In altre parole  $\tau_v$  è l'applicazione definita ponendo, per ogni  $\overrightarrow{OP} \in \mathcal{V}_O$ ,  $\tau_v(\overrightarrow{OP}) := \overrightarrow{O'P'}$  dove  $P'$  è quell'unico punto tale che  $\overrightarrow{OP'} = \overrightarrow{OP} + \overrightarrow{OO'}$ :



**9.1.5.** Siano  $O$  e  $O'$  punti del piano (rispettivamente dello spazio). La traslazione  $\tau_v$  relativa al vettore  $\underline{v} = \overrightarrow{OO'}$  è un isomorfismo dello spazio vettoriale  $\mathcal{V}_O$  nello spazio vettoriale  $\mathcal{V}_{O'}$ .

*Dimostrazione.* Per provare che  $\tau_v$  è un omomorfismo si considerino  $\overrightarrow{OP}$  e  $\overrightarrow{OQ}$  in  $\mathcal{V}_O$ , e si ponga  $\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{OT}$ ,  $\tau_v(\overrightarrow{OP}) = \overrightarrow{O'P'}$ ,  $\tau_v(\overrightarrow{OQ}) = \overrightarrow{O'Q'}$  e  $\tau_v(\overrightarrow{OT}) = \overrightarrow{O'T'}$ :



Per definizione di traslazione si ha che i vettori  $\overrightarrow{O'P'}, \overrightarrow{O'Q'}, \overrightarrow{O'T'}$  rispettivamente sono paralleli e concordi a  $\overrightarrow{OP}, \overrightarrow{OQ}, \overrightarrow{OT}$ , e inoltre i segmenti  $\overrightarrow{OP}, \overrightarrow{OQ}$  e  $\overrightarrow{OT}$  sono rispettivamente congruenti a  $\overrightarrow{O'P'}, \overrightarrow{O'Q'}$  e  $\overrightarrow{O'T'}$ . Da ciò segue che i triangoli  $OQT$  e  $O'Q'T'$  sono congruenti (perché hanno congruenti due lati omologhi e l'angolo tra essi compreso), e questo comporta che  $\overrightarrow{O'P'} + \overrightarrow{O'Q'} = \overrightarrow{O'T'}$ . Ne segue che  $\tau_v(\overrightarrow{OP} + \overrightarrow{OQ}) = \tau_v(\overrightarrow{OP}) + \tau_v(\overrightarrow{OQ})$ .

Per quanto poi riguarda la legge esterna è un facile esercizio verificare che  $\tau_v(\lambda \overrightarrow{OP}) = \lambda \tau_v(\overrightarrow{OP})$  per ogni  $\lambda \in \mathbb{R}$  e per ogni  $\overrightarrow{OP} \in \mathcal{V}_O$  (vedi (i) di Esercizio 9.1.4).

Resta infine da provare che  $\tau_v$  è biettiva. A tale scopo basta osservare che la traslazione  $\tau_{v'}$  relativa al vettore  $\underline{v}' = \overrightarrow{O'O}$  è un omomorfismo di dominio  $\mathcal{V}_{O'}$  e codominio  $\mathcal{V}_O$ , che risulta l'inversa di  $\tau_v$  (vedi (ii) di Esercizio 9.1.4).  $\square$

## Esercizi

**Esercizio 9.1.1.** Si completi la dimostrazione di 9.1.1, provando che, considerati i vettori  $\overrightarrow{OA}, \overrightarrow{OB}$  e  $\overrightarrow{OC} \in \mathcal{V}_O^2$ , riesce  $(\overrightarrow{OA} + \overrightarrow{OB}) + \overrightarrow{OC} = \overrightarrow{OA} + (\overrightarrow{OB} + \overrightarrow{OC})$  nei seguenti casi:

- (i)  $O, A, B$  sono tre punti del piano appartenenti a una stessa retta  $r$  e  $C$  è un punto non appartenente a  $r$ ;
- (ii)  $O, A, B, C$  sono quattro punti allineati del piano.

**Esercizio 9.1.2.** Si completi la dimostrazione di 9.1.2, provando che fissato un punto  $O$  del piano, per ogni  $\lambda, \mu \in \mathbb{R}$  e per ogni  $\overrightarrow{OA} \in \mathcal{V}_O^2$  riesce  $(\lambda + \mu)\overrightarrow{OA} = \lambda\overrightarrow{OA} + \mu\overrightarrow{OA}$ ,  $(\lambda\mu)\overrightarrow{OA} = \lambda(\mu\overrightarrow{OA})$  e  $1\overrightarrow{OA} = \overrightarrow{OA}$ .

**Esercizio 9.1.3.** Si dimostri che  $(\mathcal{V}_O^3, +, \cdot)$  è uno spazio vettoriale su  $\mathbb{R}$ .

**Esercizio 9.1.4.** Si completi la dimostrazione di 9.1.5, verificando che:

- (i) indicata con  $\tau_v$  la traslazione relativa al vettore  $\underline{v} = \overrightarrow{OO'} \in \mathcal{V}_O$ , si ha che  $\tau_v(\lambda \overrightarrow{OP}) = \lambda \tau_v(\overrightarrow{OP})$  per ogni  $\lambda \in \mathbb{R}$  e per ogni  $\overrightarrow{OP} \in \mathcal{V}_O$ ;
- (ii) indicate con  $\tau_v$  e  $\tau_{v'}$  le traslazioni relative ai vettori  $\underline{v} = \overrightarrow{OO'} = \overrightarrow{O'P}$  e  $\underline{v}' = \overrightarrow{O'P}$  rispettivamente, risulta  $\tau_{v'} = \tau_v^{-1}$ .

## 9.2 Equazioni vettoriali di rette e piani

I vettori di una retta  $r$  passante per un punto  $O$  del piano o dello spazio costituiscono un sottospazio di  $\mathcal{V}_O$  di dimensione 1, che ha pertanto come base il singleton di un qualsiasi vettore non nullo  $\overrightarrow{OP_1}$  con  $P_1 \in r$ . Questo comporta che un punto  $P$  appartiene alla retta  $r$  se e solo se  $\overrightarrow{OP} \in \langle \overrightarrow{OP_1} \rangle$ , cioè se e solo se esiste uno scalare  $t \in \mathbb{R}$  tale che

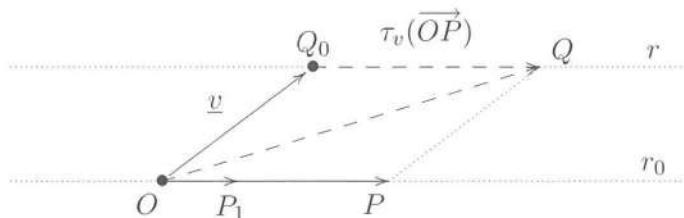
$$\overrightarrow{OP} = t \overrightarrow{OP_1}. \quad (9.2.1)$$

Analogamente, i vettori di un piano  $\pi$  per  $O$  costituiscono un sottospazio di  $\mathcal{V}_O$  di dimensione 2, che ha quindi una base costituita da due vettori  $\overrightarrow{OP_1}$  e  $\overrightarrow{OP_2}$  linearmente indipendenti, e cioè che non appartengono a una stessa retta. Da ciò segue che un punto  $P$  appartiene al piano  $\pi$  se e solo se esistono  $\alpha, \beta \in \mathbb{R}$  tali che

$$\overrightarrow{OP} = \alpha \overrightarrow{OP_1} + \beta \overrightarrow{OP_2}. \quad (9.2.2)$$

Le (9.2.1) e (9.2.2) forniscono rispettivamente l'**equazione vettoriale** di una retta e di un piano per  $O$ .

Per determinare le analoghe equazioni di rette e piani non passanti per  $O$  si utilizzano le traslazioni. Sia  $r$  una retta qualsiasi (di  $\mathbb{E}^2$  o di  $\mathbb{E}^3$ ) e sia  $r_0$  la retta per  $O$  parallela a  $r$ .



Fissato un qualsiasi punto  $Q_0 \in r$ , posto  $\underline{v} = \overrightarrow{OQ_0}$  e detta  $\tau_v$  la traslazione relativa a  $\underline{v}$ , si ha che  $\tau_v(\{\overrightarrow{OP} : P \in r_0\}) = \{Q_0Q : Q \in r\}$ . Si ha cioè che l'immagine mediante  $\tau_v$  del sottospazio di  $\mathcal{V}_O$  costituito dai vettori di  $r_0$  è il sottospazio di  $\mathcal{V}_{Q_0}$  dei vettori di  $r$ . Pertanto un punto  $Q$  appartiene alla retta  $r$  se e solo se  $\overrightarrow{Q_0Q} \in \tau_v(\{\overrightarrow{OP} : P \in r_0\})$ , e quindi se e solo se esiste un punto  $P \in r_0$  tale che  $\overrightarrow{Q_0Q} = \tau_v(\overrightarrow{OP})$ . Ciò equivale a richiedere che esista un punto  $P \in r_0$

tale che  $\overrightarrow{OQ} = \overrightarrow{OP} + \overrightarrow{OQ_0}$ . Se allora la retta  $r_0$  (passante per  $O$ ) ha equazione vettoriale  $\overrightarrow{OP} = t\overrightarrow{OP_1}$ , l'equazione vettoriale di  $r$  è:

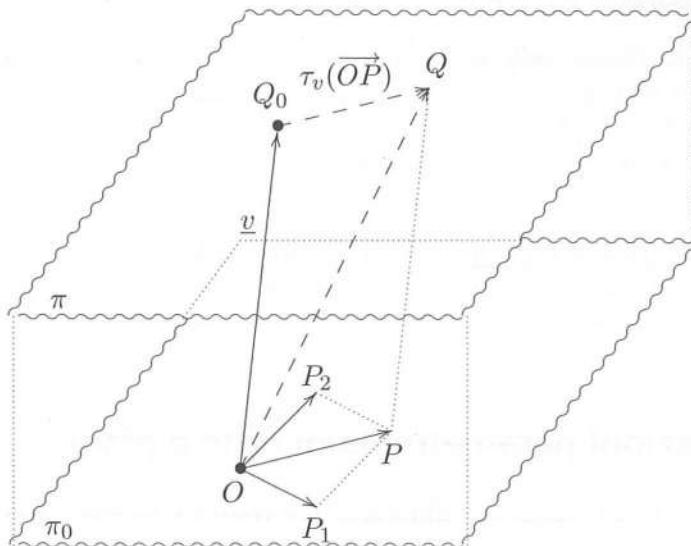
$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + t\overrightarrow{OP_1}.$$

Il punto  $Q$  descrive, al variare del parametro reale  $t$ , la retta  $r$ ; in particolare il punto  $Q_0$  si ottiene per  $t = 0$ . Il vettore  $\overrightarrow{OP_1}$  (generatore di  $r_0$ ) è detto **vettore direttore** di  $r$ . Il vettore  $\underline{v} = \overrightarrow{OQ_0}$  è detto **vettore di traslazione**.

Se una retta  $r$  è assegnata mediante due suoi punti distinti  $Q_0$  e  $Q_1$ , allora un vettore direttore di  $r$  è  $\underline{w} = \overrightarrow{OQ_1} - \overrightarrow{OQ_0}$ , che genera  $r_0$  in quanto non nullo. Pertanto per rappresentare vettorialmente  $r$  si può scegliere  $\overrightarrow{OQ_0}$  come vettore di traslazione, ottenendo l'equazione vettoriale

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + t\underline{w}.$$

Analoghe considerazioni permettono di ricavare l'equazione vettoriale di un piano non passante per  $O$  a partire dalla (9.2.2). Siano  $\pi$  un piano di  $\mathcal{E}^3$ ,  $\pi_0$  il piano per  $O$  parallelo a  $\pi$  e, fissato un punto  $Q_0 \in \pi$ , siano  $\underline{v} = \overrightarrow{OQ_0}$  e  $\tau_v$  la traslazione relativa a  $\underline{v}$ .



Allora  $\tau_v(\{\overrightarrow{OP} : P \in \pi_0\}) = \{\overrightarrow{Q_0Q} : Q \in \pi\}$ , cioè l'immagine mediante la traslazione  $\tau_v$  del sottospazio costituito dai vettori di  $\pi_0$  è il sottospazio dei vettori di  $\pi$ . Ciò comporta che un punto  $Q$  appartiene al piano  $\pi$  se e solo se  $\overrightarrow{Q_0Q} \in \tau_v(\{\overrightarrow{OP} : P \in \pi_0\})$ , ovvero se e solo se esiste un punto  $P \in \pi_0$  tale che  $\overrightarrow{Q_0Q} = \tau_v(\overrightarrow{OP})$ , e quindi se e solo se esiste  $P \in \pi_0$  tale che  $\overrightarrow{OQ} = \overrightarrow{OP} + \overrightarrow{OQ_0}$ .

Pertanto se  $\pi_0$  è rappresentato dall'equazione vettoriale  $\overrightarrow{OP} = \alpha \overrightarrow{OP_1} + \beta \overrightarrow{OP_2}$ , l'equazione vettoriale di  $\pi$  è:

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + \alpha \overrightarrow{OP_1} + \beta \overrightarrow{OP_2}.$$

Al variare di  $\alpha$  e  $\beta$  in  $\mathbb{R}$  il punto  $Q$  descrive il piano  $\pi$ ; in particolare il punto  $Q_0$  si ottiene per  $\alpha = 0 = \beta$ . La coppia  $(\overrightarrow{OP_1}, \overrightarrow{OP_2})$  di vettori di  $\pi_0$  è detta coppia di *vettori di giacitura* per  $\pi$ . Il vettore  $\underline{v} = \overrightarrow{OQ_0}$  è detto ancora *vettore di traslazione*.

Se un piano  $\pi$  è assegnato mediante tre suoi punti non allineati  $Q_0, Q_1, Q_2$ , la coppia  $(\underline{w}_1, \underline{w}_2)$  con  $\underline{w}_1 = \overrightarrow{OQ_1} - \overrightarrow{OQ_0} \in \pi_0$  e  $\underline{w}_2 = \overrightarrow{OQ_2} - \overrightarrow{OQ_0} \in \pi_0$  è una coppia di vettori di giacitura per  $\pi$ . Per ottenere una rappresentazione vettoriale di  $\pi$  si può allora scegliere  $\overrightarrow{OQ_0}$  come vettore di traslazione, ottenendo l'equazione vettoriale

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + \alpha \underline{w}_1 + \beta \underline{w}_2.$$

## Esercizi

**Esercizio 9.2.1.** Fissato nel piano un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j})$ , e considerati i punti  $A$  e  $B$  di coordinate  $(-5, 7)$  e  $(3, 2)$  rispettivamente, si determinino le componenti nella base  $\{\underline{i}, \underline{j}\}$  di  $\mathcal{V}_O^2$  dei vettori direttori delle rette  $OA$ ,  $OB$ ,  $AB$ .

**Esercizio 9.2.2.** Fissato nello spazio un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  e considerati i punti non allineati  $P$ ,  $Q$  e  $K$  di coordinate  $(0, 3, -2)$ ,  $(1, 5, -7)$  e  $(-2, 0, 0)$  rispettivamente, si determinino le componenti nella base  $\{\underline{i}, \underline{j}, \underline{k}\}$  di  $\mathcal{V}_O^3$  dei vettori delle coppie di giacitura dei piani  $\pi_1$  passante per  $P$ ,  $Q$ ,  $K$ ,  $\pi_2$  passante per  $O$ ,  $P$  e  $Q$ , e  $\pi_3$  passante per  $O$ ,  $P$  e  $K$ .

**Esercizio 9.2.3.** Fissato nello spazio un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  e considerati i punti  $H$  di coordinate  $(-3, -1, 2)$  e  $K$  di coordinate  $(11, -3, 7)$ , si determinino le componenti nella base  $\{\underline{i}, \underline{j}, \underline{k}\}$  di  $\mathcal{V}_O^3$  del vettore direttore della retta  $HK$ .

## 9.3 Equazioni parametriche di rette e piani

Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine di  $\mathbb{E}^3$  e si consideri la retta  $r$  di equazione vettoriale

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + t\underline{w}. \quad (9.3.1)$$

Se il punto  $Q_0$  ha coordinate  $(x_0, y_0, z_0)$  e  $\underline{w}$  ha come vettore coordinato nella base  $B = \{\underline{i}, \underline{j}, \underline{k}\}$  la terna  $(l, m, n) \neq (0, 0, 0)$ , allora dette  $(x, y, z)$  le coordinate del generico punto  $Q$  di  $r$ , la (9.3.1) diventa:

$$x\underline{i} + y\underline{j} + z\underline{k} = (x_0 + tl)\underline{i} + (y_0 + tm)\underline{j} + (z_0 + tn)\underline{k},$$

da cui

$$\begin{cases} x = x_0 + tl \\ y = y_0 + tm \\ z = z_0 + tn. \end{cases} \quad (9.3.2)$$

Le equazioni (9.3.2) si dicono **equazioni parametriche** della retta  $r$ , e i numeri reali  $l, m, n$  ne sono **parametri direttori**. Appartengono alla retta  $r$  tutti e soli i punti  $Q$  di  $\mathcal{E}^3$  le cui coordinate sono date dalle (9.3.2) al variare di  $t$  in  $\mathbb{R}$ .

Si noti che se  $r$  è individuata da due suoi punti distinti  $Q_0$  di coordinate  $(x_0, y_0, z_0)$  e  $Q_1$  di coordinate  $(x_1, y_1, z_1)$  allora si può considerare come vettore direttore il vettore  $\underline{w} = \overrightarrow{OQ_1} - \overrightarrow{OQ_0}$  di coordinate  $(l, m, n)$  con  $l = x_1 - x_0$ ,  $m = y_1 - y_0$ ,  $n = z_1 - z_0$ .

**9.3.1. Esempio.** Si vogliono determinare le equazioni parametriche della retta passante per i punti  $Q_0 = (1, -3, 7)$  e  $Q_1 = (2, 1, 0)$ . Si può porre  $l = 2 - 1 = 1$ ,  $m = 1 + 3 = 4$ ,  $n = -7$ , per cui le equazioni richieste sono

$$\begin{cases} x = 1 + t \\ y = -3 + 4t \\ z = 7 - 7t. \end{cases}$$

**9.3.2. Criterio di parallelismo tra rette nello spazio.** Due rette di  $\mathcal{E}^3$ , aventi parametri direttori  $(l, m, n)$  e  $(l_1, m_1, n_1)$  rispettivamente, sono parallele se e solo se la matrice

$$\begin{pmatrix} l & m & n \\ l_1 & m_1 & n_1 \end{pmatrix} \in M_{2,3}(\mathbb{R})$$

ha rango 1.

*Dimostrazione.* Siano  $r$  la retta avente equazione vettoriale data dalla (9.3.1) e equazioni parametriche (9.3.2), e  $r'$  una retta di equazione vettoriale

$$\overrightarrow{OP} = \overrightarrow{OP_0} + t'\underline{w}'$$

e di equazioni parametriche

$$\begin{cases} x = x'_0 + t'l_1 \\ y = y'_0 + t'm_1 \\ z = z'_0 + t'n_1. \end{cases} \quad (9.3.3)$$

Le rette  $r$  e  $r'$  sono parallele se e solo se, indicate con  $r_0$  la retta per  $O$  parallela a  $r$  e con  $r'_0$  la retta per  $O$  parallela a  $r'$ , risulta  $r_0 = r'_0$ . Ciò equivale a richiedere che  $\{\underline{w}, \underline{w}'\}$  sia linearmente dipendente, ovvero che la matrice

$$\begin{pmatrix} l & m & n \\ l_1 & m_1 & n_1 \end{pmatrix} \in M_{2,3}(\mathbb{R})$$

abbia rango 1. □

Si consideri ora il piano  $\pi$  di equazione vettoriale

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + \alpha \underline{w}_1 + \beta \underline{w}_2; \quad (9.3.4)$$

se  $Q_0$  ha coordinate  $(x_0, y_0, z_0)$ ,  $\underline{w}_1$  ha componenti  $(l_1, m_1, n_1)$  e  $\underline{w}_2$  ha componenti  $(l_2, m_2, n_2)$ , allora, dette  $(x, y, z)$  le coordinate di  $Q$ , la (9.3.4) diventa

$$x\underline{i} + y\underline{j} + z\underline{k} = (x_0 + \alpha l_1 + \beta l_2)\underline{i} + (y_0 + \alpha m_1 + \beta m_2)\underline{j} + (z_0 + \alpha n_1 + \beta n_2)\underline{k},$$

da cui si deduce che le *equazioni parametriche* del piano  $\pi$  sono:

$$\begin{cases} x = x_0 + \alpha l_1 + \beta l_2 \\ y = y_0 + \alpha m_1 + \beta m_2 \\ z = z_0 + \alpha n_1 + \beta n_2. \end{cases} \quad (9.3.5)$$

Si osservi che nelle (9.3.5) la matrice

$$\begin{pmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \end{pmatrix} \in M_{2,3}(\mathbb{R})$$

deve avere rango 2: ciò per il fatto che  $\underline{w}_1$  e  $\underline{w}_2$  sono linearmente indipendenti.

Come rilevato in precedenza, se il piano  $\pi$  è individuato da tre punti non allineati  $Q_0$  di coordinate  $(x_0, y_0, z_0)$ ,  $Q_1$  di coordinate  $(x_1, y_1, z_1)$  e  $Q_2$  di coordinate  $(x_2, y_2, z_2)$ , allora i vettori  $\underline{w}_1 = \overrightarrow{OQ_1} - \overrightarrow{OQ_0}$  e  $\underline{w}_2 = \overrightarrow{OQ_2} - \overrightarrow{OQ_0}$ , di coordinate  $(x_1 - x_0, y_1 - y_0, z_1 - z_0)$  e  $(x_2 - x_0, y_2 - y_0, z_2 - z_0)$  rispettivamente, sono una coppia di vettori di giacitura per  $\pi$ , e pertanto le (9.3.5) diventano facilmente

$$\begin{cases} x = x_0 + \alpha(x_1 - x_0) + \beta(x_2 - x_0) \\ y = y_0 + \alpha(y_1 - y_0) + \beta(y_2 - y_0) \\ z = z_0 + \alpha(z_1 - z_0) + \beta(z_2 - z_0). \end{cases}$$

**9.3.3. Esempio.** Per determinare le equazioni parametriche del piano  $\pi$  individuato dai tre punti non allineati

$$Q_0 = (3, -1, 0), \quad Q_1 = (0, 7, 0), \quad Q_2 = (2, 5, 9),$$

si possono scrivere le (9.3.5) ponendo  $l_1 = -3$ ,  $m_1 = 8$ ,  $n_1 = 0$ ,  $l_2 = -1$ ,  $m_2 = 6$ ,  $n_2 = 9$ . In tal modo si ottengono le equazioni

$$\begin{cases} x = 3 - 3\alpha - \beta \\ y = -1 + 8\alpha + 6\beta \\ z = 9\beta. \end{cases}$$

**9.3.4. Criterio di parallelismo tra retta e piano nello spazio.** Siano  $r$  una retta e  $\pi$  un piano di  $\mathcal{E}^3$ , di equazioni parametriche

$$\begin{cases} x = x'_0 + tl \\ y = y'_0 + tm \\ z = z'_0 + tn \end{cases} \quad e \quad \begin{cases} x = x_0 + \alpha l_1 + \beta l_2 \\ y = y_0 + \alpha m_1 + \beta m_2 \\ z = z_0 + \alpha n_1 + \beta n_2 \end{cases}$$

rispettivamente. Allora la retta  $r$  è parallela al piano  $\pi$  se e solo se la matrice

$$\begin{pmatrix} l & m & n \\ l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \end{pmatrix} \in M_{3,3}(\mathbb{R})$$

è singolare.

*Dimostrazione.* Siano

$$\begin{aligned} \overrightarrow{OP} &= \overrightarrow{OP_0} + t\underline{w} \\ \overrightarrow{OQ} &= \overrightarrow{OQ_0} + \alpha\underline{w}_1 + \beta\underline{w}_2 \end{aligned}$$

le equazioni vettoriali di  $r$  e di  $\pi$  rispettivamente. La retta  $r$  è parallela al piano  $\pi$  se e solo se il piano  $\pi_0$  per  $O$  parallelo a  $\pi$  contiene la retta  $r_0$  per  $O$  parallela a  $r$ , ossia se e solo se il vettore direttore  $\underline{w}$  di  $r$  appartiene al piano generato dai vettori di giacitura  $\underline{w}_1$  e  $\underline{w}_2$  di  $\pi$ . Ciò equivale a richiedere che  $\{\underline{w}, \underline{w}_1, \underline{w}_2\}$  sia linearmente dipendente, ovvero che la matrice che compare nell'enunciato sia singolare.  $\square$

**9.3.5. Criterio di parallelismo tra piani nello spazio.** Due piani di  $\mathcal{E}^3$ , aventi equazioni parametriche

$$\begin{cases} x = x_0 + \alpha l_1 + \beta l_2 \\ y = y_0 + \alpha m_1 + \beta m_2 \\ z = z_0 + \alpha n_1 + \beta n_2 \end{cases} \quad e \quad \begin{cases} x = x'_0 + \alpha' l'_1 + \beta' l'_2 \\ y = y'_0 + \alpha' m'_1 + \beta' m'_2 \\ z = z'_0 + \alpha' n'_1 + \beta' n'_2 \end{cases}$$

rispettivamente, sono paralleli se e solo se la matrice

$$\begin{pmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \\ l'_1 & m'_1 & n'_1 \\ l'_2 & m'_2 & n'_2 \end{pmatrix} \in M_{4,3}(\mathbb{R})$$

ha rango 2.

*Dimostrazione.* Esercizio. □

Sia ora  $\mathcal{RA}(O, i, j)$  un riferimento affine del piano  $\mathcal{E}^2$ , e si consideri la retta  $r$  di equazione vettoriale

$$\overrightarrow{OQ} = \overrightarrow{OQ_0} + t\underline{w};$$

se  $Q_0$  ha coordinate  $(x_0, y_0)$  e  $\underline{w}$  ha coordinate  $(l, m) \neq (0, 0)$ , allora le equazioni parametriche di  $r$  sono

$$\begin{cases} x = x_0 + tl \\ y = y_0 + tm. \end{cases} \quad (9.3.6)$$

I numeri reali  $(l, m)$  sono detti **parametri direttori** di  $r$ .

**9.3.6. Criterio di parallelismo tra rette nel piano.** Due rette di  $\mathcal{E}^2$ , aventi parametri direttori  $(l, m)$  e  $(l_1, m_1)$  rispettivamente, sono parallele se e solo se  $lm_1 = l_1m$ .

*Dimostrazione.* Sia  $r$  la retta di equazioni parametriche (9.3.6), e sia  $r'$  la retta di equazioni parametriche

$$\begin{cases} x = x'_0 + t'l_1 \\ y = y'_0 + t'm_1. \end{cases} \quad (9.3.7)$$

Siano poi

$$\begin{aligned} \overrightarrow{OQ} &= \overrightarrow{OQ_0} + t\underline{w}, \\ \overrightarrow{OP} &= \overrightarrow{OP_0} + t'\underline{w}' \end{aligned} \quad (9.3.8)$$

le equazioni vettoriali di  $r$  ed  $r'$  rispettivamente. Allora  $r$  e  $r'$  sono parallele se e solo se  $\underline{w}$  e  $\underline{w}'$  sono linearmente dipendenti, e cioè se e solo se la matrice

$$\begin{pmatrix} l & m \\ l_1 & m_1 \end{pmatrix}$$

ha determinante nullo. Ciò equivale a richiedere che sia  $lm_1 - l_1m = 0$ . □

Siano  $r$  e  $r'$  rette non parallele del piano o dello spazio, di equazioni vettoriali

$$\begin{aligned} \overrightarrow{OP} &= \overrightarrow{OP_0} + t\overrightarrow{OQ}, \\ \overrightarrow{OP'} &= \overrightarrow{OP'_0} + t'\overrightarrow{OQ'} \end{aligned}$$

rispettivamente. Allora i vettori direttori  $\overrightarrow{OQ}$  e  $\overrightarrow{OQ'}$  non sono proporzionali, e dunque generano un piano. Le rette  $r$  e  $r'$  sono **incidenti**, ossia si intersecano in un (unico) punto  $X$  (detto **punto di incidenza**), se e solo se esistono  $t, t' \in \mathbb{R}$  tali che

$$\overrightarrow{OP_0} + t\overrightarrow{OQ} = \overrightarrow{OX} = \overrightarrow{OP'_0} + t'\overrightarrow{OQ'},$$

e ciò accade se e solo se esistono  $t, t' \in \mathbb{R}$  tali che

$$\overrightarrow{OP_0} - \overrightarrow{OP'_0} = t'\overrightarrow{OQ'} - t\overrightarrow{OQ}.$$

Pertanto  $r$  e  $r'$  si intersecano se e solo se  $\overrightarrow{OP_0} - \overrightarrow{OP'_0}$  è un vettore del piano generato da  $\overrightarrow{OQ}$  e  $\overrightarrow{OQ'}$ . Questo criterio consente di stabilire quando due rette si intersecano, sia nel piano che nello spazio. Nel piano la condizione è sempre soddisfatta perché tali vettori costituiscono una base di  $\mathcal{V}_0^2$ . Infatti due rette del piano che non sono parallele hanno sempre un punto di intersezione. Nello spazio  $\mathcal{V}_0^3$  invece esistono le cosiddette rette *sghembe*, cioè né parallele né incidenti. Utilizzando le equazioni parametriche, (9.3.6) e (9.3.2) si completano come segue.

**9.3.7. Criterio di incidenza tra rette nel piano.** Due rette di  $\mathcal{E}^2$ , aventi parametri direttori  $(l, m)$  e  $(l_1, m_1)$  rispettivamente, sono incidenti se e solo se  $lm_1 - l_1m \neq 0$ .

*Dimostrazione.* Siano  $r$  ed  $r'$  rette del piano aventi equazioni vettoriali (9.3.8) ed equazioni parametriche (9.3.6) e (9.3.7) rispettivamente. Esiste allora un unico punto  $P \in r \cap r'$  se e solo se esiste un'unica coppia  $(t, t') \in \mathbb{R} \times \mathbb{R}$  tale che

$$\begin{cases} x_0 + tl = x'_0 + t'l_1 \\ y_0 + tm = y'_0 + t'm_1, \end{cases}$$

e quindi se e solo se il sistema lineare

$$\begin{cases} lt - l_1t' = x'_0 - x_0 \\ mt - m_1t' = y'_0 - y_0 \end{cases} \quad (9.3.9)$$

nelle incognite  $t$  e  $t'$  ammette un'unica soluzione. Per il teorema di Cramer (vedi 7.7.1) ciò equivale a richiedere che sia  $lm_1 - l_1m \neq 0$ .  $\square$

Se le rette  $r$  e  $r'$  del piano sono incidenti, detta  $(t_0, t'_0)$  la soluzione del sistema lineare (9.3.9), le coordinate del punto di incidenza sono date da

$$(x_0 + t_0l, y_0 + t_0m) = (x'_0 + t'_0l_1, y'_0 + t'_0m_1).$$

**9.3.8. Criterio di incidenza tra rette nello spazio.** Siano  $r$  ed  $r'$  rette non parallele di  $\mathcal{E}^3$ , aventi equazioni parametriche date da (9.3.2) e da (9.3.3) rispettivamente. Allora  $r$  e  $r'$  sono incidenti se e solo se il sistema lineare

$$\begin{cases} tl - t'l_1 = x'_0 - x_0 \\ tm - t'm_1 = y'_0 - y_0 \\ tn - t'n_1 = z'_0 - z_0 \end{cases} \quad (9.3.10)$$

nelle incognite  $t$  e  $t'$  è compatibile.

*Dimostrazione.* Esercizio. □

Se le rette non parallele  $r$  e  $r'$  sono incidenti, ossia se il sistema lineare (9.3.10) ammette una (e quindi una sola) soluzione  $(t_0, t'_0)$ , le coordinate del punto di incidenza sono date da

$$(x_0 + t_0 l, y_0 + t_0 m, z_0 + t_0 n) = (x'_0 + t'_0 l_1, y'_0 + t'_0 m_1, z'_0 + t'_0 n_1).$$

**9.3.9. Esempio.** Si considerino le rette  $r$  ed  $r'$  di equazioni parametriche

$$\begin{cases} x = 1 + t \\ y = -2 + 3t \\ z = 0 \end{cases} \quad \text{e} \quad \begin{cases} x = 0 \\ y = -1 + t' \\ z = 5t' \end{cases}$$

rispettivamente. Le rette  $r$  ed  $r'$  sono sghembe. Infatti non sono parallele perché la matrice

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 5 \end{pmatrix}$$

ha rango 2, e non sono incidenti perché il sistema

$$\begin{cases} t = -1 \\ 3t - t' = 1 \\ 5t' = 0 \end{cases}$$

non è compatibile.

## Esercizi

**Esercizio 9.3.1.** Si dimostri 9.3.5.

**Esercizio 9.3.2.** Si dimostri 9.3.8.

**Esercizio 9.3.3.** In un riferimento affine dello spazio euclideo  $\mathcal{E}^3$  si dimostri che i punti  $A$ ,  $B$ ,  $C$  e  $D$ , di coordinate rispettivamente  $(1, 1, 5)$ ,  $(2, 2, 1)$ ,  $(1, -2, 2)$  e  $(-2, 1, 2)$ , non appartengono a uno stesso piano. Considerate poi le rette  $AB$  e  $CD$  si stabilisca se esse sono parallele, incidenti o sghembe.

**Esercizio 9.3.4.** Sia  $\mathcal{RA}(O, i, j, k)$  un riferimento affine dello spazio euclideo  $\mathcal{E}^3$ .

- (i) Si determinino le equazioni parametriche dei seguenti piani:
  - il piano  $\pi_1$  passante per il punto  $A$  di coordinate  $(1, 1, 0)$  e parallelo ai vettori  $\underline{u}$  di componenti  $(-1, 0, -1)$  e  $\underline{v}$  di componenti  $(0, 6, 9)$ ;
  - il piano  $\pi_2$  passante per i punti  $B$  e  $C$  di rispettive coordinate  $(0, 1, -1)$  e  $(3, 2, 1)$ , e parallelo al vettore  $\underline{w}$  di componenti  $(0, -3, 0)$ .
- (ii) Si stabilisca se sono complanari le rette aventi le seguenti equazioni parametriche

$$\begin{cases} x = 1 - 2t \\ y = 1 - 6t \\ z = 4 + 2t, \end{cases} \quad \begin{cases} x = -3 + 5t' \\ y = 3 + 5t' \\ z = 5t'. \end{cases}$$

**Esercizio 9.3.5.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si considerino le rette di equazioni parametriche

$$\begin{cases} x = 1 + 2t \\ y = -1 + t \\ z = 2 + 3t, \end{cases} \quad \begin{cases} x = t' \\ y = 2 + 4t' \\ z = 2 + 3t'. \end{cases}$$

- (i) Si stabilisca se tali rette sono complanari e, in caso affermativo, si determinino le equazioni parametriche del piano  $\pi$  che le contiene.
- (ii) Siano  $A, B, C$  i punti di coordinate  $(-1, 0, 3)$ ,  $(2, 1, 1)$  e  $(7, 0, 9)$  rispettivamente. Dopo aver provato che tali punti non sono allineati, si scrivano le equazioni parametriche del piano  $\pi_1$  che li contiene.
- (iii) I piani  $\pi$  e  $\pi_1$  sono paralleli?

**Esercizio 9.3.6.** In un riferimento affine dello spazio euclideo  $\mathcal{E}^3$  si considerino le rette di equazioni parametriche

$$\begin{cases} x = 2 + t \\ y = 1 + 3t \\ z = 1 - t, \end{cases} \quad \begin{cases} x = 2 + t' \\ y = 3 + t' \\ z = -1 + t'. \end{cases}$$

Si stabilisca se tali rette sono complanari e, in caso affermativo, se esse sono parallele o incidenti, e si scrivano le equazioni parametriche del piano che le contiene.

- Esercizio 9.3.7.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine dello spazio euclideo  $\mathcal{E}^3$ .
- (i) Si determinino le equazioni parametriche dei seguenti piani:
    - il piano  $\pi_1$  passante per il punto  $A$  di coordinate  $(1, 1, 0)$  e parallelo ai vettori  $\underline{u}$  di componenti  $(1, 0, 1)$  e  $\underline{v}$  di componenti  $(0, 2, 3)$ ;
    - il piano  $\pi_2$  passante per i punti  $B$  e  $C$  di rispettive coordinate  $(0, 1, -1)$  e  $(3, 2, 1)$ , e parallelo al vettore  $\underline{w}$  di componenti  $(0, 0, 5)$ ;
    - il piano  $\pi_3$  passante per i punti  $E$ ,  $F$  e  $G$  di rispettive coordinate  $(0, 1, 0)$ ,  $(2, -1, 0)$  e  $(1, 2, 2)$ .
  - (ii) Si stabilisca se le rette di equazioni parametriche

$$\begin{cases} x = 1 + t \\ y = 1 + 3t \\ z = 4 - t, \end{cases} \quad \begin{cases} x = -1 + t' \\ y = 1 + t' \\ z = t', \end{cases}$$

sono complanari e, in caso affermativo, se esse sono parallele o incidenti.

**Esercizio 9.3.8.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si considerino le rette  $r$  e  $s_h$  di equazioni parametriche

$$\begin{cases} x = 3 - t \\ y = 15 \\ z = -1 + t, \end{cases} \quad \begin{cases} x = 1 - t' \\ y = 9 + (h+2)t' \\ z = -5 + t'. \end{cases}$$

- (i) Si stabilisca per quali valori di  $h$  tali rette sono parallele.  
(ii) Esistono valori di  $h$  per i quali la retta  $s_h$  passa per l'origine del riferimento?

**Esercizio 9.3.9.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine di  $\mathcal{E}^3$  e si considerino i punti  $Q_0$  e  $Q_1$  di coordinate  $(-1, 1, -2)$  e  $(0, 1, 1)$  rispettivamente. Siano poi  $\underline{v}_1$  e  $\underline{v}_2$  i vettori di  $\mathcal{V}_0^3$  aventi componenti  $(1, 0, 3)$  e  $(1, 1, 2)$  rispettivamente.

- (i) Si scrivano le equazioni parametriche della retta  $s$  passante per  $Q_0$  avente  $\underline{v}_1$  come vettore direttore.  
(ii) Si scrivano le equazioni parametriche del piano  $\pi$  passante per  $Q_0$  e avente  $\underline{v}_1$  e  $\underline{v}_2$  come vettori di giacitura.  
(iii) Si stabilisca se  $Q_1$  appartiene a  $s$ , e se appartiene a  $\pi$ .

**Esercizio 9.3.10.** Fissato un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  nello spazio, si determini l'equazione parametrica della retta  $r$  passante per i punti  $P_1$  e  $P_2$  di coordinate  $(1, 1, 2)$  e  $(-1, 3, 5)$ , e si stabilisca se il punto  $Q$  di coordinate  $(0, 3, -2)$  è un punto di  $r$ .

**Esercizio 9.3.11.** Fissato un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j})$  del piano, si considerino le rette  $r$  ed  $r'$  di rispettive equazioni parametriche

$$\begin{cases} x = 1 + 3t \\ y = 2 + t, \end{cases} \quad \begin{cases} x = -1 + t' \\ y = -1 + 2t'. \end{cases}$$

Si dimostri che  $r$  ed  $r'$  si intersecano e si determini il punto di intersezione.

**Esercizio 9.3.12.** Sia  $r_a$  la retta del piano avente, in un fissato riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j})$ , equazioni parametriche

$$\begin{cases} x = 2 + t \\ y = -1 + at, \end{cases}$$

dove  $a \in \mathbb{R}$ . Si stabilisca per quali valori di  $a$  l'origine  $O$  è un punto di  $r_a$ .

**Esercizio 9.3.13.** Fissato un sistema di riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j})$  nel piano, siano  $r_1$  la retta passante per i punti di coordinate  $(-1, 1)$  e  $(0, 1)$  e sia  $r_2$  la retta per i punti di coordinate  $(2, 2)$  e  $(1, 0)$ . Si provi che  $r_1$  e  $r_2$  si intersecano e si determini il punto di intersezione.

**Esercizio 9.3.14.** Fissato un sistema di riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j})$  nel piano, si consideri la retta  $r$  di equazioni parametriche

$$\begin{cases} x = 1 + 3t \\ y = 2 + t. \end{cases}$$

Sia poi  $s_a$  la retta passante per i punti di coordinate  $(0, a)$  e  $(2, -1)$ , dove  $a \in \mathbb{R}$ . Si stabilisca per quali valori di  $a$  le rette  $r$  e  $s_a$  si intersecano, e si determinino le coordinate dell'eventuale punto di intersezione.

**Esercizio 9.3.15.** Fissato un sistema di riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  nello spazio, si considerino la retta  $r$  passante per i punti di coordinate  $(3, 0, 4)$  e  $(-1, 2, -2)$  e la retta  $r_1$  passante per i punti di coordinate  $(2, 2, 5)$  e  $(0, 0, -3)$ . Si dimostri che  $r_1$  e  $r$  si intersecano, e si individui il punto di intersezione.

**Esercizio 9.3.16.** Fissato un sistema di riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  nello spazio, si considerino le rette  $r$  e  $s_a$  di equazioni parametriche

$$\begin{cases} x = -1 + t \\ y = 1 \\ z = 1 + t, \end{cases} \quad \begin{cases} x = -1 + at' \\ y = 1 + (a+1)t' \\ z = 2 - at', \end{cases}$$

dove  $a \in \mathbb{R}$ . Si stabilisca per quali valori di  $a$  le rette  $r$  e  $s_a$  si intersecano, e si determinino le coordinate dell'eventuale punto di intersezione.

## 9.4 Equazioni cartesiane di rette e piani

Sia  $\mathcal{RA}(O, \underline{i}, \underline{j})$  un riferimento affine del piano  $\mathcal{E}^2$  e siano  $P_0$  e  $P_1$  punti distinti di  $\mathcal{E}^2$ , di coordinate  $(x_0, y_0)$  e  $(x_1, y_1)$  rispettivamente. Il vettore  $\underline{w} = \overrightarrow{OP_1} - \overrightarrow{OP_0}$  di componenti  $(x_1 - x_0, y_1 - y_0)$  è un vettore direttore della retta  $r$  per i punti  $P_0$  e  $P_1$ . Ciò comporta che un punto  $P \in \mathcal{E}^2$  di coordinate  $(x, y)$  appartiene a  $r$  se e solo se il vettore  $\underline{u} = \overrightarrow{OP} - \overrightarrow{OP_0}$  di componenti  $(x - x_0, y - y_0)$  appartiene al sottospazio generato da  $\underline{w}$ , e quindi se e solo se le sue componenti risultano proporzionali a  $(x_1 - x_0, y_1 - y_0)$ . Pertanto i punti di  $r$  sono tutti e soli i punti del piano le cui coordinate  $(x, y)$  soddisfano l'equazione

$$\det \begin{pmatrix} x - x_0 & x_1 - x_0 \\ y - y_0 & y_1 - y_0 \end{pmatrix} = 0. \quad (9.4.1)$$

Nel caso in cui  $x_0 \neq x_1$  e  $y_0 \neq y_1$ , la (9.4.1) equivale a

$$\frac{x - x_0}{x_1 - x_0} = \frac{y - y_0}{y_1 - y_0},$$

ovvero

$$(y_1 - y_0)x + (x_0 - x_1)y + (y_0 - y_1)x_0 + (x_1 - x_0)y_0 = 0,$$

che, posto  $a = y_1 - y_0$ ,  $b = x_0 - x_1$  e  $c = (y_0 - y_1)x_0 + (x_1 - x_0)y_0$ , diventa

$$ax + by + c = 0. \quad (9.4.2)$$

La (9.4.2) è l'**equazione cartesiana** della retta  $r$ . Si noti che  $(-b, a)$  sono parametri direttori di  $r$ , pertanto se  $a'b' + b'a' = 0$  è l'equazione cartesiana di un'altra retta  $r'$ , allora 9.3.6 assicura che  $r$  ed  $r'$  sono parallele se e solo se

$$ab' - ba' = 0.$$

**9.4.1. Esempio.** Si considerino i punti  $A$  e  $B$  del piano che in un fissato riferimento affine hanno coordinate  $(3, 5)$  e  $(-2, -4)$  rispettivamente. Appartengono alla retta  $AB$  tutti e soli i punti  $P$  del piano le cui coordinate  $(x, y)$  sono tali che

$$\frac{x - 3}{-5} = \frac{y - 5}{-9},$$

da cui si ricava l'equazione cartesiana  $9x - 5y - 2 = 0$  della retta  $AB$ .

Sia ora  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine dello spazio e siano  $Q_0, Q_1$  e  $Q_2$  tre punti non allineati di coordinate  $(x_0, y_0, z_0)$ ,  $(x_1, y_1, z_1)$  e  $(x_2, y_2, z_2)$  rispettivamente. I vettori  $\underline{w}_1 = \overrightarrow{OQ_1} - \overrightarrow{OQ_0}$  e  $\underline{w}_2 = \overrightarrow{OQ_2} - \overrightarrow{OQ_0}$ , rispettivamente di componenti  $(x_1 - x_0, y_1 - y_0, z_1 - z_0)$  e  $(x_2 - x_0, y_2 - y_0, z_2 - z_0)$ , costituiscono una coppia di vettori di giacitura del piano  $\pi$  individuato da  $Q_0, Q_1$  e  $Q_2$ . Pertanto un punto  $P$  di coordinate  $(x, y, z)$  appartiene a  $\pi$  se e solo se il vettore  $\underline{w} = \overrightarrow{OP} - \overrightarrow{OQ_0}$  dipende linearmente da  $\{\underline{w}_1, \underline{w}_2\}$ , e quindi se e solo se la matrice

$$\begin{pmatrix} x - x_0 & y - y_0 & z - z_0 \\ x_1 - x_0 & y_1 - y_0 & z_1 - z_0 \\ x_2 - x_0 & y_2 - y_0 & z_2 - z_0 \end{pmatrix} \in M_{3,3}(\mathbb{R})$$

ha determinante uguale a zero. Sviluppando il determinante di tale matrice si ottiene un'equazione del tipo

$$ax + by + cz + d = 0. \quad (9.4.3)$$

Appartengono dunque al piano  $\pi$  tutti e soli i punti dello spazio le cui coordinate  $(x, y, z)$ , nel riferimento affine considerato, soddisfano l'equazione di primo grado (9.4.3) nelle incognite  $x, y, z$ , detta **equazione cartesiana** del piano  $\pi$ .

**9.4.2. Esempio.** Si considerino i tre punti dello spazio che in un fissato riferimento affine hanno coordinate  $(0, 3, -2)$ ,  $(-1, 7, 0)$ ,  $(5, -2, 1)$ . L'equazione cartesiana del piano  $\pi$  che contiene tali punti si ottiene ugualando a zero il determinante della matrice

$$\begin{pmatrix} x & y - 3 & z + 2 \\ -1 & 4 & 2 \\ 5 & -5 & 3 \end{pmatrix},$$

ed è quindi  $22x + 13y - 15z - 69 = 0$ .

Per determinare, in un riferimento affine dello spazio, l'equazione cartesiana della retta  $r$  per i punti di coordinate  $(x_0, y_0, z_0)$  e  $(x_1, y_1, z_1)$ , basta osservare che il punto di coordinate  $(x, y, z)$  è un punto di  $r$  se e solo se il vettore di componenti  $(x - x_0, y - y_0, z - z_0)$  è proporzionale al vettore direttore di  $r$  che ha componenti  $(x_1 - x_0, y_1 - y_0, z_1 - z_0)$ . Ciò equivale a richiedere che la matrice

$$\begin{pmatrix} x - x_0 & y - y_0 & z - z_0 \\ x_1 - x_0 & y_1 - y_0 & z_1 - z_0 \end{pmatrix}$$

abbia rango 1. Nel caso in cui  $x_0 \neq x_1$ ,  $y_0 \neq y_1$  e  $z_0 \neq z_1$  questo accade se e solo se  $x, y, z$  soddisfano la relazione

$$\frac{x - x_0}{x_1 - x_0} = \frac{y - y_0}{y_1 - y_0} = \frac{z - z_0}{z_1 - z_0}. \quad (9.4.4)$$

Tale relazione equivale a un sistema di due equazioni di primo grado in  $x, y, z$ . Ciascuna delle due equazioni di (9.4.4) è l'equazione cartesiana di un piano, e l'intersezione di tali piani è appunto la retta  $r$ . Pertanto la (9.4.4) costituisce l'**equazione cartesiana** della retta  $r$ .

**9.4.3. Esempio.** Si considerino i punti  $P$  e  $Q$  dello spazio aventi, in un assegnato riferimento affine, coordinate  $(1, -2, 5)$  e  $(-4, 0, 3)$  rispettivamente. Appartengono alla retta  $PQ$  tutti e soli i punti dello spazio le cui coordinate  $x, y, z$  sono tali che

$$\frac{x - 1}{-5} = \frac{y + 2}{2} = \frac{z - 5}{-2}.$$

Dunque i punti della retta  $PQ$  sono tutti e soli i punti del piano le cui coordinate soddisfano il sistema

$$\begin{cases} \frac{x - 1}{-5} = \frac{y + 2}{2} \\ \frac{y + 2}{2} = \frac{z - 5}{-2}, \end{cases}$$

ovvero

$$\begin{cases} 2x + 5y + 8 = 0 \\ y + z - 3 = 0. \end{cases}$$

## Esercizi

**Esercizio 9.4.1.** Siano  $A, B, C$  e  $D$  i punti che in un fissato riferimento affine del piano hanno coordinate  $(-1, 15)$ ,  $(7, 2)$ ,  $(-2, 7)$  e  $(5, -38)$  rispettivamente. Dopo aver scritto le equazioni cartesiane delle rette  $AB$  e  $CD$ , si stabilisca se esse sono parallele o incidenti, e in quest'ultimo caso si determinino le coordinate del punto di intersezione.

**Esercizio 9.4.2.** Indicato con  $h$  un parametro reale, si considerino i punti  $A_h$  e  $C$  che in un fissato riferimento affine del piano hanno coordinate  $(h + 3, 1)$  e  $(-3, 14)$  rispettivamente. Dopo aver scritto l'equazione cartesiana della retta  $A_hC$ , si determinino gli eventuali valori del parametro  $h$  per i quali la retta  $A_hC$  è parallela ad uno degli assi del riferimento,

**Esercizio 9.4.3.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine di  $\mathbb{E}^3$  e siano  $A, B$  e  $C_h$  (con  $h \in \mathbb{R}$ ) i punti di coordinate  $(1, -1, -1)$ ,  $(0, 2, 0)$  e  $(1 - h, 11, 5)$  rispettivamente.

- (i) Per quali valori di  $h$  tali punti sono allineati?
- (ii) Posto  $h = 0$  si scriva l'equazione cartesiana del piano per  $A, B$  e  $C_0$ .

**Esercizio 9.4.4.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine di  $\mathcal{E}^3$ , e siano  $A, B, C, D_h$  i punti di coordinate  $(1, 0, 2)$ ,  $(0, 3, 1)$ ,  $(1, 1, 1)$ ,  $(0, 0, h)$  rispettivamente, dove  $h$  è un parametro reale.

- (i) Per quali valori di  $h$  tali punti appartengono allo stesso piano?
- (ii) Dopo aver determinato le rispettive equazioni cartesiane, stabilire se esistono valori del parametro  $h$  per i quali la retta  $r$  per  $A$  e  $B$  e la retta  $s_h$  per  $C$  e  $D_h$  sono parallele.

**Esercizio 9.4.5.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si scrivano l'equazione cartesiana del piano  $\pi$  per l'origine  $O$  una cui coppia di vettori di giacitura sia costituita dai vettori di componenti  $(3, -2, 1)$ ,  $(-4, 0, 7)$ , e quella della retta  $r$  passante per i punti  $A$  e  $B$  di rispettive coordinate  $(-1, 4, 0)$  e  $(1, 1, -2)$ . Si stabilisca se la retta  $r$  e il piano  $\pi$  sono paralleli o incidenti, e in quest'ultimo caso si determinino le coordinate del punto di intersezione.

**Esercizio 9.4.6.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si scrivano le equazioni cartesiane del piano  $\pi$  che contiene i punti  $A, B, C$  di coordinate  $(-1, 4, 0)$ ,  $(7, -3, 5)$ ,  $(1, 1, -2)$  rispettivamente, e della retta  $r$  per l'origine  $O$  il cui vettore direttore abbia componenti  $(16, -14, 10)$ . Si stabilisca se la retta  $r$  e il piano  $\pi$  sono paralleli o incidenti.

**Esercizio 9.4.7.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si scrivano le equazioni cartesiane del piano  $\pi$  per l'origine  $O$  una cui coppia di vettori di giacitura sia costituita dai vettori di componenti  $(3, -2, 1)$  e  $(-4, 0, 7)$ , e quelle della retta  $r$  passante per i punti  $A$  e  $B$  di rispettive coordinate  $(-1, 4, 0)$  e  $(1, 1, -2)$ . Si stabilisca se la retta  $r$  e il piano  $\pi$  sono paralleli o incidenti, e in quest'ultimo caso si determinino le coordinate del punto di intersezione.

**Esercizio 9.4.8.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine dello spazio euclideo.

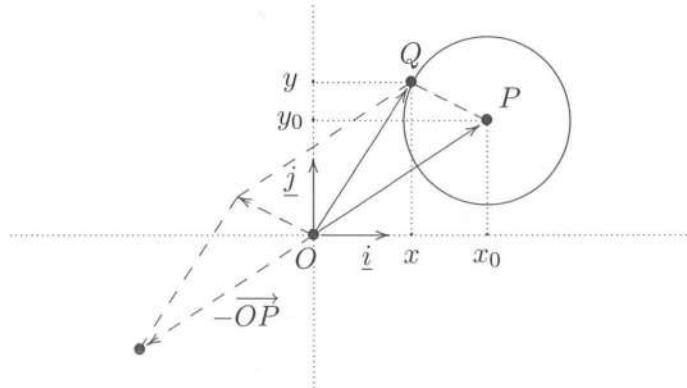
- (i) Si scriva l'equazione cartesiana della retta  $r$  per il punto  $A$  di coordinate  $(1, 2, 3)$  parallela alla retta congiungente i punti  $B$  di coordinate  $(-2, 2, 0)$  e  $C$  di coordinate  $(4, -1, 7)$ .
- (ii) Si scriva l'equazione cartesiana della retta  $s$  congiungente i punti  $E$  di coordinate  $(1, -1, 8)$  e  $F$  di coordinate  $(10, -1, 11)$ .
- (iii) Si dimostri che le rette  $r$  e  $s$  sono incidenti e si determinino le coordinate del punto di intersezione.

## 9.5 Equazione cartesiana della circonferenza

Per il resto del presente capitolo, la trattazione richiede nozioni elementari di trigonometria. Il Lettore che non ne fosse in possesso può riferirsi a un qualunque testo di trigonometria piana per le scuole medie superiori.

Sia  $\mathcal{RA}(O, \underline{i}, \underline{j})$  un riferimento affine **ortonormale** del piano  $\mathcal{E}^2$ , ossia tale che i vettori  $\underline{i}$  e  $\underline{j}$  abbiano lunghezza unitaria e siano ortogonali (cioè formino un angolo

di  $\frac{\pi}{2}$  radianti).



Se  $P$  è un punto di  $\mathcal{E}^2$  di coordinate  $(x_0, y_0)$ , il teorema di Pitagora assicura che

$$|OP|^2 = x_0^2 + y_0^2,$$

quindi la **distanza** del punto  $P$  dall'origine, ovvero la lunghezza del segmento  $\overline{OP}$ , è data da

$$d(O, P) = \sqrt{x_0^2 + y_0^2}.$$

Tale numero reale viene anche indicato con  $\|\overrightarrow{OP}\|$  e detto **norma** del vettore  $\overrightarrow{OP}$ . Se  $Q$  è un altro punto di  $\mathcal{E}^2$  di coordinate  $(x, y)$ , ancora il teorema di Pitagora assicura che

$$d(P, Q) = \sqrt{(x - x_0)^2 + (y - y_0)^2} = \|\overrightarrow{OQ} - \overrightarrow{OP}\|.$$

Dato un numero reale positivo  $r$  la **circonferenza**  $\Gamma(P, r)$  di centro il punto  $P$  e raggio  $r$  è definita come l'insieme di tutti e soli i punti del piano aventi da  $P$  distanza  $r$ ; cioè:

$$\Gamma(P, r) := \{Q \in \mathcal{E}^2 : d(P, Q) = r\}.$$

Pertanto il punto  $Q$  di coordinate  $(x, y)$  appartiene alla circonferenza  $\Gamma(P, r)$  se e solo se  $\sqrt{(x - x_0)^2 + (y - y_0)^2} = r$ , ovvero se e solo se

$$(x - x_0)^2 + (y - y_0)^2 = r^2, \quad (9.5.1)$$

da cui

$$x^2 + y^2 - 2xx_0 - 2yy_0 + x_0^2 + y_0^2 - r^2 = 0. \quad (9.5.2)$$

La (9.5.2), di secondo grado nelle incognite  $x$  e  $y$ , è l'**equazione cartesiana** della circonferenza  $\Gamma(P, r)$ .

**9.5.1. Esempio.** Sia  $P$  il punto del piano di coordinate  $(-3, 5)$ . La circonferenza di centro  $P$  e raggio  $\sqrt{2}$  è costituita da tutti e soli i punti del piano le cui coordinate  $(x, y)$  soddisfano la relazione  $(x + 3)^2 + (y - 5)^2 = 2$ , ovvero

$$x^2 + y^2 + 6x - 10y + 32 = 0.$$

Quest'ultima è appunto l'equazione della circonferenza di centro  $P$  e raggio  $\sqrt{2}$ .

È poi immediato osservare che ogni equazione di secondo grado del tipo

$$x^2 + y^2 + dx + ey + f = 0$$

nelle incognite  $x$  e  $y$ , con

$$\frac{d^2}{4} + \frac{e^2}{4} - f > 0,$$

è l'equazione cartesiana di una circonferenza, e precisamente della circonferenza di centro il punto  $P$  di coordinate  $(-\frac{d}{2}, -\frac{e}{2})$  e raggio  $\sqrt{\frac{d^2}{4} + \frac{e^2}{4} - f}$ .

**9.5.2. Esempio.** L'equazione  $x^2 + y^2 + 3x + 5y + 7 = 0$  è l'equazione della circonferenza di centro il punto di coordinate  $(-\frac{3}{2}, -\frac{5}{2})$  e raggio  $\sqrt{\frac{3}{2}}$ .

## Esercizi

**Esercizio 9.5.1.** Considerato il punto  $P$  che in un fissato riferimento ortonormale del piano ha coordinate  $(1, -5)$ , si scriva l'equazione cartesiana della circonferenza di centro  $P$  e raggio 3, e si stabilisca se l'origine del riferimento appartiene a tale circonferenza.

**Esercizio 9.5.2.** Si scriva l'equazione cartesiana della circonferenza di centro il punto di coordinate  $(-7, 1)$  e che passa per il punto di coordinate  $(-2, 5)$ .

**Esercizio 9.5.3.** Si stabilisca se l'equazione  $x^2 + y^2 - 7x + 12y - 9 = 0$  è l'equazione cartesiana di una circonferenza e, in caso affermativo, se ne determinino il raggio, le coordinate del centro e le coordinate degli eventuali punti di intersezione con gli assi del riferimento.

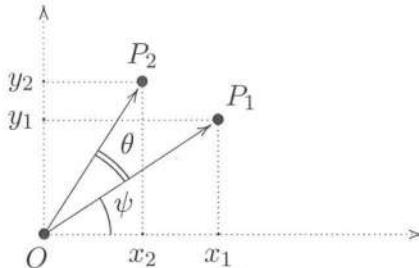
**Esercizio 9.5.4.** Si determinino le coordinate degli eventuali punti di intersezione della circonferenza di equazione  $x^2 + y^2 + 7x - 4y + 2 = 0$  con la retta di equazione  $x - 3y = 0$ .

**Esercizio 9.5.5.** Si determinino le coordinate degli eventuali punti di intersezione tra la circonferenza  $\Gamma_0$  di centro l'origine del riferimento e raggio 3 e la circonferenza  $\Gamma$  di equazione  $x^2 + y^2 - 5x + 3y = 0$ .

## 9.6 Spazi vettoriali metrici

Nel seguito, per angolo tra rette o vettori si intenderà sempre un angolo di ampiezza compresa tra  $0$  e  $\pi$  radienti. Poiché la funzione coseno è biettiva nell'intervallo  $[0, \pi]$ , per determinare l'angolo tra due vettori o tra due rette basterà calcolarne il coseno.

Si supponga dunque di voler calcolare  $\cos \theta$  dove  $\theta$  è l'angolo formato dai vettori  $\underline{v}_1 = \overrightarrow{OP_1}$  e  $\underline{v}_2 = \overrightarrow{OP_2}$  aventi, in un assegnato riferimento ortonormale del piano, componenti  $(x_1, y_1)$  e  $(x_2, y_2)$  rispettivamente.



Indicato con  $\psi$  l'angolo che  $\underline{v}_1$  forma con l'asse  $x$ , si ha che  $\underline{v}_2$  forma con l'asse  $x$  l'angolo  $\theta + \psi$ , e risulta:

$$\begin{aligned} \cos \psi &= \frac{x_1}{\|\underline{v}_1\|}, & \sin \psi &= \frac{y_1}{\|\underline{v}_1\|}, \\ \cos(\psi + \theta) &= \frac{x_2}{\|\underline{v}_2\|}, & \sin(\psi + \theta) &= \frac{y_2}{\|\underline{v}_2\|}, \end{aligned}$$

cioè, per le formule di addizione di coseno e seno,

$$\begin{cases} \cos \psi \cos \theta - \sin \psi \sin \theta = \frac{x_2}{\|\underline{v}_2\|} \\ \sin \psi \cos \theta + \cos \psi \sin \theta = \frac{y_2}{\|\underline{v}_2\|}. \end{cases} \quad (9.6.1)$$

Si riguardi (9.6.1) come un sistema lineare nelle incognite  $\sin \theta$  e  $\cos \theta$ . Allora la matrice dei coefficienti ha determinante

$$\cos^2 \psi + \sin^2 \psi = 1.$$

Pertanto il sistema ha un'unica soluzione, che si può calcolare per esempio con la regola di Cramer, ottenendo:

$$\cos \theta = \frac{x_1 x_2 + y_1 y_2}{\|\underline{v}_1\| \cdot \|\underline{v}_2\|}, \quad \sin \theta = \frac{x_1 y_2 - y_1 x_2}{\|\underline{v}_1\| \cdot \|\underline{v}_2\|}.$$

Se si definisce il *prodotto scalare*  $\langle \underline{v}_1, \underline{v}_2 \rangle$  dei vettori  $\underline{v}_1$  e  $\underline{v}_2$  ponendo

$$\langle \underline{v}_1, \underline{v}_2 \rangle := x_1 x_2 + y_1 y_2,$$

si ha che

$$\cos \theta = \frac{\langle \underline{v}_1, \underline{v}_2 \rangle}{\|\underline{v}_1\| \cdot \|\underline{v}_2\|}.$$

In particolare, per ogni  $\underline{v} \in \mathcal{V}_0^2$  risulta

$$\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle}.$$

I vettori  $\underline{v}_1$  e  $\underline{v}_2$  sono ortogonali se e solo se  $\theta = \frac{\pi}{2}$ , cioè se e solo se

$$\cos \theta = \frac{\langle \underline{v}_1, \underline{v}_2 \rangle}{\|\underline{v}_1\| \cdot \|\underline{v}_2\|} = 0,$$

e quindi se e solo se  $\langle \underline{v}_1, \underline{v}_2 \rangle = x_1x_2 + y_1y_2 = 0$ . Analogamente  $\underline{v}_1$  e  $\underline{v}_2$  sono linearmente dipendenti se e solo se si trovano sulla stessa retta, quindi se e solo se  $\theta \in \{0, \pi\}$ , ovvero se e solo se  $\cos \theta = \pm 1$ . Ciò equivale a richiedere che risulti

$$\langle \underline{v}_1, \underline{v}_2 \rangle = \pm \|\underline{v}_1\| \cdot \|\underline{v}_2\|.$$

Analoghi discorsi possono essere fatti in  $\mathbb{R}^3$  (una volta che si sia identificato ogni vettore di  $\mathcal{V}_0^3$  con il vettore numerico delle sue componenti in una base  $\{i, j, k\}$  **ortonormale**, cioè costituita da vettori di lunghezza unitaria a due a due ortogonali), o più in generale in  $\mathbb{R}^n$ .

Sia  $\mathbb{R}^n$  l'usuale spazio vettoriale di dimensione  $n$  sul campo reale  $\mathbb{R}$ ; si dice **prodotto scalare canonico** in  $\mathbb{R}^n$  l'applicazione

$$\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$$

definita ponendo

$$\langle \underline{v}, \underline{w} \rangle := v_1w_1 + v_2w_2 + \cdots + v_nw_n$$

per ogni  $\underline{v} = (v_1, v_2, \dots, v_n), \underline{w} = (w_1, w_2, \dots, w_n) \in \mathbb{R}^n$ . La **norma** di un vettore  $\underline{v} = (v_1, v_2, \dots, v_n)$  di  $\mathbb{R}^n$  è poi definita da

$$\|\underline{v}\| := \sqrt{\langle \underline{v}, \underline{v} \rangle} = \sqrt{v_1^2 + v_2^2 + \dots + v_n^2}.$$

Si noti che per ogni  $\underline{v} \in \mathbb{R}^n$  risulta  $\langle \underline{v}, \underline{v} \rangle \geq 0$ , quindi la norma di un vettore è un numero reale non negativo.

Due rette dello spazio o del piano euclideo sono perpendicolari se e solo se lo sono i rispettivi vettori direttori. Da ciò segue subito che:

**9.6.1. Criterio di ortogonalità tra rette nello spazio.** Due rette aventi, in un assegnato riferimento ortogonale dello spazio, parametri direttori  $(l, m, n)$  e  $(l_1, m_1, n_1)$  rispettivamente, sono ortogonali se e solo se

$$\langle (l, m, n), (l_1, m_1, n_1) \rangle = ll_1 + mm_1 + nn_1 = 0.$$

Analoga condizione sussiste per le rette del piano euclideo.

**9.6.2. Criterio di ortogonalità tra rette nel piano.** Due rette aventi, in un assegnato riferimento ortogonale del piano, parametri direttori  $(l, m)$  e  $(l_1, m_1)$  rispettivamente, sono ortogonali se e solo se

$$\langle(l, m), (l_1, m_1)\rangle = ll_1 + mm_1 = 0.$$

**9.6.3. Esempio.** Siano  $r$ ,  $s$  e  $t$  le rette del piano aventi, in un fissato riferimento ortogonale, equazioni  $2x + 7y + 1 = 0$ ,  $7x - 2y + 5 = 0$  e  $5x + 2y - 3 = 0$  rispettivamente. I vettori direttori hanno componenti  $(-7, 2)$ ,  $(2, 7)$  e  $(-2, 5)$  rispettivamente. Pertanto, essendo  $\langle(-7, 2), (2, 7)\rangle = 0$ ,  $\langle(-7, 2), (-2, 5)\rangle \neq 0$  e  $\langle(-2, 5), (2, 7)\rangle \neq 0$  si ha che  $r$  ed  $s$  sono perpendicolari mentre non lo sono né  $r$  e  $t$  né  $s$  e  $t$ .

Il prodotto scalare canonico in  $\mathbb{R}^n$  gode delle seguenti proprietà:

**9.6.4. Per ogni  $\underline{v}, \underline{v}_1, \underline{v}_2, \underline{w}, \underline{w}_1, \underline{w}_2 \in \mathbb{R}^n$  e per ogni  $\alpha \in \mathbb{R}$  risulta:**

- (i)  $\langle \underline{v}_1 + \underline{v}_2, \underline{w} \rangle = \langle \underline{v}_1, \underline{w} \rangle + \langle \underline{v}_2, \underline{w} \rangle$ ;
- (ii)  $\langle \alpha \underline{v}, \underline{w} \rangle = \alpha \langle \underline{v}, \underline{w} \rangle$ ;
- (iii)  $\langle \underline{v}, \underline{w}_1 + \underline{w}_2 \rangle = \langle \underline{v}, \underline{w}_1 \rangle + \langle \underline{v}, \underline{w}_2 \rangle$ ;
- (iv)  $\langle \underline{v}, \alpha \underline{w} \rangle = \alpha \langle \underline{v}, \underline{w} \rangle$ ;
- (v)  $\langle \underline{v}, \underline{w} \rangle = \langle \underline{w}, \underline{v} \rangle$ .

Inoltre:

- (vi) per ogni  $\underline{v} \in \mathbb{R}^n \setminus \{\underline{0}\}$  esiste un vettore  $\underline{w} \in \mathbb{R}^n$  tale che  $\langle \underline{v}, \underline{w} \rangle \neq 0$ ;
- (vii) per ogni  $\underline{v} \in \mathbb{R}^n \setminus \{\underline{0}\}$  risulta  $\langle \underline{v}, \underline{v} \rangle > 0$ .

*Dimostrazione.* Esercizio. □

Le proprietà (i) – (iv) esprimono il fatto che il prodotto scalare canonico in  $\mathbb{R}^n$  è *bilineare*, la (v) che esso è *simmetrico*, la (vi) che è *non degenero*, la (vii) che è *definito positivo*. Semplicemente utilizzando queste proprietà si può provare che la *distanza* tra due punti  $P$  e  $Q$  di  $\mathbb{R}^n$ , definita ponendo

$$d(P, Q) := \|\overrightarrow{OP} - \overrightarrow{OQ}\|,$$

e l'*angolo* tra due vettori  $\underline{v}$  e  $\underline{w}$ , definito ponendo

$$\cos \theta := \frac{\langle \underline{v}, \underline{w} \rangle}{\|\underline{v}\| \cdot \|\underline{w}\|},$$

godono delle usuali note proprietà. Tale approccio consente di ricostruire la geometria euclidea in  $\mathbb{R}^n$  usando il prodotto scalare canonico. In realtà quest'ultimo

può essere sostituito da una qualunque applicazione  $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$  che verifichi le proprietà elencate in 9.6.4. Ciò suggerisce di introdurre le definizioni che seguono.

Sia  $V$  uno spazio vettoriale sul campo reale  $\mathbb{R}$ . Una **forma bilineare** su  $V$  è un'applicazione  $g : V \times V \rightarrow \mathbb{R}$  tale che:

- (i)  $g(\underline{v}_1 + \underline{v}_2, \underline{w}) = g(\underline{v}_1, \underline{w}) + g(\underline{v}_2, \underline{w})$  per ogni  $\underline{v}_1, \underline{v}_2, \underline{w} \in V$ ;
- (ii)  $g(\underline{v}, \underline{w}_1 + \underline{w}_2) = g(\underline{v}, \underline{w}_1) + g(\underline{v}, \underline{w}_2)$  per ogni  $\underline{v}, \underline{w}_1, \underline{w}_2 \in V$ ;
- (iii)  $g(\alpha \underline{v}, \underline{w}) = \alpha g(\underline{v}, \underline{w})$  per ogni  $\underline{v}, \underline{w} \in V$  e per ogni  $\alpha \in \mathbb{R}$ ;
- (iv)  $g(\underline{v}, \alpha \underline{w}) = \alpha g(\underline{v}, \underline{w})$  per ogni  $\underline{v}, \underline{w} \in V$  e per ogni  $\alpha \in \mathbb{R}$ .

Una forma bilineare  $g$  su  $V$  che sia **simmetrica**, ossia tale che  $g(\underline{v}, \underline{w}) = g(\underline{w}, \underline{v})$  per ogni  $\underline{v}, \underline{w} \in V$ , è detta **prodotto scalare** su  $V$ . In tal caso il numero reale  $g(\underline{v}, \underline{w})$  viene di solito denotato col simbolo  $\langle \underline{v}, \underline{w} \rangle$ , e  $g$  col simbolo  $\langle , \rangle$ .

**9.6.5.** Sia  $\langle , \rangle : V \times V \rightarrow \mathbb{R}$  un prodotto scalare in  $V$ . Allora l'insieme

$$V^\perp := \{\underline{v} \in V : \langle \underline{v}, \underline{w} \rangle = 0, \forall \underline{w} \in V\}$$

è un sottospazio di  $V$ , detto il **nucleo** del prodotto scalare.

*Dimostrazione.* Si noti innanzitutto che  $\underline{0} \in V^\perp$  in quanto  $\langle \underline{0}, \underline{w} \rangle = 0$  per ogni  $\underline{w} \in V$  essendo  $0 + \langle \underline{0}, \underline{w} \rangle = \langle \underline{0}, \underline{w} \rangle = \langle \underline{0} + \underline{0}, \underline{w} \rangle = \langle \underline{0}, \underline{w} \rangle + \langle \underline{0}, \underline{w} \rangle$ . Siano poi  $\underline{v}_1, \underline{v}_2 \in V^\perp$  e  $\alpha, \beta \in \mathbb{R}$ . Allora, per ogni  $\underline{w} \in V$ , si ha che  $\langle \alpha \underline{v}_1 + \beta \underline{v}_2, \underline{w} \rangle = \langle \alpha \underline{v}_1, \underline{w} \rangle + \langle \beta \underline{v}_2, \underline{w} \rangle = \alpha \langle \underline{v}_1, \underline{w} \rangle + \beta \langle \underline{v}_2, \underline{w} \rangle = \alpha 0 + \beta 0 = 0$ , e questo assicura che  $\alpha \underline{v}_1 + \beta \underline{v}_2 \in V^\perp$ . L'asserto segue allora da 8.2.2.  $\square$

Un prodotto scalare  $\langle , \rangle$  in  $V$  è detto **non degenero** se il suo nucleo è il sottospazio nullo, ossia se  $V^\perp = \{\underline{0}\}$ . Infine  $\langle , \rangle$  è detto **definito positivo** se  $\langle \underline{v}, \underline{v} \rangle > 0$  per ogni  $\underline{v} \in V \setminus \{\underline{0}\}$ . Si noti che un prodotto scalare definito positivo è sempre non degenero. Infatti in tal caso da  $\underline{v} \in V^\perp$  segue  $\langle \underline{v}, \underline{w} \rangle = 0$  per ogni  $\underline{w} \in V$ ; in particolare  $\langle \underline{v}, \underline{v} \rangle = 0$ , e quindi  $\underline{v} = \underline{0}$ .

Un qualunque spazio vettoriale sul campo reale che sia munito di un prodotto scalare definito positivo viene detto uno **spazio vettoriale metrico**. Se  $V$  è uno spazio vettoriale metrico allora la **norma** o **lunghezza** di un vettore  $\underline{v} \in V$  viene definita mediante la posizione

$$\|\underline{v}\| := \sqrt{\langle \underline{v}, \underline{v} \rangle}.$$

La **distanza** tra due vettori  $\underline{v}$  e  $\underline{w}$  di  $V$  è poi il numero reale

$$d(\underline{v}, \underline{w}) := \|\underline{w} - \underline{v}\|.$$

Si noti che

$$d(\underline{v}, \underline{v}) = 0$$

essendo  $\|\underline{v} - \underline{v}\| = \|\underline{0}\| = 0$ , e che

$$d(\underline{v}, \underline{w}) = d(\underline{w}, \underline{v}),$$

in quanto  $\|\underline{w} - \underline{v}\| = \sqrt{\langle \underline{w} - \underline{v}, \underline{w} - \underline{v} \rangle} = \sqrt{\langle \underline{v} - \underline{w}, \underline{v} - \underline{w} \rangle} = \|\underline{v} - \underline{w}\|$ .

**9.6.6.** Sia  $V$  uno spazio vettoriale metrico. Allora:

- (i)  $\|\underline{v}\| = 0$  se e solo se  $\underline{v} = \underline{0}$ ;
- (ii)  $\|\underline{v}\| > 0$  per ogni  $\underline{v} \in V \setminus \{\underline{0}\}$ ;
- (iii)  $\|\lambda \underline{v}\| = |\lambda| \cdot \|\underline{v}\|$  per ogni  $\underline{v} \in V$  e per ogni  $\lambda \in \mathbb{R}$ ,
$$\|\underline{v} + \underline{w}\|^2 = \|\underline{v}\|^2 + 2\langle \underline{v}, \underline{w} \rangle + \|\underline{w}\|^2 \text{ per ogni } \underline{v}, \underline{w} \in V;$$
- (iv)  $|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{v}\| \cdot \|\underline{w}\|$  per ogni  $\underline{v}, \underline{w} \in V$ ,  

$$|\langle \underline{v}, \underline{w} \rangle| = \|\underline{v}\| \cdot \|\underline{w}\| \text{ se e solo se } \{\underline{v}, \underline{w}\} \text{ è linearmente dipendente};$$
- (v)  $|\|\underline{v}\| - \|\underline{w}\|| \leq \|\underline{v} + \underline{w}\| \leq \|\underline{v}\| + \|\underline{w}\|$ , per ogni  $\underline{v}, \underline{w} \in V$ ;
- (vi)  $\langle \underline{v}, \underline{w} \rangle = \frac{1}{4}(\|\underline{v} + \underline{w}\|^2 - \|\underline{v} - \underline{w}\|^2)$  per ogni  $\underline{v}, \underline{w} \in V$ .

*Dimostrazione.* Per provare la (i) basta osservare che  $\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle} = 0$  se e solo se  $\langle \underline{v}, \underline{v} \rangle = 0$  e quindi se e solo se  $\underline{v} = \underline{0}$ .

La (ii) segue subito dal fatto che per ogni  $\underline{v} \in V \setminus \{\underline{0}\}$  risulta  $\langle \underline{v}, \underline{v} \rangle > 0$ , e quindi  $\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle} > 0$ .

Per quanto riguarda la (iii), si noti che per ogni  $\lambda \in \mathbb{R}$  e per ogni  $\underline{v} \in V$  riesce  $\|\lambda \underline{v}\| = \sqrt{\langle \lambda \underline{v}, \lambda \underline{v} \rangle} = \sqrt{\lambda^2 \langle \underline{v}, \underline{v} \rangle} = |\lambda| \sqrt{\langle \underline{v}, \underline{v} \rangle} = |\lambda| \cdot \|\underline{v}\|$ . Inoltre, per ogni  $\underline{v}, \underline{w} \in V$ , risulta  $\|\underline{v} + \underline{w}\|^2 = \langle \underline{v} + \underline{w}, \underline{v} + \underline{w} \rangle = \langle \underline{v}, \underline{v} + \underline{w} \rangle + \langle \underline{w}, \underline{v} + \underline{w} \rangle = \langle \underline{v}, \underline{v} \rangle + 2\langle \underline{v}, \underline{w} \rangle + \langle \underline{w}, \underline{w} \rangle = \|\underline{v}\|^2 + 2\langle \underline{v}, \underline{w} \rangle + \|\underline{w}\|^2$ .

Per provare la (iv) si osservi che l'asserto è ovvio se  $\underline{v} = \underline{0}$  oppure  $\underline{w} = \underline{0}$ ; sia dunque  $\underline{v} \neq \underline{0}$  e  $\underline{w} \neq \underline{0}$ , e siano  $\alpha, \beta \in \mathbb{R}$ . Allora  $0 \leq \|\alpha \underline{v} + \beta \underline{w}\|^2 = \langle \alpha \underline{v} + \beta \underline{w}, \alpha \underline{v} + \beta \underline{w} \rangle = \alpha^2 \|\underline{v}\|^2 + 2\alpha\beta \langle \underline{v}, \underline{w} \rangle + \beta^2 \|\underline{w}\|^2$ . Posto  $\alpha = \|\underline{w}\|^2$  e  $\beta = -\langle \underline{v}, \underline{w} \rangle$  si ottiene  $\|\underline{w}\|^4 \|\underline{v}\|^2 - 2\|\underline{w}\|^2 \langle \underline{v}, \underline{w} \rangle + \|\underline{w}\|^2 \langle \underline{v}, \underline{w} \rangle \geq 0$ , cioè  $|\langle \underline{v}, \underline{w} \rangle|^2 \leq \|\underline{w}\|^2 \|\underline{v}\|^2$  e infine  $|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{w}\| \cdot \|\underline{v}\|$ . L'uguaglianza vale se e solo se  $\alpha \underline{v} + \beta \underline{w} = \underline{0}$ , cioè se e solo se  $\{\underline{v}, \underline{w}\}$  è linearmente dipendente.

La (v) segue dal fatto che  $|\|\underline{v}\| - \|\underline{w}\||^2 = \|\underline{v}\|^2 + \|\underline{w}\|^2 - 2\|\underline{v}\| \cdot \|\underline{w}\| \leq \|\underline{v}\|^2 + \|\underline{w}\|^2 - 2|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{v}\|^2 + \|\underline{w}\|^2 + 2\langle \underline{v}, \underline{w} \rangle = \|\underline{v} + \underline{w}\|^2 \leq \|\underline{v}\|^2 + \|\underline{w}\|^2 + 2\|\underline{v}\| \cdot \|\underline{w}\| = (\|\underline{v}\| + \|\underline{w}\|)^2$ .

Infine la (vi) si dimostra osservando che  $\|\underline{v} + \underline{w}\|^2 = \|\underline{v}\|^2 + \|\underline{w}\|^2 + 2\langle \underline{v}, \underline{w} \rangle$  e  $\|\underline{v} - \underline{w}\|^2 = \|\underline{v}\|^2 + \|\underline{w}\|^2 - 2\langle \underline{v}, \underline{w} \rangle$ , pertanto  $\|\underline{v} + \underline{w}\|^2 - \|\underline{v} - \underline{w}\|^2 = 4\langle \underline{v}, \underline{w} \rangle$  e quindi  $\langle \underline{v}, \underline{w} \rangle = \frac{1}{4}(\|\underline{v} + \underline{w}\|^2 - \|\underline{v} - \underline{w}\|^2)$ .  $\square$

La diseguaglianza al primo rigo in (iv) di 9.6.6 è nota come **diseguaglianza di Cauchy-Schwarz**; la (v) come **diseguaglianza triangolare**. La diseguaglianza di Cauchy-Schwarz permette di definire l'**angolo** tra due vettori non nulli in qualunque spazio vettoriale metrico  $V$ . Siano infatti  $\underline{v}, \underline{w} \in V \setminus \{\underline{0}\}$ ; allora  $|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{v}\| \cdot \|\underline{w}\|$ , da cui

$$-1 \leq \frac{\langle \underline{v}, \underline{w} \rangle}{\|\underline{v}\| \cdot \|\underline{w}\|} \leq 1,$$

ed è possibile definire angolo tra  $\underline{v}$  e  $\underline{w}$  l'unico  $\theta \in [0, \pi]$  tale che

$$\cos \theta = \frac{\langle \underline{v}, \underline{w} \rangle}{\|\underline{v}\| \cdot \|\underline{w}\|}.$$

Vettori  $\underline{v}$  e  $\underline{w}$  di uno spazio metrico  $V$  si dicono **ortogonali** se  $\langle \underline{v}, \underline{w} \rangle = 0$ . Dalla seconda uguaglianza in (iii) di 9.6.6 segue subito che se  $\underline{v}$  e  $\underline{w}$  sono ortogonali allora  $\|\underline{v} + \underline{w}\|^2 = \|\underline{v}\|^2 + \|\underline{w}\|^2$ : ciò permette di ritrovare il ben noto teorema di Pitagora.

## Esercizi

**Esercizio 9.6.1.** Fissato un riferimento ortonormale del piano, si provi che le rette aventi equazioni cartesiane  $3x - 2y + 7 = 0$  e  $4x + 6y + 1 = 0$  sono ortogonali.

**Esercizio 9.6.2.** Fissato un riferimento ortonormale del piano si scriva l'equazione cartesiana della retta  $r$  ortogonale alla retta di equazione  $ax + by + c = 0$  e che passa per l'origine del riferimento.

**Esercizio 9.6.3.** Fissato un riferimento ortonormale dello spazio euclideo, si considerino le rette  $r$  e  $r_k$  (con  $k \in \mathbb{R}$ ) di rispettive equazioni parametriche

$$\begin{cases} x = 1 + 3t \\ y = -4 + 2t \\ z = -5t, \end{cases} \quad \begin{cases} x = kt' \\ y = 3 + (2 - k)t' \\ z = 0. \end{cases}$$

Per quali valori di  $k$  le due rette sono perpendicolari? Esistono valori di  $k$  per i quali le due rette sono parallele?

**Esercizio 9.6.4.** Si dimostri 9.6.4.

## 9.7 Esercizi di riepilogo

**Esercizio 9.7.1.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento ortonormale dello spazio euclideo  $\mathcal{E}^3$ . Si considerino il piano  $\pi$  di equazione cartesiana  $3x - 2y + 5z - 1 = 0$ , e la retta  $r$  di equazioni parametriche

$$\begin{cases} x = -1 + 7t \\ y = -2t \\ z = 5 + t. \end{cases}$$

- (i) Si determinino le coordinate del punto di intersezione  $P$  del piano  $\pi$  con la retta  $r$ .
- (ii) Si scrivano le equazioni parametriche della retta  $OP$  e si stabilisca se essa è ortogonale a  $r$ .

- (iii) Nel riferimento  $\mathcal{RA}(O, \underline{i}, \underline{j})$  indotto sul piano  $xy$ , si scriva l'equazione cartesiana della circonferenza  $\Gamma$  di centro il punto  $Q$  di coordinate  $(-1, 0)$  e raggio  $\|\overrightarrow{OP}\|$ .
- (iv) Si studi l'intersezione della circonferenza  $\Gamma$  con la retta  $s$ , dove  $s$  è l'intersezione del piano  $\pi$  con il piano  $xy$ .

**Esercizio 9.7.2.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j})$  un riferimento ortonormale del piano euclideo  $\mathcal{E}^2$  e si consideri la circonferenza  $\Gamma_a$  di equazione

$$x^2 + y^2 + 2ax - 4y + 3a = 0,$$

dove  $a$  è un parametro reale.

- (i) Si determinino le coordinate del centro di  $\Gamma_a$  e il suo raggio.
- (ii) Si stabilisca per quali valori di  $a$  la circonferenza  $\Gamma_a$  passa per l'origine del riferimento.
- (iii) Si studi, in funzione di  $a$ , l'intersezione di  $\Gamma_a$  con l'asse  $y$ .
- (iv) Si scrivano le equazioni parametriche della retta passante per il centro di  $\Gamma_a$  e perpendicolare alla retta di equazione cartesiana  $x - 2y + 1 = 0$ .

**Esercizio 9.7.3.** In un fissato riferimento ortonormale  $\mathcal{RA}(O, \underline{i}, \underline{j})$  di  $\mathcal{E}^2$  si scrivano le equazioni cartesiane della circonferenza  $\Gamma_k$  di centro il punto  $P_k$  di coordinate  $(k, 2 - k)$  e raggio  $\frac{1}{2}$  (dove  $k$  è un parametro reale), e della retta  $r$  per i punti  $A$  e  $B$  di coordinate  $(0, 2)$  e  $(2, 0)$  rispettivamente, e si studi, al variare di  $k \in \mathbb{R}$ , l'insieme  $\Gamma_k \cap r$ .

**Esercizio 9.7.4.** Sia  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  un riferimento affine dello spazio euclideo  $\mathcal{E}^3$  e siano  $A, B, C_h$  i punti di coordinate  $(1, -1, 2)$ ,  $(0, 3, -1)$  e  $(-2, h, -7)$  rispettivamente, dove  $h$  è un parametro reale.

- (i) Si stabilisca per quali valori di  $h$  i punti  $A, B$  e  $C_h$  sono allineati.
- (ii) Posto  $h = 0$ , si scrivano le equazioni parametriche del piano  $\pi$  per i punti  $A, B$  e  $C_0$ .
- (iii) Si consideri il piano  $\pi'$  di equazioni parametriche

$$\begin{cases} x = 2 - \alpha \\ y = 1 + 4\alpha - 11\beta \\ z = 3 - 3\alpha \end{cases}$$

e si stabilisca se i piani  $\pi$  e  $\pi'$  sono paralleli.

**Esercizio 9.7.5.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, \underline{j}, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si considerino le rette  $r_k$  ed  $s$  di rispettive equazioni parametriche

$$\begin{cases} x = 1 + kt \\ y = -7t \\ z = -2 + (1 - k)t \end{cases}$$

$$\begin{cases} x = 5 - 2t' \\ y = 1 + 14t' \\ z = 3, \end{cases}$$

dove  $k$  è un parametro reale.

- (i) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono parallele.
- (ii) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono sghembe.
- (iii) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono incidenti.
- (iv) Sia  $\pi$  il piano di equazioni parametriche

$$\begin{cases} x = 1 + 3\alpha - 2\beta \\ y = -2 + \beta \\ z = 5 - \alpha + 5\beta. \end{cases}$$

Si determinino gli eventuali valori del parametro  $k$  per i quali la retta  $r_k$  è parallela al piano  $\pi$ .

**Esercizio 9.7.6.** In un riferimento affine  $\mathcal{RA}(O, \underline{i}, j, \underline{k})$  dello spazio euclideo  $\mathcal{E}^3$  si considerino le rette  $r_k$  ed  $s$  di rispettive equazioni parametriche

$$\begin{cases} x = -1 + kt \\ y = -10t \\ z = 3 + (k+2)t \end{cases} \quad \begin{cases} x = 3 + 4t' \\ y = 1 + 20t' \\ z = 0, \end{cases}$$

dove  $k$  è un parametro reale.

- (i) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono parallele.
- (ii) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono sghembe.
- (iii) Si determinino gli eventuali valori del parametro  $k$  per i quali le rette  $r_k$  ed  $s$  sono incidenti.
- (iv) Sia  $\pi$  il piano di equazioni parametriche

$$\begin{cases} x = 1 + \alpha \\ y = -2 + \alpha + \beta \\ z = 3 - \alpha + 2\beta. \end{cases}$$

Si determinino gli eventuali valori del parametro  $k$  per i quali la retta  $r_k$  è parallela al piano  $\pi$ .

# 10

## Reticoli, grafi, alberi

### 10.1 Reticoli

Siano  $L$  un insieme non vuoto e  $\leq$  una relazione d'ordine in  $L$ . L'insieme ordinato  $(L, \leq)$  è detto **reticolo** se per ogni  $x, y \in L$  esistono  $\sup_L\{x, y\}$  e  $\inf_L\{x, y\}$ . In tal caso, ponendo  $x \vee y := \sup_L\{x, y\}$  e  $x \wedge y := \inf_L\{x, y\}$ , restano definite due operazioni interne  $\vee$  e  $\wedge$  in  $L$ , dette rispettivamente **unione reticolare** e **intersezione reticolare**. Si verifica agevolmente che per ogni  $x, y, z \in L$  si ha:

$$x \vee x = x = x \wedge x, \quad (10.1.1)$$

$$x \vee y = y \vee x, \quad (10.1.2)$$

$$x \wedge y = y \wedge x,$$

$$x \vee (y \vee z) = (x \vee y) \vee z, \quad (10.1.3)$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z,$$

$$x \vee (x \wedge y) = x = x \wedge (x \vee y). \quad (10.1.4)$$

Le uguaglianze (10.1.2) e (10.1.3) esprimono il fatto che le operazioni  $\vee$  e  $\wedge$  sono commutative e associative; le (10.1.1) che esse sono anche **iterative**; infine le (10.1.4) sono dette **leggi di assorbimento**.

**10.1.1.** Sia  $L$  un insieme non vuoto dotato di operazioni interne  $\vee$  e  $\wedge$  che verificino (10.1.1) – (10.1.4). Allora  $y = x \vee y$  se e solo se  $x = x \wedge y$ . Inoltre la posizione

$$x \leq y \iff x = x \wedge y$$

definisce una relazione d'ordine in  $L$ , e la coppia  $(L, \leq)$  è un reticolo in cui  $x \vee y = \sup_L\{x, y\}$  e  $x \wedge y = \inf_L\{x, y\}$  per ogni  $x, y \in L$ .

*Dimostrazione.* Se  $y = x \vee y$ , la (10.1.4) assicura che  $x = x \wedge (x \vee y) = x \wedge y$ ; analogamente da  $x = x \wedge y$  segue  $y = x \vee y$ . Pertanto  $y = x \vee y$  se e solo se  $x = x \wedge y$ .

Per ogni  $x \in L$ , la (10.1.1) garantisce che  $x \leq x$ . Se poi  $x, y \in L$  sono tali che  $x \leq y$  e  $y \leq x$  allora  $x = x \wedge y = y \wedge x = y$ . Infine se  $x, y, z \in L$  verificano

$x \leq y$  e  $y \leq z$  allora risulta  $x = x \wedge y$  e  $y = y \wedge z$ , da cui  $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$ , il che significa  $x \leq z$ . Pertanto  $\leq$  è una relazione d'ordine in  $L$ .

Si ha  $x \vee (x \vee y) = (x \vee x) \vee y = x \vee y$ , cioè, per quanto provato prima,  $x \wedge (x \vee y) = x$ , e quindi  $x \leq x \vee y$ . Analogamente  $y \leq x \vee y$ , pertanto  $x \vee y$  è un maggiorante di  $\{x, y\}$ . Sia ora  $z$  un qualsiasi maggiorante di  $\{x, y\}$ . Allora  $x \leq z$  e  $y \leq z$ , e si ha anche  $x \vee z = z = y \vee z$ . Ne segue che  $z \vee (x \vee y) = (z \vee x) \vee y = z \vee y = z$ , pertanto  $x \vee y \leq z$ . Tutto ciò prova che  $x \vee y = \sup_L \{x, y\}$ .

Infine si verifica facilmente che  $(x \wedge y) \wedge x = x \wedge y$ , quindi  $x \wedge y \leq x$ , e analogamente  $(x \wedge y) \wedge y = x \wedge y$ , da cui  $x \wedge y \leq y$ . Pertanto  $x \wedge y$  è un minorante di  $\{x, y\}$ . Se  $z$  è un minorante di  $\{x, y\}$ , da  $z \leq x$  e  $z \leq y$  segue  $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$ , quindi  $z \leq x \wedge y$ . Ciò dimostra che  $x \wedge y = \inf_L \{x, y\}$ , e l'asserto è completamente provato.  $\square$

In virtù di 10.1.1 è del tutto equivalente pensare a un reticolo come a un insieme ordinato in cui esistono estremi superiore e inferiore di ogni sottoinsieme di ordine 2, oppure a una struttura algebrica dotata di due operazioni interne iterative, commutative e associative che verifichino le leggi di assorbimento. Si osservi che la (10.1.1) è conseguenza della (10.1.4), essendo  $x \vee x = (x \wedge (x \vee x)) \vee x = x \vee (x \wedge (x \vee x)) = x$ , e analogamente  $x \wedge x = x$ .

**10.1.2. Principio di dualità dei reticolati.** *Sia  $P$  un enunciato in cui intervengono le operazioni  $\vee$  e  $\wedge$ , e sia  $P^*$  l'enunciato che si ottiene da  $P$  scambiando tra loro  $\vee$  e  $\wedge$ . Se  $P$  è valido per ogni reticolo, allora anche  $P^*$  è valido per ogni reticolo.*

*Dimostrazione.* Basta tener presente che nella definizione di reticolo come struttura algebrica le operazioni  $\vee$  e  $\wedge$  si comportano in maniera simmetrica rispetto alle proprietà (10.1.1) – (10.1.4).  $\square$

Gli eventuali massimo e minimo di un reticolo vengono di solito denotati rispettivamente con 1 e 0. Nel seguito, laddove ciò non generi confusione, un reticolo  $(L, \leq)$  verrà denotato semplicemente con  $L$ . Un sottoinsieme  $M$  di  $L$  si dice un **sottoreticolo** di  $L$  se per ogni  $x, y \in M$  risulta  $x \vee y \in M$  e  $x \wedge y \in M$ . Ovviamente tra i sottoreticolari di  $L$  vi è  $L$  stesso, un sottoreticolo  $M \neq L$  è un **sottoreticolo proprio**. Dalla definizione è evidente che  $\{x\}$  è un sottoreticolo di  $L$ , per ogni  $x \in L$ . Inoltre se  $M$  è un sottoreticolo di  $L$  e  $N$  è un sottoreticolo di  $M$ , allora  $N$  è un sottoreticolo di  $L$ . Infine se  $\Omega$  è un insieme non vuoto di sottoreticolari di  $L$ , anche  $\bigcap_{M \in \Omega} M$  è un sottoreticolo di  $L$ .

**10.1.3.** *Sia  $(L, \leq)$  un insieme ordinato, e siano  $x, y \in L$ . Sono equivalenti:*

- (i)  $\sup_L \{x, y\} = y$ ;
- (ii)  $x \leq y$ ;
- (iii)  $\inf_L \{x, y\} = x$ .

*Dimostrazione.* Per provare l'equivalenza tra (i) e (ii) basta osservare che se  $\sup_L\{x, y\} = y$  allora  $y$  è un maggiorante dell'insieme  $\{x, y\}$ , quindi  $x \leq y$ . Viceversa, se  $x \leq y$ , allora  $y$  è il massimo dell'insieme  $\{x, y\}$ , pertanto  $\sup_L\{x, y\} = y$  (vedi 2.4.15).

L'equivalenza tra (ii) e (iii) è del tutto analoga.  $\square$

Per la 10.1.3, nel verificare se un insieme ordinato è un reticolo basta prendere in considerazione soltanto le coppie costituite da elementi non confrontabili.

#### 10.1.4. *Ogni insieme totalmente ordinato è un reticolo.*

*Dimostrazione.* Sia  $(L, \leq)$  un insieme totalmente ordinato. Allora due elementi di  $L$  sono sempre confrontabili, e l'asserto segue da 10.1.3.  $\square$

**10.1.5. Esempio.** Sia  $S$  un insieme, e si consideri l'insieme ordinato  $(\mathcal{P}(S), \subseteq)$ , dove  $\mathcal{P}(S)$  è l'insieme delle parti di  $S$  e  $\subseteq$  è la usuale relazione d'inclusione insiemistica. Si vede agevolmente che  $\mathcal{P}(S)$  è un reticolo, detto il **reticolo delle parti** di  $S$ . Esso ha  $S$  come massimo e  $\emptyset$  come minimo. Per ogni  $X, Y \in \mathcal{P}(S)$  risulta  $X \vee Y = X \cup Y$  e  $X \wedge Y = X \cap Y$ . È anche evidente che i sottoinsiemi finiti di  $S$  costituiscono un sottoreticolo di  $(\mathcal{P}(S), \subseteq)$ , che risulta privo di massimo se  $S$  è infinito.

**10.1.6. Esempio.** L'insieme parzialmente ordinato  $(\mathbb{N}_0, |)$ , dove  $|$  denota la relazione del “divide”, è un reticolo, detto il **reticolo dei numeri naturali**. Esso ha il numero 0 come massimo e il numero 1 come minimo. Per ogni  $x, y \in \mathbb{N}_0$  risulta  $x \vee y = \text{mcm}(x, y)$  e  $x \wedge y = \text{MCD}(x, y)$ . È anche evidente che per ogni  $n \in \mathbb{N}_0$  l'insieme dei divisori positivi di  $n$  costituisce un sottoreticolo di  $(\mathbb{N}_0, |)$ , avente  $n$  come massimo e 1 come minimo.

**10.1.7. Esempio.** Sia  $G$  un gruppo, e si denoti con  $L(G)$  l'insieme dei sottogruppi di  $G$ . Denotata con  $\subseteq$  l'usuale inclusione, l'insieme ordinato  $(L(G), \subseteq)$  è un reticolo, detto il **reticolo dei sottogruppi** di  $G$ . Esso ha  $G$  come massimo e  $\{1\}$  come minimo. Per ogni  $H, K \in L(G)$  risulta  $H \vee K = \langle H, K \rangle$  e  $H \wedge K = H \cap K$ . Se il gruppo  $G$  è infinito, l'insieme dei sottogruppi finiti di  $G$  non è, in generale, un sottoreticolo di  $L(G)$ . Invece l'insieme dei sottogruppi normali di  $G$  è sempre un sottoreticolo di  $L(G)$ .

**10.1.8. Esempio.** Sia  $S$  uno spazio vettoriale su un campo  $F$ , e si denoti con  $L$  l'insieme dei sottospazi di  $S$ . Allora  $(L, \subseteq)$  è un reticolo, detto il **reticolo dei sottospazi** di  $S$ . Esso ha  $S$  come massimo e  $\{0\}$  come minimo. Per ogni  $H, K \in L$  risulta  $H \vee K = H + K$  e  $H \wedge K = H \cap K$ .

### Esercizi

**Esercizio 10.1.1.** Si dimostri quanto affermato in 10.1.5 – 10.1.8.

**Esercizio 10.1.2.** Sia  $A = \{n \in \mathbb{N} : n|50\}$  l'insieme dei divisori positivi di 50. Si disegni il diagramma di Hasse del reticolo  $(A, |)$ , e si determinino  $(5 \vee 2) \wedge 25$ ,  $(1 \wedge 2) \vee 25$ .

**Esercizio 10.1.3.** Sia  $B = \{n \in \mathbb{N} : n|81\}$  l'insieme dei divisori positivi di 81. Si disegni il diagramma di Hasse del reticolo  $(B, |)$ , e si determinino  $(9 \vee 27) \wedge 3$ ,  $(1 \wedge 9) \vee 81$ .

**Esercizio 10.1.4.** Sia  $C = \{n \in \mathbb{N} : n|165\}$  l'insieme dei divisori positivi di 165. Si disegni il diagramma di Hasse del reticolo  $(C, |)$ , e si determinino  $(55 \vee 5) \wedge 11$ ,  $(5 \wedge 11) \vee 33$ .

**Esercizio 10.1.5.** Sia  $D = \{n \in \mathbb{N} : n|1573\}$  l'insieme dei divisori positivi di 1573. Si disegni il diagramma di Hasse del reticolo  $(D, |)$ , e si determinino  $(143 \vee 121) \wedge 13$ ,  $(143 \wedge 11) \vee 13$ .

**Esercizio 10.1.6.** Si dimostri che un reticolo non può possedere più di un elemento massimale. Se questo esiste, esso coincide col massimo del reticolo.

*Svolgimento.* Sia  $a$  un elemento massimale del reticolo  $(L, \leq)$ . Per ogni  $x \in L$  risulta  $a \leq x \vee a$ , quindi  $a = x \vee a$  per la massimalità di  $a$ , e da 10.1.3 segue  $x \leq a$ . Pertanto  $a$  è il massimo di  $L$ . L'unicità del massimo prova allora l'unicità di  $a$  come elemento massimale in  $L$ .

**Esercizio 10.1.7.** Si dimostri che un reticolo non può possedere più di un elemento minimale. Se questo esiste, esso coincide col minimo del reticolo.

**Esercizio 10.1.8.** Si consideri la relazione  $\sqsubseteq$  definita nell'insieme  $\mathbb{N}_0$  ponendo

$$a \sqsubseteq b \iff a = b \text{ oppure } 2a < b,$$

dove  $<$  denota l'usuale ordine stretto su  $\mathbb{N}_0$ . Si verifichi che  $\sqsubseteq$  è una relazione d'ordine in  $\mathbb{N}_0$ . Si stabilisca poi se l'insieme ordinato  $(\mathbb{N}_0, \sqsubseteq)$  è un reticolo.

**Esercizio 10.1.9.** Nell'insieme  $V = \{5h + 1 : h \in \mathbb{Z}\}$  si consideri la relazione  $\sqsubseteq$  definita ponendo

$$5h + 1 \sqsubseteq 5k + 1 \iff h = k \text{ oppure } |h| < |k|,$$

dove  $<$  indica la relazione d'ordine usuale in  $\mathbb{N}_0$ .

- (i) Si verifichi che  $\sqsubseteq$  è una relazione d'ordine in  $V$ .
- (ii) Si stabilisca se  $(V, \sqsubseteq)$  è un reticolo.
- (iii) Sia  $W = \{-19, -14, -9, -4, 1, 6, 11, 16, 21\}$ . Si disegni il diagramma di Hasse di  $(W, \sqsubseteq)$ .

**Esercizio 10.1.10.** Un reticolo  $L$  è **completo** se per ogni sottoinsieme non vuoto  $X$  di  $L$  esistono  $\sup_L X$  e  $\inf_L X$ . Si dimostri che ogni reticolo finito è completo.

*Suggerimento.* Se  $X$  è un qualunque sottoinsieme finito e non vuoto di un reticolo  $L$ , non necessariamente finito, si provi che esistono  $\sup_L X$  e  $\inf_L X$ , ragionando per induzione su  $|X|$ .

**Esercizio 10.1.11.** Si dimostri che per ogni insieme  $S$  il reticolo  $\mathcal{P}(S)$  delle parti di  $S$  (vedi Esempio 10.1.5) è completo, mentre il sottoreticolo di  $\mathcal{P}(S)$  costituito dai sottoinsiemi finiti di  $S$  è completo se e solo se  $S$  è finito.

**Esercizio 10.1.12.** Si dimostri che il reticolo dei numeri naturali (vedi Esempio 10.1.6) è completo.

**Esercizio 10.1.13.** Si dimostri che il reticolo dei sottogruppi di un gruppo e quello dei suoi sottogruppi normali (vedi Esempio 10.1.7) sono completi.

**Esercizio 10.1.14.** Si dimostri che il reticolo dei sottospazi di uno spazio vettoriale (vedi Esempio 10.1.8) è completo.

**Esercizio 10.1.15.** Sia  $L$  il reticolo dei sottospazi di uno spazio vettoriale  $S$  su un campo  $F$  (vedi Esempio 10.1.8). Si dimostri che i sottospazi di  $S$  di dimensione finita su  $F$  costituiscono un sottoreticolo di  $L$ , che risulta completo se e solo se la dimensione di  $S$  su  $F$  è finita.

**Esercizio 10.1.16.** Si dimostri che ogni reticolo completo possiede massimo e minimo.

**Esercizio 10.1.17.** Sia  $(L, \leq)$  un insieme ordinato dotato di massimo 1. Si provi che se per ogni sottoinsieme non vuoto  $X$  di  $L$  esiste  $\inf_L X$ , allora  $L$  è un reticolo completo.

*Svolgimento.* Siano  $x, y \in L$ . Allora per ipotesi esiste  $\inf_L \{x, y\}$ . Inoltre certamente l'insieme  $Y$  dei maggioranti di  $\{x, y\}$  in  $L$  è non vuoto, contenendo almeno l'elemento 1. Per ipotesi esiste allora  $\inf_L Y$ . Ma per definizione tale elemento è proprio  $\sup_L \{x, y\}$ . Quindi  $L$  è un reticolo. Per provarne la completezza resta da mostrare che per ogni sottoinsieme non vuoto  $X$  di  $L$  esiste  $\sup_L X$ . Sia  $X$  un sottoinsieme non vuoto di  $L$ . Per ipotesi, l'insieme  $T$  dei maggioranti di  $X$  in  $L$  è non vuoto, contenendo almeno l'elemento 1. Per ipotesi esiste allora  $\inf_L T$ . Ma per definizione tale elemento è proprio  $\sup_L X$ .

**Esercizio 10.1.18.** Sia  $(L, \leq)$  un insieme ordinato dotato di minimo 0. Si provi che se per ogni sottoinsieme non vuoto  $X$  di  $L$  esiste  $\sup_L X$ , allora  $L$  è un reticolo completo.

**Esercizio 10.1.19.** Si dimostri che se  $a, b, c$  e  $d$  sono elementi di un reticolo  $L$  tali che  $a \leq b$  e  $c \leq d$  allora  $a \vee c \leq b \vee d$ . Si utilizzi poi il principio di dualità dei reticolati (vedi 10.1.2) per dimostrare che se  $a \geq b$  e  $c \geq d$  allora  $a \wedge c \geq b \wedge d$ .

## 10.2 Omomorfismi di reticolati

Siano  $(L, \leq)$  e  $(M, \sqsubseteq)$  reticolati. Un'applicazione  $f : L \rightarrow M$  è detta un **omomorfismo di reticolati** se per ogni  $x, y \in L$  risulta  $f(x \vee y) = f(x) \vee f(y)$  e  $f(x \wedge y) = f(x) \wedge f(y)$ . È immediato verificare che ogni applicazione costante di  $L$  in  $M$  è un omomorfismo di reticolati. Un omomorfismo biettivo di reticolati è detto un **isomorfismo di reticolati**. I reticolati  $L$  ed  $M$  si dicono **isomorfi** se esiste un isomorfismo di reticolati tra di essi.

**10.2.1.** Siano  $(L, \leq)$  e  $(M, \sqsubseteq)$  reticolati,  $f : L \rightarrow M$  un omomorfismo di reticolati. Allora:

- (i)  $f(L)$  è un sottoreticolo di  $M$ ;
- (ii) se  $\max L = 1$  allora  $\max f(L) = f(1)$ ;
- (iii) se  $\min L = 0$  allora  $\min f(L) = f(0)$ ;
- (iv)  $f$  è un omomorfismo di insiemi ordinati;
- (v) se  $f$  è biettiva,  $f^{-1} : M \rightarrow L$  è un omomorfismo di reticolati.

*Dimostrazione.* (i) Per ogni  $f(x), f(y) \in f(L)$ , essendo  $f(x \vee y) = f(x) \vee f(y)$  e  $f(x \wedge y) = f(x) \wedge f(y)$ , si ha che  $f(x) \vee f(y), f(x) \wedge f(y) \in f(L)$ .

(ii) Se  $\max L = 1$  allora per ogni  $x \in L$  risulta  $x \leq 1$ , cioè  $x \vee 1 = 1$ , da cui  $f(x) \vee f(1) = f(x \vee 1) = f(1)$ . Ma ciò implica  $f(x) \sqsubseteq f(1)$  per ogni  $f(x) \in f(L)$ , pertanto  $\max f(L) = f(1)$ .

(iii) Se  $\min L = 0$  allora per ogni  $x \in L$  risulta  $0 \leq x$ , cioè  $x \wedge 0 = 0$ , da cui  $f(x) \wedge f(0) = f(x \wedge 0) = f(0)$ . Ma ciò implica  $f(0) \sqsubseteq f(x)$  per ogni  $f(x) \in f(L)$ , pertanto  $\min f(L) = f(0)$ .

(iv) Se  $x \leq y$  allora  $x = x \wedge y$  per la 10.1.3, da cui  $f(x) = f(x \wedge y) = f(x) \wedge f(y)$ , quindi  $f(x) \leq f(y)$ .

(v) Ovvia. □

La (iv) di 10.2.1 non si inverte: esistono infatti reticolati  $(L, \leq)$  e  $(M, \sqsubseteq)$  e omomorfismi di insiemi ordinati  $f : L \rightarrow M$  che non sono omomorfismi di reticolati.

**10.2.2. Esempio.** Sia  $S = \{a, b, c\}$  un insieme con 3 elementi. Si consideri poi il sottoinsieme  $L = \{\emptyset, \{a\}, \{b\}, S\}$  di  $\mathcal{P}(S)$ , ordinato per inclusione. Ovviamente  $(L, \subseteq)$  è un reticolo, e  $\{a\} \vee \{b\} = S$ . L'applicazione  $f : X \in L \mapsto X \in \mathcal{P}(S)$  è un omomorfismo di insiemi ordinati, in quanto se  $X, Y \in L$  e  $X \subseteq Y$  allora  $f(X) = X \subseteq Y = f(Y)$ . Ma  $f$  non è un omomorfismo di reticolati, giacché  $f(\{a\} \vee \{b\}) = f(S) = S$  mentre  $f(\{a\}) \vee f(\{b\}) = f(\{a\}) \cup f(\{b\}) = \{a, b\}$ .

## Esercizi

**Esercizio 10.2.1.** Si dimostri che un'applicazione tra reticolati è un isomorfismo di reticolati se e solo se essa è un isomorfismo di insiemi ordinati.

**Esercizio 10.2.2.** Si dimostri che reticolati isomorfi hanno lo stesso diagramma di Hasse.

**Esercizio 10.2.3.** Con  $S = \{1, 2, 3, 4\}$ , si consideri il reticolo  $(\mathcal{P}(S), \subseteq)$  delle parti di  $S$  (vedi Esempio 10.1.5). Sia poi  $W$  l'insieme dei numeri naturali da 0 a 10, ordinato con l'ordinamento naturale  $\leq$  di  $\mathbb{N}_0$ . Si dimostri che l'applicazione  $f : \mathcal{P}(S) \rightarrow \mathbb{N}_0$  definita ponendo

$$f(A) := \begin{cases} 0 & \text{se } A = \emptyset \\ \sum_{n \in A} n & \text{se } A \neq \emptyset \end{cases}$$

è un omomorfismo tra gli insiemi ordinati  $(\mathcal{P}(S), \subseteq)$  e  $(W, \leq)$ . Si provi poi che  $f$  non è un omomorfismo di reticolli.

### 10.3 Reticoli distributivi

Un reticolo  $(L, \leq)$  è detto **distributivo** se ciascuna delle due operazioni  $\vee$  e  $\wedge$  è distributiva rispetto all'altra. Ossia se, per ogni  $x, y, z \in L$ , risulta:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \quad (10.3.1)$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z). \quad (10.3.2)$$

Il risultato che segue mostra che nella precedente definizione è sufficiente richiedere che valga una sola tra (10.3.1) e (10.3.2).

**10.3.1.** In un qualunque reticolo  $(L, \leq)$  la (10.3.1) e la (10.3.2) sono equivalenti.

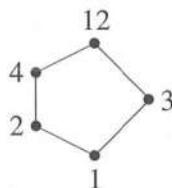
*Dimostrazione.* Si supponga valida la (10.3.1). Allora per ogni  $x, y, z \in L$  si ha

$$\begin{aligned} (x \wedge y) \vee (x \wedge z) &= ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) && \text{per (10.3.1)} \\ &= x \wedge ((x \wedge y) \vee z) && \text{per (10.1.2) e (10.1.4)} \\ &= x \wedge ((z \vee x) \wedge (z \vee y)) && \text{per (10.1.2) e (10.3.1)} \\ &= (x \wedge (z \vee x)) \wedge (z \vee y) && \text{per (10.1.3)} \\ &= x \wedge (y \vee z) && \text{per (10.1.4) e (10.1.2).} \end{aligned}$$

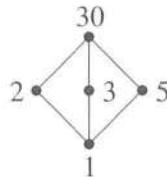
Pertanto la (10.3.1) implica la (10.3.2). Viceversa, per il principio di dualità (vedi 10.1.2), la (10.3.2) implica la (10.3.1).  $\square$

Dalla definizione segue subito che ogni sottoreticolo di un reticolo distributivo è distributivo. Utilizzando le proprietà di unione e intersezione tra insiemi si verifica facilmente che il reticolo delle parti di un insieme è distributivo (vedi Esercizio 10.3.1). Facendo poi uso delle proprietà del minimo comune multiplo e del massimo comune divisore tra naturali si può mostrare che anche il reticolo dei numeri naturali è distributivo (vedi Esempio 10.3.2). Esistono però reticolli non distributivi.

**10.3.2. Esempio.** Sia  $L = \{1, 2, 3, 4, 12\}$ , e sia  $|$  la relazione d'ordine indotta su  $L$  dalla relazione del “divide” in  $\mathbb{N}_0$ . Si verifica subito che  $(L, |)$  è un reticolo. Inoltre  $2 \vee (3 \wedge 4) = 2 \vee 1 = 2$  mentre  $(2 \vee 3) \wedge (2 \vee 4) = 12 \wedge 4 = 4$ . Pertanto  $(L, |)$  non è distributivo. Il suo diagramma di Hasse è il seguente:



**10.3.3. Esempio.** Sia  $L = \{1, 2, 3, 5, 30\}$ , e sia  $|$  la relazione d'ordine indotta su  $L$  dalla relazione del “divide” in  $\mathbb{N}_0$ . Si verifica subito che  $(L, |)$  è un reticolo. Inoltre  $2 \vee (3 \wedge 5) = 2 \vee 1 = 2$  mentre  $(2 \vee 3) \wedge (2 \vee 5) = 30 \wedge 30 = 30$ . Pertanto  $(L, |)$  non è distributivo. Il suo diagramma di Hasse è il seguente:



Un reticolo che abbia per diagramma di Hasse quello dell’Esempio 10.3.2 viene detto **pentagonale**; un reticolo che abbia per diagramma di Hasse quello dell’Esempio 10.3.3 viene detto **trirettangolo**. Risulta quindi evidente che ogni reticolo che possegga un sottoreticolo pentagonale o trirettangolo è non distributivo. Di più, si potrebbe provare che:

**10.3.4.** *Un reticolo è distributivo se e solo se è privo di sottoreticolli pentagonali e di sottoreticolli trirettangoli.*

**10.3.5. Corollario.** *Ogni insieme totalmente ordinato è un reticolo distributivo.*

## Esercizi

**Esercizio 10.3.1.** *Si dimostri che il reticolo delle parti di un insieme (vedi Esempio 10.1.5) è distributivo.*

**Esercizio 10.3.2.** *Si dimostri che il reticolo dei naturali (vedi Esempio 10.1.6) è distributivo.*

**Esercizio 10.3.3.** *Utilizzando 10.3.4, si dimostri che il reticolo dei sottospazi di uno spazio vettoriale (vedi Esempio 10.1.8) è distributivo se e solo se la dimensione dello spazio è minore di 2.*

**Esercizio 10.3.4.** *Si dimostri che in un qualunque reticolo  $L$  risulta:*

$$\begin{aligned} x \vee (y \wedge z) &\leq (x \vee y) \wedge (x \vee z), \\ x \wedge (y \vee z) &\geq (x \wedge y) \vee (x \wedge z), \end{aligned}$$

*per ogni  $x, y, z \in L$ .*

**Svolgimento.** Per provare la prima diseguaglianza si osservi che innanzitutto da  $x \leq x \vee y$  e  $x \leq x \vee z$  segue  $x \leq (x \vee y) \wedge (x \vee z)$ . Inoltre  $y \wedge z \leq y \leq x \vee y$  e  $y \wedge z \leq z \leq x \vee z$ , da cui  $y \wedge z \leq (x \vee y) \wedge (x \vee z)$ . Pertanto  $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$ , come volevasi.

La seconda diseguaglianza può essere verificata in maniera analoga, oppure dedotta dalla prima utilizzando il principio di dualità dei reticolati (vedi 10.1.2).

**Esercizio 10.3.5.** Si dimostri che in un qualunque reticolo  $L$  risulta:

$$x \vee (y \wedge z) \leq (x \vee y) \wedge z,$$

per ogni  $x, y, z \in L$  tali che  $x \leq z$ .

**Esercizio 10.3.6.** Un reticolo  $L$  è **modulare** se  $x \vee (y \wedge z) = (x \vee y) \wedge z$ , per ogni  $x, y, z \in L$  tali che  $x \leq z$ . Si verifichi che un reticolo pentagonale (vedi Esempio 10.3.2) non è modulare.

*Svolgimento.* Con riferimento al diagramma di Hasse dell'Esempio 10.3.2, risulta infatti  $2|4$  e  $2 \vee (3 \wedge 4) = 2 \vee 1 = 2 \neq 4 = 12 \wedge 4 = (2 \vee 3) \wedge 4$ .

**Esercizio 10.3.7.** Si dimostri che ogni reticolo distributivo è modulare.

*Svolgimento.* Siano  $x, y$  e  $z$  elementi di un reticolo distributivo  $L$ , con  $x \leq z$ . Allora  $x \vee z = z$  per 10.1.3, quindi  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z$ , e  $L$  è modulare.

## 10.4 Algebre di Boole

Sia  $(L, \leq)$  un reticolo dotato di massimo 1 e di minimo 0, e sia  $x$  un elemento di  $L$ . Se esiste un elemento  $y \in L$  tale che  $x \vee y = 1$  e  $x \wedge y = 0$  allora  $y$  viene detto un **complemento** di  $x$ . Le (10.1.2) assicurano che se  $y$  è un complemento di  $x$  allora  $x$  è un complemento di  $y$ . Ovviamente gli elementi 0 e 1 hanno sempre un unico complemento, rispettivamente 1 e 0. Il reticolo  $L$  è **complementato** se ogni elemento di  $L$  possiede almeno un complemento.

**Osservazione.** Il complemento non è, in generale, univocamente determinato. Esistono cioè reticolli dotati di massimo e minimo aventi elementi che posseggono più complementi. Il reticolo  $L$  dell'Esempio 10.3.3 ha massimo 30 e minimo 1. Siccome  $3 \vee 2 = 30$  e  $3 \wedge 2 = 1$ , ma anche  $3 \vee 5 = 30$  e  $3 \wedge 5 = 1$ , gli elementi 2 e 5 sono entrambi complementi dell'elemento 3.

Il reticolo  $L$  dell'osservazione precedente non è distributivo, come provato nell'Esempio 10.3.3. Questa condizione è necessaria per l'esistenza di elementi che posseggano più complementi. Infatti:

**10.4.1.** Sia  $L$  un reticolo distributivo dotato di massimo 1 e minimo 0. Allora l'eventuale complemento di un elemento  $x \in L$  è unico.

*Dimostrazione.* Siano  $x_1$  e  $x_2$  complementi di  $x$ . Allora risulta:

$$\begin{aligned} x_1 &= x_1 \vee 0 && \text{in quanto } 0 \leq x_1 \\ &= x_1 \vee (x_2 \wedge x) && \text{perché } x_2 \text{ è un complemento di } x \\ &= (x_1 \vee x_2) \wedge (x_1 \vee x) && \text{per la (10.3.1)} \end{aligned}$$

$$\begin{aligned}
 &= (x_1 \vee x_2) \wedge 1 \\
 &= x_1 \vee x_2
 \end{aligned}
 \quad \begin{array}{l} \text{perché } x_1 \text{ è un complemento di } x \\ \text{in quanto } x_1 \vee x_2 \leq 1. \end{array}$$

Da ciò segue che  $x_2 \leq x_1$ . Scambiando i ruoli di  $x_1$  e  $x_2$ , si prova anche che  $x_2 = x_2 \vee x_1$ , da cui  $x_1 \leq x_2$ . Pertanto  $x_1 = x_2$ , come volevasi.  $\square$

Un reticolo distributivo e complementato viene detto un'**algebra di Boole** (o **reticolo booleano**). La 10.4.1 assicura che se  $L$  è un'algebra di Boole allora ogni elemento  $x \in L$  possiede un unico complemento, che verrà denotato col simbolo  $x'$ . Pertanto  $x \vee x' = 1$  e  $x \wedge x' = 0$ , per ogni  $x \in L$ . In particolare  $0' = 1$  e  $1' = 0$ .

**10.4.2.** Sia  $L$  un'algebra di Boole. Allora per ogni  $x, y \in L$  si ha:

- (i)  $(x')' = x$ ,
- (ii)  $(x \vee y)' = x' \wedge y'$ ,
- (iii)  $(x \wedge y)' = x' \vee y'$ .

*Dimostrazione.* (i) Segue subito dalla definizione di complemento.

(ii) Risulta:

$$\begin{aligned}
 (x \vee y) \vee (x' \wedge y') &= ((x \vee y) \vee x') \wedge ((x \vee y) \vee y') \quad \text{per (10.3.1)} \\
 &= ((x \vee x') \vee y) \wedge (x \vee (y \vee y')) \quad \text{per (10.1.2) e (10.1.3)} \\
 &= (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1.
 \end{aligned}$$

Analogamente si prova che  $(x \vee y) \wedge (x' \wedge y') = 0$ .

(iii) Del tutto analoga a (ii).  $\square$

**10.4.3. Esempio.** Il reticolo delle parti di un insieme  $S$  (Esempio 10.1.5) è un'algebra di Boole. Infatti, come già osservato, esso è distributivo. Inoltre ha  $S$  come massimo e  $\emptyset$  come minimo. Infine per ogni  $X \in \mathcal{P}(S)$  si ha  $X' = S \setminus X$ , essendo  $X \vee (S \setminus X) = X \cup (S \setminus X) = S$  e  $X \wedge (S \setminus X) = X \cap (S \setminus X) = \emptyset$ .

Sia  $L$  un'algebra di Boole. Un sottoinsieme non vuoto  $H \subseteq L$  si dice una **sottoalgebra** di  $L$  se per ogni  $x, y \in H$  risulta  $x \vee y \in H$ ,  $x \wedge y \in H$  e  $x' \in H$ .

**10.4.4. Esempio.** Sia  $S$  un insieme con almeno 2 elementi. Come si è visto nell'Esempio 10.4.3, il reticolo delle parti di  $S$  è un'algebra di Boole. Sia  $x \in S$ . Il sottoinsieme  $H = \{\emptyset, \{x\}, S\}$  è un sottoreticolo di  $\mathcal{P}(S)$ , ma ovviamente non è una sottoalgebra, giacché  $\{x\}' = S \setminus \{x\} \notin H$ .

## Esercizi

**Esercizio 10.4.1.** Sia  $L$  un reticolo distributivo dotato di massimo 1 e di minimo 0. Si dimostri che gli elementi di  $L$  dotati di complemento formano un sottoreticolo che è un'algebra di Boole.

*Svolgimento.* Sia  $A$  l'insieme degli elementi di  $L$  dotati di complemento. Ovviamente  $1, 0 \in A$ . Siano  $x, y \in A$ . Ragionando come in (ii) e (iii) di 10.4.2 si prova che  $x \vee y$  ha complemento  $x' \wedge y'$ , e che  $x \wedge y$  ha complemento  $x' \vee y'$ . Ne segue che  $x \vee y, x \wedge y \in A$ , quindi  $A$  è un sottoreticolo di  $L$  dotato di massimo 1 e di minimo 0. Inoltre ogni elemento di  $A$  è dotato di complemento in  $A$ , per la (i) di 10.4.2. Pertanto  $A$  è un'algebra di Boole.

**Esercizio 10.4.2.** *Si dimostri che un insieme totalmente ordinato  $L$  è un'algebra di Boole se e solo se  $|L| \leq 2$ .*

*Svolgimento.* Se  $|L| \leq 2$  allora  $L$  è banalmente un'algebra di Boole. Viceversa, sia  $L$  un'algebra di Boole. Per assurdo, sia  $|L| > 2$ . Allora esiste un elemento  $x \in L \setminus \{0, 1\}$ . Sia  $x'$  il complemento di  $x$ . Allora  $x \vee x' = 1$  e  $x \wedge x' = 0$ . Siccome  $L$  è totalmente ordinato,  $x$  e  $x'$  sono confrontabili. Per la 10.1.3 si ha allora  $x \vee x' = x$  oppure  $x \wedge x' = x$ , e ciò è assurdo in quanto  $x \in L \setminus \{0, 1\}$ .

## 10.5 Anelli booleani

Un elemento  $x$  di un anello  $A$  è detto **idempotente** se  $x^2 = x$ . Un anello unitario viene detto un **anello booleano** se ogni suo elemento è idempotente.

**10.5.1.** *Sia  $A \neq \{0\}$  un anello booleano. Allora  $A$  ha caratteristica 2 ed è commutativo.*

*Dimostrazione.* Per ogni  $x \in A$  risulta

$$2x = (2x)^2 = 4x^2 = 2x^2 + 2x^2 = 2x + 2x,$$

da cui  $2x = 0$ . Quindi  $A$  ha caratteristica 2. Siano ora  $x, y \in A$ . Si ha:

$$x + y = (x + y)^2 = (x + y)(x + y) = x^2 + y^2 + xy + yx = x + y + xy + yx,$$

da cui  $xy + yx = 0$ , quindi  $xy = -yx = yx$  in quanto  $A$  ha caratteristica 2. Pertanto  $A$  è commutativo.  $\square$

In particolare, se  $A$  è un anello booleano, risulta  $x = -x$ , per ogni  $x \in A$ .

**10.5.2. Esempio.** Sia  $S$  un insieme. Poiché per ogni  $A, B \in \mathcal{P}(S)$  risulta  $A \dot{\cup} B, A \cap B \in \mathcal{P}(S)$ , si possono considerare le operazioni binarie  $\dot{\cup}$  e  $\cap$  in  $\mathcal{P}(S)$ . La 1.4.14 assicura che  $(\mathcal{P}(S), \dot{\cup})$  è un gruppo abeliano, avente  $\emptyset$  come elemento neutro, e dove l'opposto di  $A \in \mathcal{P}(S)$  è  $A$  stesso. Inoltre (1.4.7) e (1.4.8) garantiscono che  $(\mathcal{P}(S), \cap)$  è un semigruppo commutativo. Tale semigruppo è un monoide con elemento neutro  $S$ , in quanto banalmente  $A \cap S = A$  per ogni  $A \in \mathcal{P}(S)$ . Infine 1.4.15 assicura che  $(\mathcal{P}(S), \dot{\cup}, \cap)$  è un anello commutativo unitario. Avendosi  $A^2 = A \cap A = A$  per ogni  $A \in \mathcal{P}(S)$ ,  $(\mathcal{P}(S), \dot{\cup}, \cap)$  è un anello booleano.

Il risultato che segue mostra che i concetti di anello booleano e di algebra di Boole sono logicamente equivalenti.

### 10.5.3. Teorema di Stone.

- (I) Se  $A$  è un anello booleano, e per ogni  $x, y \in A$ , si pone

$$\begin{aligned} x \vee y &:= x + y - xy, \\ x \wedge y &:= xy, \end{aligned}$$

allora la struttura algebrica  $(A, \vee, \wedge)$  è un'algebra di Boole.

- (II) Se  $L$  è un'algebra di Boole, e per ogni  $x, y \in L$  si pone

$$\begin{aligned} x + y &:= (x \wedge y') \vee (x' \wedge y), \\ xy &:= x \wedge y, \end{aligned}$$

allora la struttura algebrica  $(L, +, \cdot)$  è un anello booleano. Inoltre per ogni  $x, y \in L$  risulta  $x \vee y = x + y - xy$ .

*Dimostrazione.* (I) Sia  $A$  un anello booleano, e si definisca una relazione in  $A$  ponendo, con  $x, y \in A$ :

$$x \leq y \iff xy = x.$$

La 10.5.1 assicura che  $x^2 = x$ , quindi  $x \leq x$  per ogni  $x \in A$ . Essendo  $A$  commutativo, da  $x \leq y$  e  $y \leq x$  segue poi  $x = xy = yx = y$ . Infine da  $x \leq y$  e  $y \leq z$  segue  $x = xy$  e  $y = yz$ , quindi  $x = x(yz) = (xy)z = xz$  e  $x \leq z$ . Tutto ciò assicura che  $\leq$  è una relazione d'ordine in  $A$ .

Siano  $x, y \in A$ . Siccome  $x(xy) = x^2y = xy$  e  $y(xy) = y^2x = yx = xy$ , per definizione si ha  $xy \leq x$  e  $xy \leq y$ , dunque  $xy$  è un minorante di  $\{x, y\}$ . Sia ora  $z \in A$  un arbitrario minorante di  $\{x, y\}$ . Da  $z \leq x$  e  $z \leq y$  si ottiene allora  $z = zx$  e  $z = zy$ , dunque  $z(xy) = (zx)y = zy = z$  e  $z \leq xy$ . Pertanto  $xy = \inf_A \{x, y\}$ .

Ancora con  $x, y \in A$  si ha  $x(x+y-xy) = x^2+xy-x^2y = x+xy-xy = x$ , da cui  $x \leq x+y-xy$ . Analogamente  $y \leq x+y-xy$ , quindi  $x+y-xy$  è un maggiorante di  $\{x, y\}$ . Sia ora  $z \in A$  un arbitrario maggiorante di  $\{x, y\}$ . Da  $x \leq z$  e  $y \leq z$  si ottiene allora  $x = zx$  e  $y = zy$ , dunque  $z(x+y-xy) = zx+zy-(zx)y = x+y-xy$ , quindi  $x+y-xy \leq z$ . Pertanto  $x+y-xy = \sup_A \{x, y\}$ .

Ciò prova che  $(A, \leq)$  è un reticolo. Siccome  $xy = x$  equivale a  $x \wedge y = x$ , le operazioni binarie  $\vee$  e  $\wedge$  di cui all'enunciato sono rispettivamente l'unione reticolare e l'intersezione reticolare in  $(A, \leq)$ . Quindi la struttura algebrica  $(A, \vee, \wedge)$  è un reticolo (vedi anche 10.1.1).

Per arbitrari elementi  $x, y, z \in A$  risulta inoltre  $x \wedge (y \vee z) = x(y+z-yz) = xy+xz-xyz = xy+xz-(xy)(xz) = (x \wedge y) \vee (x \wedge z)$ . Allora 10.3.1 assicura che il reticolo  $(A, \vee, \wedge)$  è distributivo. Per ogni  $x \in A$  si ha  $x = x1$  e  $0 = 0x$ , quindi  $x \leq 1$  e  $0 \leq x$ . Pertanto l'unità 1 dell'anello  $A$  è il massimo del reticolo  $(A, \vee, \wedge)$ , e lo zero 0 dell'anello  $A$  ne è il minimo. Infine, per ogni  $x \in A$ , posto

$x' = 1 - x$  si ottiene subito  $x' \vee x = (1 - x) + x - (1 - x)x = 1 - x + x^2 = 1$  e  $x' \wedge x = (1 - x)x = x - x^2 = 0$ , pertanto  $x'$  è il complemento di  $x$ . Tutto ciò assicura che  $(A, \vee, \wedge)$  è un'algebra di Boole, come volevasi.

(II) Viceversa, sia  $L$  un'algebra di Boole e si ponga  $x+y := (x \wedge y') \vee (x' \wedge y)$ , per ogni  $x, y \in L$ . L'addizione così definita è un'operazione interna commutativa in  $L$ . Inoltre 10.4.2, (10.3.1), (10.3.2) e 10.1.3 assicurano che per ogni  $x, y, z \in L$  si ha:

$$\begin{aligned} (x+y)+z &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee (((x \wedge y') \vee (x' \wedge y))' \wedge z) \\ &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee (((x' \vee y) \wedge (x \vee y')) \wedge z) \\ &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee \\ &\quad \vee (((((x' \vee y) \wedge x) \vee ((x' \vee y) \wedge y')) \wedge z) \\ &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee \\ &\quad \vee (((((x' \wedge x) \vee (y \wedge x)) \vee ((x' \wedge y') \vee (y \wedge y'))) \wedge z) \\ &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee \\ &\quad \vee (((((0 \vee (y \wedge x)) \vee ((x' \wedge y') \vee 0)) \wedge z) \\ &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee (((y \wedge x) \vee (x' \wedge y')) \wedge z) \\ &= (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee (y \wedge x \wedge z) \vee (x' \wedge y' \wedge z), \end{aligned}$$

e, analogamente,

$$(y+z)+x = (y \wedge z' \wedge x') \vee (y' \wedge z \wedge x') \vee (z \wedge y \wedge x) \vee (y' \wedge z' \wedge x).$$

Da ciò segue subito che  $(x+y)+z = (y+z)+x = x+(y+z)$ , quindi l'addizione sopra definita è associativa.

Per ogni  $x \in L$  si ha  $x+0 = (x \wedge 1) \vee (x' \wedge 0) = x \vee 0 = x$ , quindi 0 è l'elemento neutro in  $(L, +)$ . Inoltre per ogni  $x \in L$  si ha  $x+x = (x \wedge x') \vee (x' \wedge x) = 0 \vee 0 = 0$ , per cui  $x$  è il simmetrico di  $x$  in  $(L, +)$ . Tutto ciò prova che  $(L, +)$  è un gruppo abeliano.

Si ponga ora  $xy := x \wedge y$ , per ogni  $x, y \in L$ . Per (10.1.2) e (10.1.3), la moltiplicazione così definita è un'operazione associativa e commutativa in  $L$ . Infine da 10.4.2, (10.3.1), (10.3.2) e 10.1.3 segue che per ogni  $x, y, z \in L$  si ha:

$$\begin{aligned} xz + yz &= ((x \wedge z) \wedge (y \wedge z')) \vee ((x \wedge z)' \wedge (y \wedge z)) \\ &= ((x \wedge z) \wedge (y' \vee z')) \vee ((x' \vee z') \wedge (y \wedge z)) \\ &= ((x \wedge z \wedge y') \vee (x \wedge z \wedge z')) \vee ((y \wedge z \wedge x') \vee (y \wedge z \wedge z')) \\ &= (x \wedge z \wedge y') \vee (y \wedge z \wedge x') \\ &= ((x \wedge y') \vee (x' \wedge y)) \wedge z \\ &= (x+y)z. \end{aligned}$$

Tutto ciò assicura che  $(L, +, \cdot)$  è un anello. Inoltre  $x1 = x \wedge 1 = x$  per ogni  $x \in L$ , per cui  $L$  è unitario di unità 1; e  $x^2 = x \wedge x = x$ , quindi  $L$  è un anello booleano.

Per ogni  $x \in L$  risulta poi:

$$\begin{aligned}x \wedge (1+x) &= x \wedge ((1 \wedge x') \vee (0 \wedge x)) = x \wedge x' = 0, \\x \vee (1+x) &= x \vee ((1 \wedge x') \vee (0 \wedge x)) = x \vee x' = 1,\end{aligned}$$

quindi  $x' = 1 + x = 1 - x$ . Infine per ogni  $x, y \in L$  si ha:

$$\begin{aligned}x + y - xy &= x(1-y) + y \\&= xy' + y \\&= (xy' \wedge y') \vee ((xy')' \wedge y) \\&= (x \wedge y' \wedge y') \vee ((x \wedge y')' \wedge y) \\&= (x \wedge y') \vee ((x' \vee y) \wedge y) && \text{per (iii) di 10.4.2} \\&= (x \wedge y') \vee y && \text{per (10.1.4)} \\&= (x \vee y) \wedge (y' \vee y) && \text{per (10.3.1)} \\&= (x \vee y) \wedge 1 \\&= x \vee y,\end{aligned}$$

il che completa la dimostrazione.  $\square$

Si potrebbe dimostrare che l'ordine di un anello booleano finito è necessariamente una potenza di 2. Il teorema di Stone (vedi 10.5.3) assicura allora che l'ordine di un'algebra di Boole finita è necessariamente una potenza di 2.

## Esercizi

**Esercizio 10.5.1.** *Si dimostri che in un anello booleano ogni elemento diverso da 0 e da 1 è un divisore dello 0. Ne segue che un anello booleano con più di due elementi non è un dominio d'integrità.*

*Svolgimento.* Sia  $A$  un anello booleano, e sia  $x \in A \setminus \{0, 1\}$ . Allora  $1 - x \neq 0$  e  $x(1 - x) = x - x^2 = x - x = 0$ . Pertanto  $x$  è un divisore dello 0 in  $A$ .

**Esercizio 10.5.2.** *Si dimostri che la somma degli elementi di un anello booleano di ordine 4 è 0.*

*Svolgimento.* Sia  $A = \{0, 1, x, y\}$  un anello booleano di ordine 4. L'elemento  $x+y$  di  $A$  è certamente diverso da  $x$  e da  $y$ , in quanto  $x, y \neq 0$ . Se fosse  $x+y = 0$  risulterebbe  $y = -x$ , quindi  $y = x$  per la 10.5.1, assurdo perché invece  $x \neq y$ . Quindi necessariamente  $x+y = 1$ . Ne segue che  $0+1+x+y = 1+1 = 0$ , come volevasi.

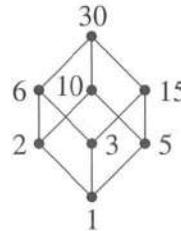
**Esercizio 10.5.3.** *Si consideri l'insieme  $L$  dei divisori positivi di 30, ordinato con la relazione  $|$  del divide.*

(i) *Si descriva l'insieme  $L$ , precisandone l'ordine.*

- (ii) Si disegni il diagramma di Hasse di  $(L, |)$ .
- (iii) Si dimostri che  $(L, |)$  è un'algebra di Boole.
- (iv) In  $(L, |)$  si calcoli:  $2 \vee 5, 10 \wedge 15$ , il complemento di  $10 \wedge 6$ .
- (v) Sia  $(L, +, \cdot)$  l'anello booleano associato a  $(L, |)$  mediante il teorema di Stone (vedi 10.5.3). In  $(L, +, \cdot)$  si calcoli:  $2 + 5, 2 \cdot 5, 10 + 15, 10 \cdot 15$ .

*Svolgimento.* (i) Si ha  $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$ , quindi  $|L| = 8$ .

(ii) Il diagramma di Hasse di  $(L, |)$  è il seguente:



(iii) Per l'Esempio 10.1.6 l'insieme ordinato  $(L, |)$  è un reticolo, in quanto sottoreticolo di  $(\mathbb{N}_0, |)$ , e ha massimo 30 e minimo 1. Siccome  $(\mathbb{N}_0, |)$  è distributivo (vedi Esercizio 10.3.2), anche  $(L, |)$  lo è. Infine si ha:  $1' = 30, 2' = 15, 3' = 10, 5' = 6$ . Pertanto  $(L, |)$  è un'algebra di Boole.

(iv) Si ha:  $2 \vee 5 = 10, 10 \wedge 15 = 5, (10 \wedge 6)' = 2' = 15$ . Si osservi che per la (iii) di 10.4.2 risulta  $(10 \wedge 6)' = 10' \vee 6' = 3 \vee 5 = 15$ .

(v) Dal teorema di Stone (vedi 10.5.3) si ricava che nell'anello booleano associato a  $(L, |)$  la somma e il prodotto sono definite ponendo  $x + y := (x \wedge y') \vee (x' \wedge y)$  e  $xy := x \wedge y$  per ogni  $x, y \in L$ . Pertanto si ha:

$$2 + 5 = (2 \wedge 5') \vee (5' \wedge 2) = (2 \wedge 6) \vee (15 \wedge 5) = 2 \vee 5 = 10,$$

$$2 \cdot 5 = 2 \wedge 5 = 1,$$

$$10 + 15 = (10 \wedge 15') \vee (10' \wedge 15) = (10 \wedge 2) \vee (3 \wedge 15) = 2 \vee 3 = 6,$$

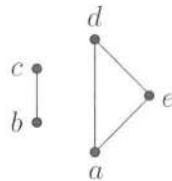
$$10 \cdot 15 = 10 \wedge 15 = 5.$$

## 10.6 Grafi

Si dice **grafo** una qualunque coppia  $\Gamma = (V, E)$ , dove  $V = V(\Gamma)$  è un insieme non vuoto, e  $E = E(\Gamma)$  è un sottoinsieme dell'insieme  $[V]^2$  delle parti di  $V$  aventi ordine 2. Gli elementi di  $V$  si dicono **vertici** del grafo, mentre gli elementi di  $E$  sono i **lati** del grafo. Se  $l = \{v, w\} \in E$  è un lato allora i vertici  $v$  e  $w$  si dicono anche gli **estremi** di  $l$ . Due vertici  $v, w$  sono **adiacenti** se  $\{v, w\}$  è un lato, e due lati  $l, l_1 \in E$  sono **incidenti** se l'insieme  $l \cap l_1$  ha ordine 1. Un grafo i cui vertici siano a due a due adiacenti è detto **completo**; è invece **vuoto** se tale è l'insieme dei suoi lati. In altre parole  $\Gamma = (V, E)$  è completo se  $E = [V]^2$  ed è vuoto se  $E = \emptyset$ . L'**ordine** di un grafo è poi, per definizione, quello dell'insieme dei suoi vertici. Un grafo **finito** è un grafo di ordine finito, e quindi con un numero finito di vertici.

Generalmente non si pensa a un grafo come a una coppia ordinata ma come a una collezione di vertici alcuni dei quali sono uniti da segmenti o da archi di curva. Pertanto è naturale disegnare il grafo rappresentando appunto i vertici come punti e unendo, mediante un segmento o un arco di curva, due punti se l'insieme dei due vertici che questi rappresentano è un lato. Di fatto il modo più facile per descrivere un grafo è appunto disegnarlo.

**10.6.1. Esempio.** Il grafo  $\Gamma = (V, E)$  avente insieme di vertici  $V = \{a, b, c, d, e\}$  e insieme di lati  $E = \{\{a, d\}, \{a, e\}, \{b, c\}, \{d, e\}\}$  può essere rappresentato come segue:



Esso ha 5 vertici e 4 lati. I vertici  $b$  e  $c$  sono adiacenti, come pure  $a$  e  $d$ ,  $a$  e  $e$ ,  $d$  e  $e$ . I lati  $\{a, d\}$  e  $\{a, e\}$  sono incidenti (come pure  $\{a, d\}$  e  $\{d, e\}$ ,  $\{d, e\}$  e  $\{a, e\}$ ).

Si noti che se  $\Gamma = (V, E)$  è un grafo e  $v, w \in V$  sono vertici esiste al più un lato  $l \in E$  i cui estremi sono  $v$  e  $w$ . La definizione di grafo può però essere generalizzata nel modo seguente. Si dice **multografo** una terna  $\Upsilon = (V, E, \psi)$ , dove  $V$  è un insieme non vuoto,  $E$  un insieme arbitrario e  $\psi : E \rightarrow [V]^2$  un'applicazione che a ogni elemento di  $E$  associa un sottoinsieme di  $V$  di ordine 2. Gli elementi di  $V$  sono i **vertici** del multografo, quelli di  $E$  ne sono i **lati**. Se  $l \in E$ ,  $v, w \in V$  e  $\psi(l) = \{v, w\}$  allora si dice che  $l$  è un lato di **estremi**  $v$  e  $w$ . Si noti che possono esistere più lati aventi gli stessi estremi a meno che l'applicazione  $\psi$  non sia iniettiva, nel qual caso la coppia  $\Gamma = (V, \psi(E))$  è un grafo.

Si considerino ora grafi  $\Gamma = (V, E)$  e  $\Gamma_1 = (V_1, E_1)$ . Un'applicazione biettiva  $f : V \rightarrow V_1$  tale che  $\{v, w\} \in E$  se e solo se  $\{f(v), f(w)\} \in E_1$  è detta **isomorfismo**. Se esiste un isomorfismo tra  $\Gamma$  e  $\Gamma_1$ , i grafi considerati si dicono **isomorfi**. Grafi isomorfi hanno banalmente lo stesso diagramma. È immediato osservare che grafi completi sono isomorfi se e solo se hanno lo stesso ordine e questo comporta che per ogni intero positivo  $n$  esiste, a meno di isomorfismi, un unico grafo completo di ordine  $n$ , che viene denotato con  $K_n$ . Analogamente, a meno di isomorfismi esiste un unico grafo vuoto di ordine  $n$ , per ogni  $n \in \mathbb{N}$ .

Si definisce **sottografo** di un grafo  $\Gamma = (V, E)$  ogni grafo  $\Gamma_1 = (V_1, E_1)$  tale che  $V_1 \subseteq V$  e  $E_1 \subseteq [V_1]^2 \cap E$ . In altre parole un sottografo di  $\Gamma$  è un grafo il cui insieme di vertici  $V_1$  è un sottoinsieme di  $V$  e i cui lati sono alcuni tra i lati di  $\Gamma$  che hanno per estremi elementi di  $V_1$ . Per ogni sottoinsieme non vuoto  $V_1 \subseteq V$  il grafo  $(V_1, [V_1]^2 \cap E)$  è detto il sottografo di  $\Gamma$  **generato** da  $V_1$ .

**10.6.2. Esempio.** Il grafo  $(V_1 = \{a, b, c, d\}, E_1 = \{\{b, c\}\})$  è un sottografo del grafo  $\Gamma$  dell'Esempio 10.6.1. Il sottografo di  $\Gamma$  generato da  $V_1$  è invece il grafo  $(V_1, \{\{a, d\}, \{b, c\}\})$ .

Siano  $\Gamma = (V, E)$  un grafo finito e  $v$  un suo vertice. Si definisce **grado** di  $v$ , e si denota con  $d(v)$ , il numero di lati che hanno  $v$  come estremo; si dice poi che  $v$  è un vertice **pari** o **dispari** a seconda che abbia grado pari o dispari. Un vertice di grado 0 è detto **isolato**. Si dice **regolare** di grado  $m$  un grafo in cui tutti i vertici hanno lo stesso grado  $m$ . Per esempio  $K_n$  è un grafo regolare di grado  $n - 1$ , mentre ogni grafo vuoto è regolare di grado 0.

Analoghe definizioni si possono dare anche in un multigrafo **finito**, cioè in cui sia  $V$  che  $E$  sono insiemi finiti. In particolare, se  $\Upsilon = (V, E, \psi)$  è un multigrafo finito e  $v$  è un suo vertice, si definisce **grado** di  $v$  il numero intero

$$d(v) := |\{l \in E : v \in \psi(l)\}|.$$

Se si conosce il grado di ciascun vertice di un grafo finito, allora si può determinare facilmente il numero dei lati del grafo.

**10.6.3.** *Sia  $\Gamma = (V, E)$  un grafo finito. Allora:*

$$|E| = \frac{1}{2} \sum_{v \in V} d(v).$$

*Dimostrazione.* Poiché ogni lato  $l \in E$  ha esattamente due estremi, il numero dei vertici di  $\Gamma$ , non necessariamente distinti, che sono estremi di qualche lato è  $m = 2|E|$ . D'altro canto ogni vertice  $v \in V$  è estremo di  $d(v)$  lati e quindi  $m = \sum_{v \in V} d(v)$ . Dunque  $2|E| = \sum_{v \in V} d(v)$  come si voleva.  $\square$

Si noti che 10.6.3 comporta che in ogni grafo finito  $\Gamma = (V, E)$  la somma dei gradi dei vertici è pari, cioè  $\sum_{v \in V} d(v) \equiv 0 \pmod{2}$ . Inoltre è immediato osservare che un grafo di ordine  $n$  regolare di grado  $t$  ha  $\frac{1}{2}tn$  lati. Dunque per esempio  $K_n$  ha  $\frac{(n-1)n}{2}$  lati.

Se  $v$  e  $w$  sono vertici di un grafo  $\Gamma$ , un **cammino** da  $v$  a  $w$  è una sequenza finita  $l_1 = \{x_1, x_2\}, l_2 = \{x_2, x_3\}, \dots, l_n = \{x_n, x_{n+1}\}$  di lati distinti tale che lati consecutivi siano incidenti,  $v = x_1$  sia estremo del primo lato e  $w = x_{n+1}$  sia estremo dell'ultimo lato. Il numero  $n \geq 0$  dei lati che costituiscono il cammino è detto **lunghezza** del cammino. Per ogni vertice  $v$  esiste un unico cammino di lunghezza 0 da  $v$  a  $v$ . Un cammino di lunghezza positiva da un vertice  $v$  a  $v$  stesso è detto **circuito**. Si definisce **foresta** un grafo privo di circuiti.

Un grafo è **connesso** se considerati comunque due dei suoi vertici  $v$  e  $w$  esiste un cammino da  $v$  a  $w$ . Il grafo dell'Esempio 10.6.1 non è connesso perché per esempio non vi è alcun cammino da  $a$  a  $b$ . Una foresta connessa è detta **albero**. Agli alberi è dedicato il Paragrafo 10.7.

Nell'insieme  $V$  dei vertici di un grafo  $\Gamma$  si può considerare la relazione  $\sim$  definita ponendo, per ogni  $v, w \in V$ ,  $v \sim w$  se e solo se esiste un cammino da  $v$  a  $w$ . La relazione  $\sim$  è d'equivalenza in  $V$ : infatti essa è banalmente riflessiva e simmetrica, inoltre è transitiva perché se  $v, w, u \in V$  sono tali che  $v \sim w$  e  $w \sim u$ ,

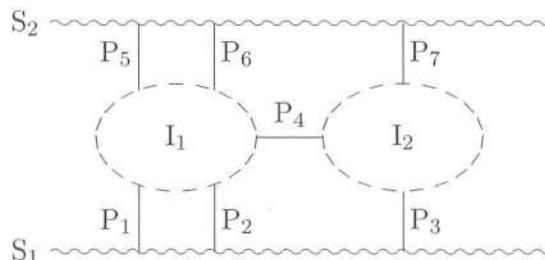
allora indicati con  $l_1, l_2, \dots, l_n$  un cammino da  $v$  a  $w$  e con  $e_1, e_2, \dots, e_m$  un cammino da  $w$  a  $u$ , si ha che  $l_1, \dots, l_n, e_1, \dots, e_m$  è un cammino da  $v$  a  $u$  per cui  $v \sim u$ . Le classi d'equivalenza modulo  $\sim$  vengono dette le **componenti connesse** del grafo. Più precisamente per ogni vertice  $v$  la classe  $[v]_\sim$  d'equivalenza di  $v$  modulo  $\sim$  è detta componente连通的 di  $v$ .

È immediato osservare che un grafo è连通的 se e solo se  $\sim$  è la relazione totale, ed è vuoto se e solo se  $\sim$  è la relazione identica. Nel primo caso c'è una sola componente connessa, nel secondo le componenti connesse sono tante quanti sono i vertici.

Si noti poi che non vi è alcun lato che abbia estremi appartenenti a componenti connesse distinte. Si osservi inoltre che le componenti connesse di una foresta sono alberi.

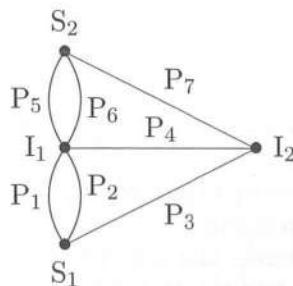
Sia ora  $\Upsilon = (V, E, \psi)$  un multigrafo finito. Si definisce **cammino** una sequenza finita di lati  $l_1, l_2, \dots, l_t \in E$  a due a due distinti, tali che per ogni  $i \in \{1, \dots, t\}$  si abbia  $\psi(l_i) = \{z_i, z_{i+1}\}$ , dove  $z_1, \dots, z_{t+1} \in V$ . Se  $z_1 = z_{t+1}$  il cammino è detto **circuito**. Un multigrafo è **connesso** se scelti arbitrariamente due suoi vertici  $a$  e  $b$  esiste un cammino  $l_1, \dots, l_t$  tale che  $l_1$  abbia  $a$  come estremo e  $l_t$  abbia come estremo  $b$ , cioè  $a \in \psi(l_1)$  e  $b \in \psi(l_t)$ .

Un cammino  $l_1, \dots, l_t$  tale che  $E = \{l_1, \dots, l_t\}$  è detto **cammino euleriano**. Un cammino euleriano che sia un circuito è detto **circuito euleriano**. Richiedere che un multigrafo finito possieda un cammino euleriano equivale a richiedere che si possano disegnare tutti i suoi lati senza staccare la penna dal foglio e senza ripassare per uno stesso lato. Si parla di cammini e circuiti euleriani perché queste definizioni sono legate al famosissimo *problema dei ponti di Königsberg* risolto appunto da Eulero nel 1736 utilizzando la Teoria dei Grafi. Königsberg, città natale del filosofo Immanuel Kant, era una città della Prussia situata su due isole e su entrambe le sponde del fiume Pregel collegate da sette ponti, come schematicamente rappresentato nella figura seguente, dove le sponde del fiume (linea ondulata), le isole (linea tratteggiata) e i ponti (linea semplice) sono indicati dalle rispettive iniziali S, I e P, e numerati progressivamente:



Il problema in questione consisteva nello stabilire se fosse possibile per un abitante di Königsberg partire da casa propria e poi ritornarvi dopo avere percorso una e una sola volta ciascuno dei sette ponti della città. La città con i suoi sette ponti

può essere rappresentata graficamente con il seguente multigrafo:



dove i vertici sono i territori urbani sulle sponde del fiume e sulle isole, e i lati sono i 7 ponti che li collegano. Il problema posto, che equivale a chiedere se tale multigrafo possiede o meno un circuito euleriano, ha risposta negativa in virtù del seguente risultato dovuto appunto a Eulero.

**10.6.4. Teorema.** *Sia  $\Upsilon = (V, E, \psi)$  un multigrafo finito privo di punti isolati.  $\Upsilon$  ha un circuito euleriano se e solo se è connesso e tutti i suoi vertici sono pari.*

*Dimostrazione.* In primo luogo si supponga che  $\Upsilon$  sia dotato di un circuito euleriano  $L = \{l_1, \dots, l_k\}$ . Per provare che  $\Upsilon$  è connesso occorre dimostrare che per ogni  $a, b \in V$  esiste in  $\Upsilon$  un cammino da  $a$  a  $b$ . Poiché per ipotesi  $\Upsilon$  è privo di punti isolati esistono due lati  $e, f \in E$  tali che  $a \in \psi(e)$  e  $b \in \psi(f)$ . Il circuito  $L$  è euleriano pertanto  $L = E$  e quindi esistono  $i, j \in \{1, \dots, k\}$  tali che  $l_i = e$  e  $l_j = f$  e supposto  $j \geq i$  si ha che  $l_i, l_{i+1}, \dots, l_j$  è il cammino richiesto.

Occorre adesso provare che ogni vertice ha grado pari, cioè è estremo di un numero pari di lati. Si fissi un vertice  $v_0 \in V$ ; chiaramente non è restrittivo assumere che il circuito euleriano  $L = \{l_1, \dots, l_k\}$  sia da  $v_0$  a  $v_0$ , ovvero che si abbia  $v_0 \in \psi(l_1) \cap \psi(l_k)$ . Si consideri un vertice  $u \in V$  diverso da  $v_0$ ; il ragionamento precedente assicura che  $u$  è estremo di almeno un lato del circuito euleriano e cioè che  $u \in \bigcup_{i=1}^k \psi(l_i)$ . Questo comporta che è non vuoto l'insieme  $J = \{j \in \{1, \dots, k\} : u \in \psi(l_j)\}$ , e posto  $m = \min J$  a  $m$  corrispondono due lati adiacenti aventi  $u$  come estremo ovvero  $u \in \psi(l_m) \cap \psi(l_{m+1})$ . Ovviamente può succedere che  $u$  sia estremo anche di altri lati  $l_j$  con  $j > m + 1$  e in tal caso risulta  $J_1 = \{j \in \{m + 2, \dots, k\} : u \in \psi(l_j)\} \neq \emptyset$ ; posto  $h = \min J_1$ , ad  $h$  corrispondono ancora due lati aventi  $u$  come estremo, in quanto  $u \in \psi(l_h)$  e  $u \in \psi(l_{h+1})$ . In ogni caso quindi  $u$  è estremo di un numero pari di lati ossia ha grado pari. Si ha dunque che ciascun vertice  $u \neq v_0$  ha grado pari. L'arbitrarietà di  $v_0$  e il fatto che  $\Upsilon$  ha almeno due vertici perché è privo di punti isolati assicurano che ogni vertice ha grado pari.

Viceversa si assuma  $\Upsilon = (V, E, \psi)$  connesso e con tutti i vertici di grado pari, e si proceda per induzione sul numero  $|E| \geq 2$  di lati. Se  $|E| = 2$ , considerato  $l \in E$  e posto  $\psi(l) := \{v_1, v_2\}$ , si ha che poiché  $v_1$  e  $v_2$  hanno grado pari necessariamente  $E = \{l, l_1\}$  con  $\psi(l_1) = \{v_1, v_2\}$  e quindi  $\{l, l_1\}$  è un circuito euleriano.

Sia dunque  $|E| > 2$  e sia  $v_1 \in V$ ; poiché  $\Upsilon$  è privo di punti isolati esiste  $l_1 \in E$  tale che  $v_1 \in \psi(l_1)$ . Sia  $\psi(l_1) := \{v_1, v_2\}$ ; esiste almeno un lato  $l_2 \neq l_1$  avente  $v_2$  come estremo perché  $v_2$  ha grado pari. Posto  $\psi(l_2) := \{v_2, v_3\}$ , se  $v_3 = v_1$  allora  $\{l_1, l_2\}$  è un circuito da  $v_1$  a  $v_1$  altrimenti, poiché  $v_3$  ha grado pari, esiste almeno un lato  $l_3 \neq l_2$  avente  $v_3$  come estremo. Indicato con  $v_4$  l'estremo di  $l_3$  diverso da  $v_3$ , se  $v_4 = v_1$  allora  $\{l_1, l_2, l_3\}$  è un circuito altrimenti si prosegue in modo analogo. Naturalmente, essendo  $\Upsilon$  finito, questo ragionamento conduce necessariamente alla costruzione di un circuito  $L_1$  da  $v_1$  a  $v_1$ . Se  $L_1 = E$ , allora  $L_1$  è un circuito euleriano. Altrimenti si consideri il multigrafo che si ottiene da  $\Upsilon$  cancellando i lati di  $L_1$  e i vertici che sono estremi solo di lati di  $L_1$  ovvero il multigrafo  $\Upsilon_1 = (V_1, E_1, \psi_1)$  con  $V_1 := \{v \in V : \exists l \in E \setminus L_1 : v \in \psi(l)\}$ ,  $E_1 = E \setminus L_1$  e  $\psi_1 = \psi|_{E_1}$ . Il multigrafo  $\Upsilon_1$  è nelle stesse ipotesi di  $\Upsilon$  ma possiede meno lati e quindi, per ipotesi di induzione ha un circuito euleriano; sia questo  $L_2$ . Banalmente  $E = L_1 \cup L_2$  è un circuito perché il fatto che  $\Upsilon$  sia connesso e ogni suo vertice sia pari garantisce l'esistenza di un lato  $e \in L_1$  e di un lato  $f \in L_2$  con un estremo  $w$  in comune. Non è restrittivo assumere che  $L_1 = \{l_1, \dots, l_t\}$  e  $L_2 = \{e_1, \dots, e_k\}$  siano circuiti da  $w$  a  $w$ . Allora  $L = \{l_1, \dots, l_t, e_1, \dots, e_k\}$  è un circuito da  $w$  a  $w$ , ed è ovviamente euleriano.  $\square$

Dal Teorema 10.6.4 discende facilmente il seguente

**10.6.5. Corollario.** *Sia  $\Upsilon = (V, E, \psi)$  un multigrafo finito privo di punti isolati.  $\Upsilon$  ha un cammino euleriano se e solo se è connesso e il numero dei suoi vertici dispari è 0 oppure 2.*

*Dimostrazione.* In primo luogo si supponga  $\Upsilon$  dotato di un cammino euleriano  $L = \{l_1, \dots, l_k\}$ ; lo stesso ragionamento fatto nella dimostrazione del Teorema 10.6.4 prova che  $\Upsilon$  è connesso. Pertanto resta da provare che i vertici di grado dispari sono 0 o 2. Se  $L$  è un circuito allora l'asserto segue dal Teorema 10.6.4, per cui si può assumere che  $L$  non sia un circuito e quindi che  $\psi(l_1) \cap \psi(l_k) = \{v_1, v_2\} \cap \{v_k, v_{k+1}\} = \emptyset$ . Considerato un vertice  $u \neq v_1, v_{k+1}$  e ragionando come nel Teorema 10.6.4 si ha che  $u$  ha grado pari. Per provare che  $v_1$  e  $v_{k+1}$  hanno grado dispari basta notare che il multigrafo che si ottiene da  $\Upsilon$  aggiungendo un lato  $l_{k+1}$  di estremi  $v_1$  e  $v_{k+1}$ , cioè  $\Upsilon_1 = (V, E_1 = E \cup \{l_{k+1}\}, \psi_1)$  con  $\psi_1 : E_1 \longrightarrow [V]^2$  definita da  $\psi_1(l_i) := \psi(l_i)$  per ogni  $i \in \{1, \dots, k\}$  e  $\psi_1(l_{k+1}) := \{v_1, v_{k+1}\}$ , possiede un circuito euleriano. Quindi per il Teorema 10.6.4 ogni vertice di  $\Upsilon_1$  ha grado pari, e in particolare di questa proprietà godono  $v_1$  e  $v_{k+1}$ . Ma se i gradi di tali vertici in  $\Upsilon_1$  sono  $d_1$  e  $d_{k+1}$  allora i loro gradi in  $\Upsilon$  sono  $d_1 - 1$  e  $d_{k+1} - 1$ , dunque dispari.

Viceversa si assuma  $\Upsilon = (V, E, \psi)$  connesso e con due vertici  $v_1$  e  $v_2$  dispari. Fissati un punto  $v_0 \notin V$  e due lati  $l_1, l_2 \notin E$ , si prenda in considerazione il multigrafo  $\Upsilon_1 = (V \cup \{v_0\}, E \cup \{l_1, l_2\}, \psi_1)$ , con  $\psi_1(l) := \psi(l)$  per ogni  $l \in E$ ,  $\psi_1(l_1) := \{v_0, v_1\}$  e  $\psi_1(l_2) := \{v_0, v_2\}$ . Ovviamente  $\Upsilon_1$  è connesso e tutti i suoi vertici hanno grado pari, pertanto per il Teorema 10.6.4 esso possiede un circuito

euleriano  $L$ . Poiché  $l_1$  e  $l_2$  sono incidenti in  $v_0$  si ha che  $L \setminus \{l_1, l_2\} = E$  è un cammino euleriano di  $\Upsilon$ .  $\square$

## Esercizi

**Esercizio 10.6.1.** Si disegni il grafo  $\Gamma = (V, E)$  avente come insieme di vertici  $V = \{a, b, c, d, e, f\}$  e lati  $\{\{a, b\}, \{a, c\}, \{b, e\}, \{b, f\}\}$ , e si stabilisca se tale grafo è connesso. Si determinino poi i gradi dei vertici e gli eventuali punti isolati.

**Esercizio 10.6.2.** Si consideri il grafo  $\Gamma = (V, E)$  dove  $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$  ed  $E = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{5, 6\}, \{5, 7\}, \{5, 8\}\}$ . Si determinino le componenti connesse di  $\Gamma$  e si stabilisca se  $\Gamma$  è una foresta e se è un albero.

**Esercizio 10.6.3.** Si consideri il multigrafo  $\Upsilon = (V, E, \psi)$ , con  $V = \{a, b, c, d, e\}$ ,  $E = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8\}$  e  $\psi : E \rightarrow [V]^2$  definita dalle posizioni

$$\begin{aligned}\psi(l_1) &= \{a, b\} = \psi(l_2), \\ \psi(l_3) &= \{c, b\} = \psi(l_4), \\ \psi(l_5) &= \{d, b\} = \psi(l_6), \\ \psi(l_7) &= \{e, b\} = \psi(l_8).\end{aligned}$$

Dopo averlo disegnato, si stabilisca, motivando la risposta, se  $\Upsilon$  possiede un circuito euleriano.

**Esercizio 10.6.4.** Si dimostri che i grafi  $\Gamma_1 = (V_1, E_1)$  e  $\Gamma_2 = (V_2, E_2)$  con

$$\begin{aligned}V_1 &= \{a, b, c, d\}, & E_1 &= \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, d\}\} \\ V_2 &= \{1, 2, 3, 4\}, & E_2 &= \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}\}\end{aligned}$$

non sono isomorfi.

**Esercizio 10.6.5.** Si dimostri che i tre grafi  $\Gamma_1 = (V_1, E_1)$ ,  $\Gamma_2 = (V_2, E_2)$  e  $\Gamma_3 = (V_3, E_3)$  con

$$\begin{aligned}V_1 &= V_2 = V_3 = \{a, b, c, d\}, \\ E_1 &= \{\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}\}, \\ E_2 &= \{\{a, b\}, \{a, c\}, \{b, c\}, \{a, d\}\}, \\ E_3 &= \{\{d, c\}, \{a, d\}, \{a, c\}, \{b, c\}\}\end{aligned}$$

sono a due a due isomorfi.

**Esercizio 10.6.6.** Esiste un grafo con 7 vertici  $v_1, v_2, v_3, v_4, v_5, v_6, v_7$  tali che  $d(v_i) = i + 1$  per ogni  $i \in \{1, 2, 3, 4, 5, 6, 7\}$ ?

**Esercizio 10.6.7.** Si consideri il grafo  $\Gamma = (V, E)$ , dove  $V = \{1, 2, 3, 4, 5\}$  ed  $E = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{3, 5\}\}$ , e se ne determini il sottografo generato da  $V_1 = \{3, 4, 5\}$ .

## 10.7 Alberi

Nel Paragrafo 10.6 è stato definito foresta un grafo privo di circuiti e albero una foresta che sia anche un grafo connesso. In particolare quindi, come del resto già osservato in precedenza, le componenti connesse di una foresta sono alberi.

Come si vedrà nel seguito, ogni grafo finito connesso  $\Gamma = (V, E)$  possiede un cosiddetto **albero di supporto**, cioè un sottografo  $\Gamma' = (V', E')$  che è un albero ed è tale che  $V' = V$ . Di qui l'interesse particolare per lo studio degli alberi. Una prima caratterizzazione degli alberi è la seguente.

**10.7.1. Teorema.** *Per un grafo  $\Gamma = (V, E)$  sono equivalenti:*

- (i)  $\Gamma$  è un albero;
- (ii) considerati comunque due vertici  $u, v \in V$  esiste un unico cammino da  $u$  a  $v$ ;
- (iii)  $\Gamma$  è connesso e il grafo  $\Gamma_1 = (V, E \setminus \{l\})$ , ottenuto da  $\Gamma$  cancellando un qualsiasi lato  $l \in E$ , non è connesso;
- (iv)  $\Gamma$  è privo di circuiti e considerati comunque due vertici  $x, y \in V$  non adiacenti, il grafo  $\Gamma_2 = (V, E \cup \{\{x, y\}\})$ , ottenuto da  $\Gamma$  aggiungendo il lato di estremi  $x$  e  $y$ , possiede un circuito.

*Dimostrazione.* Si supponga che  $\Gamma$  sia un albero. Allora per definizione  $\Gamma$  è connesso, e ciò comporta che considerati due vertici  $u, v \in V$  esiste un cammino  $\{l_1, l_2, \dots, l_n\}$  da  $u$  a  $v$ . Se  $\{e_1, \dots, e_k\}$  fosse un cammino da  $u$  a  $v$  diverso dal precedente allora  $\{l_1, l_2, \dots, l_n, e_k, \dots, e_1\}$  sarebbe un circuito, la cui esistenza è in contraddizione con la definizione di albero. Pertanto dalla (i) segue la (ii).

Sia ora  $\Gamma$  un grafo con la proprietà (ii). Banalmente  $\Gamma$  è connesso. Se poi  $l = \{x, y\}$  è un lato di  $\Gamma$ , l'unico cammino da  $x$  a  $y$  in  $\Gamma$  è  $\{l\}$ , per cui nel grafo  $\Gamma_1 = (V, E \setminus \{l\})$  non esiste alcun cammino da  $x$  a  $y$ . Ciò significa che  $\Gamma_1$  non è connesso. Pertanto la (ii) implica la (iii).

Si supponga per assurdo che un grafo  $\Gamma$  con la proprietà (iii) possieda un circuito  $L = \{l_1, l_2, \dots, l_k\}$  con  $l_1 = \{v_1, v_2\}, \dots, l_k = \{v_k, v_1\}$ . Allora il grafo che si ottiene da  $\Gamma$  cancellando per esempio  $l_k$  è ancora connesso perché  $\{l_1, l_2, \dots, l_{k-1}\}$  è ancora un cammino da  $v_1$  a  $v_k$ . Ciò è in contraddizione con la (iii). Se poi  $x$  e  $y$  sono vertici non adiacenti di  $\Gamma$ , indicato con  $\{l_1, l_2, \dots, l_t\}$  un cammino da  $x$  a  $y$ , che esiste perché  $\Gamma$  è connesso, e posto  $l = \{x, y\}$ , si ha che  $\{l_1, l_2, \dots, l_t, l\}$  è un circuito in  $\Gamma_2 = (V, E \cup \{l\})$ . Così dalla (iii) segue la (iv).

Infine si supponga che  $\Gamma$  goda della proprietà (iv). Per provare che  $\Gamma$  è un albero occorre dimostrare che esso è connesso. Si considerino quindi due vertici  $x$  e  $y$  distinti e non adiacenti di  $\Gamma$ ; per ipotesi  $\Gamma_2 = (V, E \cup \{\{x, y\}\})$  ha un circuito, sia questo  $L = \{l_1, \dots, l_t\}$ . Se nessuno dei lati coincidesse con  $\{x, y\}$  allora  $L$  sarebbe un circuito di  $\Gamma$ , in contraddizione con la (iv). Non è restrittivo assumere  $l_t = \{x, y\}$ ; ma allora  $l_{t-1} = \{v_{t-1}, x\}$  e  $l_1 = \{y, v_2\}$  per cui  $\{l_1, \dots, l_{t-1}\}$  è un cammino in  $\Gamma$  da  $y$  a  $x$ , e l'asserto è provato.  $\square$

I vertici di grado 1 di un albero si chiamano *foglie*; il prossimo risultato assicura che ogni albero finito di ordine  $\geq 2$  ha almeno una foglia.

**10.7.2.** *Sia  $\Gamma = (V, E)$  un albero finito. Se  $|V| \geq 2$  allora esiste almeno un vertice  $w \in V$  tale che  $d(w) = 1$ .*

*Dimostrazione.* Sia  $|V| \geq 2$  e per assurdo  $d(v) \neq 1$  per ogni  $v \in V$ . Poiché  $\Gamma$  ha almeno due vertici ed è connesso si ha che  $\Gamma$  ha almeno un lato  $l_1 = \{v_1, v_2\}$ . Si consideri  $v_2$ ; essendo  $d(v_2) \geq 2$  esiste almeno un lato  $l_2 \neq l_1$  tale che  $v_2 \in l_2$  e quindi  $l_2 = \{v_2, v_3\}$  con  $v_3 \neq v_1$ . Anche il vertice  $v_3$  ha grado almeno 2 e quindi esiste un lato  $l_3 \neq l_2$  che ha come estremo  $v_3$ . Indicato con  $v_4 \neq v_2$  l'altro estremo di  $l_3$  si ha che  $d(v_4) \geq 2$  e proseguendo il ragionamento si costruisce una successione di lati  $l_1, l_2, \dots, l_n, \dots$  di  $\Gamma$  tali che  $l_i \neq l_{i+1}$  e  $l_i \cap l_{i+1} \neq \emptyset$  per ogni  $i \in \mathbb{N}$ . Il grafo  $\Gamma$  è però finito per cui la sequenza considerata deve essere finita e questo vuol dire che esistono  $n, m \in \mathbb{N}$  tali che  $n \neq m$  e  $l_n = l_m$ . Pertanto  $\Gamma$  ha un circuito e questo è assurdo.  $\square$

Per stabilire se un grafo finito connesso è un albero basta contare i lati. Vale infatti il seguente risultato:

**10.7.3. Teorema.** *Per un grafo  $\Gamma = (V, E)$  finito di ordine  $n$  sono equivalenti:*

- (i)  $\Gamma$  è un albero;
- (ii)  $\Gamma$  è un grafo privo di circuiti con  $n - 1$  lati;
- (iii)  $\Gamma$  è connesso e ha  $n - 1$  lati.

*Dimostrazione.* Per provare che dalla (i) segue la (ii) occorre dimostrare che un albero  $\Gamma$  di ordine  $n$  ha  $n - 1$  lati e a tale scopo si può procedere per induzione su  $n$ . Se  $n = 1$ , allora  $E = \emptyset$  e l'asserto è banalmente verificato. Sia dunque  $n > 1$  e si supponga, per ipotesi di induzione, che ogni albero di ordine  $n - 1$  abbia  $n - 2$  lati. Per 10.7.2 l'albero  $\Gamma$  ha almeno una foglia  $v$ . Detto  $l$  quell'unico lato avente  $v$  come estremo, il grafo  $\Gamma_1 = (V \setminus \{v\}, E \setminus \{l\})$  è ancora un albero e ha ordine  $n - 1$ . Dunque  $|E \setminus \{l\}| = n - 2$  e quindi  $|E| = n - 1$  come si voleva.

Per dimostrare che dalla (ii) segue la (iii) occorre verificare che una foresta  $\Gamma = (V, E)$  con  $n$  vertici e  $n - 1$  lati è necessariamente connessa. Sia  $t$  il numero delle componenti connesse di  $\Gamma$  e siano  $V_1, \dots, V_t$  tali componenti connesse. Indicato con  $\Gamma_i$  il sottografo generato da  $V_i$  per ogni  $i \in \{1, \dots, t\}$ , si ha che  $\Gamma_i$  è un albero di ordine  $|V_i|$  e quindi ha  $|V_i| - 1$  lati. Inoltre  $|V| = n = |V_1| + \dots + |V_t|$  e  $|E| = n - 1 = (|V_1| - 1) + \dots + (|V_t| - 1) = |V_1| + \dots + |V_t| - t = n - t$ ; pertanto necessariamente  $t = 1$ , cioè  $\Gamma$  è connesso.

Resta da provare che la (iii) implica la (i), cioè che ogni grafo connesso  $\Gamma$  con  $n$  vertici e  $n - 1$  lati è privo di circuiti. Si supponga per assurdo che  $\Gamma$  possieda un circuito e sia  $l_1$  un lato di tale circuito. Allora il grafo  $\Gamma_1 = (V, E \setminus \{l_1\})$ , che si ottiene da  $\Gamma$  cancellando  $l_1$ , è un grafo connesso con  $n$  vertici e  $n - 2$  lati. Poiché si è provato che un albero con  $n$  vertici ha  $n - 1$  lati,  $\Gamma_1$  non può essere

un albero e quindi ha almeno un circuito. Detto  $l_2$  un lato di questo circuito, il grafo  $\Gamma_2 = (V, E \setminus \{l_1, l_2\})$  è connesso e ha  $n$  vertici e  $n - 3$  lati, quindi non può essere un albero. Proseguendo in questo modo si perviene, dopo  $n - 1$  passi, a un grafo connesso con  $n$  vertici e 0 lati, e ciò è assurdo perché il grafo vuoto non è connesso.  $\square$

**10.7.4. Corollario.** *Ogni grafo finito connesso possiede un albero di supporto.*

*Dimostrazione.* Sia  $\Gamma = (V, E)$  un grafo connesso di ordine  $n$ ; risulta ovviamente  $|E| \geq n - 1$ . Se  $|E| > n - 1$  allora  $\Gamma$  non può essere un albero e quindi contiene un circuito. Cancellando un lato di tale circuito si ottiene un sottografo connesso di ordine  $n$  il cui numero di lati è  $|E| - 1$ . Se  $|E| - 1 = n - 1$  allora il grafo ottenuto è un albero altrimenti proseguendo come nella dimostrazione del Teorema 10.7.3, ossia cancellando uno alla volta i lati che appartengono a circuiti, si perviene alla costruzione di un sottografo connesso di  $\Gamma$  con  $n$  vertici e  $n - 1$  lati, che risulta quindi un albero di supporto di  $\Gamma$ .  $\square$

## Esercizi

**Esercizio 10.7.1.** *Si stabilisca quanti sono, a meno di isomorfismi, gli alberi di ordine 3 e quelli di ordine 4.*

**Esercizio 10.7.2.** *Si disegnino tutti, a meno di isomorfismi, gli alberi di ordine 5.*

**Esercizio 10.7.3.** *Si consideri il grafo  $\Gamma = (V, E)$  con  $V = \{a, b, c, d, e, f\}$  ed  $E = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, e\}, \{d, f\}, \{d, c\}, \{e, a\}\}$ . Dopo aver osservato che  $\Gamma$  è connesso ma non è un albero se ne determini un albero di supporto.*

**Esercizio 10.7.4.** *Sia  $\Gamma = (V, E)$  il grafo avente  $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  ed  $E = \{\{1, 3\}, \{1, 4\}, \{2, 4\}, \{2, 7\}, \{5, 6\}, \{5, 7\}, \{6, 9\}, \{6, 8\}, \{9, 10\}\}$ . Si dimostri che  $\Gamma$  è un albero e se ne individuino le foglie.*

**Esercizio 10.7.5.** *Quanti lati ha una foresta di ordine 10 con 3 componenti connesse di cui una priva di foglie?*

## 10.8 Esercizi di riepilogo

**Esercizio 10.8.1.** *Si consideri l'insieme  $L = \{2^a 3^b : a, b \in \mathbb{N}_0\}$  costituito dai numeri naturali della forma  $2^a 3^b$ , con  $a, b \in \mathbb{N}_0$ .*

(i) *Si verifichi che la relazione  $\sqsubseteq$  definita in  $L$  ponendo*

$$2^a 3^b \sqsubseteq 2^c 3^d \iff a \leq c \quad e \quad b \leq d,$$

*dove  $\leq$  denota l'ordine usuale in  $\mathbb{N}_0$ , è una relazione d'ordine.*

- (ii) Si stabilisca se l'insieme ordinato  $(L, \sqsubseteq)$  è totalmente ordinato, se è ben ordinato, quali sono gli eventuali elementi minimi e massimali, minimo e massimo.
- (iii) Si dimostri che  $(L, \sqsubseteq)$  è un reticolo.
- (iv) Si dimostri che il reticolo  $(L, \sqsubseteq)$  è distributivo.
- (v) Nel reticolo  $(L, \sqsubseteq)$  si effettuino i seguenti calcoli:  $4 \wedge 6, 12 \wedge 18, 4 \vee 6, 6 \vee 9$ .
- (vi) Si dimostri che l'applicazione  $h : 2^a 3^b \in L \mapsto a + b \in \mathbb{N}_0$  è un omomorfismo tra gli insiemi ordinati  $(L, \sqsubseteq)$  e  $(\mathbb{N}_0, \leq)$ .
- (vii) Si dimostri che  $h$  non è un omomorfismo tra i reticolli  $(L, \sqsubseteq)$  e  $(\mathbb{N}_0, \leq)$ .
- (viii) Si consideri il sottoinsieme  $F = \{2, 3, 4, 6, 9, 12, 16, 18, 27\}$  di  $L$ , con l'ordine indotto da  $\sqsubseteq$ . Si disegni il diagramma di Hasse di  $(F, \sqsubseteq)$ , e si precisi perché  $(F, \sqsubseteq)$  non è un sottoreticolo di  $(L, \sqsubseteq)$ .

**Esercizio 10.8.2.** Si consideri l'insieme  $L = \{2^a 3^b : a, b \in \mathbb{N}\}$  costituito dai numeri naturali della forma  $2^a 3^b$ , con  $a, b \in \mathbb{N}_0$ .

- (i) Si verifichi che la relazione  $\sqsubseteq$  definita in  $L$  ponendo

$$2^a 3^b \sqsubseteq 2^c 3^d \iff a \leq c \quad e \quad b|d,$$

dove  $\leq$  denota l'ordine usuale in  $\mathbb{N}_0$  e  $|$  denota la relazione del "divide" in  $\mathbb{N}_0$ , è una relazione d'ordine.

- (ii) Si stabilisca se l'insieme ordinato  $(L, \sqsubseteq)$  è totalmente ordinato, se è ben ordinato, quali sono gli eventuali elementi minimi e massimali, minimo e massimo.
- (iii) Si dimostri che  $(L, \sqsubseteq)$  è un reticolo.
- (iv) Si dimostri che il reticolo  $(L, \sqsubseteq)$  è distributivo.
- (v) Nel reticolo  $(L, \sqsubseteq)$  si effettuino i seguenti calcoli:  $4 \wedge 6, 12 \wedge 18, 4 \vee 6, 6 \vee 9$ .
- (vi) Si consideri l'applicazione  $\sigma : L \rightarrow \mathcal{P}(\mathbb{N})$  definita ponendo

$$\sigma(2^a 3^b) := \begin{cases} \{x \in \mathbb{N} : x > a\} & \text{se } b = 0 \\ \{a+1, a+2, \dots, a+b\} & \text{se } m > 0. \end{cases}$$

Si stabilisca se  $\sigma$  è iniettiva, e se è suriettiva.

- (vii) Si provi poi che  $\sigma$  è un omomorfismo tra gli insiemi ordinati  $(L, \sqsubseteq)$  e  $(\mathcal{P}(\mathbb{N}), \subseteq)$ .
- (viii) Si stabilisca se  $\sigma$  è un omomorfismo tra i reticolli  $(L, \sqsubseteq)$  e  $(\mathcal{P}(\mathbb{N}), \subseteq)$ .
- (ix) Si consideri il sottoinsieme  $F = \{2, 3, 4, 6, 9, 12, 16, 18, 27\}$  di  $L$ , con l'ordine indotto da  $\sqsubseteq$ . Si disegni il diagramma di Hasse di  $(F, \sqsubseteq)$ , e si precisi se  $(F, \sqsubseteq)$  è un sottoreticolo di  $(L, \sqsubseteq)$ .

**Esercizio 10.8.3.** Si consideri l'insieme  $L = \{3n + 1 : n \in \mathbb{N}_0\}$ , e sia  $\sqsubseteq$  la relazione definita in  $L$  ponendo

$$3n + 1 \sqsubseteq 3m + 1 \iff n|m,$$

dove  $|$  è la relazione del “divide” in  $\mathbb{N}_0$ .

- (i) Si dimostri che  $\sqsubseteq$  è una relazione d’ordine in  $L$ .
- (ii) Si precisi se  $(L, \sqsubseteq)$  è totalmente ordinato e se è ben ordinato.
- (iii) Si dimostri che  $(L, \sqsubseteq)$  è un reticolo.
- (iv) Si dimostri che l’applicazione  $f : 3n + 1 \in L \longmapsto n \in \mathbb{N}_0$  è un isomorfismo di reticolati tra  $(L, \sqsubseteq)$  ed  $(\mathbb{N}_0, |)$ .
- (v) Si specifichi se esistono, e quali sono, il minimo e il massimo di  $(L, \sqsubseteq)$ .
- (vi) Si disegni il diagramma di Hasse del sottoinsieme  $F = \{7, 10, 13, 19, 37\}$  di  $L$ .
- (vii) Si stabilisca se  $F$  è un sottoreticolo di  $L$ .

**Esercizio 10.8.4.** Nell’insieme  $5\mathbb{N}_0 = \{5a : a \in \mathbb{N}_0\}$  si consideri la relazione  $\sqsubseteq$  definita ponendo

$$5a \sqsubseteq 5b : \iff a|b$$

dove  $|$  è la relazione del “divide” tra numeri naturali.

- (i) Si verifichi che  $\sqsubseteq$  è una relazione d’ordine in  $5\mathbb{N}_0$ .
- (ii) Si stabilisca se l’insieme ordinato  $(5\mathbb{N}_0, \sqsubseteq)$  è totalmente ordinato, se è ben ordinato, quali sono gli eventuali minimo e massimo.
- (iii) Si dimostri che  $(5\mathbb{N}_0, \sqsubseteq)$  è un reticolo.
- (iv) Qual è l’elemento  $15 \vee 25$  in  $(5\mathbb{N}_0, \sqsubseteq)$ ?
- (v) Si dimostri che l’applicazione  $\omega : 5a \in 5\mathbb{N}_0 \longmapsto a \in \mathbb{N}_0$  è un omomorfismo tra i reticolati  $(5\mathbb{N}_0, \sqsubseteq)$  e  $(\mathbb{N}_0, |)$ .
- (vi) Si verifichi se l’applicazione  $\sigma : 5a \in 5\mathbb{N}_0 \longmapsto a \in \mathbb{N}_0$  è un omomorfismo tra gli insiemi ordinati  $(5\mathbb{N}_0, \sqsubseteq)$  e  $(\mathbb{N}_0, \leq)$ , dove  $\leq$  denota l’ordine usuale in  $\mathbb{N}_0$ .
- (vii) Si verifichi se l’applicazione  $\sigma : 5a \in 5\mathbb{N}_0 \longmapsto a \in \mathbb{N}_0$  è un omomorfismo tra i reticolati  $(5\mathbb{N}_0, \sqsubseteq)$  e  $(\mathbb{N}_0, \leq)$ , dove  $\leq$  denota l’ordine usuale in  $\mathbb{N}_0$ .
- (viii) Si consideri il sottoinsieme  $H = \{10, 15, 20, 25, 50, 150\}$  di  $5\mathbb{N}_0$ , con l’ordine indotto da  $\sqsubseteq$ . Si disegni il diagramma di Hasse di  $(H, \sqsubseteq)$ .
- (ix) Si precisi se  $(H, \sqsubseteq)$  è un sottoreticolo di  $(5\mathbb{N}_0, \sqsubseteq)$ .
- (x) Qual è l’estremo superiore in  $H$  dell’insieme  $\{15, 25\}$ ?
- (xi) Si determinino gli elementi minimali e l’eventuale minimo di  $(H, \sqsubseteq)$ .
- (xii) Si determinino gli elementi massimali e l’eventuale massimo di  $(H, \sqsubseteq)$ .

**Esercizio 10.8.5.** Si consideri l’insieme  $\mathcal{P}(S)$  delle parti di un insieme  $S$  di ordine 3 e il grafo  $\Gamma = (V, E)$  i cui vertici sono gli elementi di  $\mathcal{P}(S)$  e in cui  $\{X, Y\}$  è un lato se e solo se  $X \subseteq Y$  oppure  $Y \subseteq X$ . Si dimostri che tale grafo è connesso ma non è un albero, esibendone un circuito. Si determini poi un albero di supporto di  $\Gamma$ . Si provi infine che il multigrafo  $\Upsilon = (V, E, \psi)$ , dove  $\psi$  è l’immersione di  $E$  in  $[V]^2$ , non possiede cammini euleriani.

**Esercizio 10.8.6.** Si costruisca un multigrafo di ordine 10 con 21 lati, che sia privo di punti isolati e di cammini euleriani.

# A

## Cenni di logica proposizionale e predicativa

Un enunciato che abbia un ben preciso **valore di verità**, cioè che sia vero oppure falso, è detto **proposizione**. Per esempio le affermazioni

*Parigi è una città europea*

*La Senna è un lago americano*

sono entrambe proposizioni (la prima vera e la seconda falsa), mentre l'enunciato

*Probabilmente trascorgerò le prossime vacanze estive in barca a vela*

non lo è perché non è né vero né falso.

La logica proposizionale analizza come le proposizioni possono essere combinate tra loro per ottenere nuove proposizioni più complesse il cui valore di verità è determinato da quello delle proposizioni che le costituiscono. Un modo per fare ciò è quello di utilizzare i **connettivi**:  $\neg$  (NOT),  $\vee$  (OR),  $\wedge$  (AND).

Data una proposizione A si può considerare la sua **negazione**, che si denota con  $\neg A$ .

Per esempio la negazione della proposizione

A : *Riccardo è il miglior scolaro*

è

$\neg A$  : *Riccardo non è il miglior scolaro*,

ed è vera esattamente quando A è falsa. Precisamente, utilizzando la notazione V per vero e F per falso si ha:

A	$\neg A$
V	F
F	V

Tale tabella è detta **tavola di verità** per la negazione.

Due proposizioni possono poi essere combinate tra loro mediante la **congiunzione** "e". Per esempio considerate le proposizioni

A : Riccardo stava scrivendo,

e

B : Fabrizio stava leggendo,

la loro congiunzione, denotata con  $A \wedge B$ , è la proposizione

$A \wedge B$  : Riccardo stava scrivendo e Fabrizio stava leggendo.

Si osservi che se A e B sono vere allora lo è anche  $A \wedge B$ , d'altro canto se A è falsa allora  $A \wedge B$  è falsa indipendentemente dall'essere vera o falsa la B. Elen-  
cando le ulteriori possibilità si può dare una descrizione precisa del modo in cui il connettivo “e” viene utilizzato per collegare due proposizioni tracciando anche in questo caso la tavola di verità:

A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

Tale tabella mostra che  $A \wedge B$  è vera quando sia A che B sono vere, mentre è falsa in tutti gli altri casi.

Un altro modo in cui possono essere legate tra loro due proposizioni consiste nell'utilizzare il connettivo “o”, detto *disgiunzione*.

*Questa estate Federica trascorrerà le vacanze in Inghilterra o in Francia.*

La proposizione considerata è vera se effettivamente Federica andrà in Inghilterra ma anche se andrà in Francia. La possibilità che faccia entrambe le cose non è prevista ma, se dovesse verificarsi, l'enunciato è ancora vero. Questo nella vita quotidiana potrebbe causare qualche ambiguità: se due proposizioni A e B sono entrambe vere allora la proposizione A o B è vera? Generalmente questo, nell'uso comune, viene chiarito dal contesto. Invece, secondo le regole della logica proposizionale, A o B significa sempre: A oppure B oppure entrambe. Si ha cioè che l'uso del connettivo “o” è, come suol dirsi, inclusivo. La disgiunzione di due proposizioni A e B viene denotata con  $A \vee B$ . La tavola di verità di  $A \vee B$  è la seguente:

A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

Un modo per combinare due proposizioni è anche quello di utilizzare l'**implica-  
zione**. Il modo in cui questa viene usata in matematica è leggermente diverso

dall'uso comune. La proposizione “A implica B”, oppure “se A allora B”, si denota con  $A \implies B$ , significa che A è falsa oppure B è vera, ed è descritta dalla seguente tavola di verità:

A	B	$A \implies B$
V	V	V
V	F	F
F	V	V
F	F	V

Si osservi che  $A \implies B$  è vera per ogni valore di verità di B ogni volta che A è falsa. Dunque un enunciato falso implica ogni enunciato. Si può poi notare che l'implicazione può essere definita usando i connettivi già introdotti: infatti  $A \implies B$  equivale a  $\neg A \vee B$ .

Un ulteriore connettivo di uso frequente è la **doppia implicazione o equivalenza**, indicata con  $A \iff B$ . Questa viene definita come  $(A \implies B) \wedge (B \implies A)$  ed è vera esattamente quando A e B sono entrambe vere o entrambe false:

A	B	$A \iff B$
V	V	V
V	F	F
F	V	F
F	F	V

Si noti che anche la doppia implicazione  $A \iff B$  può essere definita utilizzando solo i connettivi già introdotti: infatti essa equivale a  $(\neg A \vee B) \wedge (\neg B \vee A)$ .

I simboli  $\neg$ ,  $\wedge$ ,  $\vee$ ,  $\implies$ ,  $\iff$  si chiamano anche **connettivi proposizionali**. Ogni proposizione formata con l'applicazione di tali connettivi ha un valore di verità che dipende dai valori di verità delle proposizioni che la compongono.

Per esempio il valore di verità della proposizione  $(\neg A \vee B) \implies C$  dipende da quello di A, B e C, come espresso dalla tavola di verità seguente:

A	B	C	$\neg A$	$(\neg A \vee B)$	$(\neg A \vee B) \implies C$
V	V	V	F	V	V
F	V	V	V	V	V
V	F	V	F	F	V
F	F	V	V	V	V
V	V	F	F	V	F
F	V	F	V	V	F
V	F	F	F	F	V
F	F	F	V	V	F

Si definisce **forma enunciativa** una proposizione costituita da un numero finito di proposizioni **atomiche** (cioè non formate mediante altre proposizioni) combinate

mediante connettivi proposizionali. Se una forma enunciativa è costituita da  $t$  proposizioni atomiche allora le proposizioni atomiche hanno  $2^t$  possibili assegnazioni di verità e quindi nella tavola di verità compaiono  $2^t$  righe.

Si consideri per esempio la seguente proposizione:

*Se gli Stati Uniti sono un paese ricco, allora l'Africa è un paese povero.*

Tale proposizione è una forma enunciativa e precisamente la forma enunciativa  $A \Rightarrow B$  dove  $A$  è la proposizione atomica

*Gli Stati Uniti sono un paese ricco*

e  $B$  è la proposizione atomica

*L'Africa è un paese povero.*

Una forma enunciativa che sia vera indipendentemente dai valori di verità delle proposizioni che la costituiscono è detta **tautologia**. Per esempio

$$\neg(A \wedge B) \iff \neg A \vee \neg B$$

è una tautologia, e ha la seguente tavola di verità:

A	B	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$\neg A \vee \neg B$	$\neg(A \wedge B) \iff \neg A \vee \neg B$
V	V	F	F	F	F	V
V	F	V	F	V	V	V
F	V	V	V	F	V	V
F	F	V	V	V	V	V

La tautologia precedente assicura che la negazione della congiunzione di due proposizioni  $A$  e  $B$  non è altro che la disgiunzione delle negazioni  $\neg A$  e  $\neg B$ . Si può poi osservare che anche

$$\neg(A \vee B) \iff \neg A \wedge \neg B$$

è una tautologia, e ciò garantisce che la negazione della disgiunzione di  $A$  e di  $B$  è la congiunzione delle negazioni  $\neg A$  e  $\neg B$ . Infatti si ha:

A	B	$\neg(A \vee B)$	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$\neg(A \vee B) \iff \neg A \wedge \neg B$
V	V	F	F	F	F	V
V	F	F	F	V	F	V
F	V	F	V	F	F	V
F	F	V	V	V	V	V

Ulteriori tautologie che legano congiunzione e disgiunzione sono, come è facile osservare scrivendone le tavole di verità (vedi Esercizio A.1), le seguenti:

$$\begin{aligned} A \vee (B \wedge C) &\iff (A \vee B) \wedge (A \vee C), \\ A \wedge (B \vee C) &\iff (A \wedge B) \vee (A \wedge C). \end{aligned}$$

Siano  $P$  e  $Q$  due forme enunciative. Se  $P \implies Q$  è una tautologia allora si dice che  $P$  **implica logicamente**  $Q$ , ovvero che  $Q$  è **conseguenza logica** di  $P$ . Analogamente si dirà che  $P$  e  $Q$  sono **logicamente equivalenti** se  $P \iff Q$  è una tautologia. Per esempio  $\neg(A \vee B)$  e  $\neg A \wedge \neg B$  sono logicamente equivalenti mentre  $A \wedge B$  implica logicamente  $A$  perché  $(A \wedge B) \implies A$  è una tautologia, avendo la seguente tavola di verità:

A	B	$A \wedge B$	$(A \wedge B) \implies A$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

Una forma enunciativa che sia falsa per tutti i valori di verità delle proposizioni che la costituiscono è detta **contraddizione**. Per esempio la forma enunciativa  $A \wedge \neg A$  è una contraddizione infatti ha la seguente tavola di verità:

A	$\neg A$	$A \wedge \neg A$
V	F	F
F	V	F

Si noti che una forma enunciativa  $P$  è una tautologia se e solo se  $\neg P$  è una contraddizione, e viceversa.

Una forma enunciativa è una **forma normale disgiuntiva** (rispettivamente **congiuntiva**) se è una disgiunzione (risp. congiunzione) di una o più proposizioni ciascuna delle quali è una congiunzione (risp. disgiunzione) di una o più proposizioni atomiche. Per esempio, con  $A$ ,  $B$  e  $C$  proposizioni atomiche, la forma enunciativa  $(A \wedge B) \vee (\neg A \wedge C)$  è una forma normale disgiuntiva, mentre  $(C \vee \neg B) \wedge (A \vee \neg C)$  è una forma normale congiuntiva.

Si può dimostrare che ogni forma enunciativa è logicamente equivalente a una forma normale disgiuntiva e a una forma normale congiuntiva. Per esempio la forma enunciativa  $(A \implies B) \vee (\neg A \wedge C)$  è equivalente alla forma normale disgiuntiva  $\neg(A \wedge \neg B) \vee (\neg A \wedge C)$  ed anche alla forma normale congiuntiva  $(\neg A \vee B) \wedge (\neg A \vee \neg C)$ .

Gli enunciati semplici fin qui descritti non bastano al ragionamento matematico. È necessario infatti introdurre le **funzioni proposizionali**, anche dette **predicati**, che sono asserzioni in cui compaiono delle variabili. A differenza delle proposizioni, i predicati non sono sempre veri o falsi, ma lo diventano quando

vengono specificati i valori assunti dalle variabili. Per esempio il seguente asserto relativo ai numeri naturali

$$P(x) : x \text{ è un numero dispari}$$

è vero se  $x$  è 3 ma è falso se  $x$  è 2.

Quando si vuol precisare che un certo asserto  $P(x)$ , che coinvolga una variabile  $x$ , è vero per tutti gli  $x$  nell'universo del discorso, questo viene scritto

$$(\forall x) P(x),$$

che si legge “per ogni  $x$  è vera  $P(x)$ ”. Il simbolo  $\forall$  è detto **quantificatore universale**. Per esprimere invece che  $P(x)$  vale per qualche  $x$ , si scrive

$$(\exists x) P(x),$$

che si legge “esiste  $x$  tale che è vera  $P(x)$ ”. Il simbolo  $\exists$  è detto **quantificatore esistenziale**.

Un predicato può coinvolgere anche più di una variabile: per esempio gli asserti

$$Q(x, y) : xy = yx$$

$$R(x, y) : x \leq y$$

sono come si suol dire **predicati a due posti**.

Naturalmente, una volta che tutte le variabili che compaiono in una funzione proposizionale sono state limitate da un quantificatore universale o esistenziale, si ottiene una proposizione del tipo considerato prima. Per esempio nell'universo dei numeri naturali

$$(\forall x)(\forall y)(xy = yx)$$

esprime il fatto che il prodotto di ogni coppia di numeri naturali non dipende dall'ordine dei fattori. Analogamente

$$(\forall x)(\exists y)(x < y)$$

vuol dire che per ogni  $x$  vi è un  $y$  maggiore di  $x$  e quindi che non esiste massimo. Si osservi inoltre che se nell'ultima proposizione si inverte l'uso dei quantificatori si ottiene la proposizione

$$(\exists y)(\forall x)(x < y)$$

che vuol dire che esiste un  $y$  maggiore di ogni  $x$ , cioè  $y$  è il massimo. Quest'ultima proposizione è falsa se la precedente è vera come succede appunto se si tratta di numeri naturali. Pertanto occorre fare attenzione all'ordine in cui si adoperano i quantificatori.

I quantificatori universale ed esistenziale sono legati dalle seguenti equivalenze che consentono di definire ciascuno dei due in termini dell'altro, per cui si può scegliere uno dei due come primitivo e definire l'altro in termini di questo:

$$\neg(\exists x)\neg P(x) \iff (\forall x)P(x),$$

$$\neg(\forall x)\neg P(x) \iff (\exists x)P(x).$$

Con l'aiuto di queste formule e tenendo presente che

$$\neg\neg A \iff A,$$

è facile scrivere la negazione di una qualsiasi formula con quantificatori. Per esempio:

$$\neg[(\forall x)(\exists y)(\forall z)F(x, y, z)] \iff (\exists x)(\forall y)(\exists z)[\neg F(x, y, z)].$$

Come esempio, si consideri l'asserto

*A : esiste una coppia di numeri naturali la cui somma è 0,*

in simboli:

$$(\exists x)(\exists y)(x + y = 0);$$

la sua negazione è

$$(\forall x)(\forall y)\neg(x + y = 0),$$

ossia

*$\neg A$  : la somma di ogni coppia di numeri naturali è diversa da 0.*

Nel ragionamento matematico si utilizzano alcune regole per ricavare i teoremi da un insieme ben determinato di formule che vengono chiamate **assiomi**, procedendo con delle sequenze di passi dette **dimostrazioni**. I teoremi così come gli assiomi sono tautologie. Può essere utile descrivere brevemente alcuni metodi di dimostrazione.

Una **dimostrazione diretta** è del tipo:

*A è vera,  $A \implies B$  è vera, dunque è vera B.*

Si può poi procedere con delle **dimostrazioni indirette per contrapposizione o per assurdo**. Nel procedere per contrapposizione, per dimostrare che

$$A \implies B$$

si prova la cosiddetta **formula contronominale**, ossia che

$$\neg B \implies \neg A.$$

Questo metodo è basato sul fatto che la proposizione

$$(A \implies B) \iff (\neg B \implies \neg A)$$

è una tautologia. Essa ha infatti la seguente tavola di verità:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
V	V	F	F	V	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

Per esempio, se si vuol provare per contrapposizione che nell'universo dei numeri interi

$$(x^2 \text{ pari} \Rightarrow x \text{ pari}),$$

bisogna dimostrare che

$$(x \text{ dispari} \Rightarrow x^2 \text{ dispari}).$$

E infatti se  $x$  è un intero dispari allora  $x = 2n + 1$ , con  $n$  intero, per cui

$$x^2 = (2n + 1)^2 = 4n^2 + 4n + 1$$

è senz'altro dispari.

Infine, dimostrare per assurdo che  $A$  è vera significa provare che  $\neg A$  conduce a una proposizione falsa. Per esempio si supponga di voler provare che la proposizione

$$A : \sqrt{2} \text{ non è un numero razionale},$$

è vera. Procedendo per assurdo si suppone vera

$$\neg A : \sqrt{2} \text{ è un numero razionale},$$

dunque

$$\sqrt{2} = \frac{m}{n}$$

con  $m$  numero intero e  $n$  numero intero positivo. Ovviamente si può supporre che  $m$  e  $n$  non abbiano divisori primi in comune. Allora

$$2 = \frac{m^2}{n^2}$$

e quindi  $m^2 = 2n^2$ , il che comporta che  $m^2$  è pari, ovvero che  $m$  è pari, per quanto sopra dimostrato. Pertanto  $m = 2t$  con  $t$  opportuno intero. Dunque  $n^2 = 2t^2$  per cui  $n$  è pari. Allora  $m$  e  $n$  hanno in comune il divisore primo 2 e questa è una contraddizione.

Il ragionamento precedente mostra che, supponendo vera  $\neg A$  si perviene a una contraddizione, per cui  $\neg A$  è falsa e quindi  $A$  è vera.

A volte poi nelle dimostrazioni si esibiscono dei **controesempi**. Alcuni enunciati sono infatti del tipo

$$(\forall x)P(x),$$

e se si vuol dimostrare che tale enunciato è falso occorre provare che è vera la sua negazione, cioè che

$$(\exists x)\neg P(x);$$

ciò può essere fatto individuando un ben preciso  $c$  tale che  $\neg P(c)$ . Per esempio si supponga di voler provare che nell'universo dei numeri interi l'enunciato

$$(\forall x)(\exists y)(xy = 1)$$

è falso, e quindi che è vera la sua negazione:

$$(\exists x)(\forall y)\neg(xy = 1).$$

A tale scopo basta osservare che se si considera il numero intero 3 si ha che

$$(\forall y)\neg(3y = 1).$$

Si noti che è vero anche il seguente enunciato

$$(\exists x)(\exists y)(xy = 1).$$

Basta infatti considerare  $x = y = 1$  oppure  $x = y = -1$ . In altre parole il fatto che sia possibile individuare un ben preciso  $c$  tale che  $P(c)$  non assicura che l'enunciato  $(\forall x)P(x)$  sia vero, mentre l'individuazione di un elemento  $c$  tale che  $\neg P(c)$  garantisce che è vera la negazione  $\neg(\forall x)P(x)$  del precedente enunciato.

Quelli fin qui illustrati sono gli schemi di ragionamento generale e, a seconda dei vari argomenti, si usano schemi più specialistici, quali per esempio il principio di induzione per dimostrare proprietà relative ai numeri naturali.

## Esercizi

**Esercizio A.1.** Si verifichi che le seguenti forme enunciative sono tautologie:

$$\begin{aligned} A \vee (B \wedge C) &\iff (A \vee B) \wedge (A \vee C), \\ A \wedge (B \vee C) &\iff (A \wedge B) \vee (A \wedge C). \end{aligned}$$

**Esercizio A.2.** Si scrivano le tavole di verità delle seguenti proposizioni:

$$\begin{aligned} (A \implies B) \wedge A; \\ (A \vee \neg C) \iff B. \end{aligned}$$

**Esercizio A.3.** Si verifichi che le seguenti forme enunciative sono tautologie:

$$\begin{aligned} A \wedge A &\iff A, \\ A \vee A &\iff A, \\ A \vee B &\iff B \vee A, \\ A \wedge B &\iff B \wedge A, \\ (A \vee B) \vee C &\iff A \vee (B \vee C), \\ (A \wedge B) \wedge C &\iff A \wedge (B \wedge C). \end{aligned}$$

**Esercizio A.4.** Si provi che le seguenti forme enunciative sono contraddizioni:

$$\begin{aligned} A \wedge B &\iff \neg A \vee \neg B, \\ A \vee B &\iff \neg A \wedge \neg B. \end{aligned}$$

**Esercizio A.5.** Si scrivano le seguenti proposizioni come forme enunciative, usando lettere per le proposizioni atomiche:

- P : O Carla non è francese oppure Luigi è americano e Carla è francese;  
 Q : Un bambino è felice se e solo se è domenica, c'è il sole e mangia il gelato.

**Esercizio A.6.** Si determinino forme normali congiuntive e disgiuntive logicamente equivalenti ad  $A \iff (B \wedge \neg A)$ .

**Esercizio A.7.** Si scrivano i seguenti enunciati relativi ai numeri naturali utilizzando i quantificatori:

- A : Esistono due numeri interi  $x$  e  $y$  la cui somma è 12;  
 B : Qualunque sia il numero naturale  $x$ , il numero naturale  $2x + 16$  è pari;  
 C : Per ogni numero naturale  $x$  maggiore di 7 esiste un numero naturale  $y$  tale che  $x = y + 7$ ;  
 D : Se un numero è primo allora è dispari oppure è due.

**Esercizio A.8.** Si scrivano le negazioni dei seguenti enunciati:

- H :  $(\forall x)(\exists y)(x - 3y = 15)$ ;  
 K :  $(\forall x)((\exists y)(x > y + 7) \vee (\exists y)(x - 7 \leq y))$ ;  
 L :  $(\exists x)(\forall y)(x - 15 \leq y)$ .

**Esercizio A.9.** La proposizione

$$3 \text{ è un numero dispari}$$

può essere dimostrata come segue: "Ogni numero primo diverso da 2 è dispari, 3 è primo ed è diverso da 2, quindi 3 è dispari". Che tipo di ragionamento è stato utilizzato?

**Esercizio A.10.** Utilizzando un ragionamento per assurdo, dimostrare che l'insieme dei numeri naturali è privo di massimo.

## Bibliografia

---

- [1] M. ABATE, *Algebra lineare*, McGraw-Hill, 2000.
- [2] S. ABEASIS, *Geometria Analitica del piano e dello spazio*, Zanichelli, 2002.
- [3] A. ALZATI, M. BIANCHI, M. CARIBONI, *Matematica Discreta – Esercizi*, Pearson Education, 2006.
- [4] M. BIANCHI, A. GILLIO, *Introduzione alla Matematica Discreta*, McGraw-Hill, 2000.
- [5] B. BOLLOBÁS, *Graph Theory. An Introductory Course*, Springer-Verlag, 1979.
- [6] R.A. BRUALDI, *Introductory Combinatorics*, II edition, North-Holland, 1992.
- [7] V. BRYANT, *Aspects of Combinatorics – A wide-ranging introduction*, Cambridge University Press, 1993.
- [8] G. CAMPANELLA, *Appunti di Algebra*, Nuova Cultura, 2005.
- [9] M. CERASOLI, F. EUGENI, M. PROTASI, *Elementi di Matematica Discreta*, Zanichelli, 1988.
- [10] P.M. COHN, *Algebra Universale*, Feltrinelli, 1971.
- [11] P.M. COHN, *Classic Algebra*, Wiley, 2001.
- [12] M. CURZIO, P. LONGOBARDI, M. MAJ, *Lezioni di Algebra*, Liguori Editore, 1994.
- [13] F. DALLA VOLTA, M. RIGOLI, *Elementi di Matematica Discreta e Algebra Lineare*, Pearson Education, 2007.
- [14] R. DIESTEL, *Graph Theory*, Springer-Verlag, 2005.
- [15] A. FACCHINI, *Algebra e Matematica Discreta*, Decibel, Zanichelli, 2000.
- [16] A. FRANCHETTA, *Algebra Lineare e Geometria Analitica*, Liguori Editore, 1965.
- [17] N. JACOBSON, *Basic Algebra*, I and II, W.H. Freeman & C., 1985.
- [18] G.A. JONES, J.M. JONES, *Elementary Number Theory*, Springer, 1998.
- [19] S. LANG, *Algebra Lineare*, Boringhieri, 1981.
- [20] L. LOMONACO, *Un'introduzione all'Algebra lineare*, Aracne, 1997.
- [21] E. MENDELSON, *Introduzione alla Logica Matematica*, Bollati Boringhieri, 2004.
- [22] D.J.S. ROBINSON, *A Course in Linear Algebra with Applications*, World Scientific Publishing, 2006.

## Indice analitico

---

- A
  - albero, 415
    - di supporto, 420
  - alfabeto, 215
  - algebra di Boole, 408
  - algoritmo
    - della divisione, 22, 170, 246
    - euclideo, 180
  - anello, 152
    - booleano, 409
    - commutativo, 152
    - idempotente, 409
    - quoziente, 240
    - unitario, 152
  - angolo, 393, 395
  - antiperiodo, 200
  - appartenenza, 1
  - applicazione, 54
    - biettiva, 67
    - cancellabile a destra, 76
    - cancellabile a sinistra, 76
    - composta, 69
    - costante, 61
    - crescente, 91
    - identica, 62
    - iniettiva, 65
    - inversa, 68
    - invertibile, 72
    - lineare, 324
    - suriettiva, 66
    - vuota, 62
  - aritmetica
    - dell'orologio, 185
    - modulo  $m$ , 185
  - asse di un riferimento affine, 371, 372
  - assioma, 431
    - della scelta, 76
  - assiomi di Peano, 169
  - automorfismo, 162, 164
    - di spazi vettoriali, 324
- identico, 324
- autospazio, 351
- autovalore
  - di un endomorfismo, 357
  - di una matrice, 295
- autovettore
  - di un endomorfismo, 357
  - di una matrice, 295
  
- B
  - base
    - canonica, 318, 319
    - d'induzione, 20
    - di un monoide, 219
    - di un semigruppo, 216
    - di una rappresentazione, 173
    - di uno spazio vettoriale, 318
    - ordinata, 322
    - ortonormale, 392
  - biezione, 67
  
- C
  - cammino, 415, 416
    - euleriano, 416
  - campo, 153
    - algebricamente chiuso, 208
    - completo, 202
    - ordinato, 202
  - caratteristica di un anello unitario, 241
  - catena, 90
  - circonferenza, 389
  - circuito, 415, 416
    - euleriano, 416
  - classe d'equivalenza, 80
  - codice
    - a chiave pubblica, 190
    - RSA, 190
  - codominio, 54
  - coefficiente

- binomiale, 124
- di un polinomio, 244
- direttivo, 244
- combinazione, 123
  - con ripetizioni, 127
  - lineare, 314
- complemento, 33, 407
  - algebrico, 275
- componente
  - connessa, 416
  - di un vettore, 321
- congiunzione, 425
- congruenza, 159, 160
  - modulo  $m$ , 183
- connettivo, 425
  - proposizionale, 427
- conseguenza logica, 429
- contraddizione, 429
- controesempio, 4, 432
- controimmagine, 64
- coordinata, 42
  - cartesiana, 371, 372
- coppia, 42
- corpo, 153
  - dei quaternioni reali, 237
- corrispondenza, 51
  - biunivoca, 67
- criterio di divisibilità, 187
- crivello di Eratostene, 172
  
- D
- decomposizione diretta, 333
- denominatore, 197
- determinante
  - di una matrice, 273
  - di Vandermonde, 276
- diagonale
  - di un insieme, 42
  - principale, 258
- diagramma
  - di Hasse, 91
  - di Venn, 3
- differenza, 33
  - simmetrica, 35
- dimensione di uno spazio vettoriale, 321
- dimostrazione, 431
  - diretta, 431
  - indiretta
    - per assurdo, 431
- disgiunzione, 426
- disposizione, 121
  - con ripetizioni, 122
- distanza, 389, 393, 394
- disuguaglianza
  - di Cauchy-Schwarz, 395
  - triangolare, 395
- divisore, 12, 248
  - dello 0, 236
  - destro dello 0, 236
  - sinistro dello 0, 236
- dominio, 54
  - d'integrità, 236
  - di operatori, 152
  
- E
- elemento
  - cancellabile, 149
    - a destra, 149
    - a sinistra, 149
  - confrontabile, 90
  - di un insieme, 1
  - massimale, 93
  - minimale, 93
  - neutro, 146
    - a destra, 146
    - a sinistra, 146
  - permutabile, 144
  - regolare, 149
    - a destra, 149
    - a sinistra, 149
  - simmetrizzabile, 147
    - a destra, 148
    - a sinistra, 148
- endomorfismo, 162, 164
  - di spazi vettoriali, 324
  - diagonalizzabile, 357
  - nullo, 324
- epimorfismo, 162, 164
  - canonico, 162, 164, 240, 326
  - di spazi vettoriali, 324
- equazione
  - cartesiana
    - del piano, 386
    - della circonferenza, 389
    - della retta, 385, 387
  - congruenziale, 191
  - parametrica

- del piano, 378
- della retta, 377
- vettoriale
  - del piano, 374
  - della retta, 374
- equivalenza, 427
  - logica, 429
- estensione per linearità, 329
- estremo
  - di un intervallo reale, 203
  - di un lato, 413, 414
  - inferiore, 97
  - superiore, 97
- F**
- fattoriale, 118
- foglia, 421
- foresta, 415
- forma
  - bilineare, 394
  - simmetrica, 394
  - enunciativa, 427
  - normale
    - congiuntiva, 429
    - disgiuntiva, 429
- formula
  - contronomiale, 431
  - del binomio, 124
  - di cambiamento delle basi, 339
  - di De Morgan, 35, 42
  - di Grassmann, 332
  - di Newton, 124
- frazione, 197
  - generatrice, 201
- funzione, 54
  - di Eulero, 188
  - proposizionale, 429
- G**
- generatore, 311
- grado
  - di un polinomio, 244
  - di un vertice, 415
- grafo, 413
  - completo, 413
  - connesso, 415
  - finito, 413
  - isomorfo, 414
- regolare, 415
- vuoto, 413
- gruppo, 152
  - abeliano, 152, 220
  - alterno, 234
  - ciclico, 222
  - degli elementi simmetrizzabili
    - di un monoide, 157
  - di Klein, 228
  - di permutazioni, 231
  - generale lineare, 244
  - quadrinomio, 228
  - quoziante, 226
  - simmetrico, 231
- I**
- ideale
  - banale, 239
  - bilatero, 239
  - destro, 239
  - sinistro, 239
- immagine
  - di un elemento, 54
  - di un sottoinsieme, 62
  - di un'applicazione lineare, 326
- immersione, 62, 240, 324
- implicazione, 426
  - doppia, 427
  - logica, 429
- inclusione, 3
  - stretta, 5
- indicatore di Gauss-Eulero, 186
- indice di un sottogruppo, 225
- insieme, 1
  - ben ordinato, 95
  - dei resti modulo  $m$ , 185
  - delle parti, 6
  - di generatori, 311
  - disgiunto, 29
  - finito, 2
  - infinito, 3
  - linearmente dipendente, 314
  - linearmente indipendente, 314
  - minimale di generatori, 311
  - ordinato, 90
  - parzialmente ordinato, 90
  - potenza, 6
  - quoziante, 80
  - totalmente ordinato, 90

- uguale, 3
- vuoto, 1
- intero
  - invertibile modulo  $m$ , 186
  - modulo  $m$ , 183
- intersezione, 28
  - reticolare, 399
- intervallo reale
  - aperto, 203
  - chiuso, 203
  - illimitato, 203
  - limitato, 202
  - semiaperto, 203
- inversa
  - destra di un'applicazione, 76
  - di una matrice, 278
  - sinistra di un'applicazione, 76
- inverso di un elemento, 150
- involuzione, 68
- isomorfismo, 162, 164
  - coordinato, 331, 370
  - di grafi, 414
  - di reticolati, 403
  - di spazi vettoriali, 324
- L**
- laterale
  - destro, 224
  - sinistro, 224
- lato
  - di un grafo, 413
  - di un multigrafo, 414
  - incidente, 413
- legge
  - di annullamento del prodotto, 236
  - di assorbimento, 399
  - interna, 143
- lemma di Steinitz, 317
- lunghezza, 394
  - di un cammino, 415
  - di un ciclo, 232
  - di una parola, 215
- M**
- maggiorante, 96
- massimo, 92
- massimo comune divisore, 178
- matrice, 153, 257
  - a scala, 266
  - associata
    - a un'applicazione lineare, 336
    - complementare, 273
    - completa di un sistema lineare, 286
    - degenera, 276
    - del cambiamento di base, 340
    - di una corrispondenza, 258
    - diagonale, 258
    - diagonalizzabile, 353
    - elementare, 269
    - equivalente, 267
    - identica, 263
    - incompleta di un sistema lineare, 286
    - inversa, 278
    - invertibile, 278
    - quadrata, 258
    - ridotta, 270
    - scalare, 258
    - simile, 340, 357
    - simmetrica, 258
    - singolare, 276
    - trasposta, 258
    - triangolare inferiore, 258
    - triangolare superiore, 258
  - metodo
    - di Cramer, 287
    - di Fermat, 210
    - di Gauss-Jordan, 289
    - $p - 1$  di Pollard, 211
    - “standard”, 209
  - minimo, 92
  - minimo comune multiplo, 181
  - minorante, 96
  - minore, 282
    - orlato, 284
  - molteplicità
    - algebrica, 351
    - di una radice, 249
    - geometrica, 351
  - monoide, 152
    - associato a un semigruppo, 217
    - delle parole, 218
    - libero, 219
  - monomio, 245
  - monomorfismo, 162, 164
    - di spazi vettoriali, 324
  - multigrafo, 414
    - connesso, 416
    - finito, 415

multiplo, 12, 150, 248

## N

*n*-upla, 45

negazione, 425

norma, 389, 392, 394

di un numero complesso, 208

notazione

additiva, 150

moltiplicativa, 150

nucleo

di un omomorfismo, 223, 240

di un prodotto scalare, 394

di un'applicazione lineare, 326

numeratore, 197

numero

complesso, 207

coniugato, 207

composto, 13

decimale, 200

limitato, 200

periodico, 200

di Bell, 129

di Ramsey, 137

di Stirling, 129

intero, 13, 175

coprimo, 180

naturale, 8

dispari, 17

pari, 16

primo, 13, 178

razionale, 17, 198

reale, 202

irrazionale, 202

## O

omomorfismo, 162, 164, 165

di anelli, 240

di gruppi, 223

di insiemi ordinati, 91

di monoidi, 219

di reticolati, 403

di semigruppi, 216

di spazi vettoriali, 324

identico, 324

nullo, 240

operatore, 152

operazione

associativa, 144

commutativa, 144

di concatenazione, 215

di giustapposizione, 215

distributiva, 151

a destra, 151

a sinistra, 151

elementare, 267

esterna, 152

indotta, 156

interna, 143

quoziente, 159

opposto di un elemento, 150

ordine

del "divide", 12

di un grafo, 413

di un insieme, 2

lexicografico, 102

usuale, 11, 14

origine

di un riferimento affine, 371

origine di un riferimento affine, 372

## P

parametro direttore, 244, 377, 380

parola, 215

vuota, 218

parte

chiusa, 156

frazionaria, 203

intera, 199, 200, 202

stabile, 156

generata, 158

partizione, 79

identica, 79

totale, 79

passo induttivo, 20

periodo, 200

permutazione, 118

con ripetizioni, 119

disgiunta, 232

dispari, 234

pari, 234

pivot, 267

polinomio, 244

caratteristico

di un endomorfismo, 357

di una matrice, 296

costante, 245

- derivato, 250
- monico, 246
- nullo, 245
- potenza, 10, 14, 151
- predicato, 429
  - a più posti, 430
- principio
  - d'induzione, 20, 170
  - dei cassetti, 115
    - forma forte, 116
  - di addizione, 111
  - di dualità dei reticolati, 400
  - di inclusione-esclusione, 112
  - di moltiplicazione, 113
    - forma generale, 114
- problema dei ponti di Königsberg, 416
- prodotto
  - cartesiano, 42
  - di applicazioni, 69
  - operativo di applicazioni, 70
  - righe per colonne, 262
  - scalare, 391, 394
    - canonico, 392
    - definito positivo, 394
    - non degenere, 394
  - proiezione, 75
    - canonica, 80
  - prolungamento di un'applicazione, 75
- proposizione, 425
  - atomica, 427
- proprietà
  - di tricotomia, 12
  - iterativa, 399
  - universale
    - dei semigruppi liberi, 216
    - dell'anello dei polinomi, 250
- prova del nove, 188
- punto d'incidenza, 380
  
- Q**
- quantificatore
  - esistenziale, 4, 430
  - universale, 3, 430
- quoziente, 170, 176, 246
  
- R**
- radice
  - di un polinomio, 248, 358
- doppia, 249
- multipla, 249
- semplice, 249
- tripla, 249
- rango
  - di un'applicazione lineare, 344
  - di una matrice, 283
- rappresentazione
  - binaria, 174
  - decimale, 173
  - dei numeri naturali, 173
- regola
  - di Cramer, 287
  - di Sarrus, 274
- relazione, 51
  - antiriflessiva, 57
  - asimmetrica, 55
  - binaria, 53
  - d'equivalenza, 56
    - compatibile, 159, 160
    - compatibile a destra, 161
    - compatibile a sinistra, 161
  - d'identità, 53
  - d'ordine, 56
    - stretto, 90
    - usuale, 199
  - d'uguaglianza, 53
  - indotta, 53, 83
  - inversa, 53
  - opposta, 53
  - riflessiva, 54
  - simmetrica, 55
  - totale, 52
  - transitiva, 55
  - vuota, 52
- resto, 170, 176, 246
- modulo  $m$ , 185
- restrizione di un'applicazione, 75
- reticolo, 98, 399
  - booleano, 408
  - complementato, 407
  - completo, 402
  - dei numeri naturali, 401
  - dei sottogruppi, 401
  - dei sottospazi, 401
  - delle parti di un insieme, 401
  - distributivo, 405
  - modulare, 407
  - pentagonale, 406
  - trirettangolo, 406

- retta  
 incidente, 380  
 sgombra, 381
- riferimento affine  
 del piano, 371  
 dello spazio, 372  
 ortonormale, 388
- S**  
 scalare, 152, 306  
 segnatura di una permutazione, 234  
 semigruppo, 152  
 delle parole, 215  
 libero, 216  
 simbolo di Kronecker, 263  
 simmetrico, 147  
 a destra, 148  
 a sinistra, 148  
 singleton, 1  
 sistema lineare, 285  
 compatibile, 286  
 equivalente, 287  
 incompatibile, 287  
 omogeneo, 286  
 associato, 346  
 soluzione, 286  
 somma diretta di sottospazi, 333  
 sostituzione, 118  
 sottoalgebra, 408  
 sottoanello, 237  
 banale, 237  
 fondamentale, 241  
 generato, 239  
 sottografo, 414  
 generato, 414  
 sottogruppo, 220  
 banale, 220  
 generato, 222  
 normale, 226  
 sottoinsieme, 3  
 chiuso, 156  
 stabile, 156, 157  
 sottomatrice, 282  
 sottomonoide, 218  
 generato, 218  
 sottoreticolato, 400  
 proprio, 400  
 sottosemigruppo, 215  
 generato, 216
- sottospazio, 309  
 banale, 309  
 diagonale, 309  
 generato, 310  
 proprio, 309  
 somma, 312  
 supplementare, 333
- spazio vettoriale, 305  
 destro, 153  
 finitamente generato, 311  
 metrico, 394  
 nullo, 306  
 quoziente, 325  
 sinistro, 153
- struttura  
 algebrica, 152  
 semplice, 152  
 prodotto, 154
- successione, 61  
 successivo di un numero naturale, 169  
 supplementare, 333  
 supporto di una permutazione, 231
- T**  
 tautologia, 428  
 tavola  
 di moltiplicazione, 145  
 di verità, 425  
 teorema  
 cinese del resto, 192  
 generalizzazione, 196  
 di addizione dei gradi, 246  
 di Bézout, 180  
 di Binet, 276  
 di Cayley-Hamilton, 358  
 di Cramer, 287  
 di Euclide, 171  
 di Fermat-Eulero, 189  
 di Lagrange, 225  
 di omomorfismo, 163, 164  
 negli anelli, 241  
 negli spazi vettoriali, 326  
 nei gruppi, 226  
 di Pitagora, 396  
 di Ramsey, 137  
 di Rouché-Capelli, 346  
 di Ruffini, 248  
 generalizzato, 248  
 di Stone, 410

di Wedderburn, 237  
di Wilson, 189  
fondamentale  
    dell'algebra, 208  
    dell'aritmetica, 13, 171, 181  
    sulle relazioni d'equivalenza, 82  
piccolo di Fermat, 189  
termine noto, 286  
traccia, 323  
traslazione, 372  
    destra, 155  
    sinistra, 155  
trasposizione, 232  
triangolo  
    di Stirling, 130  
    di Tartaglia, 126

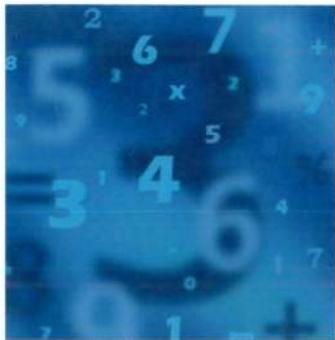
**U**

unione, 25  
    disgiunta, 35  
    reticolare, 399  
unità immaginaria, 207

**V**

valore  
    assoluto, 16  
    di verità, 425  
vertice  
    adiacente, 413  
    di un grafo, 413  
    di un multigrafo, 414  
    dispari, 415  
    isolato, 415  
    pari, 415  
vettore, 306  
    applicato, 367  
    congruente, 367  
coordinato, 322  
di giacitura, 376  
di traslazione, 375, 376  
direttore, 375  
nullo, 306  
ortogonale, 392, 396

Finito di stampare  
nel mese di gennaio 2009



Costantino Delizia  
Patrizia Longobardi  
Mercede Maj  
Chiara Nicotera

## Matematica discreta

Il testo, che nasce dalla lunga esperienza didattica degli Autori, si rivolge a tutti i corsi di Matematica discreta delle lauree triennali, ma si presta bene a essere utilizzato per qualunque corso che si ponga come obiettivo quello di fornire agli studenti conoscenze matematiche di base, abituandoli ad adottare un'impostazione rigorosa nell'approccio ai problemi.

I contenuti del libro spaziano dagli argomenti da sempre peculiari della Matematica discreta a quelli più tipici di Combinatoria, di Algebra, di Algebra lineare e di Geometria. Il volume termina con un'Appendice contenente cenni di logica proposizionale e predicativa.

La trattazione è sempre rigorosa ma non eccessivamente formale ed è accompagnata da esempi, numerosi e particolarmente curati, e da un ricchissimo apparato di esercizi che ammontano a quasi 900, parte dei quali svolti nel testo e tutti con soluzione sul sito internet dedicato.

All'indirizzo web [www.ateneonline.it/delizia](http://www.ateneonline.it/delizia) sono disponibili materiali di supporto: per i docenti i lucidi in formato PDF, per gli studenti le soluzioni di tutti gli esercizi del testo.

**Costantino Delizia** è ricercatore confermato di Algebra e insegna Matematica discreta presso l'Università degli Studi di Salerno.

**Patrizia Longobardi** è professore ordinario di Algebra e insegna Matematica discreta presso l'Università degli Studi di Salerno.

**Mercede Maj** è professore ordinario di Algebra presso l'Università degli Studi di Salerno.

**Chiara Nicotera** è ricercatore confermato di Algebra e insegna Matematica discreta presso l'Università degli Studi di Salerno.

€ 32,00 (i.i.)

ISBN 978-88-386-6512-7

► [www.mcgraw-hill.it](http://www.mcgraw-hill.it)

► [www.ateneonline.it](http://www.ateneonline.it)

9 788838 665127

