

## PARTE PRIMA

## INSIEMI

## Capitolo 1. Insiemi

Un *insieme* è una collezione di oggetti. Ad esempio sono insiemi: (1) l'insieme dei numeri 0, 1, 2, 3 e 4; (2) l'insieme delle soluzioni dell'equazione  $x^2 - 1 = 0$ ; (3) l'insieme dei punti di un piano fissato; (4) l'insieme dei numeri interi pari, cioè l'insieme dei numeri 0, 2, -2, 4, -4, 6, -6, 8, -8, .... Come mostrano questi esempi un insieme è individuato dagli oggetti che lo costituiscono, cioè dai suoi *elementi*: gli elementi del primo esempio che abbiamo visto sono cinque, e sono i numeri 0, 1, 2, 3, 4; gli elementi dell'insieme delle soluzioni dell'equazione  $x^2 - 1 = 0$  sono i numeri 1 e -1, e così via. Talvolta invece di parlare di insieme parleremo di *famiglia* o di *classe*.

Alcuni insiemi di uso particolarmente frequente in matematica vengono denotati con simboli speciali. Ad esempio denotiamo

- con  $\emptyset$  l'*insieme vuoto* (che non ha elementi);
- con  $\mathbb{N}$  l'*insieme dei numeri naturali* (cioè l'insieme i cui elementi sono i numeri 0, 1, 2, 3, 4, 5, ....);
- con  $\mathbb{N}^*$  l'insieme dei numeri naturali diversi da zero;
- con  $\mathbb{Z}$  l'*insieme dei numeri interi* (i suoi elementi sono i numeri 0, 1, -1, 2, -2, 3, -3, 4, -4, ....);
- con  $\mathbb{Q}$  l'*insieme dei numeri razionali* (i suoi elementi sono i numeri che si possono scrivere nella forma  $p/q$ , dove  $p$  e  $q$  sono numeri interi e  $q \neq 0$ );
- con  $\mathbb{R}$  l'*insieme dei numeri reali* (sono i numeri esprimibili in notazione decimale, eventualmente con infinite cifre dopo la virgola).

Se  $A$  è un insieme scriveremo  $x \in A$  per indicare che  $x$  è un *elemento* di  $A$ , e  $x \notin A$  per indicare che  $x$  non è un *elemento* di  $A$ .



Se  $A$  e  $B$  sono insiemi,  $A$  è *sottoinsieme* di  $B$  se ogni elemento di  $A$  è anche un elemento di  $B$ . In tal caso scriveremo  $A \subseteq B$ . Per dimostrare che  $A \subseteq B$  si deve far vedere che se  $x \in A$  allora  $x \in B$ . Ad esempio si ha (1)  $A \subseteq A$  per ogni insieme  $A$ ; (2)  $\mathbb{N}^* \subseteq \mathbb{N}$ ; (3)  $\mathbb{N} \subseteq \mathbb{Z}$ ; (4)  $\mathbb{Q} \subseteq \mathbb{R}$ . Inoltre si ha  $\emptyset \subseteq A$  per ogni insieme  $A$ .

Se  $A$  e  $B$  sono insiemi, scriveremo  $A = B$  per indicare che  $A \subseteq B$  e  $B \subseteq A$ . Quindi  $A = B$  significa che  $A$  e  $B$  hanno gli stessi elementi, vale a dire che  $x \in A$  se e solo se  $x \in B$ .

Scriveremo invece  $A \subset B$  per indicare che  $A$  è un *sottoinsieme proprio* di  $B$ , cioè che  $A \subseteq B$  e  $A \neq B$ . Pertanto  $A \subset B$  significa che ogni elemento di  $A$  appartiene a  $B$  ma esiste un elemento di  $B$  che non appartiene ad  $A$ . Ad esempio si ha  $\mathbb{N}^* \subset \mathbb{N}$ ,  $\mathbb{N} \subset \mathbb{Z}$ ,  $\mathbb{N} \subset \mathbb{Q}$ ,  $\mathbb{Z} \subset \mathbb{R}$ , eccetera.

**Come si denota un insieme.** Esistono vari modi per denotare un insieme. Un primo modo è quello di elencare i suoi elementi racchiudendoli tra parentesi graffe. Ad esempio l'insieme i cui elementi sono i numeri 0, 1, 2, 3 e 4 può essere denotato con  $\{0, 1, 2, 3, 4\}$ . L'insieme i cui elementi sono le soluzioni dell'equazione  $x^2 - 1$  può essere denotato con  $\{1, -1\}$ . L'insieme  $\mathbb{N}$  può anche essere denotato con  $\{0, 1, 2, 3, 4, 5, \dots\}$ .

Un secondo modo per denotare un insieme consiste nel far uso di una proprietà soddisfatta da tutti e soli gli elementi di quell'insieme. Ad esempio l'insieme  $\{0, 1, 2, 3, 4\}$  può anche essere denotato con

$$\{x \mid x \in \mathbb{N}, x < 5\}$$

(che si legge "l'insieme degli  $x$  tali che  $x \in \mathbb{N}$ ,  $x < 5$ "), l'insieme dei numeri interi pari può essere denotato con

$$\{x \mid x \in \mathbb{Z} \text{ e } x \text{ è pari}\}$$

(che si legge "l'insieme degli  $x$  tali che  $x \in \mathbb{Z}$  e  $x$  è pari"), l'insieme  $\mathbb{Q}$  dei numeri razionali può essere denotato con

$$\{x \mid x = p/q, p, q \in \mathbb{Z} \text{ e } q \neq 0\}$$

(che si legge "l'insieme degli  $x$  tali che  $x = p/q$ , dove  $p, q \in \mathbb{Z}$  e  $q \neq 0$ "). Quindi con la notazione  $\{x \mid \dots\}$  si intende l'insieme di tutti gli  $x$  che soddisfano la proprietà scritta dopo la sbarretta verticale.

Si faccia attenzione a non confondere  $x$  e  $\{x\}$ , ossia  $x$  e l'insieme che contiene  $x$ . In particolare gli insiemi  $\emptyset$ ,  $\{\emptyset\}$ ,  $\{\{\emptyset\}\}$ ,  $\{\emptyset, \{\emptyset\}\}$  sono tutti distinti tra loro. Infatti  $\emptyset$  ha zero elementi,  $\{\emptyset\}$  ha un solo elemento (che è  $\emptyset$ ),  $\{\{\emptyset\}\}$  ha un solo elemento (che è  $\{\emptyset\}$ ),  $\{\emptyset, \{\emptyset\}\}$  ha due elementi (che sono  $\emptyset$  e  $\{\emptyset\}$ ).

**Operazioni tra insiemi.** Se  $A$  e  $B$  sono insiemi definiamo

$$\begin{aligned} A \cup B &= \{x \mid x \in A \text{ oppure } x \in B\} && (\text{unione di } A \text{ e } B) \\ A \cap B &= \{x \mid x \in A \text{ e } x \in B\} && (\text{intersezione di } A \text{ e } B) \\ A \setminus B &= \{x \mid x \in A \text{ e } x \notin B\} && (\text{differenza di } A \text{ e } B) \\ A \triangle B &= (A \setminus B) \cup (B \setminus A) && (\text{differenza simmetrica di } A \text{ e } B). \end{aligned}$$

Due insiemi  $A$  e  $B$  si dicono *disgiunti* se  $A \cap B = \emptyset$ .

Se  $A, B, C$  sono insiemi si ha

$$A \cup (B \cap C) = (A \cup B) \cap C \quad \text{e} \quad A \cap (B \cup C) = (A \cap B) \cup C$$

(*proprietà associativa di  $\cup$  e  $\cap$* ). Pertanto si possono tralasciare le parentesi e scrivere semplicemente  $A \cup B \cup C$  e, rispettivamente,  $A \cap B \cap C$ .

Dato un insieme  $A$ , l'*insieme della parti* di  $A$  è l'insieme di tutti i sottoinsiemi di  $A$ . Si denota con  $\mathcal{P}(A)$ . I suoi elementi sono i sottoinsiemi di  $A$ , cioè  $\mathcal{P}(A) = \{X \mid X \subseteq A\}$ .

**ESEMPIO 1 (*proprietà distributive*).** Dimostriamo che se  $A, B, C$  sono insiemi, allora

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{e} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Dimostriamo intanto la prima uguaglianza. Per far vedere che i due insiemi  $A \cap (B \cup C)$  e  $(A \cap B) \cup (A \cap C)$  sono uguali si deve dimostrare che  $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$  e che  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ . Verificare la *doppia inclusione*, cioè dimostrare che due insiemi sono uguali facendo vedere che ciascuno dei due insiemi è sottoinsieme dell'altro, è il metodo usuale con cui si dimostra che due insiemi coincidono.

Facciamo vedere intanto che si ha  $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ . Se  $x \in A \cap (B \cup C)$ , allora  $x \in A$  e  $x \in B \cup C$ . Quindi  $x \in B$  oppure  $x \in C$ . Pertanto  $x \in A$  e  $x \in B$ , oppure  $x \in A$  e  $x \in C$ . Da qui si ricava che  $x \in A \cap B$  o  $x \in A \cap C$ , e si conclude che  $x \in (A \cap B) \cup (A \cap C)$ . Abbiamo così dimostrato l'inclusione  $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ .

Dimostriamo ora che  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ . Dato che  $x \in (A \cap B) \cup (A \cap C)$ , possono accadere due casi: che  $x \in A \cap B$  oppure che  $x \in A \cap C$ . Se  $x \in A \cap B$ , allora  $x \in A$  e  $x \in B$ . Quindi  $x \in A$  e  $x \in B \cup C$ . Se ne deduce che in questo caso  $x \in A \cap (B \cup C)$ . Analogamente se  $x \in A \cap C$  si deve avere che  $x \in A$  e  $x \in C$ . Quindi  $x \in A$  e  $x \in B \cup C$ . Anche in questo caso si ottiene quindi che  $x \in A \cap (B \cup C)$ . Pertanto in entrambi i casi  $x \in A \cap (B \cup C)$ , e abbiamo così dimostrato che  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ .

Da  $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$  e  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$  possiamo concludere che  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ .

La dimostrazione della seconda uguaglianza è analoga.  $\square$

**Notazioni "compatte".** Vogliamo presentare un modo conveniente per denotare somme e prodotti di numeri e unioni e intersezioni di insiemi.

Per scrivere la somma dei quadrati dei primi cinque numeri interi positivi possiamo scrivere  $1^2 + 2^2 + 3^2 + 4^2 + 5^2$ . Ma c'è anche una notazione più compatta per scrivere tale somma. La possiamo infatti scrivere nella forma  $\sum_{i=1}^5 i^2$ ; questo si legge "la somma, per  $i$  che va da 1 a 5, di  $i^2$ ", intendendosi in tal modo appunto la somma degli addendi del tipo  $i^2$  quando l'indice  $i$  è uguale a 1, 2, 3, 4 e 5 rispettivamente. Il simbolo  $\sum$  è una sigma maiuscola. Qualcuno invece di dire "la somma per  $i$  che va da ..." preferisce dire "la sommatoria per  $i$  di dire "la somma per  $i$  che va da ...". Un altro esempio di una somma scritta con questa notazione che va da ...". Un altro esempio di una somma scritta con questa notazione è  $\sum_{i=0}^{10} (i+2)(i-1)$ , che è la somma, per  $i$  che va da 0 a 10, di addendi del tipo  $(i+2)(i-1)$ , ossia è

$$(0+2)(0-1) + (1+2)(1-1) + (2+2)(2-1) + (3+2)(3-1) + \dots + (10+2)(10-1).$$

Analogamente

$$\sum_{i=5}^9 (i^2 - 1) = (5^2 - 1) + (6^2 - 1) + (7^2 - 1) + (8^2 - 1) + (9^2 - 1).$$

Si usa una notazione simile anche per denotare i prodotti. In questo caso scriveremo  $\prod$ , cioè una  $\pi$  greca maiuscola, invece della  $\sum$ ; ad esempio  $\prod_{i=1}^5 i^2$  è il prodotto, per  $i$  che va da 1 a 5, di  $i^2$ , cioè è  $1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 \cdot 5^2$ . Altri esempi di prodotti scritti in questa notazione sono

$$\prod_{i=0}^{10} (i+2)(i-1) = [(0+2)(0-1)][(1+2)(1-1)] \cdot [(2+2)(2-1)][(3+2)(3-1)] \dots [(10+2)(10-1)]$$

(e questo prodotto è ovviamente uguale a 0), e

$$\prod_{i=5}^9 (i^2 - 1) = (5^2 - 1)(6^2 - 1)(7^2 - 1)(8^2 - 1)(9^2 - 1).$$

Per le unioni e le intersezioni di insiemi si procede in modo analogo. Ad esempio se  $A_1, A_2, \dots, A_n$  sono insiemi, per indicare la loro unione si può scrivere  $\bigcup_{i=1}^n A_i$  invece di  $A_1 \cup A_2 \cup \dots \cup A_n$ . Analogamente per indicare l'intersezione degli  $n$  insiemi  $A_1, A_2, \dots, A_n$  si può scrivere  $\bigcap_{i=1}^n A_i$  in luogo di  $A_1 \cap A_2 \cap \dots \cap A_n$ .

**ESEMPIO 2.** Se  $A_1 = \{1, 2, 3\}$ ,  $A_2 = \{2, 3, 4\}$ ,  $A_3 = \{3, 4, 5\}$ , ...,  $A_{10} = \{10, 11, 12\}$ , allora

$$\bigcup_{i=1}^{10} A_i = \{1, 2, 3, \dots, 12\}, \quad \bigcap_{i=1}^3 A_i = \{3\}, \quad \bigcap_{i=1}^{10} A_i = \emptyset. \quad \square$$

La definizione di unione  $A_1 \cup A_2 \cup \dots \cup A_n$  di  $n$  insiemi  $A_1, A_2, \dots, A_n$  può essere estesa ulteriormente al caso in cui gli insiemi di cui si costruisce l'unione siano non solamente  $n$  (ossia un numero finito), bensì siano infiniti insiemi. Ad esempio poniamo  $A_i = \{i, i+1, i+2\}$  per ogni  $i \in \mathbb{Z}$ . Quindi abbiamo infiniti insiemi  $A_i$ , uno per ogni numero intero  $i \in \mathbb{Z}$ , e ciascun  $A_i$  ha tre elementi. Diremo in questo caso che  $\mathcal{F} = \{A_i \mid i \in \mathbb{Z}\}$  è una famiglia di insiemi  $A_i$ ; in questo esempio l'indice  $i$  appartiene all'insieme  $\mathbb{Z}$  dei numeri interi. È allora possibile formare l'unione

$$\bigcup_{i \in \mathbb{Z}} A_i = \{x \mid x \in A_i \text{ per qualche } i \in \mathbb{Z}\}$$

e l'intersezione

$$\bigcap_{i \in \mathbb{Z}} A_i = \{x \mid x \in A_i \text{ per ogni } i \in \mathbb{Z}\}.$$

In questo primo esempio si ha ovviamente  $\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{Z}$  e  $\bigcap_{i \in \mathbb{Z}} A_i = \emptyset$ .

Facciamo un altro esempio. Per ogni  $i \in \mathbb{N}$  sia

$$A_i = \{x \mid x \in \mathbb{Q}, x \neq i\}.$$

Adesso l'indice  $i$  appartiene all'insieme  $\mathbb{N}$  dei numeri naturali, ossia abbiamo un insieme  $A_i$  per ogni numero naturale  $i$ . In questo caso  $\bigcup_{i \in \mathbb{N}} A_i$  è l'insieme degli  $x \in \mathbb{Q}$  tali che  $x \neq i$  per qualche  $i \in \mathbb{N}$ . Ovviamente ogni numero razionale  $x$  ha questa proprietà, e quindi  $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{Q}$ . Invece  $\bigcap_{i \in \mathbb{N}} A_i$  è l'insieme degli  $x \in \mathbb{Q}$  tali che  $x \neq i$  per ogni  $i \in \mathbb{N}$ . Gli  $x$  che hanno questa proprietà sono ovviamente i numeri razionali che non sono numeri naturali. Quindi in questo caso  $\bigcap_{i \in \mathbb{N}} A_i = \mathbb{Q} \setminus \mathbb{N}$ .

### Esercizi svolti

**1.1.** Si dimostri che se  $A \subseteq B$ , allora  $(B \setminus A) \cap A = \emptyset$  e  $(B \setminus A) \cup A = B$ .

**Soluzione.** Per dimostrare che un certo insieme è vuoto conviene in generale ragionare per assurdo, cioè supporre che sia non vuoto e dedurre una contraddizione. Ad esempio per risolvere la prima parte di questo esercizio siano  $A \subseteq B$  due insiemi e supponiamo per assurdo che  $(B \setminus A) \cap A \neq \emptyset$ . Da  $(B \setminus A) \cap A \neq \emptyset$  segue che esiste  $x \in (B \setminus A) \cap A$ . Allora  $x \in (B \setminus A)$  e  $x \in A$ . Ne segue che  $x \notin A$

e  $x \in A$ , e questa è una contraddizione. Abbiamo così dimostrato che si deve avere  $(B \setminus A) \cap A = \emptyset$ .

Mostriamo ora che se  $A \subseteq B$ , allora  $(B \setminus A) \cup A = B$ . Dato che  $B \setminus A \subseteq B$  e  $A \subseteq B$ , abbiamo che  $(B \setminus A) \cup A \subseteq B$ . Per mostrare che  $B \subseteq (B \setminus A) \cup A$  e  $A \subseteq B$ , abbiamo che  $(B \setminus A) \cup A \subseteq B$ . Allora si possono avere i due casi  $b \in A$  oppure  $b \notin A$ . Se fissiamo  $b \in B$ . Allora si possono avere i due casi  $b \in A$  oppure  $b \notin A$ . Se invece  $b \notin A$ , si ha che  $b \in B \setminus A$ , e quindi  $b \in (B \setminus A) \cup A$ . In entrambi i casi si ha quindi  $b \in (B \setminus A) \cup A$ , e questo prova che  $B \subseteq (B \setminus A) \cup A$ .  $\square$

1.2.  $A \subseteq C$ ,  $B \subseteq C$ ,  $A \cap B = \emptyset$  e  $A \cup B = C$ , allora  $A = C \setminus B$ .

*Soluzione.* Per dimostrare che  $A = C \setminus B$  dobbiamo far vedere che  $A \subseteq C \setminus B$  e che  $C \setminus B \subseteq A$ .

Sia  $a \in A$ . Dato che  $A \subseteq C$  si deve avere  $a \in C$ . Mostriamo che  $a \notin B$ . Se per assurdo fosse  $a \in B$ , allora  $a \in A \cap B$ , e questo è assurdo perché  $A \cap B = \emptyset$ . Quindi deve essere  $a \notin B$ . Ma allora  $a \in C$  e  $a \notin B$ , da cui  $a \in C \setminus B$ . Abbiamo così dimostrato che  $A \subseteq C \setminus B$ .

Viceversa sia  $c \in C \setminus B$ . Allora  $c \in C$  e  $c \notin B$ . Mostriamo che  $c \in A$ . Se per assurdo fosse  $c \notin A$ , allora da  $c \notin A$  e  $c \notin B$  segue che  $c \notin A \cup B$ , da cui per assurdo fosse  $c \notin A$ . Questa è una contraddizione. Si deve avere quindi  $c \in A$ . Abbiamo così dimostrato che  $C \setminus B \subseteq A$ .  $\square$

1.3. Siano  $A$  e  $B$  insiemi. Si dimostri che le seguenti affermazioni sono equivalenti:

- (a)  $A \cap B = A$ ;
- (b)  $A \subseteq B$ ;
- (c)  $A \cup B = B$ .

*Soluzione.* Per dimostrare che le tre affermazioni (a), (b) e (c) sono equivalenti dimostreremo che (a) implica (b), che (b) implica (c), e che (c) implica (a).

Mostriamo innanzitutto che (a) implica (b). Se (a) è vera, cioè se  $A \cap B = A$ , allora per ogni  $a \in A$  si ha che  $a \in A \cap B$ , e quindi in particolare  $a \in B$ . Abbiamo così dimostrato che ogni  $a \in A$  sta anche in  $B$ , cioè che  $A \subseteq B$ . Questa è l'affermazione (b).

Mostriamo che (b) implica (c). Se (b) è vera, cioè se  $A \subseteq B$ , prendiamo un elemento  $x \in A \cup B$ . Allora si hanno i due casi  $x \in A$  oppure  $x \in B$ . Ma anche nel caso in cui  $x \in A$  si deve avere che  $x \in B$  perché  $A \subseteq B$ . Quindi in entrambi i casi si ha  $x \in B$ . Pertanto  $A \cup B \subseteq B$ . Dato che l'inclusione  $B \subseteq A \cup B$  è vera qualunque siano gli insiemi  $A$  e  $B$ , si conclude che  $A \cup B = B$ .

Mostriamo infine che (c) implica (a). Supponiamo che  $A \cup B = B$ , e proviamo che  $A \cap B = A$ . Certamente si ha che  $A \cap B \subseteq A$ . Viceversa sia  $x \in A$ . Si deve allora avere in particolare che  $x \in A \cup B = B$ . Quindi  $x$  appartiene sia ad  $A$  che

a  $B$ , ossia  $x \in A \cap B$ . Abbiamo così dimostrato anche l'inclusione  $A \subseteq A \cap B$ . Questo conclude la dimostrazione.  $\square$

### Altri esercizi

1.4. Sia  $A = \{0, 1, 2\}$ . Si dica se le affermazioni che seguono sono vere o false:

- (a)  $\{0\} \subseteq A$ ; (b)  $\{0\} \in A$ ; (c)  $0 \in A$ ; (d)  $\{0\} \subseteq A$ ;
- (e)  $\{\emptyset\} \in A$ ; (f)  $\emptyset \in A$ ; (g)  $\emptyset \subseteq A$ .

1.5. Si dica se le affermazioni che seguono sono vere o false:

- (a)  $\sqrt{2} \in \mathbb{N}$ ; (b)  $\sqrt{2} \in \mathbb{N}^*$ ; (c)  $\sqrt{2} \in \mathbb{Z}$ ;
- (d)  $\sqrt{2} \in \mathbb{Q}$ ; (e)  $\sqrt{2} \in \mathbb{R}$ .

1.6. Si dica se le affermazioni che seguono sono vere o false:

- (a)  $-1 \in \mathbb{N}$ ; (b)  $-1 \in \mathbb{N}^*$ ; (c)  $-1 \in \mathbb{Z}$ ;
- (d)  $-1 \in \mathbb{Q}$ ; (e)  $-1 \in \mathbb{R}$ .

1.7. Si dica se le affermazioni che seguono sono vere o false:

- (a)  $\frac{2}{3} \in \mathbb{N}$ ; (b)  $\frac{2}{3} \in \mathbb{N}^*$ ; (c)  $\frac{2}{3} \in \mathbb{Z}$ ;
- (d)  $\frac{2}{3} \in \mathbb{Q}$ ; (e)  $\frac{2}{3} \in \mathbb{R}$ .

1.8. Si dica se le affermazioni che seguono sono vere o false:

- (a)  $\mathbb{Z} \subseteq \{x \mid x \in \mathbb{N}, 1 \leq x < 6\}$ ;
- (b)  $\{-5, -4, -3, -1\} = \{x \mid x \in \mathbb{Z}, -5 \leq x \leq -1\} \setminus \{-2\}$ ;
- (c)  $\mathbb{N} \subset \{x \mid x \in \mathbb{Z}, x \geq 0\}$ ;
- (d)  $\{x \mid x \in \mathbb{R}, x(x^2 - 1)(x - 2) = 0\} = \{0, 1, -1, 2\}$ .

1.9. Quanti elementi ha

- (a) l'insieme  $\{x \mid x \in \mathbb{N}, 1 \leq x < 6\}$ ?
- (b) l'insieme vuoto  $\emptyset$ ?

1.10. Quanti elementi ha

- (a) l'insieme  $\{x \mid x \in \mathbb{Z}, 0 \leq x \leq 1\}$ ?
- (b) l'insieme  $\{x \mid x \in \mathbb{R}, 0 \leq x \leq 1\}$ ?
- (c) l'insieme  $\{\emptyset, 1\}$ ?

1.11. Se  $A = \{\emptyset, 1\}$  e  $B = \{x \mid x \in \mathbb{Z}, 0 \leq x \leq 1\}$ , quanti elementi hanno gli insiemi  $A \cup B$ ,  $A \cap B$ ,  $A \setminus B$  e  $A \triangle B$ ?

- 1.12. Gli insiemi  $\{\{\emptyset\}\}$  e  $\{\emptyset, \{\emptyset\}\}$  sono disgiunti?
- 1.13. (a) Quali e quanti sono gli elementi dell'insieme  $\mathcal{P}(\{2, 4, 8\})$ ?  
 (b) Quali e quanti sono gli elementi dell'insieme  $\mathcal{P}(\{\{\emptyset\}, 2\})$ ?
- 1.14. Se  $A$  e  $B$  sono insiemi, si dimostri che  $A \cup B = (A \setminus B) \cup B$ .
- 1.15. Se  $A$  è un insieme e  $B \subseteq A$ , si dimostri che  $A \setminus (A \setminus B) = B$ .
- 1.16. Scrivere in notazione compatta  
 (a)  $(1^3 - 1^2) + (2^3 - 2^2) + (3^3 - 3^2) + (4^3 - 4^2) + (5^3 - 5^2) + (6^3 - 6^2)$ ;  
 (b)  $(-1)^1 + (-1)^2 + (-1)^3 + (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7$ .
- 1.17. Si calcoli  $\sum_{n=1}^5 (-1)^n n$ .
- 1.18. Si calcoli  $\prod_{k=1}^5 k$ .
- 1.19. Per ogni  $n \in \mathbb{N}$  sia  $A_n = \{x \mid x \in \mathbb{N}, 0 \leq x \leq n\}$ . Si calcolino  $\bigcup_{n=0}^5 A_n$ ,  $\bigcap_{n=0}^5 A_n$ ,  $\bigcup_{n \in \mathbb{N}} A_n$ ,  $\bigcap_{n \in \mathbb{N}} A_n$ .
- 1.20. Per ogni  $i \in \mathbb{Z}$  sia  $A_i = \{x \mid x \in \mathbb{N}, x \geq i\}$ . Si determinino  $\bigcup_{i \in \mathbb{Z}} A_i$  e  $\bigcap_{i \in \mathbb{Z}} A_i$ .
- 1.21. Dimostrare che se  $A$  è un insieme, allora  

$$\bigcup_{X \subseteq A} X = A \quad \text{e} \quad \bigcap_{X \subseteq A} X = \emptyset.$$
- 1.22. Siano  $A$  e  $B$  insiemi. Si dimostri che  
 (a) se  $A = \emptyset$ , allora  $B = (A \setminus B) \cup (B \setminus A)$ ;  
 (b) se  $B = (A \setminus B) \cup (B \setminus A)$ , allora  $A = \emptyset$ .

## Capitolo 2. Applicazioni

**Prodotto cartesiano.** Per definire un sistema di coordinate su una retta  $r$  è necessario fissare un'orientamento su  $r$ , un'origine (cioè un punto di  $r$ ) e un'unità di misura. Fissato un sistema di coordinate sulla retta  $r$  otterremo che ad ogni punto  $P$  di  $r$  resta associato un unico numero reale  $a$  (la sua *coordinata*) e viceversa ad ogni numero reale  $a$  resta associato un unico punto  $P$  della retta  $r$  avente  $a$  come coordinata. Otteniamo così quella che, come vedremo in seguito, si chiama una *corrispondenza biunivoca* tra l'insieme dei punti della retta  $r$  e l'insieme  $\mathbb{R}$  dei numeri reali.

Analogamente si procede in un piano. È noto al lettore come sia possibile definire un sistema di coordinate in un piano  $\pi$  dopo aver fissato due rette orientate ortogonali nel piano (gli assi) e un'unità di misura. Si ottiene così che ad ogni punto  $P$  del piano  $\pi$  resta associata un'unica coppia ordinata  $(a, b)$  di numeri reali (le sue *coordinate*) e viceversa ad ogni coppia ordinata  $(a, b)$  di numeri reali resta associato un unico punto  $P$  del piano  $\pi$  avente  $(a, b)$  come coordinate. In questo caso si ha pertanto una corrispondenza biunivoca tra l'insieme dei punti del piano  $\pi$  e l'insieme  $\{(a, b) \mid a, b \in \mathbb{R}\}$  di tutte le coppie ordinate di numeri reali.

La costruzione dell'insieme  $\{(a, b) \mid a, b \in \mathbb{R}\}$  delle coppie ordinate di numeri reali può essere generalizzata al caso in cui gli elementi  $a, b$  nella coppia  $(a, b)$  siano non numeri reali, ma elementi di due insiemi  $A$  e  $B$  arbitrari. Siano quindi  $A, B$  due insiemi qualunque. Il *prodotto cartesiano*  $A \times B$  di  $A$  per  $B$  è l'insieme delle *coppie ordinate*  $(a, b)$  dove  $a \in A$  e  $b \in B$ , ossia

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Ad esempio se  $A = \{1, 2, 3\}$  e  $B = \{1, 2\}$ , allora

$$A \times B = \{(1, 1), (2, 1), (3, 1), (1, 2), (2, 2), (3, 2)\}.$$

Due coppie ordinate  $(a, b)$ ,  $(a', b')$  sono uguali se e solo se

$$a = a' \quad \text{e} \quad b = b'.$$

Analogamente al prodotto cartesiano  $A \times B$  di due insiemi  $A$  e  $B$ , il prodotto cartesiano  $A_1 \times A_2 \times \dots \times A_n$  di  $n$  insiemi  $A_1, A_2, \dots, A_n$  è l'insieme

$$\{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Gli elementi dell'insieme  $A_1 \times A_2 \times \dots \times A_n$  si chiamano  $n$ -uple ordinate.

**Corrispondenze e applicazioni.** Capita spesso in matematica di dover far corrispondere ad alcuni elementi di un insieme  $A$  elementi di un insieme  $B$ . Ad esempio, fissiamo un piano  $\pi$  e  $B$  è l'insieme delle rette di  $\pi$ , possiamo far corrispondere ad ogni elemento  $P$  di  $A$  la tangente alla circonferenza passante per quel punto  $P$ . In questo modo facciamo corrispondere ad (alcuni) elementi di  $A$  elementi di  $B$ . Si noti che ad alcuni elementi di  $A$  (i punti interni alla circonferenza) non corrisponde alcun elemento di  $B$ , ad altri elementi di  $A$  (i punti sulla circonferenza) corrisponde un unico elemento di  $B$  (la retta tangente in quel punto), e infine ad altri elementi di  $A$  (i punti esterni alla circonferenza) corrispondono due elementi di  $B$ .

Per fare un secondo esempio poniamo  $A = B = \mathbb{Z}$  e facciamo corrispondere ad ogni  $x \in A$  il numero  $2x \in B$ .

Per descrivere rigorosamente questa nozione intuitiva di "far corrispondere" ad elementi di un insieme  $A$  elementi di un insieme  $B$  procediamo nel modo seguente. Dati due insiemi  $A$  e  $B$  e due loro elementi  $a \in A$  e  $b \in B$ , il fatto che l'elemento  $a \in A$  corrisponda o non corrisponda all'elemento  $b \in B$  può essere rappresentato dal fatto che la coppia ordinata  $(a, b)$  stia o non stia in un certo sottoinsieme del prodotto cartesiano  $A \times B$ . Diamo quindi la seguente definizione: Una corrispondenza  $\varrho$  dell'insieme  $A$  nell'insieme  $B$  è un qualunque sottoinsieme di  $A \times B$ . Se  $(a, b) \in \varrho$  diremo che  $a$  corrisponde a  $b$  nella corrispondenza  $\varrho$ .

Quindi nel primo esempio che abbiamo dato, la corrispondenza che ai punti del piano fa corrispondere le tangenti alla circonferenza per quei punti è il sottoinsieme

$$\varrho = \{(P, r) \mid P \in A, r \in B, P \text{ è un punto di } r, r \text{ è tangente alla circonferenza}\}.$$

È una corrispondenza di  $A$  in  $B$ . Nel secondo esempio, la corrispondenza che ad ogni numero intero fa corrispondere il suo doppio è il sottoinsieme  $\varrho = \{(x, 2x) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$ . È una corrispondenza di  $\mathbb{Z}$  in  $\mathbb{Z}$ .

Siano  $A$  e  $B$  insiemi. Un'applicazione (o funzione) di  $A$  in  $B$  è una corrispondenza  $\varphi$  di  $A$  in  $B$  con la seguente proprietà: per ogni elemento  $a \in A$  esiste un unico elemento  $b \in B$  tale che  $(a, b) \in \varphi$ . Per indicare che  $\varphi$  è un'applicazione di  $A$  in  $B$  scriveremo  $\varphi: A \rightarrow B$ , e per indicare che all'elemento  $a \in A$  corrisponde l'unico elemento  $b \in B$  scriveremo  $\varphi(a) = b$  oppure  $\varphi: a \mapsto b$  invece di  $(a, b) \in \varphi$ .

Ad esempio la corrispondenza di  $\mathbb{Z}$  in  $\mathbb{Z}$  che ad ogni elemento  $x \in \mathbb{Z}$  fa corrispondere  $2x \in \mathbb{Z}$  è un'applicazione  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ . Per questa applicazione si ha  $\varphi(x) = 2x$  per ogni  $x \in \mathbb{Z}$ , o, con notazione equivalente,  $\varphi: x \mapsto 2x$ .

Un altro esempio di applicazione  $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$  si ha ponendo

$$\varphi(n) = -n$$

per ogni  $n \in \mathbb{N}$ . Questa è l'applicazione che ad ogni numero naturale  $n$  fa corrispondere il suo opposto  $-n$  (che è un elemento di  $\mathbb{Z}$ ).

Se  $\varphi: A \rightarrow B$  è un'applicazione, l'insieme  $A$  si dice il dominio di  $\varphi$ , e l'insieme  $B$  si dice il codominio di  $\varphi$ . Se  $a \in A$ ,  $\varphi(a)$  si chiama l'immagine di  $a$  secondo  $\varphi$  (o il valore di  $\varphi$  in  $a$ ); se  $A' \subseteq A$ ,

$$\varphi(A') = \{\varphi(x) \mid x \in A'\}$$

è l'immagine di  $A'$  (secondo  $\varphi$ ). L'insieme  $\varphi(A)$ , ossia l'immagine di tutto il dominio, è detto anche l'immagine dell'applicazione  $\varphi$ . Se  $B' \subseteq B$ , l'insieme

$$\varphi^{-1}(B') = \{x \mid x \in A, \varphi(x) \in B'\} \dots$$

è l'antiimmagine (o controimmagine o immagine inversa) di  $B'$ . Se  $b \in B$  si scrive  $\varphi^{-1}(b)$  invece di  $\varphi^{-1}(\{b\})$ . Quindi

$$\varphi^{-1}(b) = \{x \mid x \in A, \varphi(x) = b\}.$$

ESEMPIO 1. Sia  $A = \{1, 2, 3\}$ ,  $B = \{1, 4, 5, 6\}$ . Allora ponendo  $\varphi(1) = 1$ ,  $\varphi(2) = 4$ ,  $\varphi(3) = 1$  si definisce un'applicazione  $\varphi: A \rightarrow B$ . In questo caso l'immagine di  $2$  è  $4$ , l'immagine di  $\{1, 2\} \subseteq A$  è  $\varphi(\{1, 2\}) = \{1, 4\}$ , l'immagine dell'applicazione  $\varphi$  è  $\{1, 4\}$ , l'antiimmagine di  $\{1, 5\}$  è  $\varphi^{-1}(\{1, 5\}) = \{1, 3\}$ , l'antiimmagine di  $\{5, 6\}$  è  $\varphi^{-1}(\{5, 6\}) = \emptyset$ , le antiimmagini degli elementi  $1, 4$  e  $5$  di  $B$  sono rispettivamente  $\varphi^{-1}(1) = \{1, 3\}$ ,  $\varphi^{-1}(4) = \{2\}$  e  $\varphi^{-1}(5) = \emptyset$ . □

Un'applicazione  $\varphi: A \rightarrow B$  si dice:

- iniettiva se per ogni  $a, a' \in A$ ,  $\varphi(a) = \varphi(a')$  implica  $a = a'$ ;
- suriettiva se per ogni  $b \in B$  esiste  $a \in A$  tale che  $\varphi(a) = b$ ;
- biiettiva se è iniettiva e suriettiva.

Un'applicazione biiettiva si chiama anche una *biiezione* (o una *corrispondenza biunivoca*).

ESEMPIO 2. Sia  $\varphi: A \rightarrow B$  l'applicazione dell'esempio 1. Allora  $\varphi$  non è iniettiva perché  $\varphi(1) = \varphi(3)$ . Non è nemmeno suriettiva perché non esiste nessun  $a \in A$  tale che  $\varphi(a) = 5$ . □



ESEMPIO 3. Sia  $\psi: \mathbb{N} \rightarrow \mathbb{N}$  l'applicazione definita da  $\psi(x) = 2x$  per ogni  $x \in \mathbb{N}$ . Allora l'applicazione  $\psi$  è iniettiva, perché se  $x, x' \in \mathbb{N}$  e  $\psi(x) = \psi(x')$ , allora  $2x = 2x'$ , da cui  $x = x'$ . Invece l'applicazione  $\psi$  non è suriettiva, perché, ad esempio, non esiste nessun  $x \in \mathbb{N}$  tale che  $\psi(x) = 1$ .  $\square$

ESEMPIO 4. Sia  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  l'applicazione definita da  $\varphi(0) = 0$  e  $\varphi(x) = x - 1$  se  $x \in \mathbb{N}$  e  $x > 0$ . Allora  $\varphi$  non è iniettiva perché  $\varphi(0) = \varphi(1)$ , mentre  $\varphi$  è suriettiva perché per ogni  $x \in \mathbb{N}$  si ha  $\varphi(x+1) = x$ .  $\square$

ESEMPIO 5. Sia  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$  l'applicazione definita da  $\varphi(x) = x + 1$  per ogni  $x \in \mathbb{Z}$ . Allora  $\varphi$  è iniettiva, perché se  $x, x' \in \mathbb{Z}$  e  $\varphi(x) = \varphi(x')$ , allora  $x + 1 = x' + 1$ , da cui  $x = x'$ . L'applicazione  $\varphi$  è anche suriettiva perché per ogni  $x \in \mathbb{Z}$  si ha che  $x - 1 \in \mathbb{Z}$  e  $\varphi(x - 1) = x$ . Pertanto  $\varphi$  è una biiezione.  $\square$

Se  $A$  è un insieme, l'applicazione  $\iota_A: A \rightarrow A$  definita da  $\iota_A(a) = a$  per ogni  $a \in A$  è detta l'applicazione identica di  $A$ . È immediato verificare che  $\iota_A$  è una biiezione di  $A$  in  $A$ .

Si osservi che due applicazioni  $\varphi: A \rightarrow B$  e  $\psi: C \rightarrow D$  sono uguali se e solo se  $A = C$ ,  $B = D$ , e  $\varphi(x) = \psi(x)$  per ogni  $x \in A = C$ .

Se  $A$  e  $B$  sono insiemi, l'insieme di tutte le applicazioni di  $A$  in  $B$  si denota con  $B^A$ , ossia  $B^A = \{\varphi \mid \varphi: A \rightarrow B \text{ è un'applicazione}\}$ .

### Esercizi svolti

2.1. Sia  $X$  un insieme. Si verifichi che l'applicazione  $\chi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$  definita da  $\chi(Y) = X \setminus Y$  per ogni  $Y \in \mathcal{P}(X)$  è una biiezione.

*Soluzione.* Mostriamo che  $\chi$  è iniettiva. Dobbiamo dimostrare che per ogni  $Y, Y' \in \mathcal{P}(X)$ , da  $\chi(Y) = \chi(Y')$  segue  $Y = Y'$ . Ora se  $\chi(Y) = \chi(Y')$ , allora  $X \setminus Y = X \setminus Y'$ , da cui  $X \setminus (X \setminus Y) = X \setminus (X \setminus Y')$ , ossia (per l'esercizio 1.15)  $Y = Y'$ . Quindi  $\chi$  è iniettiva.

Mostriamo che  $\chi$  è suriettiva. Dobbiamo dimostrare che per ogni  $Z \in \mathcal{P}(X)$  esiste  $Y \in \mathcal{P}(X)$  tale che  $\chi(Y) = Z$ . Fissato  $Z \in \mathcal{P}(X)$  poniamo  $Y = X \setminus Z$ . Allora  $Y \in \mathcal{P}(X)$  e si ha  $\chi(Y) = \chi(X \setminus Z) = X \setminus (X \setminus Z) = Z$ . Questo prova che  $\chi$  è anche suriettiva, e pertanto  $\chi$  è biiettiva.  $\square$

2.2. Sia  $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$  l'applicazione definita da  $\varphi(n) = n/2$  se  $n \in \mathbb{N}$  è pari, e  $\varphi(n) = -(n+1)/2$  se  $n \in \mathbb{N}$  è dispari. Si provi che  $\varphi$  è una biiezione.

*Soluzione.* Mostriamo che  $\varphi$  è iniettiva. Dobbiamo dimostrare che per ogni  $n, n' \in \mathbb{N}$  se  $\varphi(n) = \varphi(n')$  allora  $n = n'$ . Osserviamo intanto che  $\varphi(n) \geq 0$  se  $n$  è pari, e  $\varphi(n) < 0$  se  $n$  è dispari. Quindi se  $n, n' \in \mathbb{N}$  e  $\varphi(n) = \varphi(n')$ ,  $n$  ed  $n'$  devono essere entrambi pari o entrambi dispari. Se  $n$  ed  $n'$  sono entrambi pari, da  $\varphi(n) = \varphi(n')$  segue  $n/2 = n'/2$ , da cui  $n = n'$ . Se  $n$  ed  $n'$  sono entrambi

dispari, da  $\varphi(n) = \varphi(n')$  segue  $-(n+1)/2 = -(n'+1)/2$ , da cui  $n+1 = n'+1$ , e quindi  $n = n'$ . Pertanto in entrambi i casi da  $\varphi(n) = \varphi(n')$  segue  $n = n'$ . Questo dimostra che  $\varphi$  è iniettiva.

Mostriamo che  $\varphi$  è suriettiva. Dobbiamo dimostrare che per ogni  $z \in \mathbb{Z}$  esiste  $n \in \mathbb{N}$  tale che  $\varphi(n) = z$ . Sia  $z \in \mathbb{Z}$ . Se  $z \geq 0$ , poniamo  $n = 2z$ . Allora  $n \in \mathbb{N}$  è pari e pertanto  $\varphi(n) = \varphi(2z) = (2z)/2 = z$ . Se invece  $z < 0$ , poniamo  $n = -2z - 1$ . Si osservi che in questo caso  $n \in \mathbb{N}$  perché dato che  $z < 0$  è un intero, ne segue che  $z \leq -1$ , e quindi  $-2z \geq 2$ , da cui  $n = -2z - 1 \geq 1$ . Pertanto  $n$  è un intero positivo, e in particolare  $n \in \mathbb{N}$ . Inoltre  $n = -2z - 1$  è dispari e  $\varphi(n) = \varphi(-2z - 1) = -((-2z - 1) + 1)/2 = z$ . Questo prova che  $\varphi$  è anche suriettiva.  $\square$

2.3. Sia  $\varphi: A \rightarrow B$  un'applicazione. Si dimostri che:

- se  $A', A'' \subseteq A$ , allora  $\varphi(A' \cup A'') = \varphi(A') \cup \varphi(A'')$ ;
- se  $A', A'' \subseteq A$ , allora  $\varphi(A' \cap A'') \subseteq \varphi(A') \cap \varphi(A'')$ ;
- se  $B', B'' \subseteq B$ , allora  $\varphi^{-1}(B' \cup B'') = \varphi^{-1}(B') \cup \varphi^{-1}(B'')$ ;
- se  $B', B'' \subseteq B$ , allora  $\varphi^{-1}(B' \cap B'') = \varphi^{-1}(B') \cap \varphi^{-1}(B'')$ ;
- se  $B' \subseteq B$ , allora  $\varphi^{-1}(B \setminus B') = A \setminus \varphi^{-1}(B')$ ;
- se  $A' \subseteq A$ , allora  $A' \subseteq \varphi^{-1}(\varphi(A'))$ ;
- se  $B' \subseteq B$ , allora  $\varphi(\varphi^{-1}(B')) \subseteq B'$ .

*Soluzione.* (a) Mostriamo che  $\varphi(A' \cup A'') \subseteq \varphi(A') \cup \varphi(A'')$ . Se  $y \in \varphi(A' \cup A'')$  si deve avere  $y = \varphi(x)$  con  $x \in A' \cup A''$ . Allora  $x \in A'$  oppure  $x \in A''$ , da cui  $y = \varphi(x) \in \varphi(A')$  oppure  $y = \varphi(x) \in \varphi(A'')$ . In entrambi i casi  $y \in \varphi(A') \cup \varphi(A'')$ .

Mostriamo che  $\varphi(A') \cup \varphi(A'') \subseteq \varphi(A' \cup A'')$ . Se  $y \in \varphi(A') \cup \varphi(A'')$ , allora  $y \in \varphi(A')$  oppure  $y \in \varphi(A'')$ . Se  $y \in \varphi(A')$  allora  $y = \varphi(x)$  per qualche  $x \in A'$ , e quindi a maggior ragione  $y = \varphi(x)$  per qualche  $x \in A' \cup A''$ . Se invece  $y \in \varphi(A'')$ , allora  $y = \varphi(x)$  con  $x \in A''$ , e quindi anche in questo caso  $y = \varphi(x)$  per qualche  $x \in A' \cup A''$ . Quindi in entrambi i casi  $y = \varphi(x)$  per qualche  $x \in A' \cup A''$ , e pertanto  $y \in \varphi(A' \cup A'')$ .

(b) Sia  $y \in \varphi(A' \cap A'')$ ; allora  $y = \varphi(x)$  per qualche  $x \in A' \cap A''$ . Da  $y = \varphi(x)$  e  $x \in A'$  segue che  $y \in \varphi(A')$ . Da  $y = \varphi(x)$  e  $x \in A''$  segue che  $y \in \varphi(A'')$ . Quindi  $y \in \varphi(A') \cap \varphi(A'')$ .

(c) Sia  $x \in \varphi^{-1}(B' \cup B'')$ . Allora  $\varphi(x) \in B' \cup B''$ , da cui  $\varphi(x) \in B'$  oppure  $\varphi(x) \in B''$ . Ne segue che  $x \in \varphi^{-1}(B')$  oppure  $x \in \varphi^{-1}(B'')$ . In entrambi i casi  $x \in \varphi^{-1}(B') \cup \varphi^{-1}(B'')$ . Questo dimostra che  $\varphi^{-1}(B' \cup B'') \subseteq \varphi^{-1}(B') \cup \varphi^{-1}(B'')$ . Per dimostrare che  $\varphi^{-1}(B') \cup \varphi^{-1}(B'') \subseteq \varphi^{-1}(B' \cup B'')$  basta ripercorrere in senso inverso il ragionamento.

(d) Sia  $x \in \varphi^{-1}(B' \cap B'')$ . Allora  $\varphi(x) \in B' \cap B''$ , da cui  $\varphi(x) \in B'$  e  $\varphi(x) \in B''$ . Ne segue che  $x \in \varphi^{-1}(B')$  e  $x \in \varphi^{-1}(B'')$ . Pertanto  $x \in \varphi^{-1}(B') \cap \varphi^{-1}(B'')$ .

Questo prova che  $\varphi^{-1}(B' \cap B'') \subseteq \varphi^{-1}(B') \cap \varphi^{-1}(B'')$ . Per dimostrare che  $\varphi^{-1}(B') \cap \varphi^{-1}(B'') \subseteq \varphi^{-1}(B' \cap B'')$  basta ripercorrere in senso inverso il ragionamento.

(e) Sia  $x \in \varphi^{-1}(B \setminus B')$ . Allora  $x \in A$  e  $\varphi(x) \in B \setminus B'$ , da cui  $\varphi(x) \notin B'$ . Quindi  $x \notin \varphi^{-1}(B')$ . Abbiamo così dimostrato che  $x \in A \setminus \varphi^{-1}(B')$ , facendo vedere che si ha l'inclusione  $\varphi^{-1}(B \setminus B') \subseteq A \setminus \varphi^{-1}(B')$ .

Viceversa se  $x \in A \setminus \varphi^{-1}(B')$ , allora  $x \in A$  e  $x \notin \varphi^{-1}(B')$ . Ne segue che  $\varphi(x) \in B$  e  $\varphi(x) \notin B'$ . Pertanto  $\varphi(x) \in B \setminus B'$ , da cui  $x \in \varphi^{-1}(B \setminus B')$ . Questo dimostra che  $A \setminus \varphi^{-1}(B') \subseteq \varphi^{-1}(B \setminus B')$ .

(f) Se  $a \in A'$ , allora  $\varphi(a) \in \varphi(A')$ , ossia  $a \in \{x \mid \varphi(x) \in \varphi(A')\} = \varphi^{-1}(\varphi(A'))$ .

(g) Se  $y \in \varphi(\varphi^{-1}(B'))$  allora  $y = \varphi(x)$  per qualche  $x \in \varphi^{-1}(B')$ . Ne segue che  $\varphi(x) \in B'$ , ed essendo  $y = \varphi(x)$  se ne conclude che  $y \in B'$ .  $\square$

### Altri esercizi

2.4. Quali e quanti sono gli elementi dell'insieme  $A \times B$  se

- (a)  $A = \{a, b, c, d\}$  e  $B = \{x, y, z\}$ ?
- (b)  $A = \{a, b, c, d\}$  e  $B = \mathbb{N}$ ?
- (c)  $A = \emptyset$  e  $B = \{x, y, z\}$ ?
- (d)  $A = \emptyset$  e  $B = \mathbb{N}$ ?

2.5. Quali e quanti sono gli elementi dell'insieme  $A \times B \times C$  quando  $A = \{a, b, c, d\}$ ,  $B = \{x, y, z\}$  e  $C = \{0, 1\}$ ?

2.6. Si dica se le seguenti corrispondenze sono applicazioni di  $\mathbb{R}$  in  $\mathbb{R}$ :

- (a)  $\{(x, y) \mid x, y \in \mathbb{R}, x^2 + y^2 = 1\}$ ;
- (b)  $\{(x, y) \mid x, y \in \mathbb{R}, y = \sin x\}$ ;
- (c)  $\{(y, x) \mid x, y \in \mathbb{R}, y = \sin x\}$ .

2.7. Si dica se le seguenti corrispondenze sono applicazioni di  $\mathbb{N}$  in  $\mathbb{Z}$ :

- (a)  $\{(x, y) \mid x \in \mathbb{N}, y \in \mathbb{Z}, x = 2y\}$ ;
- (b)  $\{(x, y) \mid x \in \mathbb{N}, y \in \mathbb{Z}, 2x = y\}$ ;
- (c)  $\{(x, y) \mid x \in \mathbb{N}, y \in \mathbb{Z}, x = y^2\}$ .

2.8. Si dica se la corrispondenza  $\{(x, y) \mid x, y \in \mathbb{Z}, x^2 = y^2\}$  è un'applicazione di  $\mathbb{Z}$  in  $\mathbb{Z}$ .

2.9. Sia  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  l'applicazione definita da  $\varphi(n) = n^2$  per ogni  $n \in \mathbb{N}$ . Si determini  $\varphi(10)$ ,  $\varphi(\{1, 2, 3, 4\})$ ,  $\varphi^{-1}(\{1, 2, 3, 4\})$ ,  $\varphi^{-1}(10)$ ,  $\varphi^{-1}(4)$ .

2.10. Se  $a$  e  $b$  sono numeri reali e  $a < b$ , denotiamo con  $[a, b]$  e  $]a, b[$  gli insiemi

$$[a, b] = \{x \mid x \in \mathbb{R}, a \leq x \leq b\} \quad \text{e} \quad ]a, b[ = \{x \mid x \in \mathbb{R}, a < x < b\}$$

rispettivamente. Sia  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\varphi(x) = \sin x$  per ogni  $x \in \mathbb{R}$ . Si determinino  $\varphi(\mathbb{R})$ ,  $\varphi(0)$ ,  $\varphi([0, \pi/2])$ ,  $\varphi([0, \pi])$ ,  $\varphi^{-1}(0)$ ,  $\varphi^{-1}(1)$ ,  $\varphi^{-1}(2)$ ,  $\varphi^{-1}([0, 1])$ ,  $\varphi^{-1}([-2, -1])$ .

2.11. Si dia un esempio di due insiemi  $A$  e  $B$ , di un sottoinsieme  $A' \subseteq A$  e di un'applicazione  $\varphi: A \rightarrow B$  tali che  $A' \subset \varphi^{-1}(\varphi(A'))$ .

2.12. Si dia un esempio di due insiemi  $A$  e  $B$ , di un sottoinsieme  $B' \subseteq B$  e di un'applicazione  $\varphi: A \rightarrow B$  tali che  $\varphi(\varphi^{-1}(B')) \subset B'$ .

2.13. Si dimostri che se  $\varphi: A \rightarrow B$  è un'applicazione e  $B' \subseteq B$ , allora  $\varphi(\varphi^{-1}(B')) = B' \cap \varphi(A)$ .

2.14. Siano  $A = \{a, b, c, d\}$  e  $B = \{x, y, z\}$  due insiemi di quattro e tre elementi rispettivamente. L'applicazione  $f: A \rightarrow B$  definita da  $f(a) = x$ ,  $f(b) = y$ ,  $f(c) = z$ ,  $f(d) = x$  è iniettiva? È suriettiva? È biiettiva?

2.15. L'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\varphi(x) = x^2 + 15$  per ogni  $x \in \mathbb{R}$  è iniettiva? È suriettiva? È biiettiva?

2.16. Sia  $\mathbb{R}^+ = \{x \mid x \in \mathbb{R}, x > 0\}$ . L'applicazione  $\varphi: \mathbb{R}^+ \rightarrow \mathbb{R}^+$  definita da  $\varphi(x) = x^2 + 15$  per ogni  $x \in \mathbb{R}^+$  è iniettiva? È suriettiva? È biiettiva?

2.17. Sia  $f: \mathbb{N} \rightarrow \{0, 1, 2, 3\}$  l'applicazione definita da

$$f(n) = \begin{cases} 0 & \text{se } n \text{ è pari,} \\ 1 & \text{se } n \text{ è dispari multiplo di 3,} \\ 2 & \text{se } n \text{ è dispari e non è multiplo di 3.} \end{cases}$$

L'applicazione  $f$  è iniettiva? È suriettiva? È biiettiva?

2.18. Se  $A$  e  $B$  sono insiemi non vuoti, sia  $\pi_A: A \times B \rightarrow A$  definita da  $\pi_A(a, b) = a$  per ogni  $a \in A$ ,  $b \in B$ . Si provi che  $\pi_A$  è un'applicazione suriettiva. Analogamente  $\pi_B: A \times B \rightarrow B$  definita da  $\pi_B(a, b) = b$  per ogni  $a \in A$ ,  $b \in B$  è un'applicazione suriettiva.

[Le applicazioni  $\pi_A: A \times B \rightarrow A$  e  $\pi_B: A \times B \rightarrow B$  si chiamano, rispettivamente, le *proiezioni canoniche* di  $A \times B$  su  $A$  e su  $B$ . Si osservi che a rigore avremmo dovuto scrivere  $\pi_A((a, b))$  per denotare l'immagine della coppia  $(a, b)$ . In realtà però si preferisce scrivere  $\pi_A(a, b)$  per non appesantire la notazione con troppe parentesi.]

2.19. Sia  $B$  un insieme e  $A \subseteq B$  un suo sottoinsieme. Si definisca un'applicazione  $\varepsilon: A \rightarrow B$  ponendo  $\varepsilon(a) = a$  per ogni  $a \in A$ .

- (a) Si provi che l'applicazione  $\varepsilon$  è iniettiva.  
 (b) Si provi che l'applicazione  $\varepsilon$  è biettiva se e solo se  $A = B$ .  
 [L'applicazione  $\varepsilon$  è detta l'applicazione di inclusione o l'immersione di  $A$  in  $B$ .]
- 2.20. Siano  $A, B, C$  insiemi ed  $f: A \rightarrow B, g: A \rightarrow C$  applicazioni. Sia  $h: A \rightarrow B \times C$  l'applicazione definita ponendo  $h(a) = (f(a), g(a))$  per ogni  $a \in A$ . Si dimostri che se  $B' \subseteq B$  e  $C' \subseteq C$ , allora  $h^{-1}(B' \times C') = f^{-1}(B') \cap g^{-1}(C')$ .
- 2.21. Siano  $f: A \rightarrow B$  un'applicazione tra due insiemi e  $Y \subseteq X \subseteq A$ .  
 (a) Si dimostri che  $f(X) \setminus f(Y) \subseteq f(X \setminus Y)$ .  
 (b) Si dimostri che se  $f$  è iniettiva, allora  $f(X) \setminus f(Y) = f(X \setminus Y)$ .
- 2.22. Sia  $f: A \rightarrow B$  un'applicazione tra due insiemi.  
 (a) Si provi che l'applicazione  $f$  è iniettiva se e solo se per ogni coppia di sottoinsiemi  $X$  e  $Y$  di  $A$  tali che  $X \cap Y = \emptyset$  si ha  $f(X) \cap f(Y) = \emptyset$ .  
 (b) Si provi che l'applicazione  $f$  è iniettiva se e solo se per ogni coppia di sottoinsiemi  $X$  e  $Y$  di  $A$  si ha  $f(X \setminus Y) = f(X) \setminus f(Y)$ .
- 2.23. Se  $A = \{0, 1\}$  e  $B = \{a, b, c\}$  sono insiemi con due e tre elementi rispettivamente, quanti e quali sono gli elementi di  $A^B$ ? E di  $B^A$ ?

### Capitolo 3. Applicazioni composte

Siano  $A, B, C$  insiemi e  $\varphi: A \rightarrow B, \psi: B \rightarrow C$  applicazioni. Allora l'applicazione  $\psi \circ \varphi: A \rightarrow C$  definita da  $(\psi \circ \varphi)(a) = \psi(\varphi(a))$  per ogni  $a \in A$  è detta l'applicazione composta di  $\varphi$  e  $\psi$ . Spesso scriveremo più brevemente  $\psi\varphi$  in luogo di  $\psi \circ \varphi$ .

ESEMPIO 1. Se  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  è definita da  $\varphi(n) = 2n$  per ogni  $n \in \mathbb{N}$  e  $\psi: \mathbb{N} \rightarrow \mathbb{Z}$  è definita da  $\psi(n) = -n^2$  per ogni  $n \in \mathbb{N}$ , allora  $\psi \circ \varphi: \mathbb{N} \rightarrow \mathbb{Z}$  è definita da  $(\psi \circ \varphi)(n) = \psi(\varphi(n)) = \psi(2n) = -(2n)^2 = -4n^2$  per ogni  $n \in \mathbb{N}$ .

Se  $f: \mathbb{R} \rightarrow \mathbb{R}$  è definita da  $f(x) = \frac{1}{1+x^2}$  per ogni  $x \in \mathbb{R}$  e  $g: \mathbb{Z} \rightarrow \mathbb{R}$  è definita da  $g(z) = 2^z$  per ogni  $z \in \mathbb{Z}$ , allora  $f \circ g: \mathbb{Z} \rightarrow \mathbb{R}$  è definita da  $(f \circ g)(z) = f(g(z)) = f(2^z) = \frac{1}{1+(2^z)^2} = \frac{1}{1+2^{2z}}$  per ogni  $z \in \mathbb{Z}$ .  $\square$

PROPOSIZIONE 3.1. L'applicazione composta di due funzioni iniettive (rispettivamente suriettive, biettive) è iniettiva (rispettivamente suriettiva, biettiva).

Si faccia attenzione che non vale il viceversa della proposizione 3.1. Ad esempio non è vero che se  $\varphi: A \rightarrow B$  e  $\psi: B \rightarrow C$  sono applicazioni e  $\psi \circ \varphi: A \rightarrow C$  è iniettiva allora  $\varphi$  e  $\psi$  sono entrambe iniettive. Per convincersene basta considerare le applicazioni  $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$  definita da  $\varphi(n) = n$  per ogni  $n \in \mathbb{N}$  e  $\psi: \mathbb{Z} \rightarrow \mathbb{Z}$  definita da  $\psi(z) = z^2$  per ogni  $z \in \mathbb{Z}$ . Allora  $\psi \circ \varphi: \mathbb{N} \rightarrow \mathbb{Z}$  è definita da  $(\psi \circ \varphi)(n) = \psi(\varphi(n)) = \psi(n) = n^2$  per ogni  $n \in \mathbb{N}$ , e questa è iniettiva perché se  $n, n' \in \mathbb{N}$  e  $(\psi \circ \varphi)(n) = (\psi \circ \varphi)(n')$ , allora  $n^2 = n'^2$ , da cui  $n = n'$  (perché  $n, n' \geq 0$ ). Invece  $\psi$  non è iniettiva perché  $\psi(1) = \psi(-1)$ .

Analogamente non è vero che se  $\varphi: A \rightarrow B$  e  $\psi: B \rightarrow C$  sono applicazioni e  $\psi \circ \varphi: A \rightarrow C$  è suriettiva allora  $\varphi$  e  $\psi$  sono entrambe suriettive. Ad esempio si considerino le applicazioni  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  definita da  $\varphi(n) = 2n$  per ogni  $n \in \mathbb{N}$  e  $\psi: \mathbb{N} \rightarrow \{0\}$  definita da  $\psi(n) = 0$  per ogni  $n \in \mathbb{N}$ . Allora  $\psi \circ \varphi: \mathbb{N} \rightarrow \{0\}$  è definita da  $(\psi \circ \varphi)(n) = \psi(2n) = 0$  per ogni  $n \in \mathbb{N}$ , e quindi  $\psi \circ \varphi$  è suriettiva. Invece  $\varphi$  non è suriettiva, perché ad esempio non esiste nessun  $n \in \mathbb{N}$  per il quale  $\varphi(n) = 1$ .

Per un inverso parziale della proposizione 3.1 si veda l'esercizio 3.2.

Se  $\varphi: A \rightarrow B, \psi: B \rightarrow C, \omega: C \rightarrow D$  sono tre applicazioni, allora  $\omega \circ (\psi \circ \varphi) = (\omega \circ \psi) \circ \varphi$ , e quindi è possibile usare la notazione  $\omega \circ \psi \circ \varphi$  (o più brevemente  $\omega\psi\varphi$ ) senza pericolo di ambiguità.

PROPOSIZIONE 3.2. Sia  $\varphi: A \rightarrow B$  un'applicazione. Si supponga che esistano due applicazioni  $\psi_1, \psi_2: B \rightarrow A$  tali che  $\psi_1 \circ \varphi = \iota_A$  e  $\varphi \circ \psi_2 = \iota_B$ . Allora  $\psi_1 = \psi_2$ .

PROPOSIZIONE 3.3. Un'applicazione  $\varphi: A \rightarrow B$  è biettiva se e solo se esiste un'applicazione  $\psi: B \rightarrow A$  tale che  $\psi \circ \varphi = \iota_A$  e  $\varphi \circ \psi = \iota_B$ .

Data un'applicazione biettiva  $\varphi: A \rightarrow B$ , per ogni  $b \in B$  esiste un unico elemento  $a \in A$  tale che  $\varphi(a) = b$ . È quindi possibile definire un'altra applicazione  $B \rightarrow A$  in cui l'immagine di un elemento  $b \in B$  è l'unico  $a \in A$  tale che  $\varphi(a) = b$ . Tale funzione è di solito denotata con  $\varphi^{-1}$  ed è detta l'applicazione inversa di  $\varphi$ . Pertanto, per ogni applicazione biettiva  $\varphi: A \rightarrow B$  l'applicazione inversa  $\varphi^{-1}: B \rightarrow A$  è definita, per ogni  $a \in A, b \in B$ , da  $\varphi^{-1}(b) = a$  se e solo se  $\varphi(a) = b$ .

Se si deve calcolare l'applicazione inversa di una biiezione  $\varphi: A \rightarrow B$  si può cercare di procedere nel modo seguente: dall'espressione  $\varphi(a) = b$  che definisce l'applicazione  $\varphi$  e che fornisce  $b$  in funzione di  $a$  si cerca di ricavare  $a$  in funzione di  $b$ ; l'applicazione che associa ad ogni  $b$  l' $a$  così ricavato è l'applicazione inversa cercata.

ESEMPIO 2. Sia  $\mathbb{R}^+ = \{a \mid a \in \mathbb{R}, a > 0\}$ . Consideriamo l'applicazione  $\varphi: \mathbb{R}^+ \rightarrow \mathbb{R}^+$  definita da  $\varphi(a) = a^2$  per ogni  $a \in \mathbb{R}^+$ . Mostriamo che  $\varphi$  è una

biiezione. L'applicazione  $\varphi$  è iniettiva perché se  $a, a' \in \mathbb{R}^+$  e  $\varphi(a) = \varphi(a')$ , allora  $a^2 = a'^2$ , da cui  $a = a'$  (perché  $a, a' \in \mathbb{R}^+$ ). L'applicazione  $\varphi$  è suriettiva perché per ogni  $b \in \mathbb{R}^+$  si ha che  $\sqrt{b} \in \mathbb{R}^+$  e  $\varphi(\sqrt{b}) = (\sqrt{b})^2 = b$ . Quindi  $\varphi$  è una biiezione. Cerchiamo l'applicazione inversa. L'espressione  $\varphi(a) = b$  che definisce l'applicazione  $\varphi$  è in questo caso l'espressione  $a^2 = b$  (qui  $a, b \in \mathbb{R}^+$ ). Ricavando da questa uguaglianza si ottiene  $a = \sqrt{b}$ . L'applicazione  $\psi: \mathbb{R}^+ \rightarrow \mathbb{R}^+$  definita da  $\psi(b) = \sqrt{b}$  per ogni  $b \in \mathbb{R}^+$  è quindi l'applicazione inversa della  $\varphi$ .  $\square$

Un altro modo per verificare che una certa applicazione  $\psi: B \rightarrow A$  è l'inversa di un'applicazione data  $\varphi: A \rightarrow B$ , è far vedere che  $\psi \circ \varphi = \iota_A$  e  $\varphi \circ \psi = \iota_B$ ; dimostriamo questo si ha necessariamente che  $\varphi$  è una biiezione e che  $\varphi^{-1} = \psi$ .

ESEMPIO 3. Mostriamo che l'applicazione  $\psi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\psi(x) = x^3 + 6x^2 + 12x + 5$  per ogni  $x \in \mathbb{R}$  è l'applicazione inversa dell'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\varphi(x) = \sqrt[3]{x+3} - 2$  per ogni  $x \in \mathbb{R}$ . Dobbiamo dimostrare che  $\psi \circ \varphi = \iota_{\mathbb{R}}$  e che  $\varphi \circ \psi = \iota_{\mathbb{R}}$ . Si osservi intanto che  $\psi \circ \varphi$ ,  $\varphi \circ \psi$  e  $\iota_{\mathbb{R}}$  hanno tutte dominio e codominio uguale ad  $\mathbb{R}$ . Inoltre per ogni  $x \in \mathbb{R}$  si ha

$$\begin{aligned} (\psi \circ \varphi)(x) &= \psi(\varphi(x)) = \psi(\sqrt[3]{x+3} - 2) = \\ &= (\sqrt[3]{x+3} - 2)^3 + 6(\sqrt[3]{x+3} - 2)^2 + 12(\sqrt[3]{x+3} - 2) + 5 = \\ &= (x+3) - 6(\sqrt[3]{x+3})^2 + 12\sqrt[3]{x+3} - 8 + \\ &\quad + 6((\sqrt[3]{x+3})^2 - 4\sqrt[3]{x+3} + 4) + 12(\sqrt[3]{x+3} - 2) + 5 = \\ &= x = \iota_{\mathbb{R}}(x) \end{aligned}$$

e

$$\begin{aligned} (\varphi \circ \psi)(x) &= \varphi(\psi(x)) = \varphi(x^3 + 6x^2 + 12x + 5) = \\ &= \sqrt[3]{x^3 + 6x^2 + 12x + 5} - 2 = \sqrt[3]{x^3 + 6x^2 + 12x + 8} - 2 = \\ &= \sqrt[3]{(x+2)^3} - 2 = (x+2) - 2 = x = \iota_{\mathbb{R}}(x). \end{aligned}$$

Pertanto  $\psi \circ \varphi = \iota_{\mathbb{R}}$  e  $\varphi \circ \psi = \iota_{\mathbb{R}}$ .  $\square$

ESEMPIO 4. L'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\varphi(a) = a^2$  per ogni  $a \in \mathbb{R}$  non è una biiezione (anzi, non è né iniettiva né suriettiva), e quindi non possiede un'applicazione inversa.  $\square$

ESEMPIO 5. Sia  $Q^* = \{x \mid x \in Q, x \neq 0\}$  l'insieme dei numeri razionali non nulli. Consideriamo l'applicazione  $\varphi: Q^* \rightarrow Q^*$  definita da  $\varphi(x) = 1/x$  per ogni  $x \in Q^*$ . Allora  $\varphi \circ \varphi = \iota_{Q^*}$ , perché  $\varphi \circ \varphi$  e  $\iota_{Q^*}$  hanno entrambe dominio e codominio  $Q^*$  e inoltre  $(\varphi \circ \varphi)(x) = \varphi(1/x) = 1/(1/x) = x = \iota_{Q^*}(x)$  per ogni  $x \in Q^*$ . Da  $\varphi \circ \varphi = \iota_{Q^*}$  e dalla proposizione 3.3 otteniamo immediatamente che  $\varphi$  è biiettiva e che  $\varphi = \varphi^{-1}$ , cioè che  $\varphi$  coincide con la propria inversa.  $\square$

PROPOSIZIONE 3.4. Siano  $\varphi_1: A \rightarrow B$  e  $\varphi_2: B \rightarrow C$  due applicazioni biettive. Allora  $(\varphi_1^{-1})^{-1} = \varphi_1$  e  $(\varphi_2 \circ \varphi_1)^{-1} = \varphi_1^{-1} \circ \varphi_2^{-1}$ .

Attenzione: data un'applicazione  $\varphi: A \rightarrow B$  abbiamo impiegato il simbolo  $\varphi^{-1}$  in due situazioni distinte con due significati distinti. Se  $\varphi$  è una biiezione, abbiamo denotato con  $\varphi^{-1}: B \rightarrow A$  l'applicazione inversa (che esiste solo quando  $\varphi$  è una biiezione). Se  $\varphi$  è invece un'applicazione qualsiasi, con  $\varphi^{-1}(B')$  e  $\varphi^{-1}(b)$  abbiamo denotato le antiimmagini del sottoinsieme  $B' \subseteq B$  e dell'elemento  $b \in B$ . Le antiimmagini di un sottoinsieme o di un elemento del codominio sono definite per ogni applicazione, non soltanto per le biiezioni.

ESEMPIO 6. Se  $A$  è un insieme e  $\iota_A: A \rightarrow A$  è l'applicazione identica, allora  $\iota_A^{-1} = \iota_A$ , in quanto  $\iota_A \circ \iota_A = \iota_A$ .  $\square$

ESEMPIO 7. Sia  $X$  un insieme e sia  $\chi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$  l'applicazione definita da  $\chi(Y) = X \setminus Y$  per ogni  $Y \in \mathcal{P}(X)$  (esercizio 2.1). Allora  $\chi \circ \chi = \iota_{\mathcal{P}(X)}$ , in quanto per ogni  $Y \in \mathcal{P}(X)$ , cioè per ogni  $Y \subseteq X$ , si ha  $(\chi \circ \chi)(Y) = \chi(\chi(Y)) = \chi(X \setminus Y) = X \setminus (X \setminus Y) = Y = \iota_{\mathcal{P}(X)}(Y)$ . Da  $\chi \circ \chi = \iota_{\mathcal{P}(X)}$  si deduce immediatamente che  $\chi$  è una biiezione e che  $\chi^{-1} = \chi$ .  $\square$

### Esercizi svolti

3.1. Sia  $\varphi: A \rightarrow B$  un'applicazione. Si provi che se  $\iota_A: A \rightarrow A$  e  $\iota_B: B \rightarrow B$  sono le applicazioni identiche di  $A$  e di  $B$  rispettivamente, allora

$$\varphi \circ \iota_A = \iota_B \circ \varphi = \varphi.$$

Soluzione. Si noti che le tre applicazioni  $\varphi \circ \iota_A$ ,  $\iota_B \circ \varphi$  e  $\varphi$  hanno tutte l'insieme  $A$  come dominio e l'insieme  $B$  come codominio. Inoltre per ogni  $a \in A$  si ha  $(\varphi \circ \iota_A)(a) = \varphi(\iota_A(a)) = \varphi(a)$  e  $(\iota_B \circ \varphi)(a) = \iota_B(\varphi(a)) = \varphi(a)$ . Quindi  $\varphi \circ \iota_A = \varphi$  e  $\iota_B \circ \varphi = \varphi$ .  $\square$

3.2. Siano  $\varphi: A \rightarrow B$  e  $\psi: B \rightarrow C$  applicazioni. Si dimostri che:

- se  $\psi \circ \varphi$  è iniettiva, allora  $\varphi$  è iniettiva;
- se  $\psi \circ \varphi$  è suriettiva, allora  $\psi$  è suriettiva.

Soluzione. (a) Supponiamo che  $\psi \circ \varphi$  sia iniettiva. Dobbiamo dimostrare che se  $a, a' \in A$  e  $\varphi(a) = \varphi(a')$ , allora  $a = a'$ . Da  $\varphi(a) = \varphi(a')$  segue che  $\psi(\varphi(a)) = \psi(\varphi(a'))$ , ossia  $(\psi \circ \varphi)(a) = (\psi \circ \varphi)(a')$ . Dato che per ipotesi  $\psi \circ \varphi$  è iniettiva, se ne deduce che  $a = a'$ . Quindi anche  $\varphi$  è iniettiva.

(b) Dobbiamo dimostrare che per ogni  $c \in C$  esiste  $b \in B$  tale che  $\psi(b) = c$ . Fissiamo quindi un elemento  $c \in C$ . Dato che  $\psi \circ \varphi$  è suriettiva, esiste  $a \in A$  tale che  $(\psi \circ \varphi)(a) = c$ . Se si pone  $b = \varphi(a)$  si ha quindi  $\psi(b) = \psi(\varphi(a)) = (\psi \circ \varphi)(a) = c$ . Questo prova che  $\psi$  è suriettiva.  $\square$

3.3. Sia  $\varphi: A \rightarrow B$  un'applicazione. Si provi che se  $\iota_A$  e  $\iota_B$  denotano le applicazioni identiche di  $A$  e  $B$  rispettivamente, allora  $\varphi \circ \iota_A = \iota_B \circ \varphi = \varphi$ .

*Soluzione.* Dobbiamo dimostrare che le tre applicazioni  $\varphi \circ \iota_A$ ,  $\iota_B \circ \varphi$  e  $\varphi$  coincidono. Osserviamo intanto che queste tre applicazioni hanno tutte  $A$  come dominio e  $B$  come codominio. Inoltre per ogni  $a \in A$  si ha  $(\varphi \circ \iota_A)(a) = \varphi(\iota_A(a)) = \varphi(a)$  e  $(\iota_B \circ \varphi)(a) = \iota_B(\varphi(a)) = \varphi(a)$ . Quindi  $(\varphi \circ \iota_A)(a) = \varphi(a) = (\iota_B \circ \varphi)(a)$  per ogni  $a \in A$ . Si conclude che  $\varphi \circ \iota_A = \iota_B \circ \varphi = \varphi$ .  $\square$

3.4. Calcolare l'inversa dell'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita ponendo  $\varphi(x) = x^3 - 1$  per ogni  $x \in \mathbb{R}$ .

*Soluzione.* Siano  $x, y \in \mathbb{R}$ . Si ha  $\varphi(x) = y$  se e solo se  $x^3 - 1 = y$ , cioè se e solo se  $x^3 = y + 1$ , vale a dire se e solo se  $x = \sqrt[3]{y+1}$ . Si osservi poi che ponendo  $\psi(y) = \sqrt[3]{y+1}$  per ogni  $y \in \mathbb{R}$  si definisce un'applicazione  $\psi: \mathbb{R} \rightarrow \mathbb{R}$ . Tale applicazione  $\psi$  è quindi l'applicazione inversa di  $\varphi$ .  $\square$

3.5. Siano  $A, B$  insiemi,  $A \neq \emptyset$ , e sia  $\varphi: A \rightarrow B$  un'applicazione. Si provi che le seguenti affermazioni sono equivalenti:

- (a) esiste un'applicazione  $\psi: B \rightarrow A$  tale che  $\psi \circ \varphi = \iota_A$ ;
- (b)  $\varphi$  è iniettiva.

*Soluzione.* (a)  $\Rightarrow$  (b) Segue dall'esercizio 3.2 (a) e dal fatto che  $\psi \circ \varphi = \iota_A$  è iniettiva.

(b)  $\Rightarrow$  (a) Supponiamo che  $\varphi: A \rightarrow B$  sia un'applicazione iniettiva. Dato che  $A \neq \emptyset$ , è possibile fissare un elemento  $\bar{a} \in A$ . Inoltre dato che  $\varphi$  è iniettiva, per ogni  $b \in B$  si ha che  $\varphi^{-1}(b) = \emptyset$  se  $b \notin \varphi(A)$  e che  $\varphi^{-1}(b)$  ha esattamente un elemento se  $b \in \varphi(A)$ . Quindi per ogni  $b \in \varphi(A)$  esiste un unico  $a \in A$  tale che  $\varphi(a) = b$ . Definiamo allora un'applicazione  $\psi: B \rightarrow A$  ponendo, per ogni  $b \in B$ ,

$$\psi(b) = \begin{cases} \text{"l'unico } a \in A \text{ tale che } \varphi(a) = b" & \text{se } b \in \varphi(A), \\ \bar{a} & \text{se } b \notin \varphi(A). \end{cases}$$

Visto come abbiamo definito  $\psi$ , si ha che  $\psi(\varphi(a)) = a$  per ogni  $a \in A$  (perché  $\varphi(a) \in \varphi(A)$  ed  $a$  è l'unico elemento di  $A$  la cui immagine mediante  $\varphi$  è  $\varphi(a)$ ). Quindi  $(\psi \circ \varphi)(a) = \iota_A(a)$  per ogni  $a \in A$ , ossia  $\psi \circ \varphi = \iota_A$ .  $\square$

3.6. Sia  $\varphi: A \rightarrow B$  un'applicazione. Si provi che le seguenti affermazioni sono equivalenti:

- (a) esiste un'applicazione  $\psi: B \rightarrow A$  tale che  $\varphi \circ \psi = \iota_B$ ;
- (b)  $\varphi$  è suriettiva.

*Soluzione.* (a)  $\Rightarrow$  (b) Segue dall'esercizio 3.2 (b) e dal fatto che  $\varphi \circ \psi = \iota_B$  è suriettiva.

(b)  $\Rightarrow$  (a) Supponiamo che  $\varphi: A \rightarrow B$  sia un'applicazione suriettiva. Allora per ogni  $b \in B$  esiste un elemento  $a \in A$  tale che  $\varphi(a) = b$ . Quindi per ogni  $b \in B$  è possibile fissare un elemento di  $A$ , chiamiamolo  $\psi(b)$ , tale che  $\varphi(\psi(b)) = b$ . Fissato per ogni  $b \in B$  un tale elemento  $\psi(b) \in A$ , resta definita un'applicazione  $\psi: B \rightarrow A$  tale che  $\varphi(\psi(b)) = b$  per ogni  $b \in B$ , cioè tale che  $\varphi \circ \psi = \iota_B$ .  $\square$

### Altri esercizi

3.7. Si considerino le applicazioni  $\varphi: \mathbb{N} \rightarrow \mathbb{N}^*$  definita da  $\varphi(x) = x + 1$  per ogni  $x \in \mathbb{R}$ , e  $\psi: \mathbb{N}^* \rightarrow \mathbb{Z}$  definita da  $\psi(n) = -n$  per ogni  $n \in \mathbb{N}^*$ . Si determini l'applicazione composta  $\psi \circ \varphi$ . Tra le applicazioni  $\varphi$ ,  $\psi$  e  $\psi \circ \varphi$  quali sono iniettive? suriettive? biiettive?

3.8. Si considerino le applicazioni

$$\varphi: \mathbb{R} \rightarrow \mathbb{R}, \quad \varphi(x) = \frac{1}{1+x^2} \text{ per ogni } x \in \mathbb{R},$$

e

$$\psi: \mathbb{R} \rightarrow \mathbb{Z}, \quad \psi(x) = \begin{cases} 1 & \text{se } x > 0, \\ 0 & \text{se } x = 0, \\ -1 & \text{se } x < 0. \end{cases}$$

Si determini l'applicazione composta  $\psi \circ \varphi$ . Tra le applicazioni  $\varphi$ ,  $\psi$  e  $\psi \circ \varphi$  quali sono iniettive? suriettive? biiettive?

3.9. Sia  $A$  un insieme non vuoto. Si considerino le applicazioni

$$\pi_1: A \times A \rightarrow A, \quad \pi_1(a, b) = a \text{ per ogni } (a, b) \in A \times A,$$

ed

$$\varepsilon: A \rightarrow \mathcal{P}(A), \quad \varepsilon(a) = \{a\} \text{ per ogni } a \in A.$$

Si determini l'applicazione composta  $\varepsilon \circ \pi_1$ . Tra le applicazioni  $\pi_1$ ,  $\varepsilon$  e  $\varepsilon \circ \pi_1$  quali sono iniettive? suriettive? biiettive?

[Suggerimento: distinguere il caso in cui  $A$  ha esattamente un elemento da quello in cui  $A$  ha più di un elemento.]

3.10. Si dia un esempio di un'applicazione  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  iniettiva e non suriettiva.

3.11. Si dia un esempio di un'applicazione  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  suriettiva e non iniettiva.



3.12. Si dimostri che se  $\varphi: A \rightarrow B$  è un'applicazione iniettiva ma non biiettiva, allora esiste un'applicazione  $\psi_1: B \rightarrow A$  tale che  $\psi_1 \circ \varphi = \iota_A$ , ma non esiste un'applicazione  $\psi_2: B \rightarrow A$  tale che  $\varphi \circ \psi_2 = \iota_B$ .

3.13. Si dimostri che se  $\varphi: A \rightarrow B$  è un'applicazione suriettiva ma non biiettiva, allora non esiste un'applicazione  $\psi_1: B \rightarrow A$  tale che  $\psi_1 \circ \varphi = \iota_A$ , ma esiste un'applicazione  $\psi_2: B \rightarrow A$  tale che  $\varphi \circ \psi_2 = \iota_B$ .

3.14. Si consideri l'applicazione  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  definita da  $\varphi(n) = n + 1$  per ogni  $n \in \mathbb{N}$ . L'applicazione  $\varphi$  è iniettiva? È suriettiva? Si determinino tutte le applicazioni  $\psi: \mathbb{N} \rightarrow \mathbb{N}$  tali che  $\psi \circ \varphi = \iota_{\mathbb{N}}$ .

3.15. Si consideri l'applicazione  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  definita da  $\varphi(n) = n - 1$  se  $n > 0$ , e  $\varphi(0) = 0$ . L'applicazione  $\varphi$  è iniettiva? È suriettiva? Si determinino tutte le applicazioni  $\psi: \mathbb{N} \rightarrow \mathbb{N}$  tali che  $\varphi \circ \psi = \iota_{\mathbb{N}}$ .

3.16. Siano  $\varphi: A \rightarrow B$  e  $\psi: B \rightarrow C$  due applicazioni.

- (a) Si provi che se  $\psi \circ \varphi$  è biettiva, allora  $\varphi$  è iniettiva e  $\psi$  è suriettiva.
- (b) Si trovi un esempio in cui  $\varphi$  è iniettiva,  $\psi$  è suriettiva, ma  $\psi \circ \varphi$  non è iniettiva.
- (c) Si trovi un esempio in cui  $\varphi$  è iniettiva,  $\psi$  è suriettiva, ma  $\psi \circ \varphi$  non è suriettiva.

3.17. Si considerino le applicazioni

$$\varphi: \mathbb{R} \rightarrow \mathbb{R}, \quad \varphi(x) = \begin{cases} -x & \text{se } x^2 = 1, \\ x & \text{se } x^2 \neq 1, \end{cases}$$

e

$$\psi: \mathbb{R} \rightarrow \mathbb{R}, \quad \psi(x) = \begin{cases} x^2 & \text{se } x \geq 0, \\ -x^2 & \text{se } x < 0. \end{cases}$$

Si verifichi che le applicazioni  $\varphi$ ,  $\psi$ ,  $\varphi \circ \psi$  e  $\psi \circ \varphi$  sono biettive e si calcolino le loro inverse.

3.18. Si verifichi che le applicazioni che seguono sono biettive e si calcolino le loro inverse:

- (a)  $\psi: \mathbb{N} \rightarrow A$ ,  $x \mapsto x + 28$ , dove  $A = \{x \in \mathbb{N} \mid x \geq 28\}$ ;
- (b)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(x) = -x$ , per ogni  $x \in \mathbb{Z}$ ;
- (c)  $g: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $g(x) = x - 7$ , per ogni  $x \in \mathbb{Z}$ ;
- (d)  $h: \mathbb{Q} \rightarrow \mathbb{Q}$ ,  $h(x) = -\frac{2}{3}x + 1$ , per ogni  $x \in \mathbb{Q}$ .

3.19. Si calcoli l'applicazione inversa della biiezione dell'esercizio 2.2.

3.20. Siano  $A$  un insieme non vuoto ed  $f: A \rightarrow A$  un'applicazione. Si provi che  $f \circ f = f$  se e solo se esistono due sottoinsiemi  $B$  e  $C$  di  $A$  tali che  $B \cup C = A$ ,  $B \cap C = \emptyset$ ,  $f(C) \subseteq B$  e  $f(b) = b$  per ogni  $b \in B$ .

3.21. Siano  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ ,  $h: A \rightarrow C$  tre applicazioni tali che  $g \circ f = h$ . Si dimostri che se  $f$  è suriettiva allora  $g(B) = h(A)$ .

*Handwritten notes:*  $(n-1) \text{ vera} \rightarrow n \in \mathbb{Z} \cap A$   
 $5x(n-1) + 5x = 5x(n-1) + 5x$   
 $5x(n-1) + 5x = 5x(n-1) + 5x$   
 $5x(n-1) + 5x = 5x(n-1) + 5x$   
 $5x(n-1) + 5x = 5x(n-1) + 5x$

#### Capitolo 4. Il principio di induzione e altre proprietà dei numeri interi

**Divisione tra numeri interi, numeri primi.** Se  $a, b \in \mathbb{Z}$  e  $b \neq 0$ , esiste un'unica coppia  $(q, r)$  di numeri interi tali che

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|.$$

In tal caso  $q$  si dice il *quoto* ed  $r$  si dice il *resto* della divisione di  $a$  per  $b$ . (Qui abbiamo scritto  $|b|$  per denotare il *modulo* di  $b$ ; per la definizione di *modulo* o *valore assoluto* di un numero reale si veda l'Esercizio 4.1.)

Se  $a, b \in \mathbb{Z}$ , si dice che  $b$  *divide*  $a$  o che  $b$  è un *divisore* di  $a$  o che  $a$  è un *multiplo* di  $b$  (e si scrive  $b \mid a$ ) se esiste  $c \in \mathbb{Z}$  tale che  $a = bc$ . Un numero  $p \in \mathbb{Z}$  si dice un numero *primo* se  $p \neq 1$ ,  $p \neq -1$  e i suoi divisori sono solo  $1, -1, p, -p$ . Quindi in particolare  $0, 1$  e  $-1$  non sono numeri primi, mentre  $2, -2, 3, -3, 5$  e  $-5$  lo sono.

**TEOREMA FONDAMENTALE DELL'ARITMETICA.** Ogni numero intero  $a \neq 0, 1, -1$  è prodotto di numeri primi (non necessariamente distinti). Tale fattorizzazione è essenzialmente unica nel senso seguente: se

$$a = p_1 p_2 \cdots p_r \quad \text{e} \quad a = q_1 q_2 \cdots q_s$$

sono due fattorizzazioni di  $a$  ove  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$  sono numeri primi, allora  $r = s$  e si possono riordinare i fattori in modo che

$$|p_1| = |q_1|, \quad |p_2| = |q_2|, \quad \dots, \quad |p_r| = |q_r|.$$

**Massimo comun divisore, minimo comune multiplo.** Siano  $a, b$  due numeri interi non entrambi nulli. Un numero intero  $d \in \mathbb{Z}$  si dice un *massimo comun divisore* (MCD) di  $a$  e  $b$  se valgono le seguenti proprietà:

- (a)  $d \mid a$ ,  $d \mid b$ ;
- (b) se  $c \in \mathbb{Z}$ ,  $c \mid a$  e  $c \mid b$ , allora  $c \mid d$ .

**TEOREMA 4.1.** Siano  $a, b \in \mathbb{Z}$  due numeri interi non entrambi nulli. Allora esiste un MCD positivo  $d$  di  $a$  e  $b$ . Inoltre esistono  $\alpha, \beta \in \mathbb{Z}$  tali che  $d = \alpha a + \beta b$ .

È possibile dimostrare che se  $a, b$  sono numeri interi non entrambi nulli, ci sono esattamente due loro MCD, uno l'opposto dell'altro. Pertanto  $a, b$  hanno un unico MCD positivo, che verrà da noi indicato con  $(a, b)$ . L'altro MCD di  $a, b$  è pertanto  $-(a, b)$ .

**COROLLARIO 4.2.** Se  $a, b \in \mathbb{Z}$ , allora  $a$  e  $b$  sono primi tra loro (cioè  $(a, b) = 1$ ) se e solo se esistono  $\alpha, \beta \in \mathbb{Z}$  tali che  $\alpha a + \beta b = 1$ .

Se  $a, b \in \mathbb{Z}$  sono due numeri interi entrambi non nulli, un numero intero  $m$  si dice un *minimo comune multiplo* (mcm) di  $a$  e  $b$  se valgono le seguenti proprietà:

- (a)  $a \mid m, b \mid m$ ;
- (b) se  $c \in \mathbb{Z}, a \mid c$  e  $b \mid c$ , allora  $m \mid c$ .

È possibile dimostrare (si vedano gli Esercizi 4.2 e 4.3) che se  $a, b$  sono due numeri interi entrambi non nulli, esistono esattamente due loro mcm, uno l'opposto dell'altro. Il mcm positivo di  $a, b$  verrà da noi indicato con  $[a, b]$ .

**ALGORITMO DI EUCLIDE.** Siano  $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$ . Si ponga  $r_{-1} = a, r_0 = b$  e si consideri la seguente successione:

$$r_{-1} = r_0 q_1 + r_1$$

$$r_0 = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$r_2 = r_3 q_4 + r_4$$

$$r_3 = r_4 q_5 + r_5$$

...

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$$

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_{n-1} = r_n q_{n+1}$$

ove  $q_i$  e gli  $r_i$  sono i quoti e i resti delle divisioni scritte e ove la successione termina non appena si trovi un resto  $r_{n+1} = 0$ . Allora: (a) la successione termina dopo un numero finito di passi, e (b)  $r_n$  è  $(a, b)$ .

**ESEMPIO 1.** Calcoliamo il MCD positivo di 1956 e 1992 facendo uso dell'algoritmo di Euclide.

Si ha

$$1956 = 0 \cdot 1992 + 1956;$$

$$1992 = 1956 \cdot 1 + 36;$$

$$1956 = 36 \cdot 54 + 12;$$

$$36 = 12 \cdot 3.$$

Quindi 12 (ultimo resto non nullo) è il MCD positivo di 1956 e 1992.  $\square$

**ESEMPIO 2.** Determinare il MCD positivo di 987654321 e 98765432.

Si ha

$$987654321 = 98765432 \cdot 10 + 1;$$

$$98765432 = 1 \cdot 98765432.$$

Quindi il MCD cercato è 1, cioè i due numeri sono primi tra loro.  $\square$

**Principio di induzione.** Ricordiamo il

**PRINCIPIO DI INDUZIONE (PRIMA FORMA).** Sia  $n_0 \in \mathbb{Z}$  e sia  $P$  un'asserzione sui numeri interi  $n \geq n_0$ . Supponiamo che siano soddisfatte le seguenti due condizioni:

- (a)  $P$  è vera per il numero  $n_0$ ;
- (b) per ogni intero  $n > n_0$ , se  $P$  è vera per il numero  $n-1$  allora  $P$  è vera per il numero  $n$ .

Allora  $P$  è vera per ogni numero intero  $n \geq n_0$ .

Sarebbe possibile dimostrare che il principio di induzione nella forma appena enunciata è equivalente al principio di induzione enunciato nella forma seguente:

**PRINCIPIO DI INDUZIONE (SECONDA FORMA).** Sia  $n_0 \in \mathbb{Z}$  e sia  $P$  un'asserzione sui numeri interi  $n \geq n_0$ . Supponiamo che siano soddisfatte le seguenti due condizioni:

- (a)  $P$  è vera per il numero  $n_0$ ;
- (b) per ogni intero  $n > n_0$ , se  $P$  è vera per ogni numero  $t$  soddisfacente a  $n_0 \leq t < n$  allora  $P$  è vera per il numero  $n$ .

Allora  $P$  è vera per ogni numero intero  $n \geq n_0$ .

A seconda dell'asserzione da dimostrare potrà essere più conveniente far uso del principio di induzione in una o nell'altra forma.

**ESEMPIO 3.** Dimostriamo che la somma dei primi  $n$  numeri interi positivi è  $n(n+1)/2$ :

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

Dobbiamo dimostrare che l'uguaglianza  $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  è vera quando  $n = 1$  e, supposto che questa uguaglianza sia vera per  $n-1$ , dobbiamo

dimostrare che è vera anche per il numero  $n$ . Per  $n = 1$  la somma nel membro a sinistra dell'uguaglianza è la somma avente un unico addendo uguale a 1; quindi tale somma vale 1, e lo stesso accade per l'espressione  $\frac{1 \cdot (1+1)}{2}$  nel membro a destra. Quindi il caso  $n = 1$  è verificato. Supponiamo ora che l'uguaglianza sia vera per  $n - 1$ , cioè che  $1 + 2 + 3 + \dots + (n - 1) = \frac{(n-1)n}{2}$ . Allora

$$1 + 2 + 3 + \dots + n = [1 + 2 + 3 + \dots + (n - 1)] + n = \frac{(n-1)n}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n^2 + n}{2} = \frac{n(n+1)}{2},$$

cioè l'uguaglianza è vera anche per il numero  $n$ . Per il principio di induzione si conclude che l'uguaglianza è vera per ogni  $n$ .  $\square$

**ESEMPIO 4.** Dimostriamo che la somma dei primi  $n$  numeri naturali dispari è  $n^2$ , cioè che  $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$ .

Dobbiamo dimostrare che l'uguaglianza  $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$  è vera quando  $n = 1$  e, supposto che questa uguaglianza sia vera per  $n - 1$ , dobbiamo dimostrare che è vera anche per  $n$ . Per  $n = 1$  la somma nel membro a sinistra dell'uguaglianza è la somma avente un unico addendo uguale a 1; quindi la somma vale 1, come l'espressione nel membro a destra. Quindi il caso  $n = 1$  è verificato. Supponiamo ora che l'uguaglianza sia vera per la somma dei primi  $n - 1$  numeri naturali dispari, cioè che  $1 + 3 + 5 + 7 + \dots + (2n - 3) = (n - 1)^2$ . Allora  $1 + 3 + 5 + 7 + \dots + (2n - 1) = [1 + 3 + 5 + 7 + \dots + (2n - 3)] + (2n - 1) = (n - 1)^2 + (2n - 1) = n^2$ , cioè l'uguaglianza è vera anche per  $n$  addendi. Per il principio di induzione si conclude che l'uguaglianza è vera per ogni  $n$ .  $\square$

**ESEMPIO 5.** Dimostriamo per induzione su  $n$  che 13 divide  $4^{2n+1} + 3^{n+2}$  per ogni  $n \in \mathbb{N}$ .

In questo caso l'asserzione  $P$  sui numeri interi è "13 divide  $4^{2n+1} + 3^{n+2}$ ", e si vuol dimostrare che  $P$  è vera per ogni numero intero  $n \geq 0$ . Mostriamo intanto che  $P$  è vera per  $n = 0$ . Quando  $n = 0$  l'asserzione  $P$  diventa "13 divide  $4 + 3^2$ ", ossia "13 divide 13", che è vera. Sia ora  $n > 0$  un numero intero e supponiamo che  $P$  sia vera per il numero  $n - 1$ , cioè supponiamo che 13 divida  $4^{2(n-1)+1} + 3^{(n-1)+2}$ , ossia che 13 divida  $4^{2n-1} + 3^{n+1}$ . Dato che  $4^{2n+1} + 3^{n+2} = 16 \cdot 4^{2n-1} + 3 \cdot 3^{n+1} = 13 \cdot 4^{2n-1} + 3(4^{2n-1} + 3^{n+1})$ , se ne deduce che  $4^{2n+1} + 3^{n+2}$  è somma dei due numeri  $13 \cdot 4^{2n-1}$  e  $3(4^{2n-1} + 3^{n+1})$ , entrambi divisibili per 13, e quindi anche  $4^{2n+1} + 3^{n+2}$  è divisibile per 13. Pertanto l'asserzione  $P$  è vera per ogni numero intero  $n \geq 0$ .  $\square$

### Esercizi svolti

**4.1.** Ricordiamo che per ogni  $x \in \mathbb{R}$  il modulo (o valore assoluto) di  $x$  è il numero

reale definito da

$$|x| = \begin{cases} x & \text{se } x \geq 0, \\ -x & \text{se } x < 0. \end{cases}$$

Si dimostri che per ogni  $x, y \in \mathbb{R}$  si ha  $|x + y| \leq |x| + |y|$  e  $|xy| = |x| |y|$ .

**Soluzione.** Distinguendo i quattro casi  $x \geq 0$  e  $y \geq 0$ ,  $x \geq 0$  e  $y < 0$ ,  $x < 0$  e  $y \geq 0$ ,  $x < 0$  e  $y < 0$ , si ha:

(1) Se  $x \geq 0$  e  $y \geq 0$ , allora  $x + y \geq 0$  e  $xy \geq 0$ , da cui  $|x + y| = x + y = |x| + |y|$  e  $|xy| = xy = |x| |y|$ .

(2) Se  $x \geq 0$  e  $y < 0$ , allora  $y < -y$  e quindi  $x + y < x + (-y) = |x| + |y|$ ; inoltre  $-x \leq x$  e quindi  $-(x + y) = -x - y \leq x - y = |x| + |y|$ . Quindi si ha sia che  $x + y \leq |x| + |y|$  e che  $-(x + y) \leq |x| + |y|$ . Pertanto  $|x + y| \leq |x| + |y|$ . Inoltre  $xy \leq 0$  e quindi  $|xy| = -xy = x(-y) = |x| |y|$ .

(3) Il caso  $x < 0$  e  $y \geq 0$  è simile al precedente.

(4) Se  $x < 0$  e  $y < 0$ , allora  $x + y < 0$  e  $xy > 0$ , da cui  $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$  e  $|xy| = xy = (-x)(-y) = |x| |y|$ .  $\square$

**4.2.** Si dimostri che se  $a, b$  sono due numeri interi entrambi non nulli, allora esiste un mcm positivo di  $a$  e  $b$ .

**Soluzione.** Siano  $a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$  e  $b\mathbb{Z} = \{by \mid y \in \mathbb{Z}\}$  gli insiemi di tutti i multipli interi di  $a$  e  $b$  rispettivamente, e consideriamo l'insieme  $S = a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ . Allora  $S \subseteq \mathbb{N}^*$  ed  $S \neq \emptyset$  perché  $|a| \cdot |b| \in S$ . Sia  $m$  il più piccolo degli elementi di  $S$ . Mostriamo che il numero positivo  $m$  è un mcm di  $a$  e  $b$ . Intanto  $a \mid m$  perché  $m \in a\mathbb{Z}$  e  $b \mid m$  perché  $m \in b\mathbb{Z}$ .

Sia  $c \in \mathbb{Z}$  tale che  $a \mid c$  e  $b \mid c$ . Dividiamo  $c$  per  $m$ . Allora  $c = qm + r$  con  $q, r \in \mathbb{Z}$  e  $0 \leq r < m$ . Dato che  $a \mid c$  e  $a \mid m$ , si ha che  $a$  divide anche  $c - qm = r$ , e quindi  $r \in a\mathbb{Z}$ . Analogamente  $r \in b\mathbb{Z}$ . Se per assurdo fosse  $r > 0$ , allora  $r \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* = S$ , e questo è assurdo perché  $r < m$  ed  $m$  era stato scelto come il minimo di  $S$ . Quindi deve essere  $r = 0$ , da cui  $c = qm$ , ossia  $m \mid c$ . Questo dimostra che  $m$  è un minimo comune multiplo positivo di  $a$  e  $b$ .  $\square$

**4.3.** Si dimostri che se  $a, b$  sono due numeri interi entrambi non nulli, allora  $a$  e  $b$  hanno esattamente due mcm, uno opposto all'altro.

**Soluzione.** Siano  $m, m'$  due mcm di  $a$  e  $b$ . Osserviamo intanto che  $m$  ed  $m'$  sono diversi da 0; infatti se fosse ad esempio  $m = 0$ , allora 0 dovrebbe dividere ogni numero intero che è un multiplo sia di  $a$  che di  $b$ , come ad esempio  $ab$ , e questo è assurdo perché 0 non può dividere il numero  $ab \neq 0$ . Questo prova che  $m \neq 0$ .

Dato che  $m, m'$  sono due mcm di  $a$  e  $b$ , ne segue che per ogni  $c \in \mathbb{Z}$  tale che  $a \mid c$  e  $b \mid c$  si ha  $m \mid c$ . Inoltre  $a \mid m'$  e  $b \mid m'$ . Quindi  $m \mid m'$ . Analogamente  $m' \mid m$ . Pertanto  $m' = mx$  ed  $m = m'y$  per opportuni  $x, y \in \mathbb{Z}$ . In particolare

$m = m'y = mxy$ . Ma abbiamo visto che si ha  $m \neq 0$ , e quindi  $xy = 1$ , da cui  $x = 1$  oppure  $x = -1$ . Pertanto  $m' = m$  oppure  $m' = -m$ .  $\square$

Si ricordi che se  $n$  è un numero naturale, il numero  $n!$  (che si legge *n fattoriale*) è definito da

$$n! = \begin{cases} 1 & \text{se } n = 0, \\ 1 \cdot 2 \cdot 3 \cdots (n-1)n & \text{se } n > 0. \end{cases}$$

Quindi  $0! = 1$ ,  $1! = 1$ ,  $2! = 2$ ,  $3! = 6$ ,  $4! = 24$ ,  $5! = 120$ , ecc.

4.4. Facendo uso del principio di induzione nella prima forma si dimostri che per ogni  $h \geq 1$  si ha

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + h \cdot h! = (h+1)! - 1.$$

*Soluzione.* Nel caso  $h = 1$  l'identità da dimostrare si riduce a  $1 \cdot 1! = (1+1)! - 1$ , che è vera. Sia  $h > 1$  e supponiamo che l'identità sia vera per il numero  $h-1$ , cioè supponiamo che

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + (h-1) \cdot (h-1)! = h! - 1.$$

Allora  $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + h \cdot h! = [1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + (h-1) \cdot (h-1)!] + h \cdot h! = (h! - 1) + h \cdot h! = h!(1+h) - 1 = (h+1)! - 1$ . Questo dimostra che l'identità è vera anche per il numero  $h$ . Per il principio di induzione l'identità è vera per ogni  $h \geq 1$ .  $\square$

4.5. Si dimostri per induzione su  $n$  (seconda forma) che ogni numero naturale  $n$  può essere scritto nella forma

$$n = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_h \cdot h!,$$

dove  $h, c_1, c_2, \dots, c_h \in \mathbb{N}$  e  $c_i \leq i$  per ogni  $i = 1, 2, \dots, h$ .

*Soluzione.* Nel caso  $n = 0$  l'asserzione è vera, in quanto 0 si può scrivere nella forma  $0 \cdot 1!$ . Supponiamo quindi  $n > 0$  e che tutti i numeri naturali minori di  $n$  siano esprimibili nella forma detta. Si consideri la successione crescente di numeri naturali  $1! < 2! < 3! < 4! < \dots$ . Esiste un unico numero naturale  $h$  tale che  $h! \leq n < (h+1)!$ . Dividiamo  $n$  per  $h!$ : si ottiene che esistono due numeri interi  $c_h$  ed  $r$  tali che  $n = c_h \cdot h! + r$  e  $0 \leq r < h!$ . Si osservi che  $c_h = \frac{n-r}{h!} \leq \frac{n}{h!} < \frac{(h+1)!}{h!} = h+1$ . Quindi  $c_h < h+1$ , ed essendo  $c_h$  un numero intero deve essere  $c_h \leq h$ . Quindi se  $r = 0$  siamo arrivati alla conclusione, perché  $n = c_h \cdot h!$  è una scrittura del tipo cercato. Se invece  $r > 0$ , allora  $r < h! \leq n$ , e quindi è possibile applicare l'ipotesi induttiva ad  $r$ : esistono  $\ell, c_1, c_2, \dots, c_\ell \in \mathbb{N}$  tali che  $r = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_\ell \cdot \ell!$  e  $c_i \leq i$  per ogni  $i = 1, 2, \dots, \ell$ . Dato che  $r > 0$ , si può supporre senza perdita di generalità che  $c_\ell \neq 0$ , ossia che

$c_\ell \geq 1$ . Si osservi che allora  $\ell < h$ , perché se per assurdo fosse  $\ell \geq h$ , allora  $r = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_\ell \cdot \ell! \geq \ell! \geq h!$ , e questa è una contraddizione perché  $r < h!$ . Si ha pertanto  $n = r + c_h \cdot h! = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_\ell \cdot \ell! + c_h \cdot h!$ , e questo è un modo di scrivere  $n$  nella forma desiderata (supponendo, come è ovvio,  $c_{\ell+1} = 0, c_{\ell+2} = 0, \dots, c_{h-1} = 0$ ).  $\square$

### Altri esercizi

4.6. Quali sono il quoto e il resto della divisione di  $-202$  per  $20$ ?

4.7. Sia  $a \in \mathbb{Z}$ . Si dimostri che  $0 \mid a$  se e solo se  $a = 0$ .

4.8. Si dimostri che  $a \mid 0$  e  $1 \mid a$  per ogni  $a \in \mathbb{Z}$ .

4.9. Sia  $a \in \mathbb{Z}$ . Si dimostri che  $a \mid 1$  se e solo se  $a = 1$  oppure  $a = -1$ .

4.10. Si dimostri che se  $a, b, p \in \mathbb{Z}$ ,  $p$  è primo e  $p \mid ab$ , allora  $p \mid a$  oppure  $p \mid b$ . [Suggerimento: teorema fondamentale dell'aritmetica.]

4.11. Sia  $n \in \mathbb{N}$ . Si dimostri che per il numero reale  $\sqrt{n}$  si ha  $\sqrt{n} \in \mathbb{Z}$  oppure  $\sqrt{n} \notin \mathbb{Q}$ . Quindi  $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}, \dots \notin \mathbb{Q}$ . [Suggerimento: dimostrare che se  $\sqrt{n} \in \mathbb{Q}$  allora  $\sqrt{n} \in \mathbb{Z}$ .]

4.12. Calcolare mediante l'algoritmo di Euclide il MCD positivo delle seguenti coppie di numeri:

- (a) 31 e 7;
- (b) 30 e 99;
- (c) 101 e 199;
- (d) 1111111 e 1111.

4.13. Dimostrare che la somma  $2 + 4 + 6 + \cdots + 2n$  dei primi  $n$  numeri interi pari positivi è  $n(n+1)$ .

4.14. Dimostrare per induzione su  $n$  che  $\sum_{k=0}^n \frac{1}{2^k} = 2 - \frac{1}{2^n}$ .

4.15. Dimostrare per induzione che per ogni intero  $n \geq 2$  si ha

$$\left(1 - \frac{1}{4}\right) \left(1 - \frac{1}{9}\right) \left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

4.16. Dimostrare per induzione che  $n^2 \geq 11n - 30$  per ogni intero  $n \geq 5$ .

4.17. Dimostrare che per ogni  $n \geq 1$  si ha

$$\frac{1^2}{2 \cdot 3} \cdot \frac{2^2}{3 \cdot 4} \cdot \frac{3^2}{4 \cdot 5} \cdot \frac{4^2}{5 \cdot 6} \cdots \frac{n^2}{(n+1)(n+2)} = \frac{2}{(n+1)^2(n+2)}.$$

4.18. Dimostrare che per ogni intero positivo  $n$  si ha

$$2^3 + 4^3 + 6^3 + \dots + (2n)^3 = 2n^2(n+1)^2.$$

4.19. Dimostrare che per ogni intero  $n \geq 3$  si ha

$$(2^3 + 2^4 + 2^5 + \dots + 2^n) + 2^3 = 2^{n+1}.$$

4.20. Dimostrare che per ogni  $n \in \mathbb{N}$  si ha

$$-1^2 + 2^2 - 3^2 + 4^2 - \dots + (-1)^n n^2 = (-1)^n \frac{n(n+1)}{2}.$$

4.21. Dimostrare che per ogni intero  $n \geq 1$  si ha

$$1^4 + 2^4 + 3^4 + \dots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

4.22. Dimostrare che per ogni intero  $n \geq 1$  si ha

$$1 - 2 + 3 - 4 + 5 - 6 + \dots + (-1)^{n+1} n = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari,} \\ \frac{n+1}{2} & \text{se } n \text{ è dispari.} \end{cases}$$

4.23. Dimostrare che la somma dei cubi dei primi  $n$  numeri naturali dispari è data da  $1^3 + 3^3 + 5^3 + \dots + (2n-1)^3 = n^2(2n^2-1)$ .\*

4.24. Dimostrare che ogni numero naturale  $n$  può essere scritto nella forma descritta nell'esercizio 4.5 in modo essenzialmente unico nel senso seguente: se  $n = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \dots + c_h \cdot h! = d_1 \cdot 1! + d_2 \cdot 2! + d_3 \cdot 3! + \dots + d_\ell \cdot \ell!$  con  $h, c_1, c_2, \dots, c_h, \ell, d_1, d_2, \dots, d_\ell \in \mathbb{N}$ ,  $c_i \leq i$  per ogni  $i = 1, 2, \dots, h$ ,  $d_j \leq j$  per ogni  $j = 1, 2, \dots, \ell$ , e  $\ell \geq h$ , allora  $c_i = d_i$  per ogni  $i = 1, 2, \dots, h$  e  $d_j = 0$  per ogni  $j = h+1, h+2, \dots, \ell$ .

[Suggerimento: esercizio 4.4.]

\*Quasi tutte le formule che si incontrano in questo capitolo sono note da moltissimo tempo. Ad esempio la formula di questo esercizio si trova nel *Ta'ul-kys* di Ibn Albanna del tredicesimo secolo.

## Capitolo 5. Numeri complessi

Poniamo per definizione  $\mathbb{C} = \mathbb{R} \times \mathbb{R}$  e chiamiamo *numeri complessi* gli elementi di  $\mathbb{C}$ , ossia le coppie  $(a, b)$ , dove  $a$  e  $b$  sono numeri reali. Dati due numeri complessi  $z = (a, b)$ ,  $z' = (a', b')$ , definiamo la loro somma e il loro prodotto ponendo  $z + z' = (a + a', b + b')$  e  $zz' = (aa' - bb', ab' + ba')$ .

LEMMA 5.1.  $z'' = (a'', b'') \in \mathbb{C} = \mathbb{R} \times \mathbb{R}$  si ha:

- (a)  $z + (z' + z'') = (z + z') + z''$  (associatività dell'addizione);
- (b)  $z + z' = z' + z$  (commutatività dell'addizione);
- (c)  $z(z'z'') = (zz')z''$  (associatività della moltiplicazione);
- (d)  $zz' = z'z$  (commutatività della moltiplicazione);
- (e)  $z(z' + z'') = zz' + zz''$  (distributività della moltiplicazione rispetto all'addizione);
- (f)  $z + (0, 0) = z$ ;
- (g)  $(a, b) + (-a, -b) = (0, 0)$ ;
- (h)  $z(1, 0) = z$ ;
- (i) se  $z = (a, b) \neq (0, 0)$ , allora  $(a, b)(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}) = (1, 0)$ .

*Dimostrazione.* Dimostriamo le proprietà (a), (c), (d), (e), (i) lasciando le verifiche delle altre quattro asserzioni al lettore.

(a) Si ha

$$\begin{aligned} z + (z' + z'') &= (a, b) + ((a', b') + (a'', b'')) = (a, b) + (a' + a'', b' + b'') = \\ &= (a + (a' + a''), b + (b' + b'')) = \\ &= ((a + a') + a'', (b + b') + b'') = (a + a', b + b') + (a'', b'') = \\ &= (a, b) + (a', b') + (a'', b'') = (z + z') + z''. \end{aligned}$$

(c) Si ha

$$\begin{aligned} z(z'z'') &= (a, b)((a', b')(a'', b'')) = (a, b)(a'a'' - b'b'', a'b'' + b'a'') = \\ &= (a(a'a'' - b'b'') - b(a'b'' + b'a''), a(a'b'' + b'a'') + b(a'a'' - b'b'')) = \\ &= (aa'a'' - ab'b'' - ba'b'' - bb'a'', aa'b'' + ab'a'' + ba'a'' - bb'b''). \end{aligned}$$



Analogamente

$$\begin{aligned}(zz')z'' &= ((a, b)(a', b'))(a'', b'') = (aa' - bb', ab' + ba')(a'', b'') = \\ &= ((aa' - bb')a'' - (ab' + ba')b'') = (aa'a'' - bb'a'' - ab'b'' - ba'b'') = \\ &= (aa'a'' - bb'a'' - ab'b'' - ba'b'') = (aa'a'' - bb'a'' - ab'b'' - ba'b'').\end{aligned}$$

Quindi  $z(z'z'') = (zz')z''$ .

$$(d) \quad zz' = (a, b)(a', b') = (aa' - bb', ab' + ba') = (a'a - b'b, a'b + b'a) = z'z.$$

$$\begin{aligned}(e) \quad z(z' + z'') &= (a, b)((a', b') + (a'', b'')) = (a, b)(a' + a'', b' + b'') = \\ &= (a(a' + a'') - b(b' + b''), a(b' + b'') + b(a' + a'')) = \\ &= (aa' + aa'' - bb' - bb'', ab' + ab'' + ba' + ba'') = \\ &= (aa' - bb', ab' + ba') + (aa'' - bb'', ab'' + ba'') = \\ &= (a, b)(a', b') + (a, b)(a'', b'') = zz' + zz''.\end{aligned}$$

(i) Si osservi che se  $z = (a, b) \neq (0, 0)$ , cioè se  $a$  e  $b$  non sono entrambi nulli, allora  $a^2 + b^2 > 0$ , e quindi è possibile dividere  $a$  e  $-b$  per  $a^2 + b^2$ . Si ha

$$(a, b) \left( \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left( a \frac{a}{a^2 + b^2} - b \frac{-b}{a^2 + b^2}, a \frac{-b}{a^2 + b^2} + b \frac{a}{a^2 + b^2} \right) = \left( \frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ba}{a^2 + b^2} \right) = (1, 0). \quad \square$$

Identificheremo i numeri complessi del tipo  $(a, 0)$  con i numeri reali, cioè scriveremo  $a$  in luogo di  $(a, 0)$ . Scriveremo anche  $i$  invece di  $(0, 1)$ .

ESEMPIO 1. Dimostriamo che  $i^2 = -1$ .

Si ha  $i^2 = (0, 1)(0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1$ .  $\square$

ESEMPIO 2. Dimostriamo che  $\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right)^3 = i$ .

Si ha

$$\begin{aligned}\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right)^3 &= \left(\left(\frac{\sqrt{3}}{2}, 0\right) + (0, 1)\left(\frac{1}{2}, 0\right)\right)^3 = \\ &= \left(\left(\frac{\sqrt{3}}{2}, 0\right) + \left(0, \frac{1}{2}\right)\right)^3 = \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)^3 = \\ &= \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) = \\ &= \left(\frac{3}{4} - \frac{1}{4}, \frac{\sqrt{3}}{4} + \frac{\sqrt{3}}{4}\right) \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) =\end{aligned}$$

$$= \left(\frac{\sqrt{3}}{4} - \frac{\sqrt{3}}{4}, \frac{1}{4} + \frac{3}{4}\right) = (0, 1) = i. \quad \square$$

ESEMPIO 3. Dimostriamo che se  $a, b \in \mathbb{R}$ , il numero complesso  $a + ib$  è uguale ad  $(a, b)$ .

Si ha  $a + ib = (a, 0) + (0, 1)(b, 0) = (a, 0) + (0, b) = (a, b)$ .  $\square$

In base a quanto abbiamo visto nell'esempio 3 si ha che

$$C = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\} = \{a + ib \mid a, b \in \mathbb{R}\}$$

e che due numeri complessi  $a + ib$  e  $c + id$  sono uguali (qui  $a, b, c, d \in \mathbb{R}$ ) se e solo se  $a = c$  e  $b = d$ . Inoltre la notazione  $a + ib$  permette di operare secondo le regole del calcolo letterale (quelle del lemma 5.1) tenendo presente che  $i^2 = -1$ .

ESEMPIO 4. Si ha

$$(1 + i3) + (-4 + i\sqrt{2}) = -3 + i(3 + \sqrt{2});$$

$$(1 + i3) - (-4 + i\sqrt{2}) = 5 + i(3 - \sqrt{2});$$

$$(1 + i3)(-4 + i\sqrt{2}) = -4 + i\sqrt{2} - i12 + i^2 3\sqrt{2} = (-4 - 3\sqrt{2}) + i(\sqrt{2} - 12);$$

$$\begin{aligned}\frac{1 + i3}{-4 + i\sqrt{2}} &= \frac{(1 + i3)(-4 - i\sqrt{2})}{(-4 + i\sqrt{2})(-4 - i\sqrt{2})} = \frac{-4 - i\sqrt{2} - i12 + i^2 3\sqrt{2}}{16 + 2} = \\ &= \frac{(-4 + 3\sqrt{2}) + i(-\sqrt{2} - 12)}{18} = \frac{-4 + 3\sqrt{2}}{18} + i \frac{-\sqrt{2} - 12}{18}.\end{aligned}$$

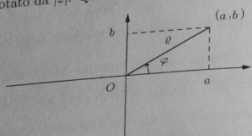
Si osservi come abbiamo proceduto per dividere due numeri complessi, cioè per scrivere nella forma  $a + ib$  una frazione del tipo  $\frac{c + id}{e + if}$ . Qui intendiamo ovviamente che  $a, b, c, d, e, f$  siano numeri reali e che  $e + if \neq 0$ , vale a dire che i due numeri reali  $e$  ed  $f$  non siano entrambi nulli. Il metodo consiste nel moltiplicare sia il numeratore che il denominatore della frazione  $\frac{c + id}{e + if}$  per il complesso coniugato di  $e + if$ , cioè per il numero complesso  $e - if$ . Si ha quindi che  $\frac{c + id}{e + if} = \frac{(c + id)(e - if)}{(e + if)(e - if)}$ . In questo modo la frazione data viene trasformata in una frazione il cui denominatore  $(e + if)(e - if)$  è il numero reale positivo  $e^2 + f^2$ .

Ecco un altro esempio:

$$\frac{1 + 2i}{3 - 4i} = \frac{(1 + 2i)(3 + 4i)}{(3 - 4i)(3 + 4i)} = \frac{3 + 4i + 6i - 8}{9 + 16} = \frac{-5 + 10i}{25} = -\frac{1}{5} + i\frac{2}{5}. \quad \square$$

C'è una biiezione tra l'insieme  $C$  dei numeri complessi e l'insieme dei punti del piano cartesiano che ad ogni numero complesso  $a + ib$  associa il punto  $P$  di coordinate  $(a, b)$  del piano. I numeri complessi possono essere quindi rappresentati

come punti di un piano, detto *piano di Argand-Gauss*. La distanza  $\rho$  del punto  $P$  di coordinate  $(a, b)$  dall'origine  $O$  è detto il *modulo* del numero complesso  $z = a + ib$ , ed è denotato da  $|z|$ . Quindi  $\rho = |z| = \sqrt{a^2 + b^2}$ .



Se  $z \neq 0$  e  $\varphi$  denota l'angolo formato dal semiasse positivo delle  $x$  e dalla semiretta di origine  $O$  e passante per  $P$ ,  $\varphi$  è detto l'*argomento* o l'*anomalia* di  $z$ , e si ha

$$a = \rho \cos \varphi, \quad b = \rho \sin \varphi,$$

da cui

$$z = a + ib = \rho(\cos \varphi + i \sin \varphi).$$

Quindi i numeri complessi possono essere scritti anche nella forma (detta *forma trigonometrica*)  $\rho(\cos \varphi + i \sin \varphi)$ , dove  $\rho \geq 0$  e  $\varphi$  sono numeri reali. Si noti che per il numero complesso  $z = 0$  l'argomento non è definito, e che per i numeri complessi  $z \neq 0$  l'argomento è definito solo a meno di multipli interi di  $2\pi$ , cioè che se  $\varphi$  è un argomento di  $z$  anche ogni numero del tipo  $\varphi + 2k\pi$ , con  $k$  intero, è un argomento di  $z$ .

**PROPOSIZIONE 5.2.** Il prodotto di due numeri complessi ha per modulo il prodotto dei loro moduli e per argomento la somma dei loro argomenti.

**COROLLARIO 5.3.** Se  $z = \rho(\cos \varphi + i \sin \varphi)$  è un numero complesso scritto in forma trigonometrica, allora  $z^n = \rho^n(\cos n\varphi + i \sin n\varphi)$  per ogni numero naturale  $n$ .

*Dimostrazione.* Induzione su  $n$ . Per  $n = 0$  si ha

$$z^n = z^0 = 1 \quad \text{e} \quad \rho^n(\cos n\varphi + i \sin n\varphi) = \rho^0(\cos 0 + i \sin 0) = 1,$$

e quindi in questo caso l'uguaglianza è vera. Supponiamo poi che l'uguaglianza sia vera per  $n-1$ , cioè che  $z^{n-1} = \rho^{n-1}(\cos(n-1)\varphi + i \sin(n-1)\varphi)$ , vale a dire che il modulo di  $z^{n-1}$  sia  $\rho^{n-1}$  e che il suo argomento sia  $(n-1)\varphi$ . Allora per la proposizione 5.2  $z^n = z^{n-1}z$  ha come modulo  $\rho^{n-1}\rho = \rho^n$  e come argomento  $(n-1)\varphi + \varphi = n\varphi$ . Quindi

$$z^n = \rho^n(\cos n\varphi + i \sin n\varphi). \quad \square$$

**COROLLARIO 5.4.** Sia  $n \geq 1$  un numero intero. Le radici  $n$ -esime dell'unità, cioè i numeri complessi  $z$  tali che  $z^n = 1$ , sono tutti e soli i numeri  $z_h = \cos(2h\pi/n) + i \sin(2h\pi/n)$ ,  $h \in \mathbb{Z}$ .

Si osservi che se  $h$  e  $h'$  sono due numeri interi, si ha  $z_h = z_{h'}$  se e solo se  $\cos(2h\pi/n) = \cos(2h'\pi/n)$  e  $\sin(2h\pi/n) = \sin(2h'\pi/n)$ , cioè se e solo se

$$\frac{2h\pi}{n} = \frac{2h'\pi}{n} + 2k\pi$$

per qualche numero intero  $k$ , vale a dire se e solo se  $h - h' = nk$  per qualche  $k \in \mathbb{Z}$ . Quindi  $z_h = z_{h'}$  se e solo se  $h$  e  $h'$  differiscono per un multiplo intero di  $n$ . Se ne ricava che le radici  $n$ -esime distinte dell'unità sono esattamente  $n$ . La loro posizione nel piano di Argand-Gauss viene descritta dalla proposizione seguente:

**PROPOSIZIONE 5.5.** Sia  $n \geq 1$  un numero intero fissato. Le radici  $n$ -esime dell'unità sono rappresentate nel piano di Argand-Gauss dai vertici del poligono regolare di  $n$  lati inscritto nella circonferenza di centro l'origine e raggio 1 e avente uno dei suoi vertici nel punto  $z = 1$ .

### Esercizi svolti

**5.1.** Si scrivano in forma trigonometrica i numeri complessi  $i$ ,  $-i$ ,  $1-i$ ,  $1-i\sqrt{3}$ ,  $5\alpha$ , dove  $\alpha$  è un numero reale negativo.

*Soluzione.* Rappresentando  $i$  nel piano di Argand-Gauss (è il punto  $(0, 1)$  del piano cartesiano) si osserva immediatamente che l'argomento di  $i$  è  $\frac{\pi}{2}$  e che il suo modulo è 1. Quindi  $i = 1 \cdot \left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}\right) = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$ .

Analogamente si vede subito che l'argomento di  $-i$  è  $\frac{3\pi}{2}$  e che il suo modulo è 1. Quindi

$$-i = 1 \cdot \left(\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}\right) = \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}.$$

Per quanto riguarda  $1-i$  si ha invece che l'argomento è  $-\frac{\pi}{4}$  e il modulo è  $\sqrt{1^2 + 1^2} = \sqrt{2}$ . Pertanto

$$1-i = \sqrt{2} \left(\cos \left(-\frac{\pi}{4}\right) + i \sin \left(-\frac{\pi}{4}\right)\right),$$

e in modo analogo

$$1-i\sqrt{3} = 2 \left(\cos \left(-\frac{\pi}{3}\right) + i \sin \left(-\frac{\pi}{3}\right)\right) \quad \text{e} \quad 5 = 5(\cos 0 + i \sin 0).$$

Infine se  $\alpha$  è un numero reale negativo, il modulo di  $\alpha$  è  $-\alpha$  e il suo argomento è  $\pi$ . Quindi  $\alpha = (-\alpha)(\cos \pi + i \sin \pi)$  è la scrittura in forma trigonometrica richiesta. Ovviamente la risposta  $\alpha = \alpha(\cos 0 + i \sin 0)$  è errata se  $\alpha$  è un numero reale negativo.  $\square$

## Altri esercizi

- 5.2. Si dimostri che se  $z, z' \in \mathbb{C}$  e  $zz' = 0$ , allora  $z = 0$  oppure  $z' = 0$ .
- 5.3. Si scrivano nella forma  $a + ib$ , con  $a$  e  $b$  numeri reali, i numeri
- (a)  $(1 + 2i) + (3 - 4i)$ ; (b)  $(1 + 2i) - (-3 - 4i)$ ; (c)  $(1 + 2i)(3 - 4i)$ ;  
 (d)  $(1 + 2i)^2$ ; (e)  $\frac{1 + 2i}{1 - 2i}$ ; (f)  $\frac{1 + 2i}{1 + i} + \frac{1 - 2i}{1 - i}$ ;  
 (g)  $\frac{1 + 2i}{1 - i} \cdot \frac{1 - 2i}{1 + i}$ ; (h)  $\frac{1}{1 + 2i}$ ; (i)  $\frac{(1 + i)(1 - 2i)}{1 + 3i}$ .
- 5.4. Rappresentare nel piano di Argand-Gauss i numeri complessi  $1 + 2i$ ,  $3 - 4i$ ,  $-3 - 4i$ ,  $1 - 2i$ ,  $1 + i$ ,  $1 - i$ .
- 5.5. Rappresentare nel piano di Argand-Gauss l'insieme dei numeri complessi  $z$  tali che  $|z^2 - 1| < 1$ .
- 5.6. Si calcolino il modulo e l'argomento dei numeri complessi  $1 + i\sqrt{3}$ ,  $2 - 2i$ ,  $-2 - 2i$ ,  $(1 + i\sqrt{3})^2$ ,  $\frac{1 + i\sqrt{3}}{1 - i\sqrt{3}}$ .
- 5.7. Si scrivano in forma trigonometrica i numeri complessi dell'Esercizio 5.6.
- 5.8. Siano  $a, b, \varphi \in \mathbb{R}$  e  $\varphi \geq 0$ .
- (a) Se il numero  $z = a + ib$  è rappresentato nel piano di Argand-Gauss dal punto  $P$  di coordinate  $(a, b)$ , quale punto rappresenta il numero  $iz$ ?
- (b) Dato un numero complesso  $z = \rho(\cos \varphi + i \sin \varphi)$  in forma trigonometrica, si scriva in forma trigonometrica il numero  $iz$ .
- 5.9. Se  $a, b \in \mathbb{R}$  e  $z = a + ib \in \mathbb{C}$ , il complesso coniugato di  $z$  è il numero complesso  $\bar{z} = a - ib$ . Come si scrive in forma trigonometrica il complesso coniugato del numero complesso  $\rho(\cos \varphi + i \sin \varphi)$ ?
- 5.10. Se  $z = \rho(\cos \varphi + i \sin \varphi) \neq 0$  è un numero complesso in forma trigonometrica, come si scrive in forma trigonometrica il suo inverso  $1/z$ ?
- 5.11. Siano  $z = \rho(\cos \varphi + i \sin \varphi)$  e  $z' = \rho'(\cos \varphi' + i \sin \varphi') \neq 0$  due numeri complessi scritti in forma trigonometrica. Si scriva, sempre in forma trigonometrica, il numero  $z/z'$ .
- 5.12. Si scrivano tutte le radici ottave dell'unità.
- 5.13. Si calcolino le soluzioni dell'equazione  $x^{12} - 1 = 0$  in  $\mathbb{C}$ .
- 5.14. Si calcolino le soluzioni dell'equazione  $x^4 + i = 0$  in  $\mathbb{C}$ .
- 5.15. Si calcolino le soluzioni dell'equazione  $x^3 - 2i = 0$  in  $\mathbb{C}$ .

5.16. Siano  $a$  e  $b$  numeri reali e  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  un polinomio i cui coefficienti  $a_0, a_1, \dots, a_n$  sono numeri reali. Si dimostri che se  $z = a + ib \in \mathbb{C}$  è una radice del polinomio, cioè se  $f(z) = 0$ , allora anche il complesso coniugato  $\bar{z} = a - ib$  di  $z$  è una radice del polinomio.

[Suggerimento: dimostrare nell'ordine

- (1) che per ogni  $z, z' \in \mathbb{C}$  si ha  $\overline{z + z'} = \bar{z} + \bar{z'}$  e  $\overline{zz'} = \bar{z} \cdot \bar{z'}$ ;  
 (2) che  $\overline{(z^n)} = (\bar{z})^n$  per ogni  $n \in \mathbb{N}$ ;  
 (3) che  $f(\bar{z}) = \overline{f(z)}$ .]

5.17. (a) Si calcolino le soluzioni dell'equazione  $z^4 + 1 = 0$  in  $\mathbb{C}$ .  
 (b) Si rappresentino nel piano di Argand-Gauss tali soluzioni e si mostri che stanno sui vertici di un quadrato inscritto nella circonferenza di centro l'origine e raggio 1.

5.18. Si dimostri la proposizione seguente:

Se  $n \geq 3$  è un numero intero fissato, l'equazione  $z^n = -1$  ha esattamente  $n$  soluzioni distinte in  $\mathbb{C}$ . Esse sono rappresentate nel piano di Argand-Gauss dai vertici di un poligono regolare di  $n$  lati inscritto nella circonferenza di centro l'origine e raggio 1. Tale poligono è simmetrico rispetto all'asse reale. Se  $n$  è dispari uno dei suoi vertici è nel punto  $z = -1$ .

## Capitolo 6. Matrici

Siano  $m, n \geq 1$  due numeri interi. Una matrice  $m \times n$  ad elementi reali è una tabella rettangolare

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

di  $mn$  numeri reali  $a_{11}, a_{12}, \dots, a_{mn}$  disposti in  $m$  righe ed  $n$  colonne. Spesso la matrice  $A$  viene indicata semplicemente con il simbolo  $(a_{ij})$ , in quanto questo permette di ridurre notevolmente le dimensioni delle formule.

Date due matrici  $m \times n$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

la loro somma è la matrice

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

Quindi la somma di due matrici  $m \times n$  è ancora una matrice  $m \times n$ , e nella matrice  $A + B$  l'elemento di posto  $(i, j)$ , vale a dire l'elemento di  $A + B$  che appare nella  $i$ -esima riga e nella  $j$ -esima colonna, è la somma dell'elemento  $a_{ij}$  di posto  $(i, j)$  in  $A$  e dell'elemento  $b_{ij}$  di posto  $(i, j)$  in  $B$ .

Siano ora  $m, n, p \geq 1$  tre numeri interi. Se

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

è una matrice  $m \times n$  e

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{pmatrix}$$

è una matrice  $n \times p$ , la matrice  $AB$  prodotto righe per colonne di  $A$  e di  $B$  è la matrice  $m \times p$

$$AB = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mp} \end{pmatrix},$$

dove per ogni  $i = 1, 2, \dots, m$  e ogni  $k = 1, 2, \dots, p$  si ha

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + a_{i3}b_{3k} + \dots + a_{in}b_{nk} = \sum_{j=1}^n a_{ij}b_{jk}.$$

Si noti che la somma di due matrici è definita solamente quando le due matrici hanno lo stesso numero di righe e lo stesso numero di colonne, mentre il prodotto

$AB$  di due matrici  $A$  e  $B$  è definito solo quando la prima matrice  $A$  ha tante colonne quante sono le righe della seconda matrice  $B$ .

ESEMPIO 1. Siano

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 2 & 3 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & -2 & 0 & -3 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}.$$

Si calcolino le matrici  $A + B$ ,  $A + C$ ,  $AB$ ,  $AC$ .

Si ha

$$A + B = \begin{pmatrix} 1+0 & 2+1 & -1+2 & 0+3 \\ 2-1 & 3-2 & 0+0 & -1-3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 1 & 3 \\ 1 & 1 & 0 & -4 \end{pmatrix}$$

e

$$AC = \begin{pmatrix} 1 \cdot 0 + 2 \cdot 0 + (-1) \cdot 1 + 0 \cdot (-1) & 1 \cdot 0 + 2 \cdot 1 + \dots & \dots \\ 2 \cdot 0 + 3 \cdot 0 + 0 \cdot 1 + (-1) \cdot (-1) & 2 \cdot 0 + 3 \cdot 1 + \dots & \dots \end{pmatrix} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix}.$$

Le matrici  $A + C$  e  $AB$  non sono invece definite.  $\square$

Dati un numero reale  $\lambda$  e una matrice  $m \times n$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

definiamo il loro prodotto (scalare)  $\lambda A$  ponendo

$$\lambda A = \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{m1} & \lambda a_{m2} & \dots & \lambda a_{mn} \end{pmatrix}.$$

Una matrice  $n \times n$  si dice anche una matrice quadrata di ordine  $n$ . In una matrice quadrata  $A = (a_{ij})$  gli elementi  $a_{ii}$ , cioè gli elementi per i quali l'indice di riga è uguale all'indice di colonna, si dice che stanno sulla diagonale principale.

Si potrebbe dimostrare che

- (1) se  $A, B, C$  sono matrici  $m \times n$ , allora

$$A + (B + C) = (A + B) + C \quad (\text{proprietà associativa dell'addizione})$$

e

$$A + B = B + A \quad (\text{proprietà commutativa dell'addizione});$$

- (2) se  $A$  è una matrice  $m \times n$  e se indichiamo con  $0$ , o con  $0_{m \times n}$  quando sarà necessario essere più precisi, la matrice  $m \times n$  avente tutti i suoi elementi uguali a zero, cioè

$$0 = \underbrace{\begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}}_{n \text{ colonne}} \left\} m \text{ righe}$$

allora  $A + 0 = 0 + A = A$ ;

- (3) se  $A = (a_{ij})$  è una matrice  $m \times n$  e  $-A$  è la matrice i cui elementi sono gli opposti degli elementi di  $A$ , cioè è la matrice definita da

$$-A = \begin{pmatrix} -a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & -a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m1} & -a_{m2} & \dots & -a_{mn} \end{pmatrix},$$

allora  $A + (-A) = (-A) + A = 0$ ;

- (4) se  $\lambda, \mu$  sono numeri reali e  $A, B$  sono matrici  $m \times n$ , allora

$$\begin{aligned} \lambda(\mu A) &= (\lambda\mu)A; \\ (\lambda + \mu)A &= \lambda A + \mu A; \\ \lambda(A + B) &= \lambda A + \lambda B; \\ 1A &= A; \end{aligned}$$

- (5) se  $A$  è una matrice  $m \times n$ ,  $B$  è una matrice  $n \times p$  e  $C$  è una matrice  $p \times q$ , allora  $A(BC) = (AB)C$  (proprietà associativa della moltiplicazione righe per colonne) (vedi esercizio 6.2);

- (6) se  $A, A'$  sono matrici  $m \times n$  e  $B, B'$  sono matrici  $n \times p$ , allora  $(A + A')B = AB + A'B$  e  $A(B + B') = AB + AB'$  (proprietà distributive);

- (7) se  $\lambda$  è un numero reale,  $A$  è una matrice  $m \times n$  e  $B$  è una matrice  $n \times p$ , allora  $(\lambda A)B = \lambda(AB) = A(\lambda B)$ ;
- (8) definiamo il simbolo  $\delta_{ij}$  ponendo  $\delta_{ij} = 1$  se  $i = j$ , e  $\delta_{ij} = 0$  se  $i \neq j$  (il simbolo  $\delta_{ij}$  è detto il simbolo di Kronecker). Per ogni numero intero positivo  $m$  indichiamo con  $I$  (o con  $I_{m \times m}$  quando sarà necessario essere più precisi) la matrice quadrata di ordine  $m$  definita da  $I = (\delta_{ij})$ , cioè la matrice avente tutti i suoi elementi uguali a zero eccetto quelli sulla diagonale principale che sono uguali a uno:

$$I_{m \times m} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}}_{m \text{ colonne}} \left\} m \text{ righe}$$

Se  $A$  è una matrice  $m \times n$  si ha  $I_{m \times m}A = AI_{n \times n} = A$  (esercizio 6.8).

Per ogni intero positivo  $p$  e ogni matrice quadrata  $A$  poniamo  $A^p = \underbrace{AA \dots A}_{p \text{ volte}}$ ,

cioè definiamo  $A^p$  come il prodotto righe per colonne di  $A$  per sé stessa  $p$  volte.

ESEMPIO 2. Sia  $A = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ . Dimostriamo per induzione su  $p$  che per

ogni  $p \geq 2$  si ha  $A^p = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix}$ . Per  $p = 2$  si ha

$$A^2 = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix}.$$

Supponiamo  $p > 2$  e che l'asserto sia vero per  $p-1$ , cioè che  $A^{p-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix}$ .

$$\text{Allora } A^p = A^{p-1}A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 1 \end{pmatrix}. \quad \square$$

Data infine una matrice  $m \times n$   $A = (a_{ij})$ , la matrice trasposta  $A^*$  di  $A$  è la matrice  $n \times m$  in cui l'elemento di posto  $(i, j)$  è l'elemento  $a_{ji}$  di posto  $(j, i)$  nella



matrice  $A$ , cioè è la matrice che si ottiene da  $A$  scambiando le righe e le colonne. Una matrice quadrata  $A = (a_{ij})$  si dice *simmetrica* se  $A^* = A$ , cioè se  $a_{ij} = a_{ji}$  per ogni  $i$  e ogni  $j$ .

ESEMPIO 3. Se  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ , allora  $A^* = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}$ . La matrice  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & -1 \\ 3 & -1 & 0 \end{pmatrix}$  è simmetrica, mentre la matrice  $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & -1 \\ 3 & -1 & 0 \end{pmatrix}$  non lo è.  $\square$

### Esercizi svolti

6.1. Siano  $A = \{a_1, a_2, \dots, a_m\}$  e  $B = \{b_1, b_2, \dots, b_n\}$  due insiemi con un numero finito di elementi. Una corrispondenza  $\varrho$  di  $A$  in  $B$  può essere descritta mediante la *matrice della corrispondenza*, che è la matrice  $m \times n$   $A_\varrho = (\varrho_{ij})$ , dove  $\varrho_{ij} = 1$  se  $(a_i, b_j) \in \varrho$ , e  $\varrho_{ij} = 0$  se  $(a_i, b_j) \notin \varrho$ . Se  $A = B = \{1, 2, 3, 4\}$  e

$$\varrho = \{(x, y) \mid x \in A, y \in B, x^2 = y\},$$

si scriva la matrice della corrispondenza  $\varrho$ .

Soluzione. La soluzione è evidentemente  $A_\varrho = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ .  $\square$

6.2. Si dimostri la proprietà associativa della moltiplicazione righe per colonne, cioè si dimostri che se  $A$  è una matrice  $m \times n$ ,  $B$  è una matrice  $n \times p$  e  $C$  è una matrice  $p \times q$ , allora  $A(BC) = (AB)C$ .

Soluzione. Si denoti con  $a_{ij}$  l'elemento di posto  $(i, j)$  nella matrice  $A$ , con  $b_{jk}$  l'elemento di posto  $(j, k)$  nella matrice  $B$ , e con  $c_{kl}$  l'elemento di posto  $(k, l)$  nella matrice  $C$ . Allora l'elemento di posto  $(j, \ell)$  nella matrice  $BC$  è  $\sum_k b_{jk} c_{k\ell}$ , e pertanto l'elemento di posto  $(i, \ell)$  nella matrice  $A(BC)$  è  $\sum_j a_{ij} (\sum_k b_{jk} c_{k\ell}) = \sum_{j,k} a_{ij} b_{jk} c_{k\ell}$ . Analogamente l'elemento di posto  $(i, k)$  nella matrice  $AB$  è  $\sum_j a_{ij} b_{jk}$ , e quindi l'elemento di posto  $(i, \ell)$  nella matrice  $(AB)C$  è  $\sum_k (\sum_j a_{ij} b_{jk}) c_{k\ell} = \sum_{j,k} a_{ij} b_{jk} c_{k\ell}$ . Quindi le matrici  $A(BC)$  e  $(AB)C$  hanno lo stesso elemento di posto  $(i, \ell)$ . Dato che questo accade per ogni  $i$  e ogni  $\ell$  se ne deduce che  $A(BC) = (AB)C$ .  $\square$

### Altri esercizi

6.3. Si eseguano le operazioni indicate:

$$(a) \begin{pmatrix} 0 & 2 & -2 \\ 0 & 3 & -3 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix};$$

$$(b) \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

6.4. Si eseguano le operazioni indicate:

$$(a) \begin{pmatrix} 0 & 2 & -2 \\ 0 & 3 & -3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

$$(b) \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & -2 \\ 0 & 3 & -3 \end{pmatrix};$$

$$(c) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

6.5. Siano  $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$  e  $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ . Si calcolino  $AB$  e  $BA$ .

[Si osservi che  $AB \neq BA$ .]

6.6. Si eseguano le operazioni indicate:

$$(a) 2 \begin{pmatrix} 1 & 2 \\ 15 & -1 \\ 0 & 2 \end{pmatrix};$$

$$(b) -7 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

$$(c) - \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix};$$

$$(d) 4 \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} - 6 \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 0 \end{pmatrix};$$

$$(e) \begin{pmatrix} 1 & 2 & 3 \\ -1 & -2 & -3 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$

$$(f) \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}^2 + 3 \begin{pmatrix} 15 & 15 \\ 0 & 0 \end{pmatrix}.$$

6.7. Si determinino quattro numeri reali  $x, y, z, w \in \mathbb{R}$  tali che

$$\begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

6.8. Si dimostri che se  $A$  è una matrice  $m \times n$  si ha  $I_{m \times m} A = A$  e  $A I_{n \times n} = A$ .

6.9. Due matrici  $A$  e  $B$  quadrate di ordine  $n$  si dicono *una l'inversa dell'altra* se  $AB = I_{n \times n}$ . (Si potrebbe dimostrare che  $AB = I_{n \times n}$  se e solo se  $BA = I_{n \times n}$ .) Si dimostri che le matrici quadrate di ordine 3

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 3 & 6 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

sono una l'inversa dell'altra.

6.10. Sia  $A$  la matrice  $\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ . Si dimostri che  $A^4 = -I$ .

6.11. Sia  $A$  la matrice  $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$ .

(a) Si dimostri che  $A^3 = A - A^2$ .

(b) Se ne deduca che  $A^{n+1} = A^{n-1} - A^n$  per ogni  $n \geq 2$ .

6.12. Si dimostri che se  $A$  è una matrice  $m \times n$ ,  $B$  è una matrice  $n \times p$  e  $*$  denota la matrice trasposta, allora  $(AB)^* = B^* A^*$ .

6.13. Sia  $M_2(\mathbb{R})$  l'insieme delle matrici quadrate di ordine  $n$ . Si consideri l'applicazione  $\varphi: \mathbb{C} \rightarrow M_2(\mathbb{R})$  definita, per ogni  $a, b \in \mathbb{R}$ , da

$$\varphi(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Si dimostri che

(a) l'applicazione  $\varphi$  è iniettiva;

(b) per ogni  $a, b, a', b' \in \mathbb{R}$  si ha  $\varphi((a + ib) + (a' + ib')) = \varphi(a + ib) + \varphi(a' + ib')$  e  $\varphi((a + ib)(a' + ib')) = \varphi(a + ib)\varphi(a' + ib')$ .

## PARTE SECONDA INSIEMI E RELAZIONI

### Capitolo 7. Equivalenze e partizioni

Come abbiamo visto nel capitolo 2, una *corrispondenza* di un insieme  $A$  in un insieme  $B$  è un sottoinsieme del prodotto cartesiano  $A \times B$ . I sottoinsiemi di  $A \times A$ , ossia le corrispondenze di  $A$  in  $A$ , si chiamano anche *relazioni su  $A$*  (o *in  $A$* ). Se  $\varrho$  è una relazione su  $A$ , ossia  $\varrho \subseteq A \times A$ , e  $a, a' \in A$ , invece di scrivere  $(a, a') \in \varrho$  si suole scrivere  $a \varrho a'$ .

ESEMPIO 1. Sia  $A = \mathbb{N}$ . Se consideriamo

$$\delta = \{ (x, y) \mid x, y \in \mathbb{N}, x = 2y \},$$

allora  $\delta \subseteq \mathbb{N} \times \mathbb{N}$  e quindi  $\delta$  è una relazione su  $\mathbb{N}$ . Invece di scrivere  $(x, y) \in \delta$  si preferisce scrivere  $x \delta y$ ; quindi, se  $x, y \in \mathbb{N}$ , scrivere  $x \delta y$  equivale a scrivere che  $x = 2y$ , cioè che  $x$  è il doppio di  $y$ . Avremmo quindi potuto definire questa relazione  $\delta$  non descrivendola come sottoinsieme di  $\mathbb{N} \times \mathbb{N}$ , ma dicendo "sull'insieme  $A = \mathbb{N}$  consideriamo la relazione  $\delta$  definita ponendo, per ogni  $x, y \in \mathbb{N}$ ,  $x \delta y$  se  $x = 2y$ ". □

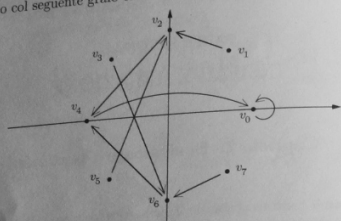
ESEMPIO 2. Sull'insieme  $\mathbb{C}$  consideriamo la relazione  $\mu$  definita ponendo, per ogni  $z, z' \in \mathbb{C}$ ,  $z \mu z'$  se  $|z| = |z'|$ , cioè se  $z$  e  $z'$  hanno lo stesso modulo. Vedendo la relazione  $\mu$  in modo più formale come sottoinsieme di  $\mathbb{C} \times \mathbb{C}$  si ha quindi che

$$\mu = \{ (z, z') \mid z, z' \in \mathbb{C}, |z| = |z'| \}. \quad \square$$

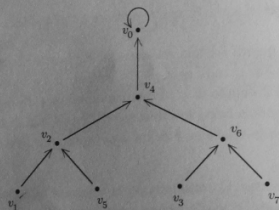
Data una relazione  $\varrho$  su un insieme  $A$  può essere molto utile, soprattutto quando l'insieme  $A$  è finito, cioè quando  $A$  ha un numero finito di elementi, rappresentare la relazione mediante un *grafo orientato*. In tal caso gli elementi dell'insieme  $A$  vengono rappresentati come punti di un piano (detti *vertici* del

grafo), e se  $a$  e  $b$  sono due elementi di  $A$  tali che  $a \varrho b$  si disegna un arco orientato di curva (detto il lato orientato da  $a$  a  $b$ ) dal punto che rappresenta  $a$  al punto che rappresenta  $b$ .

ESEMPIO 3. Sia  $A$  l'insieme delle 8 radici ottave dell'unità. Definiamo una relazione  $\varrho$  su  $A$  ponendo, per ogni  $a, b \in A$ ,  $a \varrho b$  se  $a^2 = b$ . Allora  $A$  può essere rappresentato col seguente grafo orientato.



Qui gli elementi di  $A$ , che sono numeri complessi, sono stati rappresentati nel piano di Argand-Gauss come abbiamo imparato a fare nel capitolo 5. Ma questo non era strettamente necessario. Ad esempio la relazione  $\varrho$  su  $A$  avrebbe potuto essere rappresentata nel modo seguente.



Si noti in questo esempio il lato da  $v_0$  a  $v_0$ ; un lato da un vertice  $v$  in sé stesso si dice un *cappio*. □

Una relazione  $\varrho$  su un insieme  $A$  si dice

- *riflessiva* se per ogni  $a \in A$  si ha  $a \varrho a$ ;
- *simmetrica* se per ogni  $a, b \in A$  da  $a \varrho b$  segue  $b \varrho a$ ;
- *transitiva* se per ogni  $a, b, c \in A$  da  $a \varrho b$  e  $b \varrho c$  segue  $a \varrho c$ .

Un'equivalenza (o *relazione di equivalenza*) su  $A$  è una relazione riflessiva, simmetrica e transitiva su  $A$ . Le equivalenze vengono indicate in genere con simboli come  $\sim, \equiv, \approx, \simeq, \cong$ , eccetera.

ESEMPIO 4. Fissiamo un sistema di coordinate cartesiane ortogonali su un piano  $\pi$  e denotiamo con  $A$  l'insieme dei punti di  $\pi$ . Definiamo una relazione  $\sim$  su  $A$  ponendo, se  $P, Q \in A$ ,  $P \sim Q$  se  $P$  e  $Q$  hanno la stessa ordinata. Allora:

- la relazione  $\sim$  è riflessiva, perché per ogni  $P \in A$  i punti  $P$  e  $P$  hanno la stessa ordinata;
- la relazione  $\sim$  è simmetrica, perché se  $P, Q \in A$  e i punti  $P$  e  $Q$  hanno la stessa ordinata, allora anche  $Q$  e  $P$  hanno la stessa ordinata, cioè  $Q \sim P$ ;
- la relazione  $\sim$  è transitiva; infatti, se  $P, Q, R \in A$ ,  $P \sim Q$  e  $Q \sim R$ , allora hanno la stessa ordinata sia i punti  $P$  e  $Q$  che i punti  $Q$  ed  $R$ . Pertanto  $P$  ed  $R$  hanno la stessa ordinata, cioè  $P \sim R$ .

Quindi  $\sim$  è una relazione di equivalenza sull'insieme  $A$ . □

ESEMPIO 5. Nell'esempio 1 era stata definita una relazione  $\delta$  sull'insieme  $\mathbb{N}$  ponendo, per ogni  $x, y \in \mathbb{N}$ ,  $x \delta y$  se  $x = 2y$ . La relazione  $\delta$  non è riflessiva (perché non è vero che  $x = 2x$  per ogni  $x \in \mathbb{N}$ ), non è simmetrica (perché non è vero che, per ogni  $x, y \in \mathbb{N}$ , se  $x = 2y$  allora  $y = 2x$ ) e non è transitiva (perché da  $x = 2y$  e  $y = 2z$  non segue in generale che  $x = 2z$ ). □

ESEMPIO 6. Nell'esempio 2 abbiamo incontrato la relazione  $\mu$  su  $\mathbb{C}$  definita ponendo, per ogni  $z, z' \in \mathbb{C}$ ,  $z \mu z'$  se  $|z| = |z'|$ . Allora

- la relazione  $\mu$  è riflessiva, perché per ogni  $z \in \mathbb{C}$  si ha  $|z| = |z|$ , cioè  $z \mu z$ ;
- la relazione  $\mu$  è simmetrica, perché se  $z, z' \in \mathbb{C}$  e  $z \mu z'$ , allora  $|z| = |z'|$ , da cui  $|z'| = |z|$ , ossia  $z' \mu z$ ;
- la relazione  $\mu$  è transitiva; infatti, se  $z, z', z'' \in \mathbb{C}$ ,  $z \mu z'$  e  $z' \mu z''$ , allora  $|z| = |z'|$  e  $|z'| = |z''|$ , da cui  $|z| = |z''|$ , cioè  $z \mu z''$ .

Quindi  $\mu$  è una relazione di equivalenza sull'insieme  $\mathbb{C}$ . □

ESEMPIO 7. Sia  $A$  un insieme qualunque. La *relazione di uguaglianza* = sull'insieme  $A$ , definita da  $a = b$  se  $a$  e  $b$  coincidono, è ovviamente riflessiva ( $a = a$  per ogni  $a \in A$ ), simmetrica (se  $a = b$  allora  $b = a$ ) e transitiva (se  $a = b$  e  $b = c$  allora  $a = c$ ). Quindi è una relazione di equivalenza sull'insieme  $A$ . □

ESEMPIO 8. Sia  $f: A \rightarrow B$  un'applicazione. Definiamo una relazione  $\sim_f$  su  $A$  ponendo, per ogni  $x, y \in A$ ,  $x \sim_f y$  se  $f(x) = f(y)$ . Allora:

- la relazione  $\sim_f$  è riflessiva, perché per ogni  $x \in A$  si ha  $f(x) = f(x)$  cioè  $x \sim_f x$ ;
- la relazione  $\sim_f$  è simmetrica, perché se  $x, y \in A$  e  $x \sim_f y$ , allora  $f(x) = f(y)$ , da cui  $f(y) = f(x)$ , cioè  $y \sim_f x$ ;

la relazione  $\sim_f$  è transitiva; infatti se  $x, y, z \in A$ ,  $x \sim_f y$  e  $y \sim_f z$ , allora  $f(x) = f(y)$  e  $f(y) = f(z)$ , da cui  $f(x) = f(z)$ , cioè  $x \sim_f z$ .  
Quindi  $\sim_f$  è un'equivalenza sull'insieme  $A$ , detta l'*equivalenza associata ad  $f$* .  $\square$

Sia  $A$  un insieme e  $\sim$  un'equivalenza su  $A$ . Se  $a \in A$ , la *classe di equivalenza di  $a$*  è l'insieme  $[a]_\sim = \{x \mid x \in A, x \sim a\}$ . (Quando sarà chiaro di quale equivalenza si sta parlando, scriveremo semplicemente  $[a]$  in luogo di  $[a]_\sim$ .) Definiamo poi  $A/\sim = \{[a]_\sim \mid a \in A\}$ , detto l'*insieme quoziente di  $A$  modulo  $\sim$* . È allora possibile considerare l'applicazione  $\pi: A \rightarrow A/\sim$  definita da  $\pi(a) = [a]_\sim$  per ogni  $a \in A$ . L'applicazione  $\pi$  si dice l'*applicazione canonica* (o *proiezione canonica*) di  $A$  su  $A/\sim$ .

ESEMPIO 9. Nell'esempio 2 abbiamo definito una relazione  $\mu$  su  $\mathbb{C}$  ponendo, per ogni  $z, z' \in \mathbb{C}$ ,  $z \mu z'$  se  $|z| = |z'|$ , cioè se  $z$  e  $z'$  hanno lo stesso modulo. Successivamente abbiamo osservato che  $\mu$  è una relazione di equivalenza su  $\mathbb{C}$  (esemplivamente abbiamo osservato che  $\mu$  è una relazione di equivalenza di  $z$  è più 6). Dato un qualunque numero complesso  $z$ , la classe di equivalenza di  $z$  è  $[z]_\mu = \{x \mid x \in \mathbb{C}, |x| = |z|\}$ . Quindi se per ogni numero reale  $\alpha \geq 0$  indichiamo con  $C_\alpha$  l'insieme di tutti i numeri complessi di modulo  $\alpha$ , cioè dei numeri complessi che nel piano di Argand-Gauss stanno sulla circonferenza di centro l'origine e raggio  $\alpha$ , si ha  $[z]_\mu = C_\alpha$ , dove  $\alpha = |z|$ . Inoltre l'insieme quoziente  $\mathbb{C}/\mu$  è  $\{C_\alpha \mid \alpha \in \mathbb{R}, \alpha \geq 0\}$  e la proiezione canonica  $\pi: \mathbb{C} \rightarrow \mathbb{C}/\mu$  è definita da  $\pi(z) = C_{|z|}$  per ogni  $z \in \mathbb{C}$ , cioè è l'applicazione che associa ad ogni  $z \in \mathbb{C}$  l'insieme di tutti i numeri complessi aventi il modulo uguale al modulo di  $z$ .  $\square$

ESEMPIO 10. Nell'esempio 7 abbiamo fatto osservare che la relazione di uguaglianza su un insieme  $A$  è una relazione di equivalenza su  $A$ . In questo caso si ha che per ogni  $a \in A$  la classe di equivalenza di  $a$  è  $[a] = \{x \in A \mid x = a\} = \{a\}$ . Quindi l'insieme quoziente  $A/\sim$  è  $\{\{a\} \mid a \in A\}$  e la proiezione canonica  $\pi: A \rightarrow A/\sim$  è definita da  $\pi(a) = \{a\}$  per ogni  $a \in A$ .  $\square$

Se  $A$  è un insieme non vuoto, una *partizione*  $\mathcal{F}$  di  $A$  è una famiglia (cioè un insieme)  $\mathcal{F}$  di sottoinsiemi di  $A$  tali che:

- ogni  $X \in \mathcal{F}$  è non vuoto;
- $\bigcup_{X \in \mathcal{F}} X = A$ ;
- se  $X, Y \in \mathcal{F}$  e  $X \neq Y$ , allora  $X \cap Y = \emptyset$ .

ESEMPIO 11. Sia  $A = \mathbb{C}$  l'insieme dei numeri complessi. Per ogni numero reale  $\alpha \geq 0$  poniamo  $C_\alpha = \{z \mid z \in \mathbb{C}, |z| = \alpha\}$ . Sia  $\mathcal{F} = \{C_\alpha \mid \alpha \in \mathbb{R}, \alpha \geq 0\}$ . Mostriamo che  $\mathcal{F}$  è una partizione di  $\mathbb{C}$ .

Si osservi intanto che gli elementi  $C_\alpha$  di  $\mathcal{F}$  sono sottoinsiemi non vuoti di  $\mathbb{C}$  per ogni  $\alpha \geq 0$ . Questo dimostra che vale la (a) della definizione di partizione.

Inoltre

$$\bigcup_{X \in \mathcal{F}} X = \bigcup_{\substack{\alpha \in \mathbb{R} \\ \alpha \geq 0}} C_\alpha = \mathbb{C},$$

e quindi anche la (b) vale. Infine se  $C_\alpha, C_\beta \in \mathcal{F}$  e  $C_\alpha \neq C_\beta$ , allora  $\alpha \neq \beta$ , da cui  $C_\alpha \cap C_\beta = \emptyset$  (perché non ci può essere un numero complesso il cui modulo sia contemporaneamente uguale sia ad  $\alpha$  che a  $\beta$ ). Questo prova anche la (c). Quindi  $\mathcal{F}$  è una partizione di  $\mathbb{C}$ .  $\square$

ESEMPIO 12. Sia  $A = \mathbb{Z} \times \mathbb{Z}$  l'insieme delle coppie di numeri interi. Per ogni numero intero  $z$  poniamo  $X_z = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x + y = z\}$ . Mostriamo che  $\mathcal{F} = \{X_z \mid z \in \mathbb{Z}\}$  è una partizione di  $\mathbb{Z} \times \mathbb{Z}$ .

Gli elementi  $X_z$  di  $\mathcal{F}$  sono sottoinsiemi non vuoti di  $\mathbb{Z} \times \mathbb{Z}$ , perché ad esempio  $(z, 0) \in X_z$ . Questo mostra che vale la (a) della definizione di partizione. Inoltre

$$\bigcup_{X \in \mathcal{F}} X = \bigcup_{z \in \mathbb{Z}} X_z = \mathbb{Z} \times \mathbb{Z};$$

quindi anche la (b) vale. Infine se  $z, z' \in \mathbb{Z}$  e  $X_z \neq X_{z'}$ , allora  $z \neq z'$ , da cui  $X_z \cap X_{z'} = \emptyset$  (perché non ci può essere una coppia  $(x, y)$  di interi la cui somma sia contemporaneamente sia  $z$  che  $z'$ ). Quindi  $\mathcal{F}$  è una partizione di  $\mathbb{Z} \times \mathbb{Z}$ .  $\square$

ESEMPIO 13. Sia  $\mathbb{R}^+$  l'insieme dei numeri reali positivi e poniamo  $A = \mathbb{R}^+ \times \mathbb{R}^+$ . Per ogni numero reale  $a > 0$  poniamo

$$X_a = \{(x, y) \in \mathbb{R}^+ \times \mathbb{R}^+ \mid y = ax^2\}.$$

Mostriamo che  $\mathcal{F} = \{X_a \mid a \in \mathbb{R}^+\}$  è una partizione di  $\mathbb{R}^+ \times \mathbb{R}^+$ .

Gli elementi  $X_a$  di  $\mathcal{F}$  sono insiemi non vuoti (ad esempio per ogni  $a > 0$  si ha che  $(1, a) \in X_a$ ). Poi

$$\bigcup_{X \in \mathcal{F}} X = \bigcup_{a \in \mathbb{R}^+} X_a = \mathbb{R}^+ \times \mathbb{R}^+,$$

perché per ogni  $(x, y) \in \mathbb{R}^+ \times \mathbb{R}^+$  si ha che  $(x, y) \in X_a$  dove  $a = \frac{y}{x^2}$ . Infine se  $a, b \in \mathbb{R}^+$  e  $X_a \neq X_b$ , allora  $a \neq b$ , da cui  $X_a \cap X_b = \emptyset$  (perché se  $(x, y) \in X_a \cap X_b$ , allora  $y = ax^2$  e  $y = bx^2$ , da cui  $ax^2 = bx^2$ , ed essendo  $x \neq 0$  si ricava che  $a = b$ , contraddizione). Pertanto  $\mathcal{F}$  è una partizione di  $\mathbb{R}^+ \times \mathbb{R}^+$ .  $\square$

TEOREMA 7.1. Sia  $A$  un insieme non vuoto.

- Se  $\sim$  è un'equivalenza su  $A$ , allora l'insieme quoziente  $A/\sim$  è una partizione di  $A$ .
- Se  $\mathcal{F}$  è una partizione di  $A$ , allora la relazione  $\sim_{\mathcal{F}}$  su  $A$  definita ponendo, per ogni  $a, b \in A$ ,  $a \sim_{\mathcal{F}} b$  se esiste  $X \in \mathcal{F}$  tale che  $a \in X$  e  $b \in X$ , è un'equivalenza su  $A$ .

Dimostriamo (esercizio 7.19 nelle appendici) che facendo corrispondere ad ogni equivalenza  $\sim$  su  $A$  la partizione  $A/\sim$ , e ad ogni partizione  $\mathcal{F}$  su  $A$  l'equivalenza  $\sim_{\mathcal{F}}$  su  $A$  si ottiene una biiezione tra l'insieme delle equivalenze su  $A$  e l'insieme delle partizioni di  $A$ . Si noti come è definita l'equivalenza  $\sim_{\mathcal{F}}$  associata a  $\mathcal{F}$ : due elementi  $a, b \in A$  sono equivalenti nella relazione  $\sim_{\mathcal{F}}$  se e solo se esiste un elemento  $X$  della partizione che li contiene entrambi, cioè se e solo se stanno nello stesso elemento della partizione.

**TEOREMA 7.2.** (TEOREMA FONDAMENTALE DI OMOMORFISMO PER GLI INSIEMI). Siano  $A, B$  insiemi ed  $f: A \rightarrow B$  un'applicazione. Se  $\sim_f$  è l'equivalenza su  $A$  associata ad  $f$  (definita, per ogni  $x, y \in A$ , da  $x \sim_f y$  se  $f(x) = f(y)$ ) e  $\pi: A \rightarrow A/\sim_f$  denota la proiezione canonica, allora:

- (a) esiste un'unica applicazione  $\tilde{f}: A/\sim_f \rightarrow B$  che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \searrow & & \nearrow \tilde{f} \\ A/\sim_f & & \end{array}$$

cioè tale che  $\tilde{f} \circ \pi = f$ ;

- (b) l'applicazione  $\tilde{f}$  è iniettiva;  
(c) l'applicazione  $\tilde{f}$  è biiettiva se e solo se  $f$  è suriettiva.

### Esercizi svolti

**7.1.** Si dimostri che se  $\sim$  è un'equivalenza su  $A$  e  $a, b \in A$ , allora:

- (a)  $[a]_{\sim} = [b]_{\sim}$  se e solo se  $a \sim b$ ;  
(b)  $[a]_{\sim} \neq [b]_{\sim}$  se e solo se  $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ .

**Soluzione.** (a) Si osservi che dalla riflessività di  $\sim$ , cioè dal fatto che  $a \sim a$ , segue che  $a \in [a]_{\sim}$ . Quindi se  $[a]_{\sim} = [b]_{\sim}$ , si ha anche che  $a \in [b]_{\sim}$ , e quindi  $a \sim b$ .

Viceversa supponiamo che  $a \sim b$  e dimostriamo che  $[a]_{\sim} = [b]_{\sim}$  verificando la doppia inclusione. Se  $x \in [a]_{\sim}$ , allora  $x \sim a$ . Da questo, da  $a \sim b$  e dalla transitività di  $\sim$ , segue che  $x \sim b$ . Quindi  $[a]_{\sim} \subseteq [b]_{\sim}$ .

Se invece  $x \in [b]_{\sim}$ , allora  $x \sim b$ . Da  $a \sim b$  e dalla simmetria di  $\sim$  si ha che  $b \sim a$ . Da  $x \sim b$  e  $b \sim a$  segue per la transitività che  $x \sim a$ , cioè  $x \in [a]_{\sim}$ . Questo dimostra che  $[b]_{\sim} \subseteq [a]_{\sim}$ . Pertanto  $[a]_{\sim} = [b]_{\sim}$ .

- (b) Dimostriamo che  $[a]_{\sim} = [b]_{\sim}$  se e solo se  $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset$ .

Abbiamo fatto vedere dimostrando la parte (a) che si ha  $a \in [a]_{\sim}$ , e quindi  $[a]_{\sim} \neq \emptyset$ . Pertanto se  $[a]_{\sim} = [b]_{\sim}$  si ha  $[a]_{\sim} \cap [b]_{\sim} = [a]_{\sim} \neq \emptyset$ .

Viceversa se  $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset$ , sia  $c \in [a]_{\sim} \cap [b]_{\sim}$ . Allora  $c \in [a]_{\sim}$  e  $c \in [b]_{\sim}$ , e quindi  $c \sim a$  e  $c \sim b$ . Dalla simmetria di  $\sim$  segue che  $a \sim c$ , e da questa e da  $c \sim b$  segue che  $a \sim b$  per la transitività. Per quanto visto in (a) si conclude pertanto che  $[a]_{\sim} = [b]_{\sim}$ .  $\square$

**7.2.** Sia  $f: A \rightarrow B$  un'applicazione e  $\sim_f$  la relazione di equivalenza su  $A$  associata ad  $f$  (esempio 8). Si dimostri che  $f$  è iniettiva se e solo se  $\sim_f$  coincide con la relazione di uguaglianza  $=$ .

**Soluzione.** Supponiamo che  $f: A \rightarrow B$  sia un'applicazione iniettiva. Per dimostrare che le due equivalenze  $\sim_f$  e  $=$  coincidono si deve provare che per ogni  $a, a' \in A$  si ha  $a \sim_f a'$  se e solo se  $a = a'$ . Se  $a \sim_f a'$ , allora  $f(a) = f(a')$ , da cui, per l'injectività di  $f$ ,  $a = a'$ . Viceversa se  $a = a'$ , allora dalla riflessività di  $\sim_f$  si ha  $a \sim_f a$ , cioè  $a \sim_f a'$ . Questo dimostra che le due relazioni  $\sim_f$  e  $=$  coincidono.

Supponiamo ora invece che  $\sim_f$  coincida con la relazione di uguaglianza  $=$  e dimostriamo che  $f$  è iniettiva. Se  $a, a' \in A$  e  $f(a) = f(a')$ , allora per come è definita  $\sim_f$  si ha  $a \sim_f a'$ ; ma  $\sim_f$  coincide con  $=$ , e quindi  $a = a'$ . Pertanto l'applicazione  $f$  è iniettiva.  $\square$

**7.3.** Siano  $A, B$  insiemi non vuoti. Nel prodotto cartesiano  $A \times B$  si definisca una relazione di equivalenza  $\sim$  ponendo, per ogni  $(a, b), (a', b') \in A \times B$ ,  $(a, b) \sim (a', b')$  se  $b = b'$ . Cos'è l'insieme quoziente  $A \times B / \sim$ ?

**Soluzione.** Si ha

$$A \times B / \sim = \{ [(a, b)]_{\sim} \mid (a, b) \in A \times B \} = \{ [(a, b)]_{\sim} \mid a \in A, b \in B \}.$$

Ma per ogni  $a \in A, b \in B$

$$\begin{aligned} [(a, b)]_{\sim} &= \{ (x, y) \mid (x, y) \in A \times B, (x, y) \sim (a, b) \} = \\ &= \{ (x, y) \mid x \in A, y \in B, y = b \} = \\ &= \{ (x, b) \mid x \in A \} = A \times \{b\}. \end{aligned}$$

Quindi  $A \times B / \sim = \{ A \times \{b\} \mid b \in B \}$ .  $\square$

**7.4.** Sia  $\mathbb{C}$  l'insieme dei numeri complessi. Per ogni  $\alpha \in \mathbb{R}, \alpha \geq 0$  sia

$$C_{\alpha} = \{ z \mid z \in \mathbb{C}, |z| = \alpha \}$$

e si consideri la partizione

$$\mathcal{F} = \{ C_{\alpha} \mid \alpha \in \mathbb{R}, \alpha \geq 0 \}$$

di  $\mathbb{C}$  (vedi esempio 11). Come è definita l'equivalenza  $\sim_{\mathcal{F}}$  associata ad  $\mathcal{F}$ ?





*Soluzione.* Per definizione  $\sim_{\mathcal{F}}$  è definita ponendo, per ogni  $a, b \in \mathbb{C}$ ,  $a \sim_{\mathcal{F}} b$  se esiste  $X \in \mathcal{F}$  tale che  $a \in X$  e  $b \in X$ . In questo caso si ha pertanto  $a \sim_{\mathcal{F}} b$  se e solo se esiste  $\alpha \in \mathbb{R}$ ,  $\alpha \geq 0$  tale che  $a \in C_{\alpha}$  e  $b \in C_{\alpha}$ , ossia se e solo se esiste  $\alpha \in \mathbb{R}$ ,  $\alpha \geq 0$  tale che  $|a| = \alpha$  e  $|b| = \alpha$ . Questo può accadere se e solo se  $|a| = |b|$ . Abbiamo così dimostrato che  $\sim_{\mathcal{F}}$  è definita, per ogni  $a, b \in \mathbb{C}$ , da  $a \sim_{\mathcal{F}} b$  se e solo se  $|a| = |b|$ .  $\square$

7.5. Si consideri l'applicazione  $f: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $f(x) = x^2$  per ogni  $x \in \mathbb{R}$ .

- Come è definita l'equivalenza  $\sim_f$  su  $\mathbb{R}$  associata ad  $f$ ?
- Se  $a \in \mathbb{R}$ , cos'è la classe di equivalenza  $[a]_{\sim_f}$ ?
- Come è definita l'applicazione  $\tilde{f}: \mathbb{R}/\sim_f \rightarrow \mathbb{R}$  la cui esistenza è assicurata dal teorema fondamentale di omomorfismo per gli insiemi?
- L'applicazione  $\tilde{f}$  è iniettiva?
- L'applicazione  $\tilde{f}$  è biiettiva?

*Soluzione.* (a) Per ogni  $a, b \in \mathbb{R}$  si ha  $a \sim_f b$  se e solo se  $f(a) = f(b)$ , cioè se e solo se  $a^2 = b^2$ , ossia se e solo se  $|a| = |b|$ . Quindi  $\sim_f$  è definita, per ogni  $a, b \in \mathbb{R}$ , da  $a \sim_f b$  se e solo se  $|a| = |b|$ .

(b) Per ogni  $a \in \mathbb{R}$  si ha

$$[a]_{\sim_f} = \{x \in \mathbb{R}, x \sim_f a\} = \{x \in \mathbb{R}, |x| = |a|\} = \{a, -a\}.$$

(c) L'applicazione  $\tilde{f}: \mathbb{R}/\sim_f \rightarrow \mathbb{R}$  è definita da  $\tilde{f}([a]_{\sim_f}) = a^2$  per ogni  $a \in \mathbb{R}$ , cioè da  $\tilde{f}(\{a, -a\}) = a^2$  per ogni  $a \in \mathbb{R}$ .

(d) Sì, per il teorema fondamentale di omomorfismo per gli insiemi.

(e) L'applicazione  $\tilde{f}$  è biiettiva se e solo se  $f$  è suriettiva. Ma  $f$  non è suriettiva (ad esempio non esiste nessun  $a \in \mathbb{R}$  tale che  $f(a) = -1$ ). Quindi  $\tilde{f}$  non è biiettiva.  $\square$

### Altri esercizi

7.6. Siano  $A$  un insieme e  $\omega$  la relazione su  $A$  definita da  $a \omega b$  per ogni  $a, b \in A$ . Si dimostri che  $\omega$  è un'equivalenza su  $A$ .

[La relazione  $\omega$  è detta la *relazione banale* su  $A$ .]

7.7. Sia  $X$  un insieme,  $X^X$  l'insieme di tutte le applicazioni di  $X$  in  $X$ ,  $\sim$  la relazione su  $X^X$  definita, per ogni  $f, g \in X^X$ , da  $f \sim g$  se esiste una biiezione  $\sigma: X \rightarrow X$  tale che  $f = \sigma \circ g \circ \sigma^{-1}$ . Si dimostri che  $\sim$  è una relazione di equivalenza su  $X^X$ .

7.8. Siano  $A = \{-1, 0, 1, 2, 3\}$  e  $\varrho$  la relazione su  $A$  definita, per ogni  $a, b \in A$ , da  $a \varrho b$  se  $a^2 + b^2 = 1$ . La relazione  $\varrho$  è riflessiva? Simmetrica? Transitiva? È un'equivalenza? Si disegni il grafo orientato che rappresenta la relazione  $\varrho$ .

7.9. Sia  $f: A \rightarrow B$  un'applicazione e  $\sim_f$  la relazione di equivalenza su  $A$  associata ad  $f$ . Si dimostri che se  $A' \subseteq A$ , allora

$$f^{-1}(f(A')) = \bigcup_{a \in A'} [a]_{\sim_f}.$$

7.10. Siano  $A$  un insieme,  $f: \mathbb{Z} \rightarrow A$  un'applicazione e  $\sim_f$  la relazione di equivalenza su  $\mathbb{Z}$  associata ad  $f$ .

- Si dimostri che  $\sim_f$  è la relazione banale  $\omega$  su  $\mathbb{Z}$  (cioè la relazione definita da  $x \omega y$  per ogni coppia di numeri interi  $x, y$ ) se e solo se  $f$  è costante, cioè esiste  $a \in A$  tale che  $f(x) = a$  per ogni  $x \in \mathbb{Z}$ .
- Si dimostri che se  $\sim_f$  è la relazione di uguaglianza, allora l'insieme  $A$  è infinito, cioè ha infiniti elementi distinti.

7.11. Siano  $\mathbb{R}$  ed  $\mathbb{R}^*$  gli insiemi dei numeri reali e dei numeri reali non nulli rispettivamente. Si consideri l'applicazione  $\psi: \mathbb{R}^* \rightarrow \mathbb{R}$  definita da  $\psi(a) = \max\{a, a^{-1}\}$  per ogni  $a \in \mathbb{R}^*$ .

- Si dimostri che  $\psi^{-1}(y) \subseteq \{y, y^{-1}\}$  per ogni  $y \in \mathbb{R}$ ,  $y \neq 0$ .
- Si dimostri che  $|\psi^{-1}(y)| \leq 2$  per ogni  $y \in \mathbb{R}$ .
- Si determinino tutti gli  $y \in \mathbb{R}$  tali che  $|\psi^{-1}(y)| = 1$ .
- Se  $\sim_{\psi}$  è l'equivalenza su  $\mathbb{R}^*$  associata a  $\psi$ , si dimostri che per ogni  $a, b \in \mathbb{R}^*$  si ha  $a \sim_{\psi} b$  se e solo se  $(a-b)(ab-1) = 0$ .

7.12. Sia  $\mathbb{R}^+ = \{\varrho \mid \varrho \in \mathbb{R}, \varrho > 0\}$ . Si dimostri che se per ogni  $\varphi \in \mathbb{R}$  si pone  $X_{\varphi} = \{\varrho(\cos \varphi + i \sin \varphi) \mid \varrho \in \mathbb{R}^+\}$ , cioè se  $X_{\varphi}$  è l'insieme di tutti i numeri complessi non nulli aventi argomento  $\varphi$ , allora  $\mathcal{F} = \{X_{\varphi} \mid \varphi \in \mathbb{R}\}$  è una partizione di  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ .

7.13. Siano  $\mathcal{F}$  e  $\mathcal{G}$  due partizioni di un insieme  $A$ . Si definisca

$$\mathcal{F} \wedge \mathcal{G} = \{F \cap G \mid F \in \mathcal{F}, G \in \mathcal{G}, F \cap G \neq \emptyset\}.$$

Si dimostri che  $\mathcal{F} \wedge \mathcal{G}$  è una partizione dell'insieme  $A$ .

7.14. Siano  $f: A \rightarrow B$  un'applicazione ed  $\mathcal{F}$  una partizione di  $B$ . Sia  $\mathcal{G} = \{f^{-1}(X) \mid X \in \mathcal{F}, f^{-1}(X) \neq \emptyset\}$ . Si dimostri che  $\mathcal{G}$  è una partizione di  $A$ .

7.15. Siano  $A$  un insieme e  $\iota_A: A \rightarrow A$  l'applicazione identica di  $A$ . Qual è la relazione di equivalenza  $\sim_{\iota_A}$  associata a  $\iota_A$ ? Nella notazione dell'enunciato del teorema fondamentale di omomorfismo per gli insiemi come è definita l'applicazione  $\tilde{\iota}_A: A/\sim_{\iota_A} \rightarrow A$ ? L'applicazione  $\tilde{\iota}_A: A/\sim_{\iota_A} \rightarrow A$  è una biiezione?

## Capitolo 8. L'insieme delle classi resto

In tutto questo capitolo denoteremo con  $n$  un numero intero fissato.

Se  $a, b \in \mathbb{Z}$ , diciamo che  $a$  e  $b$  sono congrui modulo  $n$ , e scriviamo  $a \equiv b \pmod{n}$  oppure  $a \equiv_n b$ , se  $n$  divide  $a - b$ .

ESEMPIO 1. Si ha  $10 \equiv 100 \pmod{9}$  perché  $9 \mid (10 - 100) = -90$ ,  $-1 \equiv 1 \pmod{2}$  perché  $2 \mid (-1 - 1) = -2$ ,  $10 \not\equiv -1 \pmod{7}$  perché  $7$  non divide  $10 - (-1) = 11$ .  $\square$

ESEMPIO 2. Si faccia attenzione ai casi particolari  $n = 0$  e  $n = 1$ . Per  $n = 0$  si ha  $a \equiv b \pmod{0}$  se e solo se  $0$  divide  $a - b$ , cioè se e solo se  $a = b$ . Per  $n = 1$  si ha  $a \equiv b \pmod{1}$  per ogni  $a, b \in \mathbb{Z}$ . Quindi la congruenza modulo  $0$  coincide con la relazione di uguaglianza su  $\mathbb{Z}$ , mentre la congruenza modulo  $1$  coincide con la relazione banale  $\omega$ .  $\square$

ESEMPIO 3. Si ha  $a \equiv b \pmod{n}$  se e solo se  $a \equiv b \pmod{-n}$ . Quindi d'ora in poi potremo sempre supporre senza perdita di generalità che  $n \geq 0$ , e anzi, visto che la congruenza modulo  $0$  coincide con l'uguaglianza (esempio 2), potremo limitarci a considerare il caso  $n > 0$ .  $\square$

La congruenza  $\equiv_n$  è una relazione nell'insieme  $\mathbb{Z}$ , ed è facile verificare che si tratta di un'equivalenza in  $\mathbb{Z}$ , in quanto:

- (1) la relazione  $\equiv_n$  è riflessiva: infatti per ogni  $a \in \mathbb{Z}$ , si ha che  $n$  divide  $a - a = 0$ , e quindi  $a \equiv_n a$ .
- (2) la relazione  $\equiv_n$  è simmetrica: infatti se  $a, b \in \mathbb{Z}$  e  $a \equiv_n b$ , allora  $n$  divide  $a - b$ , e quindi  $n$  divide anche il suo opposto  $-(a - b) = b - a$ , ossia  $b \equiv_n a$ .
- (3) la relazione  $\equiv_n$  è transitiva: infatti se  $a, b, c \in \mathbb{Z}$ ,  $a \equiv_n b$  e  $b \equiv_n c$ , allora  $n$  divide sia  $a - b$  che  $b - c$ , e quindi  $n$  divide anche la loro somma  $(a - b) + (b - c) = a - c$ , ossia  $a \equiv_n c$ .

È quindi possibile costruire l'insieme quoziente

$$\mathbb{Z}/\equiv_n = \{[a] \mid a \in \mathbb{Z}\}$$

(qui abbiamo scritto  $[a]$  intendendo  $[a]_{\equiv_n}$ ; non c'è pericolo di confusione in quanto  $n$  è fissato e la congruenza  $\equiv_n$  è l'unica equivalenza di cui parleremo in questo

capitolo). Si noti che se  $a, b \in \mathbb{Z}$ , si ha  $[a] = [b]$  se e solo se  $a \equiv_n b$ . Si noti anche che

$$\begin{aligned} [a] &= \{x \mid x \in \mathbb{Z}, x \equiv_n a\} = \{x \mid x \in \mathbb{Z}, n \text{ divide } x - a\} = \\ &= \{x \mid x - a = nq \text{ per qualche } q \in \mathbb{Z}\} = \\ &= \{x \mid x = a + nq \text{ per qualche } q \in \mathbb{Z}\} = \\ &= \{a + nq \mid q \in \mathbb{Z}\}. \end{aligned}$$

LEMMA 8.1. Se  $n \geq 1$  è un numero intero fissato e  $\equiv_n$  è la congruenza modulo  $n$ , allora  $\mathbb{Z}/\equiv_n = \{[0], [1], [2], \dots, [n-1]\}$  e gli elementi  $[0], [1], [2], \dots, [n-1]$  di  $\mathbb{Z}/\equiv_n$  sono tutti distinti tra loro. In particolare  $\mathbb{Z}/\equiv_n$  è un insieme avente esattamente  $n$  elementi.

*Dimostrazione.* Chiaramente l'insieme  $\mathbb{Z}/\equiv_n = \{[a] \mid a \in \mathbb{Z}\}$  contiene  $\{[0], [1], [2], \dots, [n-1]\}$ . Viceversa fissiamo un elemento  $[a]$  di  $\mathbb{Z}/\equiv_n$ , dove  $a$  denota un numero intero, e mostriamo che  $[a] \in \{[0], [1], [2], \dots, [n-1]\}$ . Dividiamo il numero intero  $a$  per  $n$ ; si ha  $a = nq + r$  con  $q, r \in \mathbb{Z}$  e  $0 \leq r < n$ . Allora  $n$  divide  $nq = a - r$ , e quindi  $a \equiv_n r$ . Ne segue che  $[a] = [r]$ . Ma  $0 \leq r < n$ , e quindi  $r$  è uno dei numeri  $0, 1, 2, \dots, n-1$ . Pertanto  $[a] = [r] \in \{[0], [1], [2], \dots, [n-1]\}$ . Abbiamo così dimostrato che  $\mathbb{Z}/\equiv_n = \{[0], [1], [2], \dots, [n-1]\}$ .

Facciamo vedere ora che gli  $n$  elementi  $[0], [1], [2], \dots, [n-1]$  di  $\mathbb{Z}/\equiv_n$  sono tutti distinti tra loro. Supponiamo che  $i$  e  $j$  siano due numeri interi con  $0 \leq i < j \leq n-1$  e mostriamo che  $[i] \neq [j]$ . Si ha  $j - i \leq j \leq n-1$  e  $j - i > 0$ . Pertanto  $0 < j - i < n$ , e quindi  $n$  non divide  $j - i$  (perché  $n$  divide  $0, n, 2n, 3n, \dots$ , ma non divide nessun numero strettamente compreso tra  $0$  e  $n$ ). Quindi  $j \not\equiv_n i$ , e pertanto  $[j] \neq [i]$ . Questo dimostra che gli  $n$  elementi  $[0], [1], [2], \dots, [n-1]$  di  $\mathbb{Z}/\equiv_n$  sono tutti distinti tra loro e che quindi  $\mathbb{Z}/\equiv_n$  ha esattamente  $n$  elementi.  $\square$

ESEMPIO 4. Sia  $n = 5$ . Le classi di equivalenza di  $\mathbb{Z}$  modulo  $\equiv_5$  sono:

$$\begin{aligned} [0] &= \{\dots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \dots\}, \\ [1] &= \{\dots, -19, -14, -9, -4, 1, 6, 11, 16, 21, \dots\}, \\ [2] &= \{\dots, -18, -13, -8, -3, 2, 7, 12, 17, 22, \dots\}, \\ [3] &= \{\dots, -17, -12, -7, -2, 3, 8, 13, 18, 23, \dots\}, \\ [4] &= \{\dots, -16, -11, -6, -1, 4, 9, 14, 19, 24, \dots\}. \quad \square \end{aligned}$$

C'è un modo abbastanza comodo di visualizzare l'insieme  $\mathbb{Z}/\equiv_n$  con  $n \geq 1$ . Rappresentiamo  $\mathbb{Z}/\equiv_n$  come un insieme di  $n$  oggetti distinti  $[0], [1], [2], \dots, [n-1]$ , e supponiamo di disporre questi  $n$  oggetti nei vertici di un poligono regolare di  $n$  lati come nella figura 8.1.

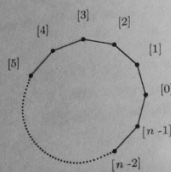


Figura 8.1

Supponiamo ora di distribuire i numeri interi tra gli oggetti  $[0], [1], [2], \dots, [n-1]$  nello stesso modo in cui si distribuisce un mazzo di carte ad  $n$  giocatori. Diamo il numero 0 al giocatore  $[0]$ , il numero 1 al giocatore  $[1]$ , il numero 2 al giocatore  $[2]$ , e così via fino al numero  $n-1$  al giocatore  $[n-1]$ . Completato così il primo giro continuiamo a distribuire i numeri interi: quindi il numero  $n$  va al giocatore  $[0]$ , il numero  $n+1$  al giocatore  $[1]$ , il numero  $n+2$  al giocatore  $[2]$ , e così via per tutti i numeri interi positivi. Distribuiamo poi anche i numeri negativi, ma questa volta in senso inverso: il numero  $-1$  al giocatore  $[n-1]$ , il numero  $-2$  al giocatore  $[n-2]$ , il numero  $-3$  al giocatore  $[n-3]$ ,  $\dots$ , il numero  $-(n-1)$  al giocatore  $[1]$ , il numero  $-n$  al giocatore  $[0]$ , e così via di seguito. In questo modo a  $[0]$  vengono dati i numeri  $0, n, 2n, 3n, \dots, -n, -2n, -3n, \dots$ , a  $[1]$  vengono dati i numeri  $1, n+1, 2n+1, 3n+1, \dots, -n+1, -2n+1, -3n+1, \dots$ , a  $[2]$  vengono dati i numeri  $2, n+2, 2n+2, 3n+2, \dots, -n+2, -2n+2, -3n+2, \dots$ , e più in generale ad  $[a]$  vengono dati tutti i numeri del tipo  $a+nq$  con  $q \in \mathbb{Z}$ . Pertanto ad  $[a]$  vengono dati esattamente tutti i numeri che stanno nella classe di equivalenza di  $a$ . In questo modo si riesce a visualizzare facilmente come i numeri interi di  $\mathbb{Z}$  vengono ripartiti nell'insieme quoziente  $\mathbb{Z}/\equiv_n = \{[0], [1], [2], \dots, [n-1]\}$ , si vede che  $\mathbb{Z}/\equiv_n$  ha esattamente  $n$  elementi, e si vede che la classe di equivalenza di  $a$  è l'insieme di tutti i numeri del tipo  $a+nq$  con  $q \in \mathbb{Z}$ .

### Esercizi svolti

**8.1.** Si dia un esempio di quattro numeri  $n, x, y, z \in \mathbb{Z}$ , con  $n > 0$ , tali che  $xz \equiv yz \pmod{n}$  e  $x \not\equiv y \pmod{n}$ .

*Soluzione.* Ci sono infinite quaterne  $(n, x, y, z)$  che sono possibili soluzioni. Ad esempio  $n = 2$ ,  $x = 0$ ,  $y = 1$  e  $z = 2$  va bene. Il lettore trovi almeno un'altra soluzione.  $\square$

**8.2.** Siano  $x, y, n \in \mathbb{Z}$  con  $n > 0$ . Si provi che  $x \equiv y \pmod{n}$  se e solo se il resto della divisione di  $x$  per  $n$  è uguale al resto della divisione di  $y$  per  $n$ .

*Soluzione.* Se si dividono  $x$  e  $y$  per  $n$  si ha che  $x = qn + r$ ,  $y = q'n + r'$ ,  $0 \leq r < n$  e  $0 \leq r' < n$  per opportuni  $q, r, q', r' \in \mathbb{Z}$ .

Se  $x \equiv y \pmod{n}$ , allora  $n$  divide  $x - y = qn + r - q'n - r' = (q - q')n + r - r'$ . Dato che  $n$  divide  $(q - q')n$ , se ne deduce che  $n$  divide anche la differenza  $r - r'$ . Ma da  $0 \leq r < n$  e  $0 \leq r' < n$  segue che  $-n < r - r' < n$ . Dato che l'unico numero strettamente compreso tra  $-n$  ed  $n$  che sia divisibile per  $n$  è 0, si ricava che  $r - r' = 0$ , cioè che  $r = r'$ . Pertanto il resto della divisione di  $x$  per  $n$  è uguale al resto della divisione di  $y$  per  $n$ .

Viceversa supponiamo  $r = r'$ . Allora

$$x - y = (qn + r) - (q'n + r) = (q - q')n$$

è divisibile per  $n$ , e quindi  $x \equiv y \pmod{n}$ .  $\square$

**8.3.** Si provi che se  $a, b, c, d \in \mathbb{Z}$ ,  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , allora  $a + c \equiv b + d \pmod{n}$  e  $ac \equiv bd \pmod{n}$ .

*Soluzione.* Da  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$  segue che  $n \mid (a - b)$  e  $n \mid (c - d)$ . Pertanto esistono  $u, v \in \mathbb{Z}$  tali che  $a - b = nu$  e  $c - d = nv$ . Ma allora  $(a + c) - (b + d) = (a - b) + (c - d) = nu + nv = n(u + v)$ , da cui  $n \mid ((a + c) - (b + d))$ , ossia  $a + c \equiv b + d \pmod{n}$ . Inoltre essendo  $a = b + nu$  e  $c = d + nv$ , si ottiene che  $ac = (b + nu)(d + nv) = bd + n(bv + ud + nuv)$ . Quindi  $n \mid (ac - bd)$ , vale a dire  $ac \equiv bd \pmod{n}$ .  $\square$

**8.4.** Si provi che se  $n, m \geq 1$  sono numeri naturali ed  $n$  divide  $m$ , ponendo  $\varphi([a]_{\equiv_m}) = [a]_{\equiv_n}$  si dà una buona definizione di un'applicazione  $\varphi: \mathbb{Z}/\equiv_m \rightarrow \mathbb{Z}/\equiv_n$ , cioè che se  $a, b \in \mathbb{Z}$  e  $[a]_{\equiv_m} = [b]_{\equiv_m}$  allora  $[a]_{\equiv_n} = [b]_{\equiv_n}$ . Si dimostri poi che tale applicazione  $\varphi$  è suriettiva.

*Soluzione.* Siano  $a, b \in \mathbb{Z}$  tali che  $[a]_{\equiv_m} = [b]_{\equiv_m}$ . Allora  $a \equiv b \pmod{m}$ , cioè  $a - b = tm$  per qualche  $t \in \mathbb{Z}$ . Ma  $n$  divide  $m$ , cioè  $m = kn$  per qualche intero  $k$ , e quindi  $a - b = tkn$ , da cui  $n \mid (a - b)$ , ossia  $a \equiv b \pmod{n}$ . Se ne conclude che  $[a]_{\equiv_n} = [b]_{\equiv_n}$ . Questo prova che ponendo  $\varphi([a]_{\equiv_m}) = [a]_{\equiv_n}$  per ogni  $[a]_{\equiv_m} \in \mathbb{Z}/\equiv_m$  si dà una buona definizione di un'applicazione  $\varphi: \mathbb{Z}/\equiv_m \rightarrow \mathbb{Z}/\equiv_n$ .

Mostriamo che  $\varphi$  è suriettiva. Se  $y \in \mathbb{Z}/\equiv_n$ , allora  $y = [a]_{\equiv_n}$  per qualche  $a \in \mathbb{Z}$ , e quindi  $\varphi([a]_{\equiv_m}) = [a]_{\equiv_n} = y$ . Questo prova che  $\varphi$  è suriettiva.  $\square$

## Altri esercizi

8.5. Siano  $a, b, m, n$  numeri interi,  $m, n \geq 1$ , e sia  $[m, n]$  il mcm positivo di  $m$  ed  $n$ . Si dimostri che  $a \equiv b \pmod{m}$  e  $a \equiv b \pmod{n}$  se e solo se  $a \equiv b \pmod{[m, n]}$ .

8.6. Si dimostri che se  $a, b, c \in \mathbb{Z}$  e i due numeri  $a$  ed  $n$  sono primi tra loro, da  $ab \equiv ac \pmod{n}$  segue che  $b \equiv c \pmod{n}$ .

[Suggerimento: corollario 4.2.]

8.7. Si dimostri che per ogni numero naturale  $n$  si ha  $7^n \equiv 1 \pmod{8}$  se  $n$  è pari, e  $7^n \equiv 7 \pmod{8}$  se  $n$  è dispari.

8.8. (a) Quanti elementi ha  $\mathbb{Z}/\equiv_0$ ? Quali sono?

(b) Quanti elementi ha  $\mathbb{Z}/\equiv_1$ ? Quali sono?

8.9. Sia  $n \geq 1$  un numero intero fissato. Si consideri l'applicazione  $r: \mathbb{Z} \rightarrow \mathbb{Z}$  definita, per ogni  $x \in \mathbb{Z}$ , da  $r(x) = \text{"resto della divisione di } x \text{ per } n"$ . Si dimostri che:

(a) l'immagine di  $r$  è  $\{0, 1, 2, \dots, n-1\}$ ;

(b) la relazione  $\sim_r$  associata all'applicazione  $r$  è la congruenza modulo  $n$ ;

(c) se  $y \in \{0, 1, 2, \dots, n-1\}$ , allora  $r^{-1}(y) = [y]_{\equiv_n}$ .

[Suggerimento per (b): esercizio 8.2.]

8.10. Siano  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  un'applicazione ed  $n$  un numero intero fissato. Si definisca una relazione  $\sim$  su  $\mathbb{Z}$  ponendo, per ogni  $a, b \in \mathbb{Z}$ ,

$$a \sim b \text{ se } f(a) \equiv f(b) \pmod{n}.$$

(a) Si dimostri che  $\sim$  è un'equivalenza su  $\mathbb{Z}$ .

(b) Si dimostri che  $[a]_{\sim} = f^{-1}([f(a)]_{\equiv_n})$  per ogni  $a \in \mathbb{Z}$ .

8.11. Si dimostri che ponendo  $\psi([a]_{\equiv_3}) = [2a]_{\equiv_6}$  per ogni  $a \in \mathbb{Z}$  si dà una buona definizione di un'applicazione  $\psi: \mathbb{Z}/\equiv_3 \rightarrow \mathbb{Z}/\equiv_6$ , cioè che se  $a$  e  $b$  sono numeri interi e  $[a]_{\equiv_3} = [b]_{\equiv_3}$  allora  $[2a]_{\equiv_6} = [2b]_{\equiv_6}$ . Si dimostri poi che l'applicazione  $\psi$  è iniettiva.

8.12. Sia  $A = \{1, 2, 3, 4, -3, -1, 14, 23, -7, 28\}$ . Sia  $\varrho$  la relazione di equivalenza su  $A$  definita ponendo, per ogni  $x, y \in A$ ,  $x \varrho y$  se  $x$  e  $y$  sono congrui tra loro modulo 5 (cioè se esiste  $z \in \mathbb{Z}$  tale che  $x - y = 5z$ ).

(a) Quanti elementi ha l'insieme quoziente  $A/\varrho$ ? Quali sono?

Si definisca  $\varphi: A/\varrho \rightarrow \mathbb{Z}/\equiv_5$  ponendo  $\varphi([x]_{\varrho}) = [x]_{\equiv_5}$  per ogni  $x \in A$ .

(b) Si dimostri che l'applicazione  $\varphi$  è ben definita, cioè che se  $x, y \in A$  e  $[x]_{\varrho} = [y]_{\varrho}$ , allora  $[x]_{\equiv_5} = [y]_{\equiv_5}$ .

(c) L'applicazione  $\varphi$  è iniettiva?

(d) L'applicazione  $\varphi$  è suriettiva?

8.13. Siano  $n \geq 1$  e  $k$  numeri interi fissati. Si consideri l'applicazione  $f: \mathbb{Z}/\equiv_n \rightarrow \mathbb{Z}/\equiv_n$  definita da  $f([a]) = [ka]$  per ogni  $a \in \mathbb{Z}$ .

(a) Si dimostri che l'applicazione  $f$  è ben definita, cioè che se  $a, b \in \mathbb{Z}$  e  $[a] = [b]$ , allora  $[ka] = [kb]$ .

(b) Si dimostri che  $f$  è iniettiva se e solo se  $n$  e  $k$  sono primi tra loro.

(c) Si dimostri che  $f$  è suriettiva se e solo se l'equazione  $kx \equiv b \pmod{n}$  ha una soluzione in  $\mathbb{Z}$  per ogni  $b \in \mathbb{Z}$ .

(d) Si dimostri l'equazione  $kx \equiv b \pmod{n}$  ha una soluzione in  $\mathbb{Z}$  per ogni  $b \in \mathbb{Z}$  se e solo se  $n$  e  $k$  sono primi tra loro.

## Capitolo 9. Cardinalità di insiemi

Due insiemi  $A$  e  $B$  si dicono *equipotenti*, o che *hanno la stessa cardinalità*, se esiste una biiezione di  $A$  in  $B$ . Se  $A$  è un insieme finito, cioè se  $A$  contiene solo un numero finito di elementi, il numero degli elementi di  $A$  è un numero naturale chiamato la *cardinalità* di  $A$  (e denotato con  $|A|$  o con  $\text{card } A$ ). Un insieme finito  $A$  o ha cardinalità 0 (e questo avviene se e solo se  $A = \emptyset$ ) oppure ha cardinalità  $n \geq 1$  (e questo avviene se e solo se  $A$  è equipotente al sottoinsieme  $\{0, 1, 2, \dots, n-1\}$  di  $\mathbb{N}$ ). Se  $A$  e  $B$  sono insiemi finiti disgiunti, è chiaro che  $|A \cup B| = |A| + |B|$ . Da questo segue che più in generale se  $A$  e  $B$  sono insiemi finiti (non necessariamente disgiunti), allora  $|A \cup B| + |A \cap B| = |A| + |B|$  (esercizio 9.1).

È anche possibile dimostrare che se  $A$  e  $B$  sono insiemi finiti si ha  $|A \times B| = |A| \cdot |B|$  e  $|B^A| = |B|^{|A|}$ , ove  $A \times B$  e  $B^A$  sono rispettivamente il prodotto cartesiano di  $A$  per  $B$  e l'insieme di tutte le applicazioni di  $A$  in  $B$ . Inoltre (esercizi 9.3 e 9.14) se  $A$  è un insieme finito si ha  $|\mathcal{P}(A)| = 2^{|A|}$ , e se  $A$  è un insieme finito di cardinalità  $n$  ci sono  $n!$  biiezioni di  $A$  in  $A$ .

Un insieme  $A$  si dice *infinito* se non è finito, ossia se contiene infiniti elementi distinti. Ad esempio  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  ed  $\mathbb{R}$  sono insiemi infiniti.

Un insieme  $A$  è *numerabile* se è equipotente all'insieme  $\mathbb{N}$  dei numeri naturali. Ad esempio l'insieme  $\mathbb{N}$  è numerabile, dato che l'applicazione identica  $\iota_{\mathbb{N}}: \mathbb{N} \rightarrow \mathbb{N}$  è una biiezione di  $\mathbb{N}$  in  $\mathbb{N}$ . Anche  $\mathbb{N}^*$  è numerabile (si consideri l'applicazione  $\mathbb{N} \rightarrow \mathbb{N}^*$ ,  $n \mapsto n+1$ ).

Nell'esercizio 2.2 abbiamo visto che è possibile definire una biiezione  $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$ ; quindi anche l'insieme  $\mathbb{Z}$  è numerabile.

**PROPOSIZIONE 9.1.** *Ogni sottoinsieme di  $\mathbb{N}$  è finito o numerabile. Più in generale ogni sottoinsieme di un insieme numerabile è finito o numerabile.*

**Dimostrazione.** Per provare che ogni sottoinsieme di  $\mathbb{N}$  è finito o numerabile faremo vedere che se  $S$  è un sottoinsieme infinito di  $\mathbb{N}$  allora  $S$  è numerabile. Fissato un sottoinsieme infinito  $S$  di  $\mathbb{N}$  definiamo induttivamente un'applicazione  $\varphi_S: \mathbb{N} \rightarrow S$  in questo modo:

$$\begin{aligned}\varphi_S(0) &= \min S, \\ \varphi_S(n) &= \min(S \setminus \{\varphi_S(0), \varphi_S(1), \dots, \varphi_S(n-1)\}) \quad \text{per ogni } n \geq 1.\end{aligned}$$

Qui con  $\min$  abbiamo denotato il minimo dell'insieme. Quindi:

$\varphi_S(0)$  è il più piccolo degli elementi di  $S$ ;  
 $\varphi_S(1)$  è il più piccolo degli elementi di  $S$  escluso  $\varphi_S(0)$ ;  
 $\varphi_S(2)$  è il più piccolo degli elementi di  $S$  escluso  $\varphi_S(0)$  e  $\varphi_S(1)$ ;  
 $\varphi_S(3)$  è il più piccolo degli elementi di  $S$  escluso  $\varphi_S(0)$ ,  $\varphi_S(1)$  e  $\varphi_S(2)$ ;  
 e così via.

Si osservi che il procedimento non può terminare, in quanto l'insieme  $S$  è infinito. L'applicazione  $\varphi_S$  così definita è ovviamente una biiezione tra  $\mathbb{N}$  ed  $S$ , e quindi  $S$  è numerabile.

Più in generale, se  $A$  è un insieme numerabile e  $B \subseteq A$ , esiste una biiezione  $\psi: \mathbb{N} \rightarrow A$ . Allora l'applicazione  $\psi': \psi^{-1}(B) \rightarrow B$  definita da  $\psi'(n) = \psi(n)$  per ogni  $n \in \psi^{-1}(B)$  ( $\psi'$  si dice l'applicazione ottenuta da  $\psi$  restringendo il codominio a  $B$  e il dominio a  $\psi^{-1}(B)$ ) è una biiezione. Quindi  $B$  è equipotente a  $\psi^{-1}(B)$ , e per quanto visto precedentemente  $\psi^{-1}(B) \subseteq \mathbb{N}$  è finito o numerabile. Quindi anche  $B$  è finito o numerabile.  $\square$

Si faccia attenzione che in altri testi un insieme  $A$  è detto numerabile se è equipotente ad un sottoinsieme di  $\mathbb{N}$ . Per la proposizione 9.1 si ha quindi che tali insiemi sono esattamente gli insiemi finiti o equipotenti a  $\mathbb{N}$ .

**LEMMA 9.2.** *Sia  $A$  un insieme non vuoto. Esiste un'applicazione suriettiva  $\varphi: \mathbb{N} \rightarrow A$  se e solo se l'insieme  $A$  è finito o numerabile.*

**Dimostrazione.** Supponiamo innanzitutto che l'insieme  $A$  sia finito o numerabile. Se  $A = \{a_1, a_2, \dots, a_n\}$  è un insieme finito di cardinalità  $n$ , è sufficiente considerare l'applicazione suriettiva  $\varphi: \mathbb{N} \rightarrow A$  definita, per ogni  $i \in \mathbb{N}$  da  $\varphi(i) = a_{i+1}$  se  $i < n$  e  $\varphi(i) = a_n$  se  $i \geq n$ . Se  $A$  è un insieme numerabile, esiste per definizione un'applicazione biiettiva  $\varphi: \mathbb{N} \rightarrow A$ . Questo dimostra una delle due implicazioni dell'enunciato del lemma.

Per dimostrare l'altra implicazione supponiamo invece che esista un'applicazione suriettiva  $\varphi: \mathbb{N} \rightarrow A$ . Per l'esercizio 3.6 esiste un'applicazione  $\psi: A \rightarrow \mathbb{N}$  tale che  $\varphi \circ \psi = \iota_A$ . Dato che l'applicazione composta  $\varphi \circ \psi = \iota_A$  è iniettiva, anche l'applicazione  $\psi$  è iniettiva (vedi esercizio 3.2 (a)). Quindi l'applicazione  $\psi': A \rightarrow \psi(A)$  definita da  $\psi'(a) = \psi(a)$  per ogni  $a \in A$  ( $\psi'$  è l'applicazione ottenuta da  $\psi$  restringendo il codominio a  $\psi(A)$ ) è una biiezione. Ma allora  $A$  è equipotente a  $\psi(A)$ , e per la proposizione 9.1  $\psi(A) \subseteq \mathbb{N}$  deve essere finito o numerabile. Quindi anche  $A$  è finito o numerabile.  $\square$

**PROPOSIZIONE 9.3.** *Se  $A = \bigcup_{i \in I} A_i$ , dove gli insiemi  $A_i$  sono finiti o numerabili per ogni  $i \in I$  e l'insieme degli indici  $I$  è finito o numerabile, allora anche l'insieme  $A$  è finito o numerabile.*

**Dimostrazione.** Si può evidentemente supporre che tutti gli insiemi  $I$  e  $A_i$  siano non vuoti. Allora in base al lemma 9.2 esiste per ogni  $i \in I$  un'applicazione suriettiva  $\varphi_i: \mathbb{N} \rightarrow A_i$  ed esiste un'applicazione suriettiva  $\psi: \mathbb{N} \rightarrow I$ . Siano  $p_0 < p_1 < p_2 < \dots$  tutti gli elementi di  $\mathbb{N}$  che sono numeri primi e sia  $S = \{p_k^{t+1} \mid k, t \in \mathbb{N}\}$  l'insieme di tutti i numeri naturali che sono potenze ad esponente intero positivo di un primo. Definiamo un'applicazione  $f: S \rightarrow A = \bigcup_{i \in I} A_i$  ponendo  $f(p_k^{t+1}) = \varphi_{\psi(k)}(t)$ . Allora  $f$  è un'applicazione suriettiva che manda le potenze di  $p_k$  in  $A_{\psi(k)}$ . Per la proposizione 9.1 l'insieme infinito  $S$  è numerabile, e dunque esiste una biiezione  $g: \mathbb{N} \rightarrow S$ . Se ne deduce che  $f \circ g: \mathbb{N} \rightarrow A$  è un'applicazione suriettiva, e quindi l'insieme  $A$  è finito o numerabile per il lemma 9.2.  $\square$

**ESEMPIO 1.** Mostriamo che  $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$  è numerabile. Per ogni  $n \in \mathbb{N}^*$  sia  $A_n = \left\{ \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n}{n} \right\}$  l'insieme dei numeri razionali positivi che possono essere scritti come una frazione in cui la somma del numeratore e del denominatore è  $n+1$ . Ogni  $A_n$  è un insieme finito di cardinalità  $n$  e quindi  $\mathbb{Q}^+ = \bigcup_{n \in \mathbb{N}^*} A_n$  è un insieme numerabile per la proposizione 9.3.  $\square$

**ESEMPIO 2.** Mostriamo che  $\mathbb{Q}$  è numerabile. Abbiamo visto nell'esempio precedente che  $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$  è un insieme numerabile. Se  $\mathbb{Q}^- = \{q \in \mathbb{Q} \mid q < 0\}$ , anche  $\mathbb{Q}^-$  è numerabile (si consideri la biiezione  $\mathbb{Q}^+ \rightarrow \mathbb{Q}^-$ ,  $x \mapsto -x$ ). Ma allora  $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ , unione di due insiemi numerabili e di un insieme finito, è un insieme numerabile per la proposizione 9.3.  $\square$

### Esercizi svolti

**9.1.** Se  $A$  e  $B$  sono insiemi finiti, si provi che  $|A \cup B| + |A \cap B| = |A| + |B|$ .

**Soluzione.** Si ha  $|A \cup B| + |A \cap B| = |A \cup (B \setminus A)| + |A \cap B| = |A| + |B \setminus A| + |A \cap B|$  (quest'ultima uguaglianza vale perché gli insiemi  $A$  e  $B \setminus A$  sono disgiunti). Ma anche  $B \setminus A$  e  $A \cap B$  sono disgiunti, per cui si ha che  $|A \cup B| + |A \cap B| =$



$|A| + |B \setminus A| + |A \cap B| = |A| + |(B \setminus A) \cup (A \cap B)| = |A| + |B|$  in quanto  $(B \setminus A) \cup (A \cap B) = B$ .  $\square$

9.2. Si dimostri per induzione su  $n$  che se  $A_1, A_2, \dots, A_n$  sono insiemi finiti e  $A_i \cap A_j = \emptyset$  per ogni  $i \neq j$ , allora

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|.$$

*Soluzione.* Il caso  $n = 1$  è immediato (in questo caso si ha che  $\bigcup_{i=1}^n A_i = A_1$  e  $\sum_{i=1}^n |A_i| = |A_1|$ ). Supponiamo quindi  $n > 1$ , che l'identità da dimostrare valga per le unioni di  $n-1$  insiemi finiti a due a due disgiunti, e proviamo l'identità per l'unione di  $n$  insiemi  $A_1, A_2, \dots, A_n$  finiti e a due a due disgiunti, cioè tali che  $A_i \cap A_j = \emptyset$  per ogni  $i \neq j$ . Si osservi che in questo caso  $\bigcup_{i=1}^{n-1} A_i$  e  $A_n$  sono insiemi disgiunti in quanto  $\left( \bigcup_{i=1}^{n-1} A_i \right) \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n) = \emptyset$ . Quindi

$$\left| \bigcup_{i=1}^n A_i \right| = \left| \left( \bigcup_{i=1}^{n-1} A_i \right) \cup A_n \right| = \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n|.$$

Per l'ipotesi induttiva applicata agli  $n-1$  insiemi disgiunti  $A_1, A_2, \dots, A_{n-1}$  si ha  $\left| \bigcup_{i=1}^{n-1} A_i \right| = \sum_{i=1}^{n-1} |A_i|$ , e quindi  $\left| \bigcup_{i=1}^n A_i \right| = \left( \sum_{i=1}^{n-1} |A_i| \right) + |A_n| = \sum_{i=1}^n |A_i|$ . Questo prova l'identità anche per le unioni di  $n$  insiemi a due a due disgiunti.  $\square$

9.3. Siano  $A$  un insieme finito,  $\mathcal{P}(A)$  l'insieme delle parti di  $A$ , e  $n = |A|$ . Si dimostri per induzione su  $n$  che  $|\mathcal{P}(A)| = 2^n$ .

*Soluzione.* Se  $n = 0$ , cioè se  $A = \emptyset$ , allora  $\mathcal{P}(A) = \{\emptyset\}$ , e quindi  $|\mathcal{P}(A)| = 1 = 2^0$ . Pertanto l'asserzione è vera in questo caso. Supponiamo quindi che  $n$  sia un numero intero  $> 0$  e che l'insieme delle parti di un insieme di  $n-1$  elementi abbia  $2^{n-1}$  elementi. Fissiamo un insieme  $A$  di cardinalità  $n$  e un suo elemento  $a_0 \in A$ . Un sottoinsieme di  $A$  può non contenere l'elemento  $a_0$  o può contenerlo. I sottoinsiemi di  $A$  che non contengono l'elemento  $a_0$  sono esattamente i sottoinsiemi di  $A \setminus \{a_0\}$ ; poiché  $|A \setminus \{a_0\}| = n-1$ , tali sottoinsiemi sono, per l'ipotesi induttiva,  $2^{n-1}$ . I sottoinsiemi di  $A$  che contengono  $a_0$  sono quelli del tipo  $S \cup \{a_0\}$  ove  $S$  è un sottoinsieme di  $A \setminus \{a_0\}$ ; quindi anche tali sottoinsiemi sono, per l'ipotesi induttiva  $2^{n-1}$ . Quindi i sottoinsiemi di  $A$  sono in tutto  $2^{n-1} + 2^{n-1} = 2^n$ , cioè  $|\mathcal{P}(A)| = 2^n$ .  $\square$

9.4. Il coefficiente binomiale  $\binom{n}{k}$ , dove  $n \geq k \geq 0$  sono numeri interi, è definito da

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Si dimostri che

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

per ogni intero  $k$  tale che  $1 \leq k \leq n-1$ .

*Soluzione.* Si ha

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} = \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \left( \frac{1}{n-k} + \frac{1}{k} \right) = \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{n}{(n-k)k} = \\ &= \frac{n!}{k!(n-k)!} = \binom{n}{k}. \quad \square \end{aligned}$$

Il risultato dimostrato nell'esercizio precedente ha un'interessante interpretazione geometrica. Supponiamo di scrivere i coefficienti binomiali disponendoli in un triangolo illimitato (detto *triangolo di Tartaglia* o *triangolo di Pascal*) nel modo seguente:

$$\begin{array}{cccccccc} & & & & \binom{0}{0} & & & \\ & & & \binom{1}{0} & & \binom{1}{1} & & \\ & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\ & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} \\ & \dots & & \dots & & \dots & & \dots & & \dots & & \dots \end{array}$$

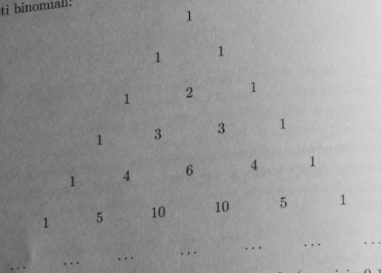
Dato che

$$\binom{n}{0} = \binom{n}{n} = 1$$

per ogni  $n$ , il primo e l'ultimo coefficiente binomiale su ogni riga del triangolo di Tartaglia sono uguali a 1, cioè tutti i coefficienti binomiali sui due lati obliqui del triangolo sono uguali a 1. Per quanto riguarda invece i coefficienti binomiali  $\binom{n}{k}$  all'interno del triangolo si osservi che i coefficienti binomiali immediatamente sopra  $\binom{n}{k}$  sono  $\binom{n-1}{k-1}$  e  $\binom{n-1}{k}$ , e per l'esercizio precedente

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Quindi ogni coefficiente binomiale all'interno del triangolo è la somma dei due coefficienti binomiali che gli stanno immediatamente sopra. Questo permette di riscrivere il triangolo di Tartaglia calcolando molto facilmente il valore dei coefficienti binomiali:



Il nome di *coefficienti binomiali* deriva dalla formula (esercizio 9.17)

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k;$$

i coefficienti binomiali

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}, \binom{n}{n}$$

sono proprio i coefficienti di  $x^n, x^{n-1}y, x^{n-2}y^2, \dots, xy^{n-1}, y^n$  che si ottengono sviluppando il binomio  $(x+y)^n$ . Il lettore confronti i valori dei coefficienti binomiali nella terza e nella quarta riga del triangolo di Tartaglia ed i coefficienti di  $(x+y)^2 = x^2 + 2xy + y^2$  e  $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$  a lui noti dalle scuole medie.

### Altri esercizi

9.5. Si dimostri che se  $f: A \rightarrow B$  è un'applicazione e  $\sim_f$  è la relazione di equivalenza su  $A$  associata ad  $f$ , allora gli insiemi  $A/\sim_f$  e  $f(A)$  sono equipotenti.

9.6. Gli insiemi  $\mathbb{Z}$  e  $\mathbb{Q}$  sono equipotenti?

9.7. Quante matrici  $m \times n$  i cui elementi sono tutti scelti nell'insieme  $\{1, 2, 3, \dots, p\}$  si possono costruire?

9.8. La matricola di un certo tipo di macchina fotografica è una sequenza di sette simboli dei quali i primi due sono lettere dell'alfabeto, gli ultimi cinque sono cifre ma di queste la prima è diversa da zero, e l'ultima può essere solo 0 o 1. Quante matricole di questo tipo esistono?

9.9. Siano  $A$  e  $B$  due insiemi finiti, non vuoti e disgiunti, con  $m$  ed  $n$  elementi rispettivamente.

- Quante coppie  $(a, b)$  si possono costruire con  $a \in A$  e  $b \in B$ ?
- Quante coppie  $(a, a')$  si possono costruire con  $a \in A$  e  $a' \in A$ ?
- Quante coppie  $(a, a')$  si possono costruire con  $a \in A$ ,  $a' \in A$  e  $a \neq a'$ ?
- Quanti insiemi  $\{a, a'\}$  si possono costruire con  $a \in A$ ,  $a' \in A$  e  $a \neq a'$ ?
- Quanti insiemi  $\{a, b\}$  si possono costruire con  $a \in A$  e  $b \in B$ ?
- Quanti insiemi  $\{x, y\}$  si possono costruire con  $x \in A$ ,  $y \in A \cup B$  e  $x \neq y$ ?

9.10. In quanti modi è possibile mettere in fila indiana 10 bambini?

9.11. Si dimostri che se  $A$  e  $B$  sono insiemi finiti,  $|A| = m$  e  $|B| = n$ , allora il numero delle applicazioni iniettive di  $A$  in  $B$  è 0 se  $m > n$ , ed è  $n!/(n-m)!$  se  $(n-m+1)(n-m+2)(n-m+3) \cdots (n-1)n$  se  $m \leq n$ .

9.12. Quante e quali sono le relazioni di equivalenza su un insieme  $X$  se

- $X$  ha un solo elemento?
- $X$  ha due elementi?
- $X$  ha tre elementi?

9.13. Si dimostri che se  $A$  e  $B$  sono insiemi numerabili, anche  $A \times B$  è un insieme numerabile.

[Suggerimento: proposizione 9.3.]

9.14. Sia  $A$  un insieme. Per ogni suo sottoinsieme  $S \subseteq A$ , consideriamo la funzione  $\chi_S: A \rightarrow \{0, 1\}$  così definita:

$$\chi_S(a) = \begin{cases} 0 & \text{se } a \in A \setminus S, \\ 1 & \text{se } a \in S. \end{cases}$$

L'applicazione  $\chi_S$  si chiama la *funzione caratteristica* del sottoinsieme  $S$  di  $A$ . Definiamo ora un'applicazione  $\sigma: \mathcal{P}(A) \rightarrow \{0, 1\}^A$  dall'insieme delle parti di  $A$  nell'insieme di tutte le applicazioni di  $A$  in  $\{0, 1\}$  ponendo  $\sigma(S) = \chi_S$  per ogni  $S \in \mathcal{P}(A)$ .

- Si dimostri che  $\sigma$  è una bijezione.
- Come è definita l'applicazione inversa  $\sigma^{-1}: \{0, 1\}^A \rightarrow \mathcal{P}(A)$ ?
- Si deduca da (a) che se  $A$  è un insieme finito e  $\mathcal{P}(A)$  è l'insieme delle parti di  $A$ , allora  $|\mathcal{P}(A)| = 2^{|A|}$ .

[Questo è un altro modo di dimostrare quanto avevamo già fatto vedere nell'esercizio 9.3.]

9.15. Siano  $n \geq k$  numeri naturali. Si dimostri per induzione su  $n$  che un insieme di cardinalità  $n$  ha esattamente  $\binom{n}{k}$  sottoinsiemi di cardinalità  $k$ .

9.16. Siano  $n \geq k$  numeri naturali. Si dimostri che  $\binom{n}{k} = \binom{n}{n-k}$ .

[Quindi il triangolo di Tartaglia è simmetrico rispetto al suo asse verticale.]

9.17. Si dimostri che se  $x, y \in \mathbb{R}$ , si ha  $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$  per ogni intero  $n \geq 1$ .

[Suggerimento: induzione su  $n$  ed esercizio 9.4.]

Quindi nelle righe del triangolo di Tartaglia sono scritti ordinatamente i valori dei coefficienti di  $x^n, x^{n-1}y, x^{n-2}y^2, \dots, xy^{n-1}, y^n$  che si ottengono sviluppando il binomio  $(x+y)^n$ . Questo fatto è la ragione del nome *coefficienti binomiali*.

9.18. Si dimostri che  $\sum_{k=0}^n \binom{n}{k} = 2^n$  per ogni  $n \geq 0$ .

[Suggerimento: nell'esercizio 9.17 porre  $x = y = 1$ .]

9.19. Si dimostri che  $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots \pm \binom{n}{n} = 0$  per ogni  $n \geq 1$ .

[Suggerimento: nell'esercizio 9.17 porre  $x = 1$  e  $y = -1$ .]

9.20. Sviluppare  $(1+x)^5$  facendo uso del triangolo di Tartaglia e della formula vista nell'esercizio 9.17.

## Capitolo 10. Insiemi ordinati

Se  $A$  è un insieme e  $\rho$  è una relazione su  $A$ ,  $\rho$  si dice *antisimmetrica* se per ogni  $a, b \in A$ , da  $a \rho b$  e  $b \rho a$  segue che  $a = b$ . Una relazione  $\rho$  su  $A$  che sia riflessiva, antisimmetrica e transitiva si dice un *ordinamento parziale* (o un *ordine parziale* o un *semiordinamento*) su  $A$ .

ESEMPIO 1. Sia  $\mathbb{N}^*$  l'insieme dei numeri naturali positivi. Su  $\mathbb{N}^*$  definiamo la relazione  $\leq$  (si legge "la relazione minore o uguale") ponendo, per ogni  $x, y \in \mathbb{N}^*$ ,  $x \leq y$  se esiste  $z \in \mathbb{N}$  tale che  $x+z = y$ . La relazione  $\leq$  è quindi il solito modo con cui si considerano ordinati i numeri naturali positivi (e per questo motivo  $\leq$

è detto l'*ordinamento usuale* su  $\mathbb{N}^*$ ). La relazione  $\leq$  è un ordinamento parziale sull'insieme  $\mathbb{N}^*$  nel senso da noi appena definito in quanto:

- (1)  $\leq$  è riflessiva (perché per ogni  $x \in \mathbb{N}^*$  si ha  $x \leq x$ );
- (2)  $\leq$  è antisimmetrica (perché se  $x, y \in \mathbb{N}^*$ ,  $x \leq y$  e  $y \leq x$ , allora  $x = y$ );
- (3)  $\leq$  è transitiva (perché se  $x, y, z \in \mathbb{N}^*$ ,  $x \leq y$  e  $y \leq z$ , allora  $x \leq z$ ).  $\square$

ESEMPIO 2. Sia ancora  $\mathbb{N}^*$  l'insieme dei numeri naturali positivi. Su  $\mathbb{N}^*$  definiamo la relazione  $|$  (si legge "la relazione divide") ponendo, per ogni  $x, y \in \mathbb{N}^*$ ,  $x | y$  se esiste  $a \in \mathbb{Z}$  tale che  $xa = y$ . La relazione  $|$  è un ordinamento parziale sull'insieme  $\mathbb{N}^*$  in quanto:

- (1)  $|$  è riflessiva (perché per ogni  $x \in \mathbb{N}^*$  si ha  $x \cdot 1 = x$  e quindi  $x | x$ ).
- (2)  $|$  è antisimmetrica (perché se  $x, y \in \mathbb{N}^*$ ,  $x | y$  e  $y | x$ , allora esistono  $a, b \in \mathbb{Z}$  tali che  $xa = y$  e  $yb = x$ . Ne segue che  $a > 0$ ,  $b > 0$  e  $y = xa = yba$ ; essendo  $y \neq 0$ , se ne ricava che  $1 = ba$ , e quindi  $a = b = 1$ . Pertanto  $x = y$ ).
- (3)  $|$  è transitiva (perché se  $x, y, z \in \mathbb{N}^*$ ,  $x | y$  e  $y | z$ , esistono  $a, b \in \mathbb{Z}$  tali che  $xa = y$  e  $yb = z$ . Ne segue che  $xab = yb = z$  e  $ab \in \mathbb{Z}$ , e pertanto  $x | z$ ).  $\square$

ESEMPIO 3. Sempre sull'insieme  $\mathbb{N}^*$  definiamo ora una relazione  $\rho$  ponendo, per ogni  $x, y \in \mathbb{N}^*$ ,  $x \rho y$  se  $\frac{1}{x} \leq \frac{1}{y}$ . Anche questa relazione  $\rho$  è un ordinamento parziale su  $\mathbb{N}^*$  in quanto:

- (1)  $\rho$  è riflessiva (perché per ogni  $x \in \mathbb{N}^*$  si ha  $\frac{1}{x} \leq \frac{1}{x}$  e quindi  $x \rho x$ ).
- (2)  $\rho$  è antisimmetrica (perché se  $x, y \in \mathbb{N}^*$ ,  $x \rho y$  e  $y \rho x$ , allora  $\frac{1}{x} \leq \frac{1}{y}$  e  $\frac{1}{y} \leq \frac{1}{x}$ ; ne segue che  $\frac{1}{x} = \frac{1}{y}$  e pertanto  $x = y$ ).
- (3)  $\rho$  è transitiva (perché se  $x, y, z \in \mathbb{N}^*$ ,  $x \rho y$  e  $y \rho z$ , allora  $\frac{1}{x} \leq \frac{1}{y}$  e  $\frac{1}{y} \leq \frac{1}{z}$ , e quindi  $\frac{1}{x} \leq \frac{1}{z}$ . Ne segue che  $x \rho z$ ).  $\square$

Un insieme  $A$  su cui è definito un ordinamento parziale  $\rho$  si dice un *insieme parzialmente ordinato*. Come mostrano gli esempi 1, 2 e 3, su uno stesso insieme  $A$  possono essere definiti vari ordinamenti parziali. Per indicare che si sta studiando un insieme ordinato  $A$  dotato di un certo ordinamento parziale  $\rho$  indicheremo talvolta tale insieme ordinato come  $(A, \rho)$ . Quindi nell'esempio 1 abiteremo considerato l'insieme parzialmente ordinato  $(\mathbb{N}^*, \leq)$ , nell'esempio 2 l'insieme parzialmente ordinato  $(\mathbb{N}^*, |)$ , nell'esempio 3 l'insieme parzialmente ordinato  $(\mathbb{N}^*, \rho)$ . Quando però sarà ben chiaro quale ordinamento  $\rho$  si sta considerando su un insieme  $A$ , continueremo a dire che  $A$  è un insieme parzialmente ordinato invece di specificare che  $(A, \rho)$  è l'insieme parzialmente ordinato, sottintendendo così l'ordinamento  $\rho$ .



dice un *minorante* di  $B$  se  $a \leq b$  per ogni  $b \in B$ , mentre si dice un *maggiorante* di  $B$  se  $a \geq b$  per ogni  $b \in B$ . Infine se  $B \subseteq A$  e  $a \in A$ ,  $a$  si dice l'*estremo inferiore* di  $B$  se  $a \geq b$  per ogni  $b \in B$ . Quindi  $a$  è l'estremo inferiore di  $B$  se  $a$  è il massimo dei minoranti di  $B$ ; quindi  $a$  è l'estremo inferiore di  $B$  se e solo se  $a$  è un minorante di  $B$  e per ogni minorante  $a' \in A$  di  $B$  si ha  $a' \leq a$ . Pertanto  $a$  è l'estremo inferiore di  $B$  se e solo se (1)  $a \leq b$  per ogni  $b \in B$  e (2) per ogni  $a' \in A$  con la proprietà che  $a' \leq b$  per tutti i  $b \in B$  si ha  $a' \leq a$ . Analogamente se  $B \subseteq A$  e  $a \in A$ , l'elemento  $a$  si dice l'*estremo superiore* di  $B$  se e solo se  $a$  è il minimo dei maggioranti di  $B$ ; quindi  $a$  è l'estremo superiore di  $B$  se e solo se (1)  $a \geq b$  per tutti i  $b \in B$  e (2) per ogni  $a' \in A$  con la proprietà che  $a' \geq b$  per tutti i  $b \in B$  si ha  $a' \geq a$ .

ESEMPIO 7. Sia  $(N^*, |)$  l'insieme parzialmente ordinato che abbiamo già considerato nell'esempio 2. Allora  $N^*$  ha un minimo (il numero 1, in quanto  $1 \mid n$  per ogni  $n \in N^*$ ), e non ha massimo (perché non esiste nessun  $n_0 \in N^*$  tale che per ogni  $n \in N^*$ ,  $n \mid n_0$ ). Inoltre 1 è un elemento minimale di  $N^*$  (perché se  $n \mid n_0$  per ogni  $n \in N^*$ ), mentre  $N^*$  non ha elementi massimali (perché per  $n \in N^*$  e  $n \mid 1$ , allora  $n = 1$ ), mentre  $N^*$  non ha elementi massimali (perché per  $n \in N^*$  esiste  $n_1 \in N^*$  tale che  $n_0 \mid n_1$  e  $n_0 \neq n_1$ ). Cerchiamo l'estremo inferiore in  $N^*$  dell'insieme  $P^+ = \{2t \mid t \in N^*\}$  dei numeri pari positivi: i minoranti di  $P^+$  in  $N^*$  sono i numeri  $n \in N^*$  che dividono tutti i numeri pari, e quindi sono solo 1 e 2. Nell'insieme  $\{1, 2\}$  il numero 2 è il massimo perché  $1 \mid 2$ . Quindi 2 è l'estremo inferiore di  $P^+$  in  $N^*$ . Invece non esistono  $n \in N^*$  che sono divisi da tutti gli elementi di  $P^+$ ; pertanto  $P^+$  non ha maggioranti in  $N^*$ , e quindi, a maggior ragione,  $P^+$  non ha un estremo superiore in  $N^*$ .

Sia ora  $D_{>1} = \{2t+1 \mid t \in N^*\}$  l'insieme dei numeri dispari maggiori di 1, sia  $A = D_{>1} \cup \{2\}$ , e supponiamo che  $A$  abbia l'ordine indotto da  $(N^*, |)$ . Mostriamo che  $A$  ha esattamente un elemento massimale ma che  $A$  non ha massimo. Intanto 2 è un elemento massimale di  $A$ , perché se  $x \in A$  e  $2 \mid x$  allora  $x = 2$ . Invece gli elementi di  $D_{>1}$  non sono elementi massimali di  $A$ , perché per ogni  $n \in D_{>1}$  si ha  $n \mid n^2$  e  $n \neq n^2$ . Quindi 2 è l'unico elemento massimale di  $A$ . Mostriamo che  $A$  non ha massimo: il massimo di  $A$  dovrebbe essere un numero diviso da 2 e da tutti i numeri dispari maggiori di 1. Dato che non esiste un elemento  $n \in A$  con questa proprietà,  $A$  non ha massimo.

Cerchiamo l'estremo inferiore di  $A$  in  $N^*$ . I minoranti di  $A$  in  $N^*$  sono gli  $n \in N^*$  che dividono tutti gli elementi di  $A$ . Poiché solo  $n = 1$  ha questa proprietà, ne segue che 1 è l'unico minorante di  $A$  in  $N^*$ . In particolare 1 è l'estremo inferiore di  $A$  in  $N^*$ . □

Un insieme parzialmente ordinato  $(A, \leq)$  può essere talvolta rappresentato in un piano nel modo seguente: gli elementi di  $A$  vengono rappresentati da punti del piano; se  $x, y \in A$ , si disegna una linea spezzata dal punto che rappresenta  $x$  al punto che rappresenta  $y$  dal basso verso l'alto se e solo se  $x \leq y$ .

ESEMPIO 8. Si considerino gli insiemi parzialmente ordinati rappresentati nella figura 10.1:

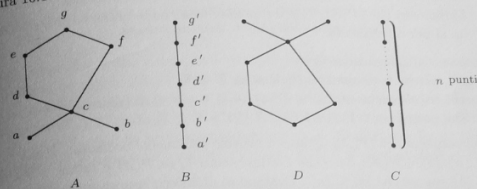


Figura 10.1

Nell'insieme parzialmente ordinato  $A$  si ha  $a \leq c, c \leq e, e \leq g$ . Invece  $a \not\leq b$  e  $d \not\leq f$ , perché non c'è una linea spezzata dal basso verso l'alto dal punto che rappresenta  $a$  al punto che rappresenta  $b$ , né dal punto che rappresenta  $d$  al punto che rappresenta  $f$ .

Si noti che  $A$  non è totalmente ordinato (perché ad esempio  $a \not\leq b$  e  $b \not\leq a$ ), mentre l'ordine su  $B$  è totale. L'insieme parzialmente ordinato  $C$  è l'insieme  $A$  dotato dell'ordine parziale inverso dell'ordinamento di  $A$ .

A proposito di ordini totali su insiemi finiti si noti che dato un qualunque insieme totalmente ordinato con  $n$  elementi, il diagramma che lo rappresenta dovrà essere costituito da  $n$  punti allineati verticalmente, cioè dovrà essere il diagramma dell'insieme parzialmente ordinato  $D$ . Quindi tutti gli insiemi totalmente ordinati con  $n$  elementi sono isomorfi a  $D$ . Ne segue che due insiemi totalmente ordinati finiti sono isomorfi se e solo se sono equipotenti. □

Un insieme parzialmente ordinato  $A$  si dice *bene ordinato* se ogni sottoinsieme non vuoto di  $A$  ha minimo. Ad esempio  $N$  con l'ordine usuale è un insieme parzialmente ordinato, mentre  $Z, Q$  ed  $R$  con gli ordinamenti usuali non sono bene ordinati (perché, ad esempio, non hanno minimo). Ogni sottoinsieme ordinato di un insieme bene ordinato è bene ordinato. Ogni insieme bene ordinato è totalmente ordinato (perché se  $A$  è un insieme bene ordinato e  $a, b \in A$  il sottoinsieme  $\{a, b\}$  di  $A$  ha minimo; se tale minimo è  $a$ , allora  $a \leq b$ ; se invece il minimo è  $b$ , allora  $b \leq a$ . Quindi  $A$  è totalmente ordinato.)

### Esercizi svolti

10.1. Siano  $A$  un insieme e  $\mathcal{P}(A)$  l'insieme delle parti di  $A$ . Se  $X, Y \in \mathcal{P}(A)$ , scrivendo come di consueto  $X \subseteq Y$  se  $X$  è sottoinsieme di  $Y$ , resta definita una



relazione  $\subseteq$  nell'insieme  $\mathcal{P}(A)$ .

- (a) Si dimostri che  $(\mathcal{P}(A), \subseteq)$  è un insieme parzialmente ordinato.  
 (b) Si dimostri che  $(\mathcal{P}(A), \subseteq)$  è un insieme totalmente ordinato se e solo se  $A$  ha al più un elemento.

**Soluzione.** (a) La relazione  $\subseteq$  è riflessiva, perché per ogni  $X \in \mathcal{P}(A)$  si ha  $X \subseteq X$ ; è transitiva, perché se  $X, Y, Z \in \mathcal{P}(A)$ ,  $X \subseteq Y$  e  $Y \subseteq Z$ , allora  $X \subseteq Z$ .  
 (b) Supponiamo che  $(\mathcal{P}(A), \subseteq)$  sia un insieme totalmente ordinato. Se  $a, b \in A$ , allora  $\{a\}, \{b\} \in \mathcal{P}(A)$ ; dato che l'ordinamento  $\subseteq$  su  $\mathcal{P}(A)$  è totale, si ha che  $\{a\} \subseteq \{b\}$  oppure che  $\{b\} \subseteq \{a\}$ . Trattandosi di insiemi con un solo elemento, in entrambi i casi si ha che  $\{a\} = \{b\}$ , e pertanto se ne conclude che  $a = b$ . Questo dimostra che  $A$  ha al più un elemento.

Viceversa, supponiamo che  $A$  abbia al più un elemento. Se  $A$  è l'insieme vuoto allora  $\mathcal{P}(A) = \{\emptyset\}$  ha esattamente un elemento, e quindi è certamente totalmente ordinato dalla relazione  $\subseteq$ . Se invece  $A$  ha esattamente un elemento, allora  $\mathcal{P}(A) = \{\emptyset, X\}$ , e si ha  $\emptyset \subseteq A$ . Quindi anche in questo caso  $\mathcal{P}(A)$  è un insieme totalmente ordinato dalla relazione  $\subseteq$ .  $\square$

**10.2.** Sia  $(A, \leq)$  un insieme parzialmente ordinato. Si provi che se  $A$  ha un minimo, allora tale minimo è unico.

**Soluzione.** Se  $a, a' \in A$  sono entrambi minimi di  $A$ , allora  $a \leq a'$  perché  $a$  è un minimo di  $A$ , e  $a' \leq a$  perché  $a'$  è un minimo di  $A$ . Dall'antisimmetria della relazione  $\leq$  si deduce che  $a = a'$ .  $\square$

**10.3.** Sia  $(A, \leq)$  un insieme parzialmente ordinato. Si dimostri che se un sottoinsieme  $B$  di  $A$  ha un estremo superiore in  $A$ , allora tale estremo superiore è unico.

**Soluzione.** Sia  $M$  l'insieme dei maggioranti di  $B$  in  $A$ . Un estremo superiore di  $B$  in  $A$  è per definizione un minimo di  $M$ . Per l'esercizio 10.2 il minimo di  $M$ , se esiste, è unico. Quindi l'estremo superiore di  $B$  in  $A$ , se esiste, è unico.  $\square$

### Altri esercizi

**10.4.** Nell'insieme  $\mathbb{N} \times \mathbb{N}$  si definisca, per ogni  $(a, b), (a', b') \in \mathbb{N} \times \mathbb{N}$ ,

$$(a, b) \preceq (a', b') \quad \text{se} \quad \frac{2^a 3^b}{2^{a'} 3^{b'}} \leq 1.$$

Si dimostri che:

- (a) la relazione  $\preceq$  è un ordinamento totale su  $\mathbb{N} \times \mathbb{N}$ ;

- (b) l'applicazione  $\varphi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  definita da  $\varphi(a, b) = 2^a 3^b$  per ogni  $(a, b) \in \mathbb{N} \times \mathbb{N}$  è iniettiva;  
 (c) l'applicazione  $\varphi$  è un omomorfismo di insiemi ordinati di  $(\mathbb{N} \times \mathbb{N}, \preceq)$  nell'insieme  $\mathbb{N}$  dei numeri naturali dotato dell'ordine usuale  $\leq$ .

**10.5.** Siano  $A$  e  $B$  due insiemi non vuoti. Si consideri l'insieme  $\mathcal{F}$  i cui elementi sono tutte le coppie  $(X, f)$  dove  $X$  è un sottoinsieme di  $A$  ed  $f: X \rightarrow B$  è un'applicazione. Si definisca una relazione  $\leq$  su  $\mathcal{F}$  ponendo, se  $(X, f)$  e  $(Y, g)$  sono elementi di  $\mathcal{F}$ ,  $(X, f) \leq (Y, g)$  se  $X \subseteq Y$  ed  $f(x) = g(x)$  per ogni  $x \in X$ . Si dimostri che  $\leq$  è un ordinamento parziale su  $\mathcal{F}$ . Si dimostri che gli elementi massimali di  $\mathcal{F}$  sono tutti e soli gli elementi  $(X, f) \in \mathcal{F}$  per i quali  $X = A$ .

**10.6.** Si dia un esempio di un insieme totalmente ordinato  $A$  avente un elemento  $a$  con la seguente proprietà: l'insieme totalmente ordinato  $A$  ha minimo ma il suo sottoinsieme ordinato  $A \setminus \{a\}$  non ha minimo.

**10.7.** Nell'esempio 8 abbiamo fatto osservare che due insiemi finiti totalmente ordinati sono isomorfi se e solo se sono equipotenti. Questo non vale per gli insiemi totalmente ordinati infiniti. Si dimostri infatti che:

- (a) Gli insiemi totalmente ordinati  $(\mathbb{N}, \leq)$  e  $(\mathbb{Z}, \leq)$  con i loro ordinamenti usuali non sono isomorfi, ma  $\mathbb{N}$  e  $\mathbb{Z}$  sono equipotenti.  
 (b) Se  $A = \left\{ \frac{1}{z} \mid z \in \mathbb{Z}, z \neq 0 \right\} \subseteq \mathbb{R}$  è ordinato dall'ordinamento indotto dall'ordinamento usuale di  $\mathbb{R}$ , allora  $A$  è equipotente sia a  $\mathbb{N}$  che a  $\mathbb{Z}$ , ma non è isomorfo né a  $(\mathbb{N}, \leq)$  né a  $(\mathbb{Z}, \leq)$ .  
 (c) Il lettore trovi un quarto esempio di un insieme totalmente ordinato numerabile che non sia isomorfo né a  $\mathbb{N}$ , né a  $\mathbb{Z}$ , né ad  $A$ .

**10.8.** Siano  $A$  e  $B$  gli insiemi parzialmente ordinati rappresentati nella figura 10.1. Si dimostrino i fatti seguenti (qui alcune delle cose da provare si dimostrano semplicemente dando un'occhiata ai diagrammi di  $A$  e di  $B$ ):

- (a) l'applicazione  $\varphi: A \rightarrow B$  definita da  $\varphi(a) = a'$ ,  $\varphi(b) = b'$ ,  $\varphi(c) = c'$ ,  $\varphi(d) = d'$ ,  $\varphi(e) = e'$ ,  $\varphi(f) = f'$ ,  $\varphi(g) = g'$  è un omomorfismo di insiemi ordinati, ma non è un isomorfismo;  
 (b) il sottoinsieme  $\{a, b, c\}$  di  $A$  con l'ordine indotto dall'ordine di  $A$  non è totalmente ordinato;  
 (c) il sottoinsieme  $\{a, c, d\}$  di  $A$  con l'ordine indotto dall'ordine di  $A$  è totalmente ordinato;  
 (d) l'elemento  $g$  è il massimo di  $A$ , mentre  $A$  non ha minimo;  
 (e) l'unico elemento massimale di  $A$  è  $g$ , gli elementi minimali di  $A$  sono  $a$  e  $b$ ;  
 (f) in  $A$  i maggioranti del sottoinsieme  $\{a, b, c\}$  di  $A$  sono  $c, d, e, f, g$ ; non esistono invece minoranti di  $\{a, b, c\}$  in  $A$ ;

- (g) il sottoinsieme  $\{c, d, e, f, g\}$  di  $A$  ha minimo e tale minimo è  $c$ . Quindi  $c$  è l'estremo superiore di  $\{a, b, c\}$  in  $A$ . Invece non esiste l'estremo inferiore di  $\{a, b, c\}$  in  $A$ .
- (h) l'estremo superiore di  $\{c, d, e, f\}$  in  $A$  è  $g$ ; l'estremo inferiore è  $c$ .

10.9. Sia  $(\mathcal{F}, \leq)$  l'insieme parzialmente ordinato dell'esercizio 10.5 e sia  $\mathcal{G}$  un sottoinsieme di  $\mathcal{F}$ .

- (a) Si dimostri che se esiste un maggiorante di  $\mathcal{G}$  in  $\mathcal{F}$ , allora per ogni  $(X, f), (Y, g) \in \mathcal{G}$  e ogni  $a \in X \cap Y$  si ha  $f(a) = g(a)$ .
- (b) Si supponga ora che per ogni  $(X, f), (Y, g) \in \mathcal{G}$  e ogni  $a \in X \cap Y$  si abbia  $f(a) = g(a)$ . Sia

$$S = \bigcup_{(X, f) \in \mathcal{G}} X$$

e si definisca un'applicazione  $\varphi: S \rightarrow B$  nel modo seguente: per ogni  $a \in S$  se  $(X, f) \in \mathcal{G}$  è una coppia tale che  $a \in X$  si ponga  $\varphi(a) = f(a)$ . Si dimostri che l'applicazione  $\varphi$  è ben definita, e che la coppia  $(S, \varphi)$  è l'estremo superiore di  $\mathcal{G}$  in  $\mathcal{F}$ .

- (c) Se ne concluda che esiste un maggiorante di  $\mathcal{G}$  in  $\mathcal{F}$  se e solo se per ogni  $(X, f), (Y, g) \in \mathcal{G}$  e ogni  $a \in X \cap Y$  si ha  $f(a) = g(a)$ .

10.10. Siano  $X$  un insieme e  $Y$  un suo sottoinsieme avente almeno due elementi distinti. Si consideri l'insieme parzialmente ordinato  $(\mathcal{P}(X), \subseteq)$  e si ponga  $B = \{y \mid y \in Y\} \subseteq \mathcal{P}(X)$ . Si fissi poi un elemento  $Z$  di  $\mathcal{P}(X)$ .

- (a) Si dimostri che  $Z$  è un maggiorante di  $B$  se e solo se  $Y \subseteq Z$ .
- (b) Si dimostri che  $Z$  è un minorante di  $B$  se e solo se  $Z = \emptyset$ .
- (c) Si dica se esistono, e in caso affermativo si calcolino, l'estremo inferiore e l'estremo superiore di  $B$  in  $\mathcal{P}(X)$ .

10.11. Sia  $\mathbb{N}$  l'insieme dei numeri naturali e  $P = \mathcal{P}(\mathbb{N})$  l'insieme delle parti di  $\mathbb{N}$  parzialmente ordinato dall'inclusione  $\subseteq$ . Si consideri il sottoinsieme

$$A = \{X \mid X \in P, |X| \geq 2\}$$

di  $P$ .

- (a) Si calcolino, se esistono, il massimo, il minimo, gli elementi massimali e gli elementi minimali del sottoinsieme ordinato  $A$  di  $P$ .
- (b) Si consideri il sottoinsieme  $B = \{N \setminus \{n\} \mid n \in \mathbb{N}\}$  di  $A$ . Si calcolino, se esistono, l'estremo inferiore e l'estremo superiore di  $B$  in  $A$ .

## Capitolo 11. Reticoli

Un insieme parzialmente ordinato  $(L, \leq)$  si dice un *reticolo* se per ogni  $x, y \in L$  il sottoinsieme  $\{x, y\}$  di  $L$  ha estremi inferiore e superiore in  $L$ . Si è visto nell'esercizio 10.3 che l'estremo superiore, se esiste, è unico, e lo stesso avviene per l'estremo inferiore. Se  $x, y$  sono elementi di un insieme parzialmente ordinato denotiamo l'estremo inferiore di  $\{x, y\}$  con  $x \wedge y$ , e l'estremo superiore di  $\{x, y\}$  con  $x \vee y$ . Ricordando le definizioni di estremo superiore ed inferiore, si ha quindi che un insieme parzialmente ordinato  $(L, \leq)$  è un reticolo se e solo se per ogni  $x, y \in L$  esistono due elementi  $x \vee y, x \wedge y \in L$  tali che:

- (1)  $x \leq x \vee y, y \leq x \vee y$ ;
- (2) se  $z \in L, x \leq z$  e  $y \leq z$ , allora  $x \vee y \leq z$ ;
- (3)  $x \wedge y \leq x, x \wedge y \leq y$ ;
- (4) se  $z \in L, z \leq x$  e  $z \leq y$ , allora  $z \leq x \wedge y$ .

ESEMPIO 1. Dimostriamo che se  $x, y$  sono elementi di un insieme parzialmente ordinato  $A$ , le seguenti affermazioni sono equivalenti:

- (a)  $x \wedge y = x$ ;
- (b)  $x \leq y$ ;
- (c)  $x \vee y = y$ .

(a)  $\Rightarrow$  (b) Dato che si ha sempre  $x \wedge y \leq y$ , dalla (a) segue che  $x \leq y$ .

(b)  $\Rightarrow$  (a) Per dimostrare che  $x \wedge y = x$  si deve far vedere che  $x \leq x$ , che  $x \leq y$ , e che se  $z \in A, x \leq z$  e  $y \leq z$ , allora  $x \leq z$ . Queste tre condizioni sono tutte evidentemente verificate sotto l'ipotesi (b).

(b)  $\Rightarrow$  (c) Per dimostrare che  $x \vee y = y$  si deve far vedere che  $x \leq y$ , che  $y \leq y$ , e che se  $z \in A, x \leq z$  e  $y \leq z$ , allora  $y \leq z$ . Queste tre condizioni sono tutte evidentemente verificate sotto l'ipotesi (b).

(c)  $\Rightarrow$  (b) Dato che si ha sempre  $x \leq x \vee y$ , dalla (c) segue che  $x \leq y$ .  $\square$

PROPOSIZIONE 11.1. Se  $(L, \leq)$  è un reticolo e  $x, y, z \in L$  allora

- (a)  $x \vee y = y \vee x, \quad x \wedge y = y \wedge x$ ;
- (b)  $x \vee (y \vee z) = (x \vee y) \vee z, \quad x \wedge (y \wedge z) = (x \wedge y) \wedge z$ ;

$$(c) \quad x \vee (x \wedge y) = x,$$

$$x \wedge (x \vee y) = x.$$

ESEMPIO 2. Se  $A$  è un insieme, mostriamo che l'insieme parzialmente ordinato  $(\mathcal{P}(A), \subseteq)$  dell'esercizio 10.1 è un reticolo. In questo caso per ogni  $X, Y \in \mathcal{P}(A)$  si ha, come dimostreremo ora,  $X \vee Y = X \cup Y$  e  $X \wedge Y = X \cap Y$ .

Dobbiamo far vedere che in  $\mathcal{P}(A)$  per l'unione e l'intersezione valgono le quattro condizioni (1), (2), (3) e (4) enunciate prima dell'esempio 1. Per ogni  $X, Y \in \mathcal{P}(A)$  si ha:

- (1)  $X \subseteq X \cup Y$  e  $Y \subseteq X \cup Y$ ;
- (2) se  $Z \in \mathcal{P}(X)$ ,  $X \subseteq Z$  e  $Y \subseteq Z$ , allora  $X \cup Y \subseteq Z$ ;
- (3)  $X \cap Y \subseteq X$  e  $X \cap Y \subseteq Y$ ;
- (4) se  $Z \in \mathcal{P}(X)$ ,  $Z \subseteq X$  e  $Z \subseteq Y$ , allora  $Z \subseteq X \cap Y$ .  $\square$

ESEMPIO 3. Sia  $\mathbb{R}^{\mathbb{R}}$  l'insieme di tutte le applicazioni di  $\mathbb{R}$  in  $\mathbb{R}$ . Nell'insieme  $\mathbb{R}^{\mathbb{R}}$  si definisca una relazione  $\preceq$  ponendo, per ogni  $f, g \in \mathbb{R}^{\mathbb{R}}$ ,  $f \preceq g$  se  $f(x) \leq g(x)$  per ogni  $x \in \mathbb{R}$ . Allora  $\preceq$  è un ordinamento parziale su  $\mathbb{R}^{\mathbb{R}}$  in quanto:

- (1)  $\preceq$  è riflessiva (perché per ogni  $f \in \mathbb{R}^{\mathbb{R}}$  e per ogni  $x \in \mathbb{R}$  si ha  $f(x) \leq f(x)$ , e quindi  $f \preceq f$  per ogni  $f \in \mathbb{R}^{\mathbb{R}}$ );
- (2)  $\preceq$  è antisimmetrica (perché se  $f, g \in \mathbb{R}^{\mathbb{R}}$ ,  $f \preceq g$  e  $g \preceq f$ , allora  $f(x) \leq g(x)$  e  $g(x) \leq f(x)$  per ogni  $x \in \mathbb{R}$ ; ne segue che  $f(x) = g(x)$  per ogni  $x \in \mathbb{R}$ , e quindi  $f = g$ );
- (3)  $\preceq$  è transitiva (perché se  $f, g, h \in \mathbb{R}^{\mathbb{R}}$ ,  $f \preceq g$  e  $g \preceq h$ , allora  $f(x) \leq g(x)$  e  $g(x) \leq h(x)$  per ogni  $x \in \mathbb{R}$ ; ne segue che  $f(x) \leq h(x)$  per ogni  $x \in \mathbb{R}$ , e pertanto  $f \preceq h$ ).

Denotiamo, se  $a, b \in \mathbb{R}$ , con  $\max\{a, b\}$  e  $\min\{a, b\}$  il maggiore e il minore tra i due numeri reali  $a$  e  $b$  rispettivamente. Se poi  $f, g \in \mathbb{R}^{\mathbb{R}}$ , denotiamo con  $f \vee g: \mathbb{R} \rightarrow \mathbb{R}$  e  $f \wedge g: \mathbb{R} \rightarrow \mathbb{R}$  le due applicazioni definite, per ogni  $x \in \mathbb{R}$ , da

$$(f \vee g)(x) = \max\{f(x), g(x)\} \quad \text{e} \quad (f \wedge g)(x) = \min\{f(x), g(x)\}$$

rispettivamente. Il lettore verifichi che le applicazioni  $f \vee g$  e  $f \wedge g$  così definite sono proprio gli estremi superiore e inferiore del sottoinsieme  $\{f, g\}$  dell'insieme parzialmente ordinato  $(\mathbb{R}^{\mathbb{R}}, \preceq)$ . Quindi  $(\mathbb{R}^{\mathbb{R}}, \preceq)$  è un reticolo.  $\square$

ESEMPIO 4. Sia  $\mathcal{P}_{\infty}(\mathbb{Z})$  l'insieme di tutti i sottoinsiemi infiniti di  $\mathbb{Z}$ . Ad esempio se  $P = \{2z \mid z \in \mathbb{Z}\}$  e  $D = \{2z+1 \mid z \in \mathbb{Z}\}$  sono gli insiemi dei numeri interi pari e dispari rispettivamente, allora  $P \in \mathcal{P}_{\infty}(\mathbb{Z})$  e  $D \in \mathcal{P}_{\infty}(\mathbb{Z})$ , mentre  $\emptyset \notin \mathcal{P}_{\infty}(\mathbb{Z})$ . Si ordini parzialmente  $\mathcal{P}_{\infty}(\mathbb{Z})$  mediante l'inclusione  $\subseteq$ . In tal modo  $\mathcal{P}_{\infty}(\mathbb{Z})$  risulta essere un sottoinsieme ordinato dell'insieme  $(\mathcal{P}(\mathbb{Z}), \subseteq)$ . Ma  $\mathcal{P}_{\infty}(\mathbb{Z})$  non è un reticolo, perché, ad esempio, in  $\mathcal{P}_{\infty}(\mathbb{Z})$  non esiste  $P \wedge D$ . Cerchiamo infatti l'estremo inferiore di  $\{P, D\}$  in  $\mathcal{P}_{\infty}(\mathbb{Z})$ : i minoranti di  $\{P, D\}$  in  $\mathcal{P}_{\infty}(\mathbb{Z})$  sono i sottoinsiemi infiniti di  $\mathbb{Z}$  che sono contenuti sia in  $P$  che in  $D$ . Dato che non

esistono sottoinsiemi infiniti contenuti sia in  $P$  che in  $D$ , se ne deduce che l'estremo inferiore di  $\{P, D\}$  in  $(\mathcal{P}_{\infty}(\mathbb{Z}), \subseteq)$  non esiste. Quindi l'insieme parzialmente ordinato  $(\mathcal{P}_{\infty}(\mathbb{Z}), \subseteq)$  non è un reticolo.  $\square$

ESEMPIO 5. Ogni insieme totalmente ordinato è un reticolo, in quanto se  $x, y \in A$  e  $(A, \leq)$  è totalmente ordinato, allora o  $x \leq y$  oppure  $x \geq y$ . Se  $x \leq y$ , per l'esempio 1 si ha  $x \wedge y = x$  e  $x \vee y = y$ . Se invece  $x \geq y$ , allora  $x \wedge y = y$  e  $x \vee y = x$ .  $\square$

Se  $A$  è un enunciato sui reticoli, l'enunciato duale  $A^*$  di  $A$  si ottiene da  $A$  scambiando  $\leq$  con  $\geq$ ,  $\wedge$  con  $\vee$  e  $\vee$  con  $\wedge$ .

ESEMPIO 6. Se  $A$  è l'enunciato "Per ogni  $x \in L$  esiste  $y \in L$  tale che  $x \leq y$ ", il suo duale  $A^*$  è l'enunciato "Per ogni  $x \in L$  esiste  $y \in L$  tale che  $x \geq y$ ".

Se  $B$  è l'enunciato "Se  $x \in L$ , allora per ogni  $y \in L$  si ha  $x \leq y$  oppure  $x \wedge y \neq x$ ", il suo duale  $B^*$  è l'enunciato "Se  $x \in L$ , allora per ogni  $y \in L$  si ha  $x \geq y$  oppure  $x \vee y \neq x$ ".

Se  $C$  è l'enunciato "Se  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$  per ogni  $x, y, z \in L$ , allora  $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$  per ogni  $x, y, z \in L$ ", il suo duale  $C^*$  è l'enunciato "Se  $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$  per ogni  $x, y, z \in L$ , allora  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$  per ogni  $x, y, z \in L$ ".

Se  $D$  è l'enunciato "Per ogni  $x, y \in L$  si ha  $x \wedge y = y \wedge x$  e  $x \vee y = y \vee x$ ", allora il suo duale  $D^*$  è l'enunciato "Per ogni  $x, y \in L$  si ha  $x \vee y = y \vee x$  e  $x \wedge y = y \wedge x$ ". In questo caso si noti come  $D$  si possa considerare equivalente a  $D^*$ , ossia come  $D$  sia essenzialmente un enunciato "autoduale".

Se  $E$  è l'enunciato "Per ogni  $x, y \in L$  si ha  $x \leq y$  oppure  $x \geq y$ ", allora il suo duale  $E^*$  è l'enunciato "Per ogni  $x, y \in L$  si ha  $x \geq y$  oppure  $x \leq y$ ".  $\square$

Vale il

PRINCIPIO DI DUALITÀ PER I RETICOLI. Se  $A$  è un enunciato vero per ogni reticolo, allora anche il suo enunciato duale  $A^*$  è vero per ogni reticolo.

ESEMPIO 7. Siano  $A, B, C, D, E$  gli enunciati dell'esempio 6. Allora:  $A$  è vero in ogni reticolo (basta prendere come  $y$  lo stesso elemento  $x$ ), e quindi anche  $A^*$  è vero in ogni reticolo per il principio di dualità dei reticoli; l'enunciato  $B$  è vero in ogni reticolo (perché  $x \wedge y \neq x$  equivale a  $x \not\leq y$  in base a quanto abbiamo dimostrato nell'esempio 1), e quindi anche  $B^*$  è vero per il principio di dualità dei reticoli; nella proposizione 11.2 vedremo che  $C$  è vero in ogni reticolo, e quindi il suo duale  $C^*$  è vero. Anche  $D$  è vero in ogni reticolo (proposizione 11.1), e quindi  $D^*$  è vero in ogni reticolo, ma questo è evidente perché  $D$  è autoduale. Invece  $E$  non è vero in ogni reticolo, ma solo per gli insiemi totalmente ordinati.  $\square$

ESEMPIO 8. Attenzione: è errato enunciare il principio di dualità per i reticoli nel modo seguente: "Se  $A$  è un enunciato vero per un reticolo  $L$ , allora anche il suo enunciato duale  $A^*$  è vero per il reticolo  $L$ ". Che questo non sia vero si vede ad esempio considerando l'enunciato "Esiste  $x \in L$  tale che  $x \leq y$  per ogni  $y \in L$ ". Questo enunciato, che essenzialmente dice "In  $L$  c'è un minimo", è vero nel reticolo  $(\mathbb{N}, \leq)$ , mentre il suo duale, che è "Esiste  $x \in L$  tale che  $x \geq y$  per ogni  $y \in L$ " (cioè "In  $L$  c'è un massimo"), non è vero in  $(\mathbb{N}, \leq)$ .  $\square$

PROPOSIZIONE 11.2. Sia  $L$  un reticolo. Le seguenti affermazioni sono equivalenti:

- (a)  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$  per ogni  $a, b, c \in L$ ;
- (b)  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$  per ogni  $a, b, c \in L$ .

Un reticolo  $L$  si dice *distributivo* se soddisfa alle proprietà equivalenti della proposizione 11.2.

ESEMPIO 9. Sappiamo (vedi esempio 1 del capitolo 1) che se  $\cup$  e  $\cap$  denotano l'unione e l'intersezione di insiemi, allora valgono le proprietà distributive di  $\cup$  rispetto a  $\cap$  e di  $\cap$  rispetto a  $\cup$ . Quindi se  $A$  è un insieme, il reticolo  $(\mathcal{P}(A), \subseteq)$  dell'esempio 2 è un reticolo distributivo.  $\square$

ESEMPIO 10. Se  $N_5$  è l'insieme parzialmente ordinato disegnato nella figura 11.1, è possibile dimostrare che  $N_5$  è un reticolo. Però  $N_5$  non è distributivo perché  $a \wedge (b \vee c) = a \wedge e = a$ , mentre  $(a \wedge b) \vee (a \wedge c) = b \vee d = b$ .  $\square$

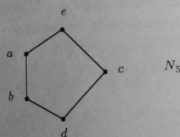


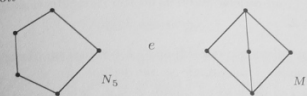
Figura 11.1

Sia  $(L, \leq)$  un reticolo. Un sottoinsieme  $L'$  di  $L$  si dice un *sottoreticolo* di  $L$  se  $x \vee y \in L'$  e  $x \wedge y \in L'$  per ogni  $x, y \in L'$ .

Siano  $(L, \leq)$  e  $(L', \leq)$  due reticoli. Un *omomorfismo di reticoli*  $\varphi$  di  $L$  in  $L'$  è un'applicazione  $\varphi: L \rightarrow L'$  tale che  $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$  e  $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$  per ogni  $x, y \in L$ . È facile dimostrare che ogni omomorfismo di reticoli è un omomorfismo di insiemi ordinati, e che non vale il viceversa, cioè che esistono omomorfismi di insiemi ordinati che non sono omomorfismi di reticoli (l'omomorfismo dell'esempio 4 del capitolo 10 è uno di questi). Un omomorfismo biiettivo di reticoli si dice un *isomorfismo di reticoli*, e un isomorfismo di un

reticolo  $L$  nello stesso reticolo  $L$  si dice un *automorfismo* di  $L$ . Si vede facilmente che un'applicazione tra due reticoli è un isomorfismo di reticoli se e solo se è un isomorfismo di insiemi parzialmente ordinati. Se esiste un isomorfismo di reticoli di  $L$  in  $L'$ , i reticoli  $L$  e  $L'$  si dicono *isomorfi*.

TEOREMA 11.3. Un reticolo è distributivo se e solo se non ha sottoreticoli isomorfi ai due reticoli



In un reticolo il minimo viene di solito indicato con il simbolo 0 e il massimo con il simbolo 1. Un reticolo si dice *limitato* se ha un massimo e un minimo. In un reticolo limitato  $L$  un elemento  $a$  si dice un *complemento* di un elemento  $b$  se  $a \vee b = 1$  e  $a \wedge b = 0$ . Un reticolo si dice *complementato* se è limitato ed ogni suo elemento ha almeno un complemento. Un reticolo si dice un *reticolo di Boole* se è complementato e distributivo.

ESEMPIO 11. Il reticolo  $(\mathbb{N}, \leq)$  ha minimo (il numero naturale 0), ma non ha massimo. Quindi non è un reticolo limitato.  $\square$

ESEMPIO 12. Il reticolo  $(\mathcal{P}(A), \subseteq)$  degli esempi 2 e 9 è un reticolo limitato perché ha un massimo (che è  $A$ ) e un minimo (l'insieme  $\emptyset$ ). Mostriamo che per ogni  $X \in \mathcal{P}(A)$  l'elemento  $A \setminus X$  di  $\mathcal{P}(A)$  è il complemento di  $X$  nel reticolo  $(\mathcal{P}(A), \subseteq)$ . Si deve dimostrare che  $X \vee (A \setminus X) = 1$  e  $X \wedge (A \setminus X) = 0$ . E infatti si ha che  $X \vee (A \setminus X) = X \cup (A \setminus X) = A = 1$  e  $X \wedge (A \setminus X) = X \cap (A \setminus X) = \emptyset = 0$ . Quindi  $(\mathcal{P}(A), \subseteq)$  è un reticolo complementato. Come abbiamo visto nell'esempio 9 tale reticolo è anche distributivo, e quindi  $(\mathcal{P}(A), \subseteq)$  è un reticolo di Boole.  $\square$

ESEMPIO 13. Consideriamo l'intervallo

$$[-1, 2] = \{x \mid x \in \mathbb{R}, -1 \leq x \leq 2\}$$

e denotiamo con  $\leq$  l'ordine usuale su  $[-1, 2]$ . L'insieme  $([-1, 2], \leq)$  è totalmente ordinato, e quindi come abbiamo visto nell'esempio 5 è un reticolo. Si tratta chiaramente di un reticolo limitato (il massimo è il numero reale 2 e il minimo è il numero reale -1) che non è complementato (gli unici suoi elementi che hanno un complemento sono i numeri -1 e 2).  $\square$

PROPOSIZIONE 11.4. Se in un reticolo distributivo e limitato un elemento ha un complemento, allora tale complemento è unico.

Dalla proposizione 11.4 segue che in un reticolo di Boole ogni elemento ha esattamente un complemento. Se  $L$  è un reticolo di Boole e  $x \in L$ , l'unico complemento di  $x$  viene di solito denotato con  $x'$ .

### Esercizi svolti

11.1. Siano  $(L, \leq)$  un reticolo e  $a \in L$  un suo elemento massimale. Si provi che  $a$  è il massimo di  $L$ .

*Soluzione.* Sia  $a$  un elemento massimale di  $L$  e si fissi un elemento  $x \in L$ . Allora  $x \vee a \geq a$ , ed essendo  $a$  massimale se ne deduce che  $x \vee a = a$ . Per quanto visto nell'esempio 1 si deve avere quindi  $x \leq a$ . Abbiamo così dimostrato che qualunque sia  $x \in L$  si ha  $x \leq a$ . Dunque  $a$  è il massimo di  $L$ .  $\square$

11.2. Si provi che se  $(L, \leq)$  è un reticolo limitato, allora  $0$  è l'unico complemento di  $1$  e  $1$  è l'unico complemento di  $0$ .

*Soluzione.* Mostriamo che  $0$  e  $1$  sono uno un complemento dell'altro. Si deve dimostrare che  $0 \vee 1 = 1$  e  $0 \wedge 1 = 0$ . Dato che  $0 \leq 1$ , queste uguaglianze seguono immediatamente da quanto visto nell'esempio 1.

Dimostriamo ora che  $0$  è l'unico complemento di  $1$  facendo vedere che se  $x \in L$  è un complemento di  $1$  allora  $x = 0$ . Se  $x \in L$  è un complemento di  $1$ , allora  $x \wedge 1 = 0$ . Ma  $1$  è il massimo di  $L$ , e quindi  $x \leq 1$ , e pertanto  $x \wedge 1 = x$  per l'esempio 1. Se ne deduce che  $x = x \wedge 1 = 0$ .

Per dimostrare che  $1$  è l'unico complemento di  $0$  si procede in modo analogo.  $\square$

11.3. (Formule di De Morgan per i reticoli booleani). Si dimostri che se  $a, b \in L$  ed  $(L, \leq)$  è un reticolo booleano allora  $(a \vee b)' = a' \wedge b'$  e  $(a \wedge b)' = a' \vee b'$ .

*Soluzione.* Per dimostrare che  $(a \vee b)' = a' \wedge b'$ , cioè che  $a' \wedge b'$  è il complemento di  $a \vee b$ , si deve far vedere che  $(a' \wedge b') \vee (a \vee b) = 1$  e  $(a' \wedge b') \wedge (a \vee b) = 0$ . Calcolando si ha

$$\begin{aligned} (a' \wedge b') \vee (a \vee b) &= && \text{per la proprietà distributiva} \\ = (a' \vee (a \vee b)) \wedge (b' \vee (a \vee b)) && \text{per le proprietà associativa} \\ = ((a' \vee a) \vee b) \wedge (a \vee (b' \vee b)) && \text{e commutativa (proposizione 11.1)} \\ = (1 \vee b) \wedge (a \vee 1) && \text{per la definizione di complemento} \\ = 1 \wedge 1 && \text{perché } b \leq 1 \text{ e } a \leq 1 \\ = 1 \end{aligned}$$

e analogamente

$$\begin{aligned} (a' \wedge b') \wedge (a \vee b) &= ((a' \wedge b') \wedge a) \vee ((a' \wedge b') \wedge b) = \\ &= ((a' \wedge a) \wedge b') \vee (a' \wedge (b' \wedge b)) = (0 \wedge b') \vee (a' \wedge 0) = 0 \vee 0 = 0. \end{aligned}$$

Questo dimostra la prima formula. Per la seconda si può procedere in modo analogo.  $\square$

### Altri esercizi

11.4. Si consideri la relazione di uguaglianza  $=$  su un insieme  $A$ .

- (a) Si provi che  $(A, =)$  è un insieme parzialmente ordinato.
- (b) Si dimostri che tutti gli elementi di  $(A, =)$  sono sia massimali che minimali.
- (c) Si provi che se  $A$  ha almeno due elementi, allora  $(A, =)$  non è un reticolo.

11.5. Si consideri l'insieme

$$A = \{\emptyset, \{1\}, \{2\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$$

parzialmente ordinato dall'inclusione  $\subseteq$ .

- (a) Si calcoli, se esiste, l'estremo inferiore del suo sottoinsieme

$$B = \{\{1, 2, 3\}, \{1, 2, 4\}\}.$$

- (b) Si dica se l'insieme parzialmente ordinato  $(A, \subseteq)$  è un reticolo.

11.6. Sia  $L$  un reticolo. Si considerino i seguenti due enunciati  $A$  e  $B$ :

$A =$  "Esiste  $x \in L$  tale che per ogni  $y \in L$  si ha  $x \leq y$  oppure  $x = y$ ".

$B =$  "Esiste  $x \in L$  tale che se  $y \in L$  e  $x \wedge y = x$  allora  $x \leq y$ ".

- (a) Si dica se gli enunciati  $A$  e  $B$  sono veri per ogni reticolo  $L$ .
- (b) Si scrivano gli enunciati  $A^*$  e  $B^*$ , duali di  $A$  e  $B$ .

11.7. Siano  $(L, \leq)$  un reticolo distributivo,  $a \in L$  un elemento fissato, e  $\varphi: L \rightarrow L$  l'applicazione definita da  $\varphi(x) = x \vee a$  per ogni  $x \in L$ . Si dimostri che  $\varphi$  è un omomorfismo di reticoli.

Si dimostri poi che le seguenti affermazioni sono equivalenti:

- (a)  $\varphi$  è un isomorfismo di reticoli;
- (b)  $L$  ha minimo e  $a$  è tale minimo;
- (c)  $\varphi: L \rightarrow L$  è l'applicazione identica.

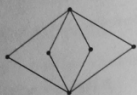
11.8. Sia  $D = \{z \mid z \in \mathbb{Z}, z > 0, z \mid 70\}$  l'insieme dei divisori interi positivi di  $70$ , la relazione d'ordine in  $D$  definita, per ogni  $z, z' \in \mathbb{Z}$  da  $z \mid z'$  se  $z$  divide  $z'$  (cioè se esiste  $k \in \mathbb{Z}$  tale che  $z' = zk$ ).

- (a) Si definisca un isomorfismo tra i reticoli  $(D, \mid)$  e  $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ .



(b) Il reticolo  $(D, |)$  è distributivo?

11.9. Si dica se può esistere un insieme  $X$  tale che il reticolo  $\mathcal{P}(X)$  sia isomorfo al reticolo



11.10. Sia  $\mathcal{P}_\infty(\mathbb{Z})$  l'insieme i cui elementi sono tutti i sottoinsiemi infiniti di  $\mathbb{Z}$ . Si ponga  $L = \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$  e si ordini parzialmente  $L$  mediante l'inclusione  $\subseteq$ .

(a) Si dimostri che nell'insieme parzialmente ordinato  $(L, \subseteq)$  si ha, per ogni  $A, B \in L$ ,  $A \vee B = A \cup B$  e

$$A \wedge B = \begin{cases} A \cap B & \text{se } A \cap B \text{ è un insieme infinito,} \\ \emptyset & \text{se } A \cap B \text{ è un insieme finito.} \end{cases}$$

Pertanto l'insieme parzialmente ordinato  $(L, \subseteq)$  è un reticolo.

(b) Si dimostri che il reticolo  $L$  è limitato.  
(c) Si dimostri che se  $A \in L$  è un sottoinsieme di  $\mathbb{Z}$  per il quale  $\mathbb{Z} \setminus A$  è un insieme finito e non vuoto, allora  $A$  non ha un complemento in  $L$ . Pertanto il reticolo  $(L, \subseteq)$  non è complementato.  
(d) Siano  $2\mathbb{Z}_{\geq 0} = \{2z \mid z \in \mathbb{Z}, z \geq 0\}$ ,  $2\mathbb{Z}_{\leq 0} = \{2z \mid z \in \mathbb{Z}, z \leq 0\}$  e  $D = \{2z + 1 \mid z \in \mathbb{Z}\}$ . Si dimostri che  $(2\mathbb{Z}_{\geq 0} \wedge 2\mathbb{Z}_{\leq 0}) \vee D = D$  e  $(2\mathbb{Z}_{\geq 0} \vee D) \wedge (2\mathbb{Z}_{\leq 0} \vee D) = D \cup \{0\}$ . Pertanto il reticolo  $(L, \subseteq)$  non è distributivo.

11.11. Sia  $X$  un insieme infinito e sia  $\mathcal{P}_f(X)$  l'insieme i cui elementi sono tutti i sottoinsiemi finiti di  $X$ . Si ordini parzialmente  $\mathcal{P}_f(X)$  mediante l'inclusione  $\subseteq$ . Si dimostri che  $(\mathcal{P}_f(X), \subseteq)$  è un reticolo distributivo che non è limitato.

11.12. Sia  $X$  un insieme infinito e sia  $\mathcal{P}_{\text{cof}}(X)$  l'insieme i cui elementi sono tutti i sottoinsiemi *cofiniti* di  $X$ , cioè i sottoinsiemi  $Y$  di  $X$  tali che  $X \setminus Y$  è un insieme finito. Si ordini parzialmente  $\mathcal{P}_{\text{cof}}(X)$  mediante l'inclusione  $\subseteq$ . Si dimostri che  $(\mathcal{P}_{\text{cof}}(X), \subseteq)$  è un reticolo distributivo che non è limitato.

11.13. Siano  $a, b, c$  tre oggetti distinti. Si consideri l'insieme

$$A = \mathcal{P}(\{a, b\}) \times \mathcal{P}(\{c\}) = \{(X, Y) \mid X \subseteq \{a, b\}, Y \subseteq \{c\}\}.$$

Sull'insieme  $A$  si definisca un ordinamento parziale  $\leq$  ponendo, per ogni  $(X, Y), (X', Y') \in A$ ,

$$(X, Y) \leq (X', Y') \text{ se } X \subseteq X' \text{ e } Y \subseteq Y'.$$

È possibile verificare che  $(A, \leq)$  è un reticolo distributivo in cui per ogni  $(X, Y), (X', Y') \in A$  si ha  $(X, Y) \vee (X', Y') = (X \cup X', Y \cup Y')$  e  $(X, Y) \wedge (X', Y') = (X \cap X', Y \cap Y')$ .

(a) Si determinino il massimo e il minimo di  $A$ .  
(b) Il reticolo  $(A, \leq)$  è complementato?  
(c) Il reticolo  $(A, \leq)$  è isomorfo al reticolo  $(\mathcal{P}(\{a, b, c\}), \subseteq)$ ?

11.14. Sia  $A$  l'insieme delle applicazioni  $f: \mathbb{R} \rightarrow \mathbb{R}$  tali che  $0 \leq f(x) \leq 1$  per ogni  $x \in \mathbb{R}$ . Sull'insieme  $A$  si definisca un ordinamento parziale  $\leq$  ponendo, per ogni  $f, g \in A$ ,  $f \leq g$  se  $f(x) \leq g(x)$  per ogni  $x \in \mathbb{R}$ .

(a) Si provi che l'insieme parzialmente ordinato  $(A, \leq)$  è un reticolo.

(b) Il reticolo  $(A, \leq)$  è limitato?  
(c) Sia  $f: \mathbb{R} \rightarrow \mathbb{R}$  l'applicazione definita da  $f(x) = 0$  per ogni  $x \leq 1$  e  $f(x) = 1$  per ogni  $x > 1$ . Si calcoli il complemento dell'elemento  $f$  nel reticolo  $(A, \leq)$ .  
(d) Il reticolo  $(A, \leq)$  è complementato?

11.15. Siano  $(B, \leq)$  e  $(C, \leq)$  due reticoli di Boole ed  $f: B \rightarrow C$  un omomorfismo di reticoli di Boole, cioè un'applicazione tale che  $f(0_B) = 0_C$ ,  $f(1_B) = 1_C$ ,  $f(x \vee y) = f(x) \vee f(y)$  e  $f(x \wedge y) = f(x) \wedge f(y)$  per ogni  $x, y \in B$ .

(a) Si dimostri che  $f(x') = (f(x))'$  per ogni  $x \in B$ .

Si ponga  $K = \{x \in B \mid f(x) = 0_C\}$ .

(b) Si provi che  $x \vee y \in K$  per ogni  $x, y \in K$ .  
(c) Si provi che  $x \wedge y \in K$  per ogni  $x \in K$  e ogni  $y \in B$ .

Sia  $\sim_f$  la relazione di equivalenza su  $B$  associata ad  $f$ , cioè la relazione d'equivalenza definita ponendo, per ogni  $x, y \in B$ ,  $x \sim_f y$  se  $f(x) = f(y)$ . Sull'insieme quoziente  $B/\sim_f$  si definisca una relazione  $\preceq$  ponendo, se  $x, y \in B$ ,  $[x]_{\sim_f} \preceq [y]_{\sim_f}$  se  $f(x) \leq f(y)$ .

(d) Si dimostri che la relazione  $\preceq$  su  $B/\sim_f$  è ben definita, cioè che se  $x, x', y, y' \in B$ ,  $[x]_{\sim_f} = [x']_{\sim_f}$  e  $[y]_{\sim_f} = [y']_{\sim_f}$ , allora  $f(x) \leq f(y)$  se e solo se  $f(x') \leq f(y')$ .

(e) Si dimostri che  $\preceq$  è un ordinamento parziale su  $B/\sim_f$ .

11.16. Sia  $X = \{a, b, c\}$  un insieme di cardinalità 3 e sia

$$L = \mathcal{P}(X) \setminus \{\{a\}\}$$

l'insieme di tutti i sottoinsiemi di  $X$  diversi da  $\{a\}$ . Si ordini parzialmente  $L$  mediante l'inclusione  $\subseteq$ . Si dica se l'insieme parzialmente ordinato  $(L, \subseteq)$  è un reticolo di Boole.

## Capitolo 12. Grafi e multigrafi

Un grafo consiste di due insiemi  $V$  ed  $L$  (detti rispettivamente l'insieme dei vertici e l'insieme dei lati) in modo che gli elementi di  $L$  siano sottoinsiemi di  $V$  di cardinalità due. Il grafo avente  $V$  come insieme dei vertici ed  $L$  come insieme dei lati verrà indicato con il simbolo  $(V, L)$ .

Due vertici  $v, w \in V$  si dicono *adiacenti* se  $\{v, w\} \in L$ . Due lati distinti  $\ell, \ell' \in L$  si dicono *incidenti* se  $\ell \cap \ell' \neq \emptyset$ .

Il grafo  $G = (V, L)$  viene spesso visualizzato mediante un diagramma nel modo seguente: gli elementi di  $V$  sono rappresentati come punti del piano, e ogni lato  $\ell = \{v, w\} \in L$  è rappresentato da un arco di curva avente gli estremi nei punti corrispondenti a  $v$  e  $w$ .

ESEMPIO 1. Il grafo  $G = (V, L)$  dove

$$V = \{v_1, v_2, v_3, v_4, v_5\} \quad \text{ed} \quad L = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6\}$$

con  $\ell_1 = \{v_1, v_2\}$ ,  $\ell_2 = \{v_1, v_3\}$ ,  $\ell_3 = \{v_2, v_3\}$ ,  $\ell_4 = \{v_2, v_4\}$ ,  $\ell_5 = \{v_3, v_4\}$ ,  $\ell_6 = \{v_4, v_5\}$  può essere rappresentato indifferentemente nei modi seguenti:

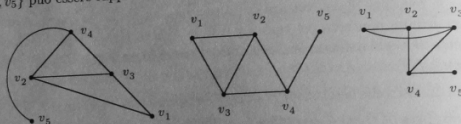


Figura 12.1

In pratica per descrivere un grafo conviene disegnarne il diagramma invece che elencare tutti i suoi vertici e tutti i suoi lati.  $\square$

Dati due grafi  $G = (V, L)$  e  $G' = (V', L')$ , un *isomorfismo* di  $G$  in  $G'$  è una biiezione  $\varphi: V \rightarrow V'$  tale che per ogni  $v, w \in V$  si ha  $\{v, w\} \in L$  se e solo se  $\{\varphi(v), \varphi(w)\} \in L'$ . Se esiste un isomorfismo di  $G$  in  $G'$  i due grafi  $G$  e  $G'$  si dicono *isomorfi*. Ovviamente se un diagramma rappresenta un grafo  $G$ , lo stesso diagramma rappresenta anche ogni grafo isomorfo a  $G$ . Un *automorfismo* di un grafo  $G$  è un isomorfismo di  $G$  in  $G$ .

Se  $G = (V, L)$  è un grafo,  $V'$  è un sottoinsieme di  $V$  ed  $L'$  è un sottoinsieme di  $L$  tale che per ogni lato  $\ell = \{v, w\} \in L'$  i suoi estremi  $v, w$  stanno in  $V'$ , allora  $G' = (V', L')$  è un grafo, detto un *sottografo* di  $G$ . Dato un grafo  $G = (V, L)$  e un qualunque sottoinsieme  $V'$  di  $V$ , il grafo  $G' = (V', L')$ , avente  $V'$  come insieme dei vertici ed avente come insieme  $L'$  dei lati l'insieme di tutti i lati di  $L$  i cui estremi stanno in  $V'$ , si dice il sottografo di  $G$  generato da  $V'$ .

Un grafo  $G = (V, L)$  si dice *finito* se l'insieme  $V$  dei suoi vertici è finito in tal caso anche l'insieme  $L$  dei suoi lati è finito (perché  $L \subseteq \mathcal{P}(V)$ ).

Se  $G = (V, L)$  è un grafo finito e  $v \in V$  è un vertice di  $G$ , diremo che  $v$  ha *grado*  $n$  se  $v$  appartiene ad esattamente  $n$  lati. Il grado del vertice  $v$  si indica con  $d(v)$ . Diremo che il vertice  $v$  è *pari* o *dispari* a seconda che  $d(v)$  è pari o dispari. Un vertice di grado 0 si dice un *vertice isolato*.

LEMMA 12.1.

$$|L| = \frac{1}{2} \sum_{v \in V} d(v).$$

COROLLARIO 12.2. Ogni grafo finito ha un numero pari di vertici dispari.

Un grafo finito si dice *regolare* di grado  $d$  se tutti i suoi vertici hanno grado  $d$ .

COROLLARIO 12.3. Un grafo finito regolare di grado  $d$  con  $n$  vertici ha  $\frac{1}{2}dn$  lati.

Ricordiamo che avevamo già parlato di grafi orientati nel capitolo 7, quando avevamo visto che le relazioni su un insieme potevano essere rappresentate mediante grafi orientati. Un *grafo orientato*  $G = (V, L)$  è un insieme  $V$  su cui è definita una relazione  $L$ . Quindi  $L \subseteq V \times V$ . I grafi orientati sono detti talvolta anche *grafi diretti* o *digrafi*. Sia la nozione di grafo orientato che quella di grafo non orientato si possono generalizzare al caso di grafi con lati multipli, cioè ai *multigrafi*. Nella figura 12.2 sono rappresentati i diagrammi di un multigrafo e di un multigrafo orientato.

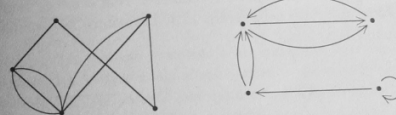


Figura 12.2

Ecco le definizioni rigorose. Un *multigrafo orientato*  $G = (V, L, \varphi)$  consiste di due insiemi  $V$  ed  $L$  (detti rispettivamente l'insieme dei vertici e l'insieme dei lati) e di un'applicazione  $\varphi: L \rightarrow V \times V$ . Se  $\ell \in L$ ,  $v, w \in V$  e  $\varphi(\ell) = (v, w)$  allora si dice che  $\ell$  è un *lato orientato* da  $v$  a  $w$ . Nel caso particolare in cui  $v = w$  si ha che

$\varphi(\ell) = (v, v)$ , e in tal caso il lato  $\ell$  si dice un *cappio*. Dato un multigrafo orientato  $G = (V, L, \varphi)$ ,  $G$  è un multigrafo orientato *semplice*, cioè c'è al più un lato da  $v$  a  $w$  per ogni coppia  $(v, w) \in V \times V$ , se e solo se l'applicazione  $\varphi$  è iniettiva. È chiaro che la nozione di grafo orientato e quella di multigrafo orientato semplice sono essenzialmente equivalenti.

Dato un insieme  $V$  denotiamo con  $\mathcal{P}_2(V)$  l'insieme di tutti i sottoinsiemi di  $V$  di cardinalità due. Un *multigrafo*  $G = (V, L, \varphi)$  consiste di due insiemi  $V$  ed  $L$  (detti rispettivamente l'insieme dei *vertici* e l'insieme dei *lati* del multigrafo) e di un'applicazione  $\varphi: L \rightarrow \mathcal{P}_2(V)$ . Se  $\ell \in L$ ,  $v, w \in V$  e  $\varphi(\ell) = \{v, w\}$ , si dice che  $\ell$  è un *lato* da  $v$  a  $w$ .

Nella letteratura matematica, quando si parla di grafi, è quasi sempre chiaro dal contesto se si sta parlando di grafi orientati o non orientati, e quando vi è pericolo di ambiguità si specifica sempre se il grafo in questione è un grafo orientato o un grafo non orientato. In questo testo continueremo a fare come abbiamo fatto fino ad ora, ossia quando si parla di grafi si intenderà grafi non orientati, mentre per i grafi orientati si continuerà a precisarlo ogni volta.

Si noti che con la terminologia da noi introdotta grafi e multigrafi orientati possono avere *cappi*, cioè lati da un vertice  $v$  allo stesso vertice  $v$ , mentre grafi e multigrafi non orientati non hanno cappi.

Un *cammino* dal vertice  $v$  al vertice  $w$  in un grafo (non orientato)  $G$  è una sequenza finita  $\ell_1 = \{z_1, z_2\}$ ,  $\ell_2 = \{z_2, z_3\}$ , ...,  $\ell_n = \{z_n, z_{n+1}\}$  di lati distinti di  $G$  tali che  $v = z_1$  e  $w = z_{n+1}$ . Diremo in tal caso che  $n$  è la *lunghezza* del cammino. Per ogni vertice  $v$  c'è un unico cammino di lunghezza zero da  $v$  allo stesso  $v$ , detto il *cammino nullo*. Un *circuito* è un qualunque cammino di lunghezza  $> 0$  da un vertice  $v$  allo stesso vertice  $v$ .

Un grafo  $G = (V, L)$  si dice *connesso* se per ogni  $v, w \in V$  esiste un cammino da  $v$  a  $w$ . Un grafo che non è connesso si dice *sconnesso*.

ESEMPIO 2. Il grafo dell'esempio 1 è connesso. Non è invece connesso il grafo con sette vertici riportato nella figura 12.3, in quanto, ad esempio, non esiste nessun cammino da  $v_2$  a  $v_6$ . □

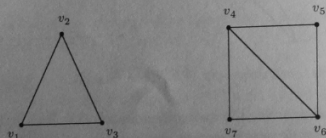


Figura 12.3

Se  $v \in V$ , l'insieme  $C_v$  i cui elementi sono tutti i vertici  $w$  per i quali esiste un cammino da  $v$  a  $w$  è un sottoinsieme di  $V$  detto la *componente connessa* di  $v$ . A volte, quando non ci sarà pericolo di confusione, chiameremo componente  $v$  il sottografo di  $G$  generato da  $C_v$ . Si noti che  $v \in C_v$  (perché c'è il cammino nullo da  $v$  a  $v$ ). Se si indica con  $\sim$  la relazione su  $V$  definita, per ogni  $v, w \in V$ , da  $v \sim w$  se esiste un cammino da  $v$  a  $w$ , allora  $\sim$  è una relazione di equivalenza su  $V$ , e per ogni  $v \in V$  la classe di equivalenza  $[v]_{\sim}$  di  $v$  modulo  $\sim$  è esattamente la componente connessa  $C_v$ .

ESEMPIO 3. Un grafo si dice *completo* se tutti i suoi vertici sono a due a due adiacenti. Ovviamente per ogni numero intero  $n \geq 1$  c'è un unico grafo completo con  $n$  vertici a meno di isomorfismi, cioè tutti i grafi che hanno  $n$  vertici e sono completi sono tra loro isomorfi. Indicheremo con  $K_n$  l'unico (a meno di isomorfismi) grafo completo con  $n$  vertici. La figura 12.4 mostra i grafi  $K_n$  per ogni  $n$  da 1 a 6. Il grafo  $K_n$  è un grafo connesso regolare di grado  $n-1$ , e quindi per il corollario 12.3 il grafo completo  $K_n$  ha  $\frac{n(n-1)}{2}$  lati. □

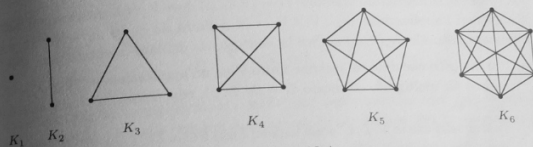


Figura 12.4

La maggior parte delle nozioni viste in questo capitolo a proposito dei grafi non orientati si estende facilmente al caso dei grafi orientati; questa estensione viene quindi lasciata al lettore per esercizio. Ad esempio un *cammino orientato* di lunghezza  $n$  dal vertice  $v$  al vertice  $w$  in un grafo orientato  $G$  è una sequenza di lati distinti di  $G$  tali che  $\ell_1 = (z_1, z_2)$ ,  $\ell_2 = (z_2, z_3)$ , ...,  $\ell_n = (z_n, z_{n+1})$  di  $n$  lati distinti di  $G$  tali che  $v = z_1$  e  $w = z_{n+1}$ . Un *circuito orientato* è un qualunque cammino orientato di lunghezza  $> 0$  da un vertice  $v$  allo stesso vertice  $v$ . Dato un grafo orientato  $G = (V, L)$  il *grafo non orientato*  $G'$  associato a  $G$  è il grafo  $G' = (V, L')$ , ove  $L' = \{(v, w) \mid (v, w) \in L, v \neq w\}$ . Quindi il grafo non orientato  $G'$  associato a  $G$  si ottiene da  $G$  cancellando tutti i cappi e sostituendo i lati orientati con lati non orientati.

Se  $G = (V, L)$  è un grafo orientato finito e  $v \in V$ , il *grado di entrata*  $d^+(v)$  di  $v$  è il numero di lati orientati che terminano in  $v$ , cioè

$$d^+(v) = |\{(w, v) \mid w \in V\}|.$$

Analogamente il grado di uscita  $d^-(v)$  di  $v$  è il numero di lati orientati che iniziano in  $v$ , cioè  $d^-(v) = |\{(v, w) \mid w \in V\}|$ . Il grado complessivo  $d(v)$  di  $v$  è  $d^+(v) + d^-(v)$ .

Un'altra facile estensione delle nozioni incontrate in questo capitolo può essere fatta passando dai grafi ai multigrafi. Ad esempio dati due multigrafi orientati  $G = (V, L, \varphi)$  e  $G' = (V', L', \varphi')$ , un isomorfismo di multigrafi orientati  $(f, g) : G \rightarrow G'$  è una coppia di biiezioni  $f : V \rightarrow V'$ ,  $g : L \rightarrow L'$  tale che il diagramma

$$\begin{array}{ccc} L & \xrightarrow{g} & L' \\ \varphi \downarrow & & \downarrow \varphi' \\ V \times V & \xrightarrow{f \times f} & V' \times V' \end{array}$$

sia commutativo. Qui  $f \times f : V \times V \rightarrow V' \times V'$  è l'applicazione definita da  $(f \times f)(v_1, v_2) = (f(v_1), f(v_2))$  per ogni  $(v_1, v_2) \in V \times V$ .

### Esercizi svolti

**12.1.** Per ogni multigrafo orientato  $G = (V, L, \varphi)$  dove  $V$  ed  $L$  sono insiemi finiti, si consideri l'applicazione  $\psi_G : V \times V \rightarrow \mathbb{N}$  definita da  $\psi_G(v, w) = |\varphi^{-1}(v, w)|$ . Il numero naturale  $\psi_G(v, w)$  si dice la molteplicità del lato orientato da  $v$  a  $w$ .

- (a) Si dimostri che dato un insieme finito  $V$  ed un'applicazione  $\psi : V \times V \rightarrow \mathbb{N}$ , esiste un multigrafo orientato  $G = (V, L, \varphi)$ , con  $L$  insieme finito, tale che  $\psi_G = \psi$ .
- (b) Si dimostri che se  $V, L, L'$  sono insiemi finiti e  $G = (V, L, \varphi)$ ,  $G' = (V, L', \varphi')$  sono due multigrafi orientati tali che  $\psi_G = \psi_{G'}$ , allora esiste un isomorfismo  $(\iota_V, g) : G \rightarrow G'$  dove  $\iota_V : V \rightarrow V'$  è l'identità.

[Questo significa che dati un insieme finito  $V$  ed un'applicazione  $\psi : V \times V \rightarrow \mathbb{N}$ , esiste un multigrafo orientato  $G = (V, L, \varphi)$  tale che  $\psi_G = \psi$ , e che tale multigrafo è unico a meno di isomorfismi che inducono l'identità su  $V$ .]

**Soluzione.** (a) Sia  $L$  l'insieme delle terne  $(v, w, i)$  dove  $v, w \in V$  ed  $i$  è un numero naturale tale che  $1 \leq i \leq \psi(v, w)$ . In particolare se  $v, w \in V$  e  $\psi(v, w) = 0$ , non esiste in  $L$  alcuna terna del tipo  $(v, w, i)$ . Dato che l'insieme  $V$  è finito, anche l'insieme  $L$  è finito. Si consideri l'applicazione  $\varphi : L \rightarrow V \times V$  definita da  $\varphi(v, w, i) = (v, w)$  per ogni  $(v, w, i) \in L$ . Allora  $G = (V, L, \varphi)$  è un multigrafo orientato, e si ha

$$\begin{aligned} \psi_G(v, w) &= |\varphi^{-1}(v, w)| = |\{(x, y, z) \in L \mid \varphi(x, y, z) = (v, w)\}| = \\ &= |\{(x, y, z) \in L \mid x = v, y = w\}| = \\ &= |\{(v, w, z) \mid z \in \mathbb{N}, 1 \leq z \leq \psi(v, w)\}| = \psi(v, w). \end{aligned}$$

Quindi  $\psi_G = \psi$ .

(b) Dato che  $\psi_G = \psi_{G'}$ , cioè che  $|\varphi^{-1}(v, w)| = |\varphi'^{-1}(v, w)|$  per ogni  $v, w \in V$ , è possibile definire una biiezione  $g_{v, w} : \varphi^{-1}(v, w) \rightarrow \varphi'^{-1}(v, w)$  per ogni  $v, w \in V$ . Ma  $\{\varphi^{-1}(v, w) \mid v, w \in V, \varphi^{-1}(v, w) \neq \emptyset\}$  è una partizione di  $L$  e analogamente  $\{\varphi'^{-1}(v, w) \mid v, w \in V, \varphi'^{-1}(v, w) \neq \emptyset\}$  è una partizione di  $L'$ . Ne segue che esiste una biiezione  $g : L \rightarrow L'$  tale che per ogni  $v, w \in V$  l'applicazione che si ottiene da  $g$  restringendo il dominio a  $\varphi^{-1}(v, w)$  e il codominio a  $\varphi'^{-1}(v, w)$  è esattamente la biiezione  $g_{v, w}$ . Per dimostrare che  $(\iota_V, g) : G \rightarrow G'$  è un isomorfismo di multigrafi ci resta solo da dimostrare che  $(\iota_V \times \iota_V) \circ \varphi = \varphi' \circ g$ . Ma

$$g(\varphi^{-1}(v, w)) = \varphi'^{-1}(v, w) \text{ per ogni } v, w \in V, \text{ e quindi se } \ell \in L \text{ e } \varphi(\ell) = (v, w) \text{ si ha}$$

$$((\iota_V \times \iota_V) \circ \varphi)(\ell) = (\iota_V \times \iota_V)(\varphi(\ell)) = (\iota_V \times \iota_V)(v, w) = (v, w)$$

e  $\ell \in \varphi'^{-1}(v, w)$ , da cui  $g(\ell) \in \varphi'^{-1}(v, w)$ , e quindi anche  $\varphi'(g(\ell)) = (v, w)$ . Pertanto  $(\varphi' \circ g)(\ell) = (v, w)$ , e abbiamo così dimostrato che  $((\iota_V \times \iota_V) \circ \varphi)(\ell) = (\varphi' \circ g)(\ell)$  per ogni  $\ell \in L$ . Quindi  $(\iota_V \times \iota_V) \circ \varphi = \varphi' \circ g$ .  $\square$

**12.2.** Sia  $G = (V, L)$  un grafo orientato finito. Si dimostri che

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |L|$$

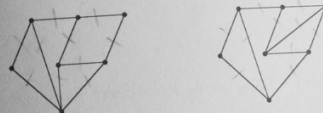
e che

$$\sum_{v \in V} d(v) = 0.$$

**Soluzione.** Per la prima formula è sufficiente osservare che ogni lato inizia in esattamente un vertice e termina esattamente in un vertice. Per la seconda si ha

$$\begin{aligned} \sum_{v \in V} d(v) &= \sum_{v \in V} (d^+(v) - d^-(v)) = \\ &= \left( \sum_{v \in V} d^+(v) \right) - \left( \sum_{v \in V} d^-(v) \right) = |L| - |L| = 0. \quad \square \end{aligned}$$

### 12.3. I due grafi



sono isomorfi?

**Soluzione.** Si osservi che ogni isomorfismo  $\varphi : V \rightarrow V'$  tra due grafi  $G = (V, L)$  e  $G' = (V', L')$  conserva i gradi, cioè  $d(v) = d(\varphi(v))$  per ogni  $v \in V$ . Ora il primo dei due grafi della figura ha un vertice di grado 4, mentre il secondo non ha vertici di grado 4. Ne segue che non può esistere un isomorfismo tra questi due grafi.  $\square$

## Altri esercizi

- 12.4. È possibile disegnare un grafo con esattamente 100 vertici  $v_1, v_2, \dots, v_{100}$  tale che  $d(v_i) = i$  per ogni  $i = 1, 2, \dots, 100$ ?
- 12.5. È possibile disegnare un grafo con esattamente 100 vertici  $v_1, v_2, \dots, v_{100}$  tale che  $d(v_i) = 1$  per ogni  $i$  dispari e  $d(v_i) = 2$  per ogni  $i$  pari?
- 12.6. È possibile disegnare un grafo con esattamente 98 vertici  $v_1, v_2, \dots, v_{98}$  tale che  $d(v_i) = 1$  per ogni  $i$  dispari e  $d(v_i) = 2$  per ogni  $i$  pari?
- 12.7. Si disegnino tutti i grafi non orientati regolari con 5 vertici a meno di isomorfismi, cioè si disegnino i grafi di un insieme  $I$  di grafi regolari con 5 vertici con le proprietà che: (a) due grafi distinti qualunque di  $I$  non sono tra loro isomorfi; (b) ogni grafo regolare con 5 vertici è isomorfo a un grafo dell'insieme  $I$ .
- 12.8. (a) I grafi



sono isomorfi?



(b) I grafi



sono isomorfi?



(c) Si determinino tutti gli automorfismi del grafo



12.9. Il lettore provi a dire quale potrebbe essere, secondo lui, la definizione di isomorfismo di grafi orientati.

12.10. Per un qualunque insieme  $A$  chiamiamo *diagonale* di  $A \times A$  l'insieme  $D_A = \{(a, a) \mid a \in A\}$ . Quindi  $D_A \subseteq A \times A$ .

Precisiamo meglio quanto avevamo già visto nel capitolo 7. Data una relazione  $\rho$  su un insieme  $V$ , (cioè  $\rho \subseteq V \times V$ ), definiamo *grafo di  $\rho$*  il grafo orientato  $G_\rho = (V, \rho)$ , ossia il grafo in cui l'insieme dei lati è lo stesso insieme  $\rho$ .

- (a) Si dimostri che per la relazione di uguaglianza  $=$  su  $V$ , il grafo di  $=$  è  $G_=(V, D_V)$ .
- (b) Si dimostri che se  $\rho$  è un'equivalenza su  $V$ , il suo grafo è  $G_\rho = (V, L)$ , dove  $L = (\pi \times \pi)^{-1}(D_{V/\rho})$ . Qui  $\pi: V \rightarrow V/\rho$  è la proiezione canonica, e  $\pi \times \pi: V \times V \rightarrow V/\rho \times V/\rho$  è definita da  $(\pi \times \pi)(v, v') = (\pi(v), \pi(v'))$  per ogni  $(v, v') \in V \times V$ .

## Capitolo 13. Cammini e circuiti

Sia  $G = (V, L, \varphi)$  un multigrafo non orientato *finito*, cioè un multigrafo per il quale entrambi gli insiemi  $V$  ed  $L$  sono finiti. Un *cammino euleriano* in  $G$  è un cammino  $\ell_1, \ell_2, \dots, \ell_m$  in  $G$  tale che  $L = \{\ell_1, \ell_2, \dots, \ell_m\}$ . Un cammino euleriano che sia anche un circuito si dice un *circuito euleriano*. Quindi percorrendo un cammino o un circuito euleriano "si passa una ed una sola volta per tutti i lati del multigrafo"; questo significa che un multigrafo finito ha un cammino euleriano se e solo se si riescono a disegnare tutti i suoi lati senza mai staccare la penna dal foglio.

**TEOREMA 13.1 (TEOREMA DI EULERO).** Sia  $G$  un multigrafo finito privo di vertici isolati. Il multigrafo  $G$  ha un circuito euleriano se e solo se è connesso e tutti i suoi vertici sono pari.

**COROLLARIO 13.2.** Sia  $G$  un multigrafo finito privo di vertici isolati. Il multigrafo  $G$  ha un cammino euleriano se e solo se è connesso e ha zero o due vertici dispari.

Un *cammino hamiltoniano* in un multigrafo finito è un cammino che passa esattamente una volta per ogni vertice del multigrafo.

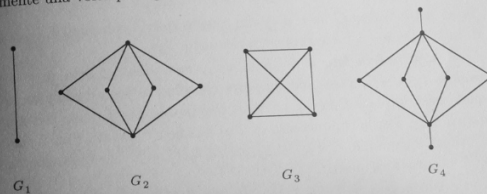


Figura 13.1



ESEMPIO 1. Nella figura 13.1 i multigrafi  $G_1$  e  $G_2$  hanno un cammino euleriano, mentre i multigrafi  $G_3$  e  $G_4$  non hanno un cammino euleriano; i multigrafi  $G_1$  e  $G_3$  hanno un cammino hamiltoniano, mentre i multigrafi  $G_2$  e  $G_4$  non hanno un cammino hamiltoniano. Questi esempi fanno vedere che non c'è alcun rapporto tra l'esistenza di un cammino euleriano e l'esistenza di un cammino hamiltoniano.  $\square$

Le definizioni di cammini e circuiti euleriani e hamiltoniani che abbiamo dato per i multigrafi finiti non orientati possono essere ripetute anche per i multigrafi finiti orientati. In un multigrafo finito orientato  $G = (V, L, \varphi)$ , cioè in un multigrafo tale che entrambi gli insiemi  $V$  ed  $L$  siano finiti, un *cammino euleriano orientato* è un cammino orientato  $\ell_1, \ell_2, \dots, \ell_m$  in  $G$  tale che  $L = \{\ell_1, \ell_2, \dots, \ell_m\}$ . Un cammino euleriano orientato che sia anche un circuito si dice un *circuito euleriano orientato*. Un *cammino hamiltoniano orientato* in un multigrafo orientato è un cammino orientato che passa esattamente una volta per ogni vertice del multigrafo.

Un multigrafo orientato  $G = (V, L, \varphi)$  si dice *completo* se per ogni  $v, w \in V$ ,  $v \neq w$ , esiste un lato orientato da  $v$  a  $w$  oppure un lato orientato da  $w$  a  $v$ .

TEOREMA 13.3. Ogni multigrafo finito orientato completo ha un cammino orientato hamiltoniano.

*Dimostrazione.* Sia  $G = (V, L, \varphi)$  un multigrafo finito orientato completo con  $n$  vertici. Mostriamo che dato un qualunque cammino orientato di  $G$  di lunghezza  $d$  che passa per  $d+1 < n$  vertici distinti di  $G$ , esiste un cammino orientato di  $G$  di lunghezza  $d+1$  che passa per  $d+2$  vertici distinti di  $G$ . Da questo segue immediatamente l'esistenza di un cammino orientato in  $G$  di lunghezza  $n-1$  che passa esattamente una volta per tutti gli  $n$  vertici di  $G$ .

Sia  $\ell_1, \ell_2, \dots, \ell_d$  un cammino di lunghezza  $d$ , dove  $\ell_i = \varphi(v_i, v_{i+1})$ , e supponiamo che i vertici  $v_1, v_2, \dots, v_d, v_{d+1}$  siano tutti distinti e che  $d+1 < n$ . Con queste ipotesi esiste un vertice  $v \in V$  distinto da  $v_1, v_2, \dots, v_d, v_{d+1}$ . Si avrà allora almeno uno dei seguenti tre casi:

- (1) Esiste un lato  $\ell$  in  $G$  da  $v$  a  $v_1$ . In questo caso il cammino  $\ell, \ell_1, \ell_2, \dots, \ell_d$  di lunghezza  $d+1$  ha le proprietà richieste.
- (2) Non esiste nessun lato in  $G$  da  $v$  a  $v_1$ , ma esiste un lato da  $v$  a  $v_j$  per qualche  $j \leq d+1$ . Possiamo supporre che l'indice  $j$  sia il più piccolo per il quale esiste un lato  $\ell$  da  $v$  a  $v_j$  in  $G$ . Per ipotesi  $j > 1$  e non esiste un lato da  $v$  a  $v_{j-1}$ . Per la completezza di  $G$  si ha che c'è un lato  $\ell'$  in  $G$  da  $v_{j-1}$  a  $v$ . Allora il cammino  $\ell_1, \ell_2, \dots, \ell_{j-2}, \ell', \ell, \ell_j, \ell_{j+1}, \dots, \ell_d$  di lunghezza  $d+1$  ha le proprietà richieste.
- (3) Non esiste nessun  $j \leq d+1$  tale che ci sia in  $G$  un lato da  $v$  a  $v_j$ . In particolare non c'è in  $G$  un lato da  $v$  a  $v_{d+1}$ . Per la completezza del grafo

c'è in  $G$  un lato  $\ell$  da  $v_{d+1}$  a  $v$ . Ma allora il cammino  $\ell_1, \ell_2, \dots, \ell_d, \ell$  di lunghezza  $d+1$  ha le proprietà richieste.  $\square$

ESEMPIO 2. Non è vero che ogni multigrafo finito orientato completo ha un circuito orientato hamiltoniano. Ad esempio



è un multigrafo finito orientato completo privo di circuiti orientati. Quindi il teorema 13.3 non può essere migliorato in questa direzione.  $\square$

Dati due vertici  $v, w$  in un multigrafo connesso  $G = (V, L, \varphi)$ , la *distanza*  $d(v, w)$  tra i due vertici  $v$  e  $w$  è il minimo delle lunghezze di tutti i cammini da  $v$  a  $w$ . Si noti che si ha  $d(v, w) = 0$  se e solo se  $v = w$ , che  $d(v, w) = d(w, v)$  per ogni  $v, w \in V$ , e che  $d(u, v) + d(v, w) \geq d(u, w)$  per ogni  $u, v, w \in V$ .

Se  $G = (V, L)$  è un multigrafo connesso, il *diametro* di  $G$  è il massimo dell'insieme  $\{d(v, w) \mid v, w \in V\}$ .

ESEMPIO 3. Nel multigrafo della figura 13.2 la distanza tra i vertici  $v$  e  $w$  è 2. Il diametro del multigrafo è 3.  $\square$

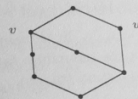


Figura 13.2

Sia  $G = (V, L)$  un grafo. Diremo che il grafo  $G$  è *bipartito* se esiste una partizione  $\{V_1, V_2\}$  di  $V$  tale che ogni lato di  $G$  ha un estremo in  $V_1$  e l'altro in  $V_2$ . Equivalentemente il grafo  $G = (V, L)$  è bipartito se e solo se esiste una partizione  $\{V_1, V_2\}$  di  $V$  tale che i due sottografi di  $G$  generati l'uno da  $V_1$  e l'altro da  $V_2$  consistono entrambi di soli vertici isolati.

ESEMPIO 4. Siano  $1 \leq m \leq n$  numeri naturali. Il *grafo bipartito completo*  $K_{m,n} = (V, L)$  è il grafo tale che

$$V = \{v_1, v_2, \dots, v_m, w_1, w_2, \dots, w_n\},$$

$$L = \{\ell_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$$

ed  $\ell_{ij} = \{v_i, w_j\}$ . Quindi  $K_{m,n}$  è il grafo bipartito con  $m+n$  vertici in cui, se  $V_1 = \{v_1, v_2, \dots, v_m\}$  e  $V_2 = \{w_1, w_2, \dots, w_n\}$ , ogni vertice di  $V_1$  è adiacente ad ogni vertice di  $V_2$ . Il grafo  $K_{m,n}$  ha  $mn$  lati. La figura 13.3 mostra  $K_{1,1}$ ,  $K_{1,2}$ ,  $K_{1,3}$ ,  $K_{2,2}$ ,  $K_{2,3}$ ,  $K_{3,3}$ .  $\square$

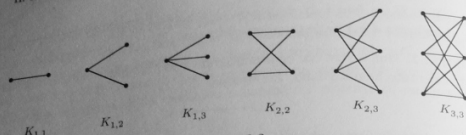


Figura 13.3

Sia  $G = (V, L)$  un grafo finito e poniamo

$$V = \{v_1, v_2, \dots, v_n\}.$$

Sia  $A = (a_{ij})$  la matrice  $n \times n$  definita da  $a_{ij} = 1$  se i vertici  $v_i$  e  $v_j$  sono adiacenti, cioè se  $\{v_i, v_j\} \in L$ , e  $a_{ij} = 0$  se  $v_i$  e  $v_j$  non sono adiacenti. La matrice  $A$  è simmetrica ed è detta la *matrice di adiacenza* di  $G$ .

Nell'enunciato del teorema che segue se  $G = (V, L)$  è un grafo e  $v, w \in V$ , una *catena* da  $v$  a  $w$  è una sequenza finita

$$\ell_1 = \{z_1, z_2\}, \ell_2 = \{z_2, z_3\}, \dots, \ell_n = \{z_n, z_{n+1}\}$$

di lati di  $G$  tali che  $v = z_1$  e  $w = z_{n+1}$ . In tal caso  $n$  si dice la *lunghezza* della catena. Si noti che la differenza tra cammini e catene è che per i cammini si richiedeva anche che i lati fossero distinti tra loro.

**TEOREMA 13.4.** Sia  $G = (V, L)$  un grafo finito con  $n$  vertici e sia  $V = \{v_1, v_2, \dots, v_n\}$ . Se  $A$  è la matrice di adiacenza di  $G$  ed  $l$  è un numero intero positivo, allora per ogni  $i$  ed ogni  $j$  l'elemento di posto  $(i, j)$  nella matrice  $A^l$  è uguale al numero di catene di lunghezza  $l$  da  $v_i$  a  $v_j$ .

*Dimostrazione.* Induzione su  $l$ . Per  $l = 1$  si ha che il numero di catene di lunghezza 1 da  $v_i$  a  $v_j$  è 1 se  $\{v_i, v_j\} \in L$  ed è 0 altrimenti; quindi tale numero è uguale all'elemento di posto  $(i, j)$  nella matrice di adiacenza  $A = A^1$ . Pertanto l'enunciato è vero per  $l = 1$ . Supponiamo  $l > 1$  e che il teorema valga per  $l - 1$ . Allora il numero di catene di lunghezza  $l$  da  $v_i$  a  $v_j$  è uguale alla somma dei numeri di catene di lunghezza  $l - 1$  da  $v_i$  a  $v_k$  per ogni  $k = 1, \dots, n$  tale che  $\{v_k, v_j\} \in L$ . Ponendo  $A = (a_{ij})$  e  $A^{l-1} = (b_{ij})$ , per l'ipotesi induttiva l'elemento  $b_{ik}$  della matrice  $A^{l-1}$  è uguale al numero di catene di lunghezza  $l - 1$  da  $v_i$  a  $v_k$ . Ne segue che il numero delle catene di lunghezza  $l$  da  $v_i$  a  $v_j$  è uguale alla somma dei  $b_{ik}$  per ogni  $k = 1, \dots, n$  tale che  $\{v_k, v_j\} \in L$ . Ricordando che  $a_{kj} = 1$  se  $\{v_k, v_j\} \in L$  e  $a_{kj} = 0$  se  $\{v_k, v_j\} \notin L$ , se ne deduce che il numero delle catene di lunghezza  $l$  da  $v_i$  a  $v_j$  è uguale a  $\sum_{k=1}^n b_{ik} a_{kj}$ , cioè all'elemento di posto  $(i, j)$  nella matrice  $A^{l-1} A = A^l$ .  $\square$

Sia  $G = (V, L, \varphi)$  un multigrafo connesso e sia  $v \in V$ . Si dice che  $v$  è un *punto di taglio* per  $G$  se il sottografo di  $G$  che si ottiene togliendo  $v$  e tutti i lati incidenti a  $v$ , cioè il sottografo di  $G$  generato da  $V \setminus \{v\}$ , è sconnesso.

**TEOREMA 13.5.** Sia  $G = (V, L, \varphi)$  un multigrafo connesso e sia  $v \in V$ . Allora  $v$  è un punto di taglio per  $G$  se e solo se esistono  $u, w \in V$  tali che ogni cammino da  $u$  a  $w$  passa per  $v$ .

*Dimostrazione.* Sia  $v$  un punto di taglio per  $G$ . Allora il sottografo  $G'$  di  $G$  generato da  $V \setminus \{v\}$  è sconnesso. Siano  $U \subseteq V$  e  $W \subseteq V$  due componenti connesse distinte di questo sottografo  $G'$ . Se  $u \in U$  e  $w \in W$ , ogni cammino da  $u$  a  $w$  in  $G$  deve passare per  $v$  perché  $u$  e  $w$  appartengono a componenti connesse distinte di  $G'$ .

Viceversa si supponga che esistano  $u, w \in V$  tali che ogni cammino da  $u$  a  $w$  passi per  $v$ . Sia  $G'$  il sottografo di  $G$  generato da  $V \setminus \{v\}$ . Dobbiamo mostrare che  $G'$  è sconnesso. Questo è ovvio, perché se nel grafo  $G'$  ci fosse un cammino tra i suoi vertici  $u$  e  $w$ , questo cammino sarebbe un cammino in  $G$  tra  $u$  e  $w$  che non passa per  $v$ , e questo è contrario a quanto era stato supposto.  $\square$

### Esercizi svolti

**13.1.** Per scrivere la matrice di adiacenza  $A$  di un grafo finito  $G = (V, L)$  è stato necessario fissare un ordinamento sull'insieme  $V = \{v_1, v_2, \dots, v_n\}$  dei vertici. Infatti modificando l'ordinamento di  $V$  la matrice di adiacenza di  $G$  cambia. Vediamo come ciò avviene.

Sia  $A = (a_{ij})$  la matrice di adiacenza di  $G$  relativa all'ordinamento  $v_1, v_2, \dots, v_n$  di  $V$ . Fissare un altro ordinamento di  $V$  equivale a fissare una biiezione  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ ; calcoleremo infatti la matrice di adiacenza di  $G$  relativa all'ordinamento  $v_{f(1)}, v_{f(2)}, \dots, v_{f(n)}$  di  $V$ . Sia  $P_f = (p_{ij})$  la matrice  $n \times n$  definita da  $p_{ij} = 1$  se  $i = f(j)$ , e  $p_{ij} = 0$  se  $i \neq f(j)$ . Si dimostri che:

- se  $f$  e  $g$  sono due biiezioni di  $\{1, 2, \dots, n\}$  in  $\{1, 2, \dots, n\}$ , allora  $P_f P_g = P_{fg}$ ;
- $P_f^t = P_{f^{-1}}$  per ogni biiezione  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  (qui  $P_f^t$  è la trasposta della matrice  $P_f$ ; vedi capitolo 6);
- $P_f^t P_f = P_f P_f^t = I_{n \times n}$ , matrice identica  $n \times n$ ;
- la matrice di adiacenza del grafo  $G = (V, L)$  rispetto all'ordinamento  $v_{f(1)}, v_{f(2)}, \dots, v_{f(n)}$  di  $V$  è  $P_f^t A P_f$ .

*Soluzione.* (a) Se  $f, g: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  sono biiezioni,  $P_f = (p_{ij})$  e  $P_g = (p'_{ij})$ , allora  $P_f P_g$  ha come elemento nel posto  $(i, k)$  il numero reale  $\sum_{j=1}^n p_{ij} p'_{jk}$ . Ma  $p_{ij}$  è sempre zero eccetto quando  $i = f(j)$ , e  $p'_{jk}$  è sempre zero eccetto che nel caso  $j = g(k)$ . Quindi  $\sum_{j=1}^n p_{ij} p'_{jk}$  è sempre zero eccetto che quando esiste un  $j$  tale che  $i = f(j)$  e  $j = g(k)$ , cioè quando  $i = f(g(k))$ ,

nel qual caso vale 1. Anche  $P_{fg}$  ha nel posto  $(i, k)$  sempre zero eccetto quando  $i = f(g(k))$ . Pertanto  $P_f P_g$  e  $P_{fg}$  hanno lo stesso elemento di posto  $(i, k)$  per ogni  $i$  e ogni  $k$ , ossia  $P_f P_g = P_{fg}$ .

(b) L'elemento di posto  $(i, j)$  nella matrice  $P_{f^{-1}}$  è 1 se  $i = f^{-1}(j)$ , ed è 0 altrimenti, cioè è 1 se  $f(i) = j$ , ed è 0 altrimenti. Nella matrice  $P_f$  l'elemento di posto  $(j, i)$  è 1 se  $f(i) = j$ , ed è 0 altrimenti. Quindi nella sua trasposta  $P_f^t$  l'elemento di posto  $(i, j)$  è 1 se  $f(i) = j$ , ed è 0 altrimenti. Abbiamo così dimostrato che  $P_f^t$  e  $P_f$  hanno lo stesso elemento di posto  $(i, j)$  per ogni  $i$  e ogni  $j$ , e quindi coincidono.

(c) Per quanto dimostrato in (a) e (b) si ha  $P_f^t P_f = P_{f^{-1}}$ ,  $P_f = P_{f^{-1}f} = P_f$ , dove  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  è l'applicazione identica, e similmente  $P_f^t P_f^t = P_f$ . Quindi basta provare che  $P_f$  è l'identità. Ma  $P_f$  ha come elemento di posto  $(i, j)$  il numero 1 se  $i = f(j)$ , e 0 altrimenti. Quindi  $P_f$  ha come elemento di posto  $(i, j)$  il numero 1 se  $i = j$ , e 0 altrimenti. Se ne conclude che  $P_f = I_{n \times n}$ .

(d) La matrice di adiacenza  $A'$  del grafo  $G = (V, L)$  rispetto all'ordinamento  $v_{f(1)}, v_{f(2)}, \dots, v_{f(n)}$  ha come elemento di posto  $(i, j)$  il numero 1 se  $v_{f(i)}$  è adiacente a  $v_{f(j)}$ , e 0 altrimenti. La matrice  $P_f^t A P_f$  ha come elemento di posto  $(i, j)$  il numero  $\sum_{k,l} p_{ki} a_{kl} p_{lj}$ , dove  $P_f = (p_{ij})$  e  $A = (a_{ij})$ . Per come è definita la matrice  $P_f$  si ha  $p_{ki} = 1$  se  $k = f(i)$  e  $p_{ki} = 0$  altrimenti, e  $p_{lj} = 1$  se  $l = f(j)$  e  $p_{lj} = 0$  altrimenti. Quindi nella somma  $\sum_{k,l} p_{ki} a_{kl} p_{lj}$  tutti gli addendi  $p_{ki} a_{kl} p_{lj}$  sono nulli eccetto che per  $k = f(i)$  ed  $l = f(j)$ , nel qual caso si ha  $p_{ki} a_{kl} p_{lj} = a_{kl} = a_{f(i)f(j)}$ . Ma allora  $\sum_{k,l} p_{ki} a_{kl} p_{lj} = a_{f(i)f(j)}$  è 1 se  $v_{f(i)}$  è adiacente a  $v_{f(j)}$ , ed è 0 altrimenti. Se ne conclude che la matrice di adiacenza  $A'$  e la matrice  $P_f^t A P_f$  hanno lo stesso elemento di posto  $(i, j)$  per ogni riga  $i$  e ogni colonna  $j$ , e quindi coincidono.  $\square$

**13.2.** Sia  $G$  un grafo finito. Si dimostri che  $G$  ha un circuito euleriano se e solo se ha tutti i vertici pari e inoltre tutte le componenti connesse di  $G$ , eccetto al più una, consistono di vertici isolati.

*Soluzione.* Sia  $G$  un grafo finito con un circuito euleriano. Denotiamo con  $C_1, C_2, \dots, C_t$  le componenti connesse di  $G$ . Ragioniamo per assurdo e supponiamo che ci siano almeno due di queste componenti connesse che non consistono di vertici isolati. Scambiando eventualmente gli indici possiamo supporre che  $C_1$  e  $C_2$  non consistano di soli vertici isolati. Allora sia in  $C_1$  che in  $C_2$  ci sono dei lati. Dato che il circuito euleriano deve passare per entrambi questi lati, ne segue che il circuito euleriano passa sia per un vertice di  $C_1$  che per un vertice di  $C_2$ . Questo contraddice il fatto che i due vertici stiano su diverse componenti connesse e che quindi non esista un cammino che li unisce. Abbiamo così dimostrato che tutte le componenti connesse di  $G$ , eccetto al più una, consistono di vertici isolati. Ora che sappiamo che il grafo  $G$  consiste di vertici isolati e di al più un'ulteriore

componente connessa, diciamo  $C_1$ , è chiaro che il fatto che  $G$  abbia un cammino euleriano implica che  $C_1$  abbia un cammino euleriano. I vertici isolati di  $G$  hanno grado zero, e quindi sono pari. Per gli eventuali vertici non isolati di  $G$  basta ora osservare che essi debbono stare sulla componente connessa  $C_1$  di  $G$ . Ma  $C_1$  è un grafo finito, privo di vertici isolati e con un cammino euleriano, e quindi per il teorema di Eulero 13.2 anche tutti i vertici su  $C_1$  devono essere di grado pari.

Per dimostrare l'implicazione inversa supponiamo che  $G$  sia un grafo finito con tutti i vertici pari e che tutte le componenti connesse di  $G$ , eccetto al più una, consistano di vertici isolati. Siano  $C_1, C_2, \dots, C_t$  le componenti connesse di  $G$ , e supponiamo che, se  $t \geq 2$ , le componenti connesse  $C_2, C_3, \dots, C_t$  consistano di un solo vertice isolato ciascuna. Allora  $C_1$  è un grafo finito, connesso e con tutti i vertici pari. Dal teorema 13.2 segue che  $C_1$  deve avere un circuito euleriano. Ma tutti i lati di  $G$  sono lati di  $C_1$ , e pertanto un circuito euleriano di  $C_1$  è anche un circuito euleriano di  $G$ .  $\square$

### Altri esercizi

**13.3.** Sia  $n \geq 1$  un numero intero. Si dimostri che un grafo completo con  $n$  vertici ha un cammino euleriano se e solo se  $n$  è dispari oppure  $n = 2$ .

**13.4.** Sia  $G = (V, L, \varphi)$  un multigrafo finito orientato completo. Si dimostri che  $|L| \geq \frac{|V|(|V|-1)}{2}$ .

**13.5.** Sia  $G = (V, L)$  un grafo finito connesso privo di circuiti euleriani,  $v_0 \notin V$  un vertice ulteriore e

$$L' = \{ \{v, v_0\} \mid v \in V \text{ è un vertice di grado dispari in } G \}.$$

Si supponga  $|V| > 1$  e si consideri il grafo  $G' = (V \cup \{v_0\}, L \cup L')$ .

(a) Si dimostri che il grafo  $G'$  è connesso.

(b) Si dimostri che il vertice  $v_0$  di  $G'$  ha grado pari.

(c) Si dimostri che il grafo  $G'$  ha un circuito euleriano.

(d) Se ne deduca che ogni grafo finito connesso è un sottografo di un grafo con un circuito euleriano.

**13.6.** Si disegnino quattro grafi finiti  $G_1, G_2, G_3, G_4$  in modo che  $G_1$  abbia sia un circuito euleriano che un circuito hamiltoniano,  $G_2$  abbia un circuito euleriano ma non abbia un cammino hamiltoniano,  $G_3$  abbia un circuito hamiltoniano ma non abbia un cammino euleriano,  $G_4$  non abbia né un cammino euleriano né un cammino hamiltoniano.

**13.7.** Si consideri il grafo con 12 vertici rappresentato nella figura 13.4 (a).

(a) Tale grafo ha un cammino euleriano?

- (b) Ha un circuito euleriano?  
 (c) Si calcoli il diametro del grafo.
- 13.8. Sia  $G = (V, L)$  un grafo con  $n$  vertici. Si dimostri che  $G$  è bipartito se e solo se esiste un numero intero positivo  $k \leq n-1$ , tale che  $G$  è isomorfo a un sottografo del grafo bipartito completo  $K_{k, n-k}$ .
- 13.9. (a) Determinare tutte le coppie  $(m, n)$ , con  $1 \leq m \leq n$  numeri naturali, per le quali il grafo bipartito completo  $K_{m, n}$  ha un circuito euleriano.  
 (b) Determinare tutte le coppie  $(m, n)$ , con  $1 \leq m \leq n$  numeri naturali, per le quali il grafo bipartito completo  $K_{m, n}$  ha un cammino euleriano.
- 13.10. Il lettore provi a definire cosa si intende per matrice di adiacenza di un grafo finito orientato, e adatti il teorema 13.3 al caso dei grafi finiti orientati.
- 13.11. Sia  $G = (V, L)$  un grafo. Si definisca una relazione  $\approx$  in  $V$  ponendo, per ogni  $v, w \in V$ ,  $v \approx w$  se per ogni lato  $\ell \in L$  esiste un cammino da  $v$  a  $w$  che non passa per  $\ell$ .

(a) Si dimostri che  $\approx$  è una relazione di equivalenza in  $V$ .  
 Per ogni  $v \in V$  sia  $CC_v$  la classe di equivalenza di  $v$  modulo  $\approx$ . Il grafo  $G$  si dice *doppiamente connesso* se tutti gli elementi di  $V$  sono tra loro equivalenti nella relazione  $\approx$ .

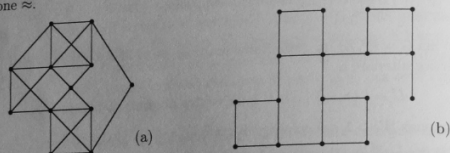


Figura 13.4

- (b) Si dimostri che il grafo con 17 vertici rappresentato nella figura 13.4 (b) è connesso, se ne determinino le classi di equivalenza modulo  $\approx$ , e si dica se tale grafo è doppiamente connesso.

## Capitolo 14. Alberi e grafi piani

In questo capitolo, quando non viene esplicitamente indicato il contrario, si intende che tutti i grafi considerati sono grafi non orientati.

Una *foresta* è un grafo (non necessariamente finito) privo di circuiti. Un *albero* è un grafo connesso privo di circuiti. Quindi le componenti connesse delle foreste sono alberi.

**TEOREMA 14.1.** Sia  $G = (V, L)$  un grafo (non necessariamente finito) con almeno due vertici. Le seguenti affermazioni sono equivalenti:

- (a)  $G$  è un albero;  
 (b) per ogni  $v, w \in V$  esiste un unico cammino da  $v$  a  $w$ .  
 (c)  $G$  è connesso e per ogni  $\ell \in L$  il grafo  $G' = (V, L \setminus \{\ell\})$  è un grafo sconnesso.  
 (d)  $G$  è un grafo privo di circuiti, e per ogni  $v, w \in V$ , ove  $v$  e  $w$  sono vertici distinti non adiacenti di  $G$ , se  $\ell = \{v, w\}$  il grafo  $G'' = (V, L \cup \{\ell\})$  ha un unico circuito.

*Dimostrazione.* (a)  $\Rightarrow$  (b) Dato che ogni albero è connesso, per ogni  $v, w \in V$  esiste un cammino da  $v$  a  $w$ . Se esistessero due cammini distinti da  $v$  a  $w$ , allora il grafo avrebbe un circuito.

(b)  $\Rightarrow$  (c) Sia  $G = (V, L)$  un grafo con la proprietà che per ogni  $v, w \in V$  esiste un unico cammino da  $v$  a  $w$ . Allora  $G$  è un grafo connesso. Sia  $\ell \in L$  un qualunque lato del grafo. Se  $\ell = \{v, w\}$ , allora per ipotesi c'è un unico cammino da  $v$  a  $w$ , e questo è necessariamente il cammino di lunghezza uno che consiste del solo lato  $\ell$ . Quindi se lo si toglie non ci può più essere nessun cammino da  $v$  a  $w$ , e pertanto il grafo  $G' = (V, L \setminus \{\ell\})$  è sconnesso.

(c)  $\Rightarrow$  (d) Supponiamo che valga la (c) e mostriamo che  $G$  è un grafo privo di circuiti. Se  $G$  avesse un circuito ed  $\ell$  fosse un lato di questo circuito, allora il grafo  $G' = (V, L \setminus \{\ell\})$  sarebbe connesso, perché togliendo un lato di un circuito "non si interrompe la connessione". Questo contraddirebbe (c).

Mostriamo che se  $v, w \in V$ , ove  $v$  e  $w$  sono vertici distinti non adiacenti di  $G$ , ed  $\ell = \{v, w\}$ , il grafo  $G'' = (V, L \cup \{\ell\})$  ha un circuito. Dato che  $G$  è connesso, c'è un cammino  $\ell_1, \ell_2, \dots, \ell_n$  in  $G$  da  $v$  a  $w$ . Ne segue che in  $G' = (V, L \cup \{\ell\})$  il cammino  $\ell_1, \ell_2, \dots, \ell_n, \ell$  è un circuito. Mostriamo che  $\ell_1, \ell_2, \dots, \ell_n, \ell$  è l'unico circuito di  $G'$ . Sia  $\ell'_1, \ell'_2, \ell'_3, \dots, \ell'_m$  un altro circuito di  $G' = (V, L \cup \{\ell\})$ . Allora  $\ell$

deve essere un lato di questo circuito, perché  $G$  è un grafo privo di circuiti. Senza perdita di generalità si può supporre che  $\ell = \ell'_1$ . Ma allora, come si può vedere anche nella figura 14.1, il grafo  $G$  avrebbe il circuito  $\ell_1, \ell_2, \dots, \ell_n, \ell'_2, \ell'_3, \dots, \ell'_m$ , e questo contraddice quanto avevamo già dimostrato, cioè che  $G$  è privo di circuiti.

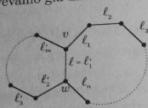


Figura 14.1

(d)  $\Rightarrow$  (a) Si deve dimostrare che se vale (d) allora il grafo  $G$  è connesso, cioè che se  $v, w$  sono due vertici distinti di  $G$  c'è un cammino da  $v$  a  $w$  in  $G$ . Ora se  $v$  e  $w$  sono adiacenti in  $G$  il cammino esiste certamente. Se invece  $v$  e  $w$  non sono adiacenti in  $G$  ed  $\ell = \{v, w\}$ , il grafo  $G'' = (V, L \cup \{\ell\})$  ha un unico circuito per la condizione (d). Dato che  $G$  non ha circuiti, questo unico circuito di  $G'' = (V, L \cup \{\ell\})$  deve passare per  $\ell$ . Sia dunque  $\ell_1, \ell_2, \dots, \ell_n, \ell$  questo unico circuito di  $G''$ . Allora  $\ell_1, \ell_2, \dots, \ell_n$  è un cammino in  $G$  da  $v$  a  $w$ . Questo dimostra che  $G$  è connesso.  $\square$

**PROPOSIZIONE 14.2.** Ogni albero finito con almeno due vertici ha almeno un vertice di grado uno.

Nel caso dei grafi finiti, gli alberi, oltre che nei modi visti nel teorema 14.1, possono essere caratterizzati anche mediante le condizioni del seguente teorema.

**TEOREMA 14.3.** Sia  $G = (V, L)$  un grafo finito con  $n$  vertici. Le seguenti affermazioni sono equivalenti:

- (a)  $G$  è un albero;
- (b)  $G$  è un grafo privo di circuiti ed ha  $n - 1$  lati.
- (c)  $G$  è un grafo connesso ed ha  $n - 1$  lati.

**Dimostrazione.** (a)  $\Rightarrow$  (b) Si deve dimostrare che un albero con  $n$  vertici ha  $n - 1$  lati. Dimostriamolo per induzione su  $n$ . Il caso  $n = 1$  è ovvio (un albero con un unico vertice non ha lati). Se  $n \geq 2$ , l'albero  $G$  ha almeno un vertice  $v$  di grado uno per la proposizione 14.2. Sia  $l$  l'unico lato avente  $v$  come estremo. Rimuovendo da  $G$  il vertice  $v$  e il lato  $l$  si ottiene un sottografo  $G'$  di  $G$  che è ancora connesso e che certamente non contiene circuiti; quindi  $G'$  è un albero con  $n - 1$  vertici. Per l'ipotesi induttiva  $G'$  ha  $n - 2$  lati. Pertanto il grafo  $G$  ha  $n - 1$  lati.

(b)  $\Rightarrow$  (c) Si deve dimostrare che un grafo con  $n$  vertici,  $n - 1$  lati e privo di circuiti (cioè una foresta) deve essere connesso. Supponiamo che  $G$  abbia  $k$

componenti connesse  $G_1 = (V_1, L_1), G_2 = (V_2, L_2), \dots, G_k = (V_k, L_k)$ . Allora se  $G$  ha  $n$  vertici, dato che  $G_i$  è un albero per ogni  $i = 1, 2, \dots, k$ ,  $G_i$  deve avere  $n_i - 1$  lati per quanto è stato dimostrato nell'implicazione (a)  $\Rightarrow$  (b). Quindi  $G$  ha complessivamente  $n_1 + n_2 + \dots + n_k$  vertici e  $(n_1 - 1) + (n_2 - 1) + \dots + (n_k - 1) = (n_1 + n_2 + \dots + n_k) - k$  lati. Ma  $G$  ha  $n$  vertici e  $n - 1$  lati per ipotesi, e pertanto  $n_1 + n_2 + \dots + n_k = n$  e  $k = 1$ . Quindi il grafo  $G$  deve essere connesso.

(c)  $\Rightarrow$  (a) Si deve dimostrare che se un grafo  $G = (V, L)$  è connesso, ha  $n$  vertici e  $n - 1$  lati, allora  $G$  deve essere privo di circuiti. Si supponga per assurdo che  $G$  abbia un circuito. Sia  $\ell_1$  un lato di questo circuito. Allora  $G_1 = (V, L \setminus \{\ell_1\})$  è un grafo connesso con  $n$  vertici e  $n - 2$  lati. Se  $G_1$  contiene un circuito ed  $\ell_2$  appartiene a questo circuito, allora  $G_2 = (V, L \setminus \{\ell_1, \ell_2\})$  è un grafo connesso con  $n$  vertici e  $n - 3$  lati. Continuando con questo procedimento, cioè interrompendo uno ad uno tutti i circuiti, si costruisce un grafo  $G_t$  con  $n$  vertici e meno di  $n - 1$  lati, connesso e privo di circuiti. Allora  $G_t$  è un albero con  $n$  vertici e meno di  $n - 1$  lati, e questo contraddice l'implicazione (a)  $\Rightarrow$  (b) da noi già dimostrata. Questa contraddizione prova che  $G$  è un albero.  $\square$

Se  $G = (V, L)$  è un grafo (o un multigrafo) connesso, un albero di supporto di  $G$  è un sottografo  $G' = (V, L')$  di  $G$  che è un albero e che ha lo stesso insieme di vertici di  $G$ . Ovviamente ogni grafo (o multigrafo) finito connesso ha un albero di supporto: è sufficiente ottenere  $G'$  da  $G$  cancellando uno alla volta i lati appartenenti ai circuiti (come si è fatto nella dimostrazione di (c)  $\Rightarrow$  (a) nel teorema precedente) e cancellando i lati multipli nei multigrafi. Applicando il teorema 14.3 ad un albero di supporto di un qualunque grafo o multigrafo finito connesso si ottiene il seguente corollario.

**COROLLARIO 14.4.** Ogni grafo (o multigrafo) finito connesso con  $n$  vertici ha almeno  $n - 1$  lati.

Un albero con radice  $r$  è un albero nel quale è stato fissato un vertice  $r$ , detto radice dell'albero. I vertici di grado 1 diversi dalla radice  $r$  di un albero con radice  $r$  si dicono le foglie dell'albero.

Dato un albero con radice  $r$ , si dice livello di un qualunque vertice  $v$  dell'albero la distanza  $d(v, r)$ . Si noti che in ogni albero c'è un unico cammino tra  $v$  ed  $r$ . Si noti qualsiasi, e quindi  $d(v, r)$  è la lunghezza dell'unico cammino tra  $v$  ed  $r$ . Dato un albero con radice  $r$  è possibile orientare in modo naturale i lati dell'albero: se  $\{v, w\}$  è un lato dell'albero si orienta il lato da  $v$  a  $w$  se e solo se il livello di  $v$  è minore del livello di  $w$ . Ne segue che ogni albero finito con radice ha una struttura naturale di grafo orientato, e ogni suo vertice  $v$  ha un grado di entrata  $d^+(v)$  e un grado di uscita  $d^-(v)$ . Si noti che il livello di un vertice  $v$  è zero se e solo se  $v = r$ . Quindi il livello di  $r$  è minore del livello di ogni altro vertice  $v$ . Ne segue che non esistono



lati orientati che entrano in  $r$ , cioè  $d^+(r) = 0$ . Se invece  $v \neq r$  è un qualunque altro vertice dell'albero con radice  $r$ , c'è un unico lato orientato che entra in  $v$  (perché se ce ne fossero due o più, ci sarebbero due vertici  $v_1$  e  $v_2$  di livello inferiore al livello di  $v$  e tali che i lati  $\{v, v_1\}$  e  $\{v, v_2\}$  appartengono all'albero; ma allora con questi due lati, con il cammino da  $v_2$  ad  $r$  e con il cammino da  $r$  a  $v_1$  sarebbe possibile costruire un circuito, e questo è assurdo). Quindi  $d^+(v) = 1$  per ogni vertice  $v \neq r$  dell'albero.

Rappresenteremo un albero con radice disponendo i vertici su righe successive a seconda del loro livello: nella prima riga disegneremo l'unico vertice di livello 0 (la radice stessa), nella seconda riga tutti i vertici di livello 1, nella terza tutti quelli di livello 2, nella successiva quelli di livello 3, e così via. Ad esempio il grafo della figura 14.2 (a) è un albero perché è connesso ed è privo di circuiti. Fissiamo come radice il vertice  $r$ . Abbiamo ora un albero con radice. Rappresentiamolo disponendo i vertici di livello  $\ell$  nella  $(\ell + 1)$ -esima riga. Si ottiene allora il diagramma della figura 14.2 (b).

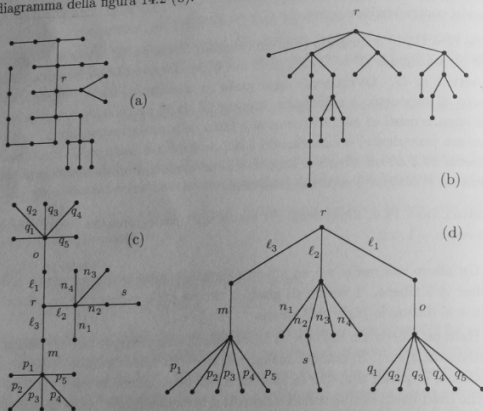


Figura 14.2

Un albero ordinato con radice è un albero con radice nel quale l'insieme dei lati che escono da ogni vertice  $v$  è totalmente ordinato. Nel disegnare un albero ordinato finito con radice rappresentiamo i lati uscenti da un qualunque vertice secondo l'ordine totale fissato in cui si succedono.

ESEMPIO 1. Si consideri l'albero con radice disegnato nella figura 14.2 (c). Lo si rappresenta disponendo i vertici di livello  $\ell$  nella  $(\ell + 1)$ -esima riga. Si ottiene il diagramma della figura 14.2 (d). Tale albero con radice diventa poi un albero ordinato con radice se si fissa un ordine sugli insiemi di lati  $\{\ell_1, \ell_2, \ell_3\}$ ,  $\{m\}$ ,  $\{n_1, n_2, n_3, n_4\}$ ,  $\{o\}$ ,  $\{p_1, p_2, p_3, p_4, p_5\}$ ,  $\{q_1, q_2, q_3, q_4, q_5\}$ ,  $\{s\}$ . Ordiniamo totalmente questi sette insiemi ponendo, ad esempio,  $\ell_2 < \ell_3 < \ell_1$ ,  $n_4 < n_1 < n_2 < n_3$ ,  $p_1 < p_2 < p_3 < p_4 < p_5$  e  $q_5 < q_4 < q_3 < q_2 < q_1$  (ovviamente non serve fissare un ordinamento sugli insiemi con un solo elemento, in quanto su di essi c'è un unico ordinamento possibile). Abbiamo così ottenuto un albero ordinato con radice. Rappresentando i lati uscenti da un qualunque vertice secondo l'ordine totale appena fissato il grafo diventa quello della figura 14.3. □

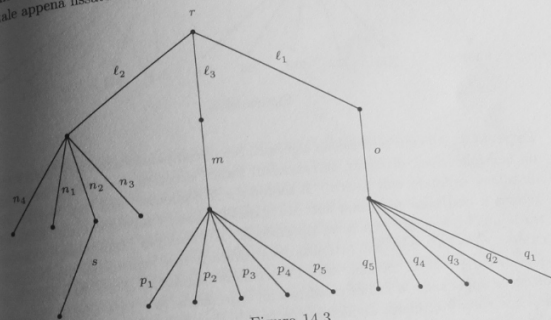


Figura 14.3

È possibile dare un indice in modo naturale ai vertici di un albero finito ordinato con radice. L'indice di un vertice  $v$  è una successione finita  $S(v)$  di numeri naturali di lunghezza uguale al livello del vertice  $v$ . Alla radice  $r$  si assegna come indice  $S(r)$  l'unica successione di lunghezza 0, ossia la successione vuota. Ad ogni vertice  $v \neq r$ , se  $u$  è il predecessore di  $v$ , e  $v$  è l'estremo del  $k$ -esimo lato che esce da  $u$ , si assegna a  $v$  come indice la successione  $S(u)$  ottenuta dalla giustapposizione della successione  $S(u)$  e del numero naturale  $k$ . L'esempio seguente servirà a capire questo concetto, molto più facile da comprendere che da spiegare.

ESEMPIO 2. Nell'esempio 1 abbiamo studiato l'albero ordinato con radice  $r$  rappresentato nella figura 14.3. Gli indici assegnati ai vertici nel modo appena descritto sono quelli della figura 14.4. □

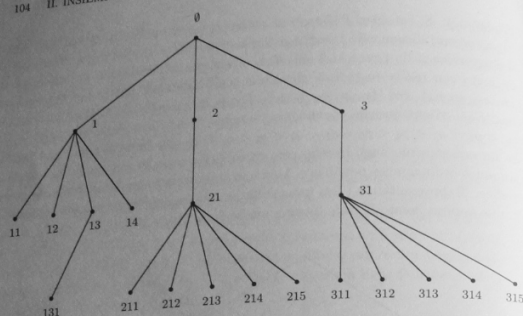


Figura 14.4

ESEMPIO 3. Ad ogni espressione algebrica in cui compaiono addizioni, sottrazioni, moltiplicazioni, divisioni, estrazioni di radici, eccetera, può essere associato un albero ordinato con radice. Il metodo è il seguente: ogni espressione algebrica è costituita per passi successivi da espressioni algebriche più semplici tra le quali è eseguita una certa operazione. Ad esempio l'espressione algebrica  $c + \sqrt{(d - (a + bc))}/a$  è ottenuta sommando le due espressioni algebriche  $c$  e  $\sqrt{(d - (a + bc))}/a$ . A sua volta l'espressione algebrica  $\sqrt{(d - (a + bc))}/a$  è ottenuta applicando la radice quadrata all'espressione  $(d - (a + bc))/a$ , la quale a sua volta è ottenuta dividendo tra loro le due espressioni  $d - (a + bc)$  e  $a$ . L'espressione  $d - (a + bc)$  si ottiene poi sottraendo le due espressioni  $d$  e  $a + bc$ ; quest'ultima si ottiene sommando le due espressioni  $a$  e  $bc$ . Infine  $bc$  è ottenuta moltiplicando  $b$  e  $c$ . Tutta questa lunga descrizione può essere rappresentata dal grafo ordinato con radice raffigurato nella figura 14.5 (a). Si noti che in queste figure le foglie dell'albero rappresentano le variabili che compaiono nell'espressione, mentre tutti gli altri vertici dell'albero rappresentano le operazioni che compaiono nell'espressione stessa. Si noti anche che l'albero associato ad una espressione algebrica nel modo appena descritto è un albero ordinato con radice. Cambiando l'ordine nell'insieme dei lati che escono da un vertice  $v$  si ottiene un albero ordinato che rappresenta un'espressione algebrica diversa dalla precedente. Ad esempio l'albero ordinato con radice rappresentato nella figura 14.5 (b), ottenuto dall'albero ordinato della figura 14.5 (a) invertendo gli ordini sugli insiemi dei lati che escono da due vertici, è l'albero ordinato associato all'espressione  $c + \sqrt{a}/(d - (bc + a))$ .

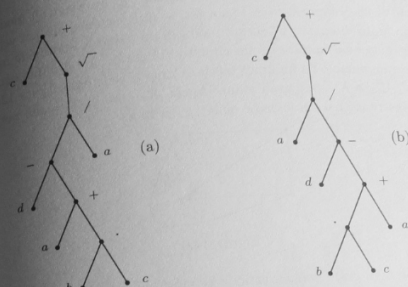


Figura 14.5

La notazione da noi usata per scrivere un'espressione algebrica è quella cosiddetta *a infisso*. Infatti nel denotare un'espressione ottenuta sommando, sottraendo, moltiplicando o dividendo due espressioni, il simbolo  $+$ ,  $-$ ,  $\cdot$  o  $/$  viene scritto tra le due espressioni. Ad esempio scriviamo  $a + bc$  e  $a - bc$  per denotare le espressioni algebriche ottenute rispettivamente sommando e sottraendo le due espressioni  $a$  e  $bc$ . Si noti che l'addizione, la sottrazione, la moltiplicazione e la divisione sono operazioni *binarie*, cioè si applicano a due argomenti. Diverso è il caso dell'estrazione di radice quadrata, che è un'operazione *unaria*, ossia si applica ad un solo argomento. Premesso questo, le espressioni algebriche possono essere scritte senza pericolo di ambiguità ponendo il simbolo dell'operazione prima degli operandi. Tale notazione è detta *notazione polacca* (perché introdotta dal matematico polacco Lukasiewicz). Ad esempio le espressioni algebriche da noi usualmente denotate  $a + b$ ,  $a \cdot b$ ,  $c + \sqrt{(d - (a + bc))}/a$  e  $c + \sqrt{a}/(d - (bc + a))$ , in notazione polacca si scrivono  $+ab$ ,  $\cdot ab$ ,  $+c\sqrt{-d + a \cdot bca} + c\sqrt{a - d + bca}$  rispettivamente. Si noti che la notazione polacca permette di eliminare completamente l'uso delle parentesi, mentre deve essere invece noto a priori a quanti operandi si applica ciascun simbolo (la cosiddetta *arietà* di un'operazione: qui avevamo precedentemente stabilito che i simboli  $+$ ,  $-$ ,  $\cdot$ ,  $/$  si applicano a due operandi, cioè rappresentano operazioni binarie, mentre  $\sqrt{\phantom{x}}$  si applica ad un solo operando, ossia l'estrazione di radice quadrata è un'operazione unaria.\* □

\*Nel capitolo 17 definiremo in modo preciso ciò che deve intendersi per operazione. In base a quella definizione non sarà ad esempio possibile considerare come operazione tra numeri reali la divisione. Nel presente contesto stiamo usando la parola "operazione" in modo informale.

Un grafo si dice *piano* se può essere disegnato in un piano in modo che gli archi di curva che rappresentano i suoi lati si intersechino solo nei vertici. Un grafo piano finito disegnato in questo modo in un piano lo suddivide in regioni, dette *facce*, ciascuna limitata da un circuito del grafo. Ad esempio ogni albero finito è un grafo piano e ha un'unica faccia. Come si vede dalla figura 12.4 i grafi completi  $K_1$ ,  $K_2$  e  $K_3$  sono grafi piani. Anche  $K_4$  è un grafo piano perché può essere rappresentato nel piano come nella figura 14.6.

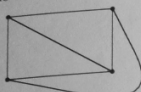


Figura 14.6

È chiaro che ogni grafo con  $n$  vertici è isomorfo ad un sottografo di  $K_n$ . Ne segue che ogni grafo con al più quattro vertici è piano. Si potrebbe dimostrare invece che  $K_5$  non è un grafo piano, e anzi vale il seguente teorema la cui dimostrazione non è elementare.

**TEOREMA 14.5 (TEOREMA DI KURATOWSKI).** *Un grafo finito è piano se e solo se non contiene sottografi isomorfi a  $K_5$  o a  $K_{3,3}$ .*

Ricordiamo infine il seguente famoso teorema.

**TEOREMA 14.6.** *Sia  $G$  un grafo piano finito connesso con  $|V|$  vertici,  $|L|$  lati e  $|F|$  facce. Allora*

$$|V| - |L| + |F| = 2 \quad (\text{Formula di Eulero}).$$

### Esercizi svolti

**14.1.** Un grafo in cui tutti i vertici sono isolati si dice un *grafo nullo*.

Quanti lati, quante facce e quante componenti connesse ha un grafo nullo con  $n$  vertici? Un grafo nullo è piano? Quanto vale  $|V| - |L| + |F|$  per un grafo nullo? Perché non si può applicare sempre la formula di Eulero?

**Soluzione.** Sia  $G$  un grafo nullo con  $n \geq 1$  vertici. Allora  $G$  ha ovviamente 0 lati, 1 faccia,  $n$  componenti connesse, ed è un grafo piano. Per un tale grafo si ha  $|V| - |L| + |F| = n + 1$ . Se  $n = 1$ , allora  $G$  è un grafo piano connesso e quindi per esso vale la formula di Eulero (in tal caso si ha infatti  $|V| - |L| + |F| = 1 - 0 + 1 = 2$ ). Se  $n \geq 2$ , allora il grafo piano  $G$  non è connesso e quindi ad esso non si può applicare il teorema 14.6 (e in tal caso si ha infatti  $|V| - |L| + |F| = n + 1 \geq 3$ ).  $\square$

**14.2.** Impariamo un metodo per passare da un'espressione algebrica scritta in notazione polacca all'albero ordinato con radice corrispondente e viceversa. Tale metodo si basa sull'osservazione, illustrata nella figura 14.7, che se partendo dalla radice si percorre l'albero ordinato associato ad un'espressione seguendo il percorso tratteggiato (quello che "costeggia" l'albero in senso antiorario), si incontrano i vertici per i quali non si è ancora passati esattamente nell'ordine in cui compaiono nell'espressione scritta in notazione polacca.

Ad esempio l'albero ordinato dell'espressione  $c + \sqrt{(d - (a + bc)) / a}$  è quello della figura 14.7 (a), e la stessa espressione in notazione polacca è  $+c\sqrt{-d+a \cdot bca}$ .

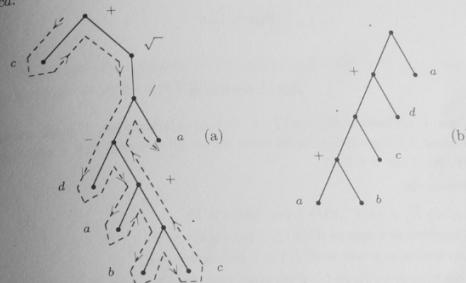


Figura 14.7

- Si disegni l'albero ordinato associato all'espressione algebrica in notazione a infisso  $((a + ab) + (ab)c) + ((ab)c)d$  e la si scriva in notazione polacca.
- Si scriva l'espressione algebrica associata al grafo della figura 14.7 (b) sia in notazione a infisso che in notazione polacca.
- Si rappresenti l'albero ordinato associato all'espressione algebrica che in notazione polacca si scrive  $-ab + ab$  e la si scriva in notazione ad infisso (qui i simboli  $+$ ,  $-$ ,  $\cdot$  indicano tutti operazioni binarie).

**Soluzione.** (a) L'albero è quello disegnato nella figura 14.8 (a). L'espressione in notazione polacca è  $+ + + a \cdot ab \cdot abc \cdots abcd$ .

(b)  $((a + b)c + d)a$ ;  $\cdot + \cdot + abcd$ .

(c) L'albero ordinato è quello della figura 14.8 (b). L'espressione in notazione a infisso è  $(a - b)(a + b)$ .  $\square$

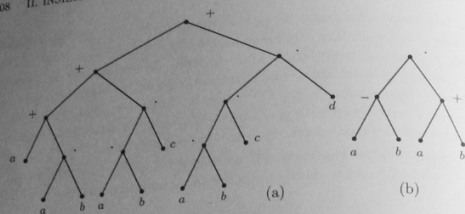


Figura 14.8

## Altri esercizi

14.3. Siano  $V$  un insieme finito ed  $f: V \rightarrow V$  un'applicazione. Il grafo orientato della funzione  $f$  è il grafo  $G_f$  che ha come vertici gli elementi di  $V$  e come lati le coppie  $(v, f(v))$  con  $v \in V$ .

Si dimostri che

- (a) nel grafo  $G_f$  si ha  $d^-(v) = 1$  per ogni  $v \in V$ ;
- (b)  $f$  è iniettiva se e solo se  $d^+(v) \leq 1$  per ogni  $v \in V$ ;
- (c)  $f$  è suriettiva se e solo se  $d^+(v) \geq 1$  per ogni  $v \in V$ ;
- (d)  $f$  è biiettiva se e solo se  $G_f$  è un grafo orientato regolare di grado 0, cioè se e solo se  $d(v) = 0$  per ogni  $v \in V$ ;
- (e) dato un qualunque grafo orientato finito  $G = (V, L)$  tale che  $d^-(v) = 1$  per ogni  $v \in V$ , esiste un'unica applicazione  $f: V \rightarrow V$  tale che  $G_f = G$ .

14.4. Siano  $n, m$  numeri interi positivi fissati. Si consideri il grafo  $G$  con  $nm$  vertici disegnato nella figura 14.9.

- (a) Quanti lati ha il grafo  $G$ ?
- (b) Quante facce ha il grafo  $G$ ?
- (c) Per quali valori di  $n$  ed  $m$  il grafo  $G$  ha un cammino euleriano?

14.5. Si dimostri il seguente corollario al teorema di Kuratowski (teorema 14.5): Ogni grafo finito con  $t$  lati, ove  $t < 9$ , è piano.

- 14.6. (a) È possibile disegnare un grafo connesso con 5 vertici, 8 lati e con un cammino euleriano?
- (b) È possibile disegnare un grafo piano connesso con 5 vertici e 8 lati?

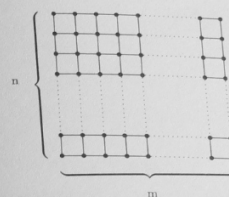


Figura 14.9

14.7. Si dimostri che togliendo un lato qualunque al grafo  $K_5$  o al grafo  $K_{3,3}$  si ottiene sempre un grafo piano.

## PARTE TERZA

## QUALCHE NOZIONE DI LOGICA MATEMATICA

## Capitolo 15. Il calcolo proposizionale

**Proposizioni e connettivi logici.** Una *proposizione* è un'espressione che è o vera o falsa, ma non contemporaneamente vera e falsa.

ESEMPIO 1. Sono proposizioni:

$A$  = "La mosca è un insetto",

$B$  = "L'elefante è un insetto",

$C$  = " $\sqrt{2} = 5$ ",

$D$  = "Singapore è in Europa".

Non sono invece proposizioni, nel senso da noi appena definito, le domande ("Quanti anni hai?"), le esclamazioni ("Buongiorno!"), allineamenti di parole o di simboli privi di significato ("La insetto mosca un è"); queste non sono proposizioni perché non sono né vere né false.  $\square$

*Vero e falso* si dicono i *valori di verità*. Ad esempio, il valore di verità della proposizione  $A$  dell'esempio 1 è vero, il valore di verità delle proposizioni  $B$ ,  $C$  e  $D$  è falso. Date due proposizioni  $A$  e  $B$  è possibile formare le proposizioni

- (1) " $A$  e  $B$ ", detta la *coniunzione* di  $A$  e  $B$ , e indicata in simboli con  $A \wedge B$ ;
- (2) " $A$  o  $B$ ", detta la *disgiunzione* di  $A$  e  $B$ , e indicata in simboli con  $A \vee B$ ;
- (3) "non  $A$ ", detta la *negazione* di  $A$  e indicata con  $\neg A$ ;
- (4) " $A$  implica  $B$ " (o "se  $A$  allora  $B$ "), detta *implicazione* (o meglio *implicazione materiale*) e indicata con  $A \rightarrow B$ ;
- (5) " $A$  se e solo se  $B$ ", detta *doppia implicazione*, indicata con  $A \leftrightarrow B$ .



Se  $A, B, C, D$  sono le proposizioni dell'esempio 1, allora  $A \wedge D$  è "La mosca è un insetto e Singapore è in Europa",  $B \vee C$  è "L'elefante è un insetto o  $\sqrt{2} = 5$ ",  $\neg B$  è "L'elefante non è un insetto",  $\neg C$  è " $\sqrt{2} \neq 5$ ",  $B \rightarrow C$  è "Se l'elefante è un insetto allora  $\sqrt{2} = 5$ ",  $B \leftrightarrow D$  è "L'elefante è un insetto se e solo se Singapore è in Europa". I simboli  $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$  si dicono i *connettivi logici*.

Il valore di verità di una proposizione composta dipende dai valori di verità delle proposizioni che la compongono nel modo descritto nella seguente *tabella di verità*, nella quale  $V$  denota il valore di verità *vero* ed  $F$  il valore di verità *falso*.

$A$	$B$	$A \wedge B$	$A \vee B$	$\neg A$	$A \rightarrow B$	$A \leftrightarrow B$
$V$	$V$	$V$	$V$	$F$	$V$	$V$
$V$	$F$	$F$	$V$	$F$	$F$	$F$
$F$	$V$	$F$	$V$	$V$	$V$	$F$
$F$	$F$	$F$	$F$	$V$	$V$	$V$

Quindi se  $A, B, C, D$  sono le proposizioni dell'esempio 1, si ha che  $A \wedge D$  (= "La mosca è un insetto e Singapore è in Europa") è falsa,  $A \vee D$  (= "La mosca è un insetto oppure Singapore è in Europa") è vera,  $\neg B$  (= "L'elefante non è un insetto") è vera,  $A \rightarrow C$  (= "Se la mosca è un insetto allora la mosca è un insetto") è vera,  $A \rightarrow D$  (= "Se la mosca è un insetto allora  $\sqrt{2} = 5$ ") è falsa,  $B \rightarrow A$  (= "Se l'elefante è un insetto allora la mosca è un insetto") è vera,  $B \rightarrow C$  (= "Se l'elefante è un insetto allora  $\sqrt{2} = 5$ ") è vera,  $D \rightarrow D$  (= "Se Singapore è in Europa allora Singapore è in Europa") è vera, e infine  $B \leftrightarrow C$  (= "L'elefante è un insetto se e solo se  $\sqrt{2} = 5$ ") è vera.

Si faccia attenzione a come viene definito il valore di verità di  $A \rightarrow B$ . Il fatto che proposizioni del tipo "Se l'elefante è un insetto allora  $\sqrt{2} = 5$ " e "Se  $\sqrt{2} = 5$  allora la mosca è un insetto" siano per noi vere può sembrare un po' strano. Il motivo è che nella implicazione di cui si fa solitamente uso nel linguaggio comune si è abituati ad una correlazione di tipo causa ed effetto tra l'antecedente e il conseguente (come ad esempio in "Se Singapore è in Europa allora gli abitanti di Singapore sono europei"). Per noi, invece,  $A \rightarrow B$  è una proposizione, cioè è vera o falsa, qualunque siano le proposizioni  $A$  e  $B$ , anche se tra di esse non c'è una relazione di causa ed effetto:  $A \rightarrow B$  è falsa se e solo se  $A$  è vera e  $B$  è falsa; in tutti gli altri casi  $A \rightarrow B$  è vera.

Applicando ripetutamente i connettivi logici a delle proposizioni  $A, B, C, \dots$ , è possibile formare proposizioni composte sempre più complesse. Naturalmente il valore di verità di una proposizione composta dipende dal valore di verità delle proposizioni che la compongono.

**Forme proposizionali.** Per meglio comprendere il concetto di *forma proposizionale* che definiremo tra breve, compiamo una breve digressione ricordando come vengono introdotti i polinomi nelle scuole medie. Il metodo adottato consiste usualmente nell'introdurre dei simboli  $x, y, z, \dots$  che vengono chiamati *variabili (numeriche)* e che poi vengono trattati, cioè sommati, moltiplicati, eccetera, come se fossero dei numeri reali. Tale procedimento può essere descritto con un po' più di rigore nel modo seguente: Si considerino  $n$  simboli  $x_1, x_2, \dots, x_n$ . Le *forme polinomiali* (a coefficienti reali nelle variabili  $x_1, x_2, \dots, x_n$ ) sono le espressioni definite nel modo seguente:

- $x_1, x_2, \dots, x_n$  e tutti i numeri reali sono forme polinomiali;
- se  $f$  e  $g$  sono forme polinomiali, allora  $(f + g)$ ,  $(-f)$ ,  $(f \cdot g)$  sono forme polinomiali;
- sono forme polinomiali (nelle variabili  $x_1, x_2, \dots, x_n$ ) solo le espressioni determinate per mezzo di (a) e (b).

Effettueremo un procedimento simile per le proposizioni invece che per i numeri reali, ottenendo forme proposizionali invece che forme polinomiali.

Si considerino  $n$  simboli  $A_1, A_2, \dots, A_n$  che chiameremo *variabili proposizionali*. Le *forme proposizionali* (nelle variabili  $A_1, A_2, \dots, A_n$ ) sono le espressioni definite nel modo seguente:

- $A_1, A_2, \dots, A_n$  sono forme proposizionali;
- se  $P$  e  $Q$  sono forme proposizionali, allora  $(P \wedge Q)$ ,  $(P \vee Q)$ ,  $(\neg P)$ ,  $(P \rightarrow Q)$  e  $(P \leftrightarrow Q)$  sono forme proposizionali;
- sono forme proposizionali (nelle variabili  $A_1, A_2, \dots, A_n$ ) solo le espressioni determinate per mezzo di (a) e (b).

**ESEMPIO 2.** Consideriamo le variabili proposizionali  $A$  e  $B$ . Allora  $(A \rightarrow B)$  e  $(\neg A)$  sono forme proposizionali, e quindi  $((\neg A) \vee B)$  è una forma proposizionale, e pertanto anche  $((A \rightarrow B) \leftrightarrow ((\neg A) \vee B))$  è una forma proposizionale.  $\square$

Per limitare l'uso delle parentesi nelle forme proposizionali, conviene innanzitutto eliminare le parentesi più esterne. Poi, come con le forme polinomiali si "eseguono prima" l'operazione  $\cdot$  e poi le operazioni  $+$  e  $-$ , così noi "eseguiremo prima" l'operazione  $\neg$ , poi  $\wedge$  e  $\vee$ , e infine  $\rightarrow$  e  $\leftrightarrow$ . Abbiamo quindi una precedenza tra operatori: l'operatore  $\neg$  precede gli operatori  $\wedge$  e  $\vee$ , e questi precedono a loro volta gli operatori  $\rightarrow$  e  $\leftrightarrow$ .

**ESEMPIO 3.** Invece di scrivere  $((A \rightarrow B) \leftrightarrow ((\neg A) \vee B))$  scriveremo  $(A \rightarrow B) \leftrightarrow \neg A \vee B$ . Invece di scrivere  $((A \wedge B) \rightarrow (A \rightarrow (A \rightarrow B)))$  scriveremo  $A \wedge B \rightarrow (A \rightarrow (A \rightarrow B))$ . Invece di scrivere  $((A \wedge (A \rightarrow B)) \rightarrow B)$  scriveremo  $A \wedge (A \rightarrow B) \rightarrow B$ .  $\square$

Per ogni forma proposizionale nelle variabili  $A_1, A_2, \dots, A_n$  è possibile costruire una tavola di verità; è facile dimostrare che la tavola di verità di una tale forma proposizionale in  $n$  variabili ha  $2^n$  righe.

ESEMPIO 4. Ecco le tavole di verità delle forme proposizionali

$$A \wedge B \rightarrow (A \rightarrow (A \rightarrow B)) \quad \text{e} \quad A \wedge (A \rightarrow B) \rightarrow B :$$

A	B	$A \wedge B$	$A \rightarrow B$	$A \rightarrow (A \rightarrow B)$	$A \wedge B \rightarrow (A \rightarrow (A \rightarrow B))$
V	V	V	V	V	V
V	F	F	F	F	V
F	V	F	V	V	V
F	F	F	V	V	V

A	B	$A \rightarrow B$	$A \wedge (A \rightarrow B)$	$A \wedge (A \rightarrow B) \rightarrow B$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

Entrambe le forme proposizionali  $A \wedge B \rightarrow (A \rightarrow (A \rightarrow B))$  e  $A \wedge (A \rightarrow B) \rightarrow B$  dell'esempio 4 sono sempre vere, qualunque siano i valori di verità assegnati alle variabili  $A$  e  $B$ . Una forma proposizionale nelle variabili  $A_1, A_2, \dots, A_n$ , che sia sempre vera, indipendentemente dai valori di verità assegnati ad  $A_1, A_2, \dots, A_n$ , si dice una *tautologia*. Quindi le due forme proposizionali dell'esempio 4 sono entrambe tautologie. Una forma proposizionale che sia sempre falsa, indipendentemente dai valori di verità assegnati alle variabili proposizionali, si dice una *contraddizione*. Quindi una forma proposizionale  $P$  è una contraddizione se e solo se  $\neg P$  è una tautologia. Infine due forme proposizionali  $P$  e  $Q$  si dicono *logicamente equivalenti* se  $P \leftrightarrow Q$  è una tautologia.

### Esercizi svolti

15.1. Si dimostri che se  $P$  e  $Q$  sono forme proposizionali, le seguenti affermazioni sono equivalenti:

- $P$  e  $Q$  sono logicamente equivalenti;
- $P$  e  $Q$  hanno le stesse tavole di verità;
- $P$  è vera per una data assegnazione di valori di verità alle variabili se e solo se  $Q$  è vera per la stessa assegnazione;

(d)  $P$  è falsa per una data assegnazione di valori di verità alle variabili se e solo se  $Q$  è falsa per la stessa assegnazione.

Soluzione. (a)  $\Leftrightarrow$  (b) Per definizione dire che  $P$  e  $Q$  sono logicamente equivalenti vuol dire che  $P \leftrightarrow Q$  è una tautologia, cioè che  $P \leftrightarrow Q$  è sempre vera. Per come è stata definita la tavola di verità di  $\leftrightarrow$ , questo vuol dire che  $P$  e  $Q$  hanno le stesse tavole di verità.

Le equivalenze (b)  $\Leftrightarrow$  (c)  $\Leftrightarrow$  (d) sono ovvie.  $\square$

15.2. Si dimostri che se  $P$  e  $Q$  sono forme proposizionali allora  $P \rightarrow Q, \neg P \vee Q, \neg(P \wedge \neg Q), \neg Q \rightarrow \neg P$  sono logicamente equivalenti tra loro.

Soluzione. Per l'esercizio precedente è sufficiente dimostrare che  $P \rightarrow Q, \neg P \vee Q, \neg(P \wedge \neg Q), \neg Q \rightarrow \neg P$  hanno tutte le stesse tavole di verità. Le loro tavole di verità sono

P	Q	$P \rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

P	Q	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

P	Q	$\neg P$	$\neg P \vee Q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

P	Q	$\neg P$	$\neg Q$	$\neg Q \rightarrow \neg P$
V	V	F	F	V
V	F	F	V	F
F	V	V	F	V
F	F	V	V	V

Pertanto le quattro forme proposizionali indicate sono tutte equivalenti tra loro.  $\square$

L'equivalenza logica delle forme proposizionali  $P \rightarrow Q, \neg Q \rightarrow \neg P$  e  $\neg(P \wedge \neg Q)$  appena dimostrata è in qualche modo collegata a tre diverse possibilità che si hanno quando si vuole dimostrare una certa implicazione in matematica. Se si vuole dimostrare che da  $P$  segue  $Q$  è possibile o procedere direttamente (e quindi assumendo vero  $P$  dedurre la verità di  $Q$ , *dimostrazione diretta*), o sfruttare la prima equivalenza logica e dimostrare che da  $\neg Q$  segue  $\neg P$  (*dimostrazione per contrapposizione*, o *indiretta*), oppure ragionare *per assurdo*, supponendo la verità della negazione di  $P \rightarrow Q$ , nella forma di  $P \wedge \neg Q$  per la seconda equivalenza logica, e giungendo a una contraddizione.

Illustriamo queste tre possibilità con un facile esempio. Ricordiamo che dato un numero intero  $a$  è possibile dividere  $a$  per 2, e quindi esistono due interi

univocamente determinati  $q, r \in \mathbb{Z}$  tali che  $a = 2q + r$  e  $0 \leq r < 2$ . Vi sono quindi due possibilità che si escludono a vicenda:  $r = 0$  oppure  $r = 1$ . Se  $r = 0$ , cioè se  $a = 2q$  per qualche  $q \in \mathbb{Z}$ , ossia se 2 divide  $a$ , il numero  $a$  si dice *pari*. Se invece  $r = 1$ , cioè  $a = 2q + 1$  per qualche  $q \in \mathbb{Z}$ , il numero  $a$  si dice *dispari*. Vogliamo dimostrare che: *Se  $a, b \in \mathbb{Z}$  sono entrambi dispari, allora anche  $ab$  è dispari*. Questo semplicissimo risultato può essere dimostrato in tre modi:

*Dimostrazione diretta.* Se  $a$  e  $b$  sono interi dispari, esistono  $q, q' \in \mathbb{Z}$  tali che  $a = 2q + 1$  e  $b = 2q' + 1$ . Ne segue che  $ab = (2q + 1)(2q' + 1) = 2(2qq' + q + q') + 1$  dove  $2qq' + q + q' \in \mathbb{Z}$ , e quindi il prodotto  $ab$  è dispari.  $\square$

*Dimostrazione per contrapposizione.* Supponiamo che  $ab$  non sia dispari e dimostriamo che allora  $a$  e  $b$  non sono entrambi dispari. Se  $ab$  non è dispari,  $ab$  deve essere pari, e quindi  $2 \mid ab$ . Come è stato dimostrato nell'esercizio 4.10, se un numero primo divide un prodotto, esso divide uno dei fattori. Quindi  $2 \mid a$  oppure  $2 \mid b$ . Pertanto  $a$  è pari oppure  $b$  è pari. Se ne conclude che  $a$  e  $b$  non sono entrambi dispari.  $\square$

*Dimostrazione per assurdo.* Ragioniamo per assurdo e supponiamo che  $a$  e  $b$  siano entrambi dispari ma  $ab$  non sia dispari, cioè sia pari. Allora esistono  $a', b', c' \in \mathbb{Z}$  tali che  $a = 2a' + 1$ ,  $b = 2b' + 1$ ,  $ab = 2c'$ . Ma allora  $2c' = ab = (2a' + 1)(2b' + 1) = 4a'b' + 2a' + 2b' + 1$ , da cui  $2(c' - 2a'b' - a' - b') = 1$  con  $c' - 2a'b' - a' - b' \in \mathbb{Z}$ . Pertanto 2 divide 1, e questa è una contraddizione.  $\square$

### Altri esercizi

15.3. Si determini il valore di verità delle seguenti proposizioni:

- Se  $\sqrt{2} \neq 5$  allora  $\mathbb{N}$  è un insieme infinito.
- Se  $\mathbb{N}$  è un insieme finito allora  $\sqrt{2} = 5$ .
- Se  $\mathbb{N}$  è un insieme finito, si ha che  $\sqrt{2} = 5$  e che Palermo è una città della Sicilia.
- Se  $\mathbb{N}$  è un insieme finito e Palermo è una città della Sicilia, allora  $\sqrt{2} = 5$ .
- Se  $\mathbb{N}$  è un insieme finito e Palermo non è una città della Sicilia, allora  $\sqrt{2} = 5$ .

15.4. La forma proposizionale nelle variabili  $A, B, C$

$$A \vee (\neg A \wedge B) \vee \neg(B \wedge \neg C) \rightarrow C$$

è una tautologia?

15.5. La forma proposizionale nelle variabili  $A$  e  $B$

$$A \wedge B \rightarrow A \vee B$$

© 88-08-10250-5

è una tautologia?

15.6. Si dimostri che la forma proposizionale

$$(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$$

è una tautologia.

15.7. La forma proposizionale nelle variabili  $A, B, C$

$$(A \rightarrow B \vee C) \leftrightarrow (C \rightarrow (A \wedge \neg B))$$

è una contraddizione?

15.8. Le forme proposizionali

$$(\neg A \wedge C) \vee B \vee \neg(A \vee C) \quad \text{e} \quad (A \rightarrow B) \wedge (A \vee B \rightarrow B)$$

nelle variabili  $A, B, C$  sono logicamente equivalenti?

15.9. Si dimostri che le forme proposizionali

$$A \vee B \rightarrow C \quad \text{e} \quad (A \rightarrow C) \wedge (B \rightarrow C)$$

nelle variabili proposizionali  $A, B$  e  $C$  sono logicamente equivalenti.

15.10. Per ciascuna delle forme proposizionali seguenti si trovi una forma proposizionale logicamente equivalente ma "più semplice":

- $A \wedge (A \rightarrow B)$ ;
- $A \wedge (A \vee B)$ ;
- $(A \rightarrow B) \wedge \neg B$ ;
- $A \vee \neg A \rightarrow B$ .

## Capitolo 16. I quantificatori

Siano  $D_1, D_2, \dots, D_n$   $n$  insiemi fissati. Una *funzione proposizionale* (nelle  $n$  variabili individuali  $x_1, x_2, \dots, x_n$ ) su  $D_1 \times D_2 \times \dots \times D_n$  è un'espressione  $p(x_1, x_2, \dots, x_n)$  tale che  $p(a_1, a_2, \dots, a_n)$  sia una proposizione per ogni  $a_1 \in D_1, a_2 \in D_2, \dots, a_n \in D_n$ , cioè tale che  $p(a_1, a_2, \dots, a_n)$  sia vera o falsa quando si sostituisce una qualunque elemento  $a_1 \in D_1$  al posto della variabile  $x_1$ , un qualunque elemento  $a_2 \in D_2$  al posto della variabile  $x_2, \dots$ , un qualunque elemento  $a_n \in D_n$  al posto della variabile  $x_n$ . L'insieme  $D_1 \times D_2 \times \dots \times D_n$  è detto il *dominio* della funzione proposizionale  $p(x_1, x_2, \dots, x_n)$ , ed è talvolta sottointeso.

ESEMPIO 1. Siano  $D_1 = \mathbb{Z}$  e  $D_2 = \mathbb{N}$ , e supponiamo che  $p(x_1, x_2)$  sia l'espressione " $x_1^2 = x_2$ ". Allora  $p(x_1, x_2)$ , che certamente non è una proposizione perché non è né vera né falsa, è una funzione proposizionale nelle due variabili  $x_1, x_2$  su  $\mathbb{Z} \times \mathbb{N}$ , perché per ogni  $a_1 \in \mathbb{Z}$  e  $a_2 \in \mathbb{N}$   $p(a_1, a_2)$  è vera (quando  $a_1$  al quadrato fa  $a_2$ ) oppure è falsa (quando  $a_1$  al quadrato è diverso da  $a_2$ ).  $\square$

ESEMPIO 2. Siano  $D_1 = D_2 = D_3 = \mathbb{R}$ . Se  $p(x_1, x_2, x_3)$  è l'espressione "se  $x_1^2 + x_2^2 + x_3^2 = 0$  allora  $x_1 = x_2 = x_3 = 0$ ", allora  $p(x_1, x_2, x_3)$  è una funzione proposizionale su  $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ , perché per ogni  $a_1, a_2, a_3 \in \mathbb{R}$   $p(a_1, a_2, a_3)$  è o vera o falsa. In questo caso, comunque,  $p(a_1, a_2, a_3)$  non è mai falsa, qualunque siano i numeri reali  $a_1, a_2, a_3$ . Si noti invece che se  $p'(x_1, x_2, x_3)$  è sempre l'espressione "se  $x_1^2 + x_2^2 + x_3^2 = 0$  allora  $x_1 = x_2 = x_3 = 0$ ", ma intesa ora come funzione proposizionale su  $\mathbb{C} \times \mathbb{C} \times \mathbb{C}$ , allora non è vero che  $p'(a_1, a_2, a_3)$  è sempre una proposizione vera. Ad esempio  $p'(1, i, 0)$  è falsa.  $\square$

Se  $p(x_1, x_2, \dots, x_n)$  è una funzione proposizionale su  $D_1 \times D_2 \times \dots \times D_n$ , indicheremo con  $\forall x_1 p(x_1, x_2, \dots, x_n)$  l'espressione

$$\text{"per ogni } x_1 \in D_1, p(x_1, x_2, \dots, x_n)\text{"},$$

che spesso leggeremo "per ogni  $x_1$   $p(x_1, x_2, \dots, x_n)$ " sottintendendo l'insieme  $D_1$ . Similmente indicheremo con  $\forall x_2 p(x_1, x_2, \dots, x_n)$  l'espressione

$$\text{"per ogni } x_2 \in D_2, p(x_1, x_2, \dots, x_n)\text{"},$$

e così via per le altre variabili individuali  $x_i$ . Il simbolo  $\forall$  si legge quindi "per ogni" ed è detto *quantificatore universale*. Ad esempio se  $p(x_1, x_2)$  è la funzione proposizionale " $x_1^2 = x_2$ " su  $\mathbb{Z} \times \mathbb{N}$ , allora  $\forall x_1 p(x_1, x_2)$  è l'espressione "per ogni  $x_1 \in \mathbb{Z}$   $x_1^2 = x_2$ " e  $\forall x_2 p(x_1, x_2)$  è l'espressione "per ogni  $x_2 \in \mathbb{N}$   $x_1^2 = x_2$ ".

Similmente indicheremo con  $\exists x_1 p(x_1, x_2, \dots, x_n)$  l'espressione

$$\text{"esiste } x_1 \in D_1 \text{ tale che } p(x_1, x_2, \dots, x_n)\text{"},$$

che spesso leggeremo "esiste  $x_1$  tale che  $p(x_1, x_2, \dots, x_n)$ " sottintendendo l'insieme  $D_1$ . Il simbolo  $\exists$  si legge quindi "esiste" ed è detto *quantificatore esistenziale*. Si osservi che  $p(x_1, x_2, \dots, x_n)$  è una funzione proposizionale su  $D_1 \times D_2 \times \dots \times D_n$ , mentre  $\forall x_1 p(x_1, x_2, \dots, x_n)$  ed  $\exists x_1 p(x_1, x_2, \dots, x_n)$  sono funzioni proposizionali su  $D_2 \times D_3 \times \dots \times D_n$ . Ad esempio se  $p(x_1, x_2)$  è ancora la funzione proposizionale " $x_1^2 = x_2$ " su  $\mathbb{Z} \times \mathbb{N}$ , allora

$\forall x_1 p(x_1, x_2)$  è la funzione proposizionale su  $\mathbb{N}$  "per ogni  $x_1 \in \mathbb{Z}$  si ha  $x_1^2 = x_2$ ",  $\forall x_2 p(x_1, x_2)$  è la funzione proposizionale su  $\mathbb{Z}$  "per ogni  $x_2 \in \mathbb{N}$  si ha  $x_1^2 = x_2$ ",  $\exists x_1 p(x_1, x_2)$  è la funzione proposizionale su  $\mathbb{N}$  "esiste  $x_1 \in \mathbb{Z}$  tale che  $x_1^2 = x_2$ ",  $\exists x_2 p(x_1, x_2)$  è la funzione proposizionale su  $\mathbb{Z}$  "esiste  $x_2 \in \mathbb{N}$  tale che  $x_1^2 = x_2$ ".

Diremo *formule* le espressioni definite nel modo seguente:

- (a) le funzioni proposizionali sono formule;
- (b) se  $\alpha$  e  $\beta$  sono formule, anche  $(\alpha \wedge \beta)$ ,  $(\alpha \vee \beta)$ ,  $(\neg \alpha)$ ,  $(\alpha \rightarrow \beta)$ ,  $(\alpha \leftrightarrow \beta)$  sono formule;
- (c) se  $\alpha$  è una formula e  $x$  è una variabile individuale, anche  $\forall x \alpha$  ed  $\exists x \alpha$  sono formule;
- (d) un'espressione è una formula solo se è ottenuta in base ad (a), (b) e (c).

Ogni formula ha un dominio, spesso sottinteso.

La formula a cui è applicato un quantificatore si dice il *campo d'azione* del quantificatore. Ad esempio nella formula

$$\forall x \exists y (p(x, y) \rightarrow q(x, y))$$

il campo d'azione del quantificatore  $\forall x$  è  $\exists y (p(x, y) \rightarrow q(x, y))$ , e il campo d'azione del quantificatore  $\exists y$  è  $(p(x, y) \rightarrow q(x, y))$ . Invece nella formula

$$(\forall x p(x, y)) \rightarrow (\exists y q(x, y))$$

il campo d'azione del quantificatore  $\forall x$  è  $p(x, y)$ , mentre il campo d'azione del quantificatore  $\exists y$  è  $q(x, y)$ .

Passiamo ad esaminare le possibili occorrenze delle variabili in una formula. Per capire cosa si intende per occorrenza di una variabile facciamo un esempio: nella formula  $\forall x \exists y (p(x, y) \wedge p(x, x) \rightarrow q(x, y))$  la variabile  $x$  ha cinque occorrenze e la variabile  $y$  ha tre occorrenze, cioè  $x$  e  $y$  compaiono cinque e tre volte rispettivamente. Un'occorrenza di una variabile  $x$  si dice *vincolata* ogniqualvolta essa appare:

- (1) immediatamente dopo i simboli  $\forall$  e  $\exists$  (cioè in  $\forall x$  ed  $\exists x$ ), oppure
- (2) l'occorrenza di  $x$  è nel campo di azione dei quantificatori  $\forall x$  o  $\exists x$ .

Un'occorrenza non vincolata di una variabile si dice un'occorrenza *libera*.

ESEMPIO 3. Siano  $x, y, z$  tre variabili individuali, e

$$p(x, y, z), \quad q(x, z), \quad r(y)$$

tre funzioni proposizionali nelle variabili  $x, y, z$  la prima,  $x, z$  la seconda, e  $y$  la terza. Consideriamo le seguenti tre formule:

- (a)  $p(x, y, z)$
- (b)  $(\forall x p(x, y, z)) \rightarrow ((\exists z q(x, z)) \wedge r(y))$
- (c)  $\forall x \exists y (\forall z p(x, y, z) \rightarrow ((\exists z q(x, z)) \vee r(y)))$

In (a) le occorrenze di  $x, y$  e  $z$  sono tutte tre libere. In (b) si ha che: la  $x$  ha tre occorrenze, le prime due delle quali sono vincolate e la terza è libera; entrambe le occorrenze di  $y$  sono libere; la variabile  $z$  ha tre occorrenze, delle quali la prima è

libera e le altre due sono vincolate. In (c) tutte le occorrenze delle variabili sono vincolate.  $\square$

Una formula si dice *chiusa* se tutte le occorrenze delle variabili che in essa compaiono sono vincolate. Ogni formula chiusa è una proposizione.

ESEMPIO 4. Le formule considerate in (a) e (b) dell'esempio 3 non sono chiuse, mentre quella in (c) è una formula chiusa. Anche

$$\exists y \forall x (q(x, y) \rightarrow r(y))$$

è una formula chiusa.  $\square$

Se  $\alpha$  è una formula, le due formule  $\neg \forall x \alpha$  ed  $\exists x \neg \alpha$  sono equivalenti. Similmente  $\neg \exists x \alpha$  e  $\forall x \neg \alpha$  sono equivalenti.

### Esercizi svolti

16.1. Sia  $D$  un insieme con almeno due elementi e sia  $p(x, y)$  la funzione proposizionale " $x = y$ " su  $D \times D$ . Le due formule chiuse  $\forall x \exists y p(x, y)$  ed  $\exists y \forall x p(x, y)$  sono vere o false? Se ne deduca che bisogna fare molta attenzione nello scambiare i quantificatori.

Soluzione. La proposizione  $\forall x \exists y p(x, y)$  è vera. È infatti sufficiente prendere per ogni elemento  $x \in D$  lo stesso elemento  $y = x$ . Invece la proposizione  $\exists y \forall x p(x, y)$  è falsa perché  $D$  ha almeno due elementi. Quindi bisogna fare attenzione nello scambio dei quantificatori.  $\square$

16.2. Siano  $p(x, y)$  e  $q(x, y, z)$  funzioni proposizionali. Si neghino per esercizio le seguenti formule chiuse:

- (a)  $\exists x \exists y p(x, y)$ ;  
(b)  $\forall x \exists y (p(x, y) \vee \exists z q(x, y, z))$ .

Soluzione. (a) Negando la formula chiusa  $\exists x \exists y p(x, y)$  si hanno le seguenti formule chiuse tutte equivalenti tra loro:

$$\neg \exists x \exists y p(x, y) \\ \forall x \neg \exists y p(x, y) \\ \forall x \forall y \neg p(x, y).$$

(b) Negando  $\forall x \exists y (p(x, y) \vee \exists z q(x, y, z))$  si ha la seguente successione di formule chiuse equivalenti tra loro:

$$\neg \forall x \exists y (p(x, y) \vee \exists z q(x, y, z)) \\ \exists x \neg \exists y (p(x, y) \vee \exists z q(x, y, z)) \\ \exists x \forall y \neg (p(x, y) \vee \exists z q(x, y, z))$$

$$\exists x \forall y (\neg p(x, y) \wedge \neg \exists z q(x, y, z)) \\ \exists x \forall y (\neg p(x, y) \wedge \forall z \neg q(x, y, z)). \quad \square$$

16.3. Si neghino le seguenti formule chiuse:

- (a)  $\exists x \forall y \forall z (p(x, y) \rightarrow q(x, z))$ ;  
(b)  $\exists x \forall y (p(x, y) \rightarrow (\exists z q(x, y, z)))$ ;  
(c)  $\forall x \forall y \forall z (p(x, y) \leftrightarrow q(x, y, z))$ .

Soluzione. (a) Negando  $\exists x \forall y \forall z (p(x, y) \rightarrow q(x, z))$  si hanno le seguenti formule chiuse tutte equivalenti tra loro:

$$\neg \exists x \forall y \forall z (p(x, y) \rightarrow q(x, z)) \\ \forall x \exists y \exists z \neg (p(x, y) \rightarrow q(x, z)) \\ \forall x \exists y \exists z \neg (\neg (p(x, y) \wedge \neg q(x, z))) \\ \forall x \exists y \exists z (p(x, y) \wedge \neg q(x, z)).$$

(b) Negando  $\exists x \forall y (p(x, y) \rightarrow (\exists z q(x, y, z)))$  si ha la seguente successione di formule chiuse equivalenti tra loro:

$$\neg \exists x \forall y (p(x, y) \rightarrow (\exists z q(x, y, z))) \\ \forall x \exists y \neg (p(x, y) \rightarrow (\exists z q(x, y, z))) \\ \forall x \exists y \neg (\neg (p(x, y) \wedge \neg (\exists z q(x, y, z)))) \\ \forall x \exists y (p(x, y) \wedge \neg \exists z q(x, y, z)) \\ \forall x \exists y (p(x, y) \wedge \forall z \neg q(x, y, z)).$$

(c) Negando  $\forall x \forall y \forall z (p(x, y) \leftrightarrow q(x, y, z))$  si ha la seguente successione di formule chiuse equivalenti tra loro:

$$\neg \forall x \forall y \forall z (p(x, y) \leftrightarrow q(x, y, z)) \\ \exists x \exists y \exists z \neg (p(x, y) \leftrightarrow q(x, y, z)) \\ \exists x \exists y \exists z ((p(x, y) \wedge q(x, y, z)) \vee (\neg p(x, y) \wedge \neg q(x, y, z))) \\ \exists x \exists y \exists z (\neg (p(x, y) \wedge q(x, y, z))) \wedge (\neg (\neg p(x, y) \wedge \neg q(x, y, z))) \\ \exists x \exists y \exists z (\neg p(x, y) \vee \neg q(x, y, z)) \wedge (\neg (\neg p(x, y) \vee \neg q(x, y, z))) \\ \exists x \exists y \exists z (\neg p(x, y) \vee \neg q(x, y, z)) \wedge (p(x, y) \wedge q(x, y, z)). \quad \square$$

### Altri esercizi

16.4. Delle seguenti proposizioni si dica se sono vere o false, e si enunci una loro negazione:

- (a) Per ogni  $x \in \mathbb{Z}$  esiste  $y \in \mathbb{Z}$  tale che  $xy = 1$ .  
(b) Per ogni  $x \in \mathbb{R}$  esiste  $y \in \mathbb{R}$  tale che  $x^2 = y$ .  
(c) Esiste  $y \in \mathbb{R}$  tale che per ogni  $x \in \mathbb{R}$  si ha  $x^2 = y$ .  
(d) Per ogni  $x \in \mathbb{R}$  esiste  $y \in \mathbb{R}$  tale che per ogni  $z \in \mathbb{R}$  si ha  $x = yz$ .



- (e) Per ogni  $x \in \mathbb{R}$  esiste  $y \in \mathbb{R}$  con la seguente proprietà: o  $x = 0$ , oppure non esiste  $z \in \mathbb{R}$  tale che  $xy = z^2$ .  
 (f) Per ogni  $x \in \mathbb{R}$  si ha che se  $x \neq 0$  allora esiste  $y \in \mathbb{R}$  tale che  $xy = 1$ .

16.5. Si dica se le seguenti formule sono chiuse:

- (a)  $\forall x \exists y (p(x, y) \rightarrow q(x, y))$ ;  
 (b)  $\forall x (p(x, y) \rightarrow \exists y q(x, y))$ ;  
 (c)  $\forall x \exists y ((\forall z p(y, z)) \vee (\exists z q(x, y, z)))$ .

16.6. Sia  $D$  un insieme e  $p(x)$  una funzione proposizionale su  $D$  tale che  $\exists x p(x)$  sia una proposizione vera. Si provi che  $(\forall x \neg p(x)) \rightarrow (\forall x p(x))$  è una proposizione vera.

16.7. Si considerino le funzioni proposizionali

$$p(x) = "x = 0" \quad \text{e} \quad q(x, y) = "xy = 1".$$

Pensiamo la prima come funzione proposizionale in una variabile su  $\mathbb{R}$ , e la seconda come funzione proposizionale nelle due variabili  $x, y$  su  $\mathbb{R} \times \mathbb{R}$ . Si formalizzi la proposizione "Ogni numero reale non nullo ha un inverso reale" facendo uso delle funzioni proposizionali  $p(x)$  e  $q(x, y)$ .

16.8. Sia  $f: \mathbb{R} \rightarrow \mathbb{R}$  un'applicazione fissata. Si considerino le funzioni proposizionali  $p(x, y) = "f(x) = y"$  e  $q(x, y) = "x = y"$ . Si tratta di due funzioni proposizionali in due variabili su  $\mathbb{R} \times \mathbb{R}$ . Si formalizzi la proposizione " $f$  è iniettiva, ma non è suriettiva" facendo uso delle funzioni proposizionali  $p(x, y)$  e  $q(x, y)$ .

## PARTE QUARTA

## INSIEMI DOTATI DI UN'OPERAZIONE

## Capitolo 17. Semigrupp

Se  $A$  è un insieme, un'operazione (o più precisamente un'operazione binaria, o anche una legge di composizione) su  $A$  è un'applicazione  $\omega: A \times A \rightarrow A$ . Più in generale un'operazione  $n$ -aria su  $A$  è un'applicazione  $A \times A \times \cdots \times A \rightarrow A$ . Il numero naturale  $n$  si dice la *arietà* dell'operazione.

ESEMPIO 1. L'addizione tra numeri reali è un'operazione su  $\mathbb{R}$ , perché è l'applicazione  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  definita da  $(\alpha, \beta) \mapsto \alpha + \beta$  per ogni  $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$ . Analogamente la moltiplicazione tra numeri reali è un'operazione su  $\mathbb{R}$ , perché è l'applicazione  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ ,  $(\alpha, \beta) \mapsto \alpha\beta$ . Anche la sottrazione è un'operazione su  $\mathbb{R}$ . Invece la divisione non è un'operazione su  $\mathbb{R}$ , perché  $\alpha/\beta$  è definito solo quando  $\beta \neq 0$ .  $\square$

ESEMPIO 2. Se  $A$  è un insieme, l'intersezione tra sottoinsiemi di  $A$  è un'operazione su  $\mathcal{P}(A)$ , perché è l'applicazione  $\mathcal{P}(A) \times \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ ,  $(X, Y) \mapsto X \cap Y$ .  $\square$

Le operazioni vengono denotate di solito con simboli del tipo  $+$ ,  $-$ ,  $\cdot$ ,  $\times$ ,  $*$ ,  $\circ$ ; se  $\omega$  è un'operazione su  $A$  e  $a, b \in A$ , si suole scrivere  $a \omega b$  in luogo di  $\omega(a, b)$ . Ad esempio, abbiamo visto che l'addizione tra numeri reali è un'operazione su  $\mathbb{R}$ ; denotandola, come di consueto, con il simbolo  $+$  dovremmo scrivere  $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  per denotare l'applicazione, e  $+(\alpha, \beta)$  per denotare l'immagine dell'elemento  $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$ , cioè la somma di  $\alpha$  e  $\beta$ . In realtà sappiamo che si suole scrivere  $\alpha + \beta$  in luogo di  $+(\alpha, \beta)$ . Similmente nell'esempio 2 abbiamo visto che se  $A$  è un insieme, l'intersezione tra sottoinsiemi di  $A$  è un'operazione su  $\mathcal{P}(A)$ ; denotandola, come di consueto, con il simbolo  $\cap$  dovremmo scrivere  $\cap: \mathcal{P}(A) \times \mathcal{P}(A) \rightarrow \mathcal{P}(A)$  per denotare l'applicazione, e  $\cap(X, Y)$  per denotare

l'immagine dell'elemento  $(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A)$  cioè l'intersezione di  $X$  e  $Y$ . In realtà finora abbiamo sempre scritto  $X \cap Y$  in luogo di  $\cap(X, Y)$ , e continueremo a usare questa scrittura più consueta.

Analogamente a quanto avevamo già fatto nei capitoli precedenti, in cui facevamo uso del simbolo  $(A, \leq)$  per mettere in evidenza che si stava considerando l'insieme  $A$  parzialmente ordinato dalla relazione  $\leq$ , così ora, se  $A$  è un insieme e  $*$  è un'operazione su  $A$ , useremo la notazione  $(A, *)$  per indicare che sull'insieme  $A$  l'operazione considerata è l'operazione  $*$ . Nell'esempio 1 avevamo quindi considerato  $(\mathbb{R}, +)$  e  $(\mathbb{R}, \cdot)$ , mentre nell'esempio 2 avevamo considerato  $(\mathcal{P}(A), \cap)$ .

Un *semigrupp* è un insieme  $S$  sul quale è definita un'operazione  $*$  tale che  $(a * b) * c = a * (b * c)$  per ogni  $a, b, c \in S$  (associatività). Un semigrupp  $(S, *)$  si dice *commutativo* se  $a * b = b * a$  per ogni  $a, b \in S$ .

ESEMPIO 3. L'insieme  $\mathbb{R}$  dotato dell'addizione  $+$  è ovviamente un semigrupp commutativo, perché per ogni  $a, b, c \in \mathbb{R}$  si ha  $(a + b) + c = a + (b + c)$  e  $a + b = b + a$ . Anche  $(\mathbb{R}, \cdot)$  è un semigrupp commutativo, perché per ogni  $a, b, c \in \mathbb{R}$  si ha  $(ab)c = a(bc)$  e  $ab = ba$ .  $\square$

ESEMPIO 4. Se  $A$  è un insieme, definiamo un'operazione  $*$  su  $A$  ponendo  $a * b = a$  per ogni  $a, b \in A$ . Allora  $(A, *)$  è un semigrupp, perché per ogni  $a, b, c \in A$  si ha  $(a * b) * c = a * c = a$  e  $a * (b * c) = a * b = a$ . Però se  $|A| \geq 2$ , il semigrupp  $(A, *)$  non è commutativo, in quanto da  $|A| \geq 2$  segue che esistono in  $A$  due elementi distinti  $a, b$ , e si ha  $a * b = a \neq b = b * a$ .  $\square$

La notazione più usata per denotare l'operazione in un semigrupp è quella *moltiplicativa*; in tal caso l'operazione è detta *moltiplicazione* ed è denotata con  $\cdot$ ; se  $a, b$  sono due elementi del semigrupp, si dice allora che  $a \cdot b$  è il *prodotto* di  $a$  e  $b$  (e spesso si scrive  $ab$  invece che  $a \cdot b$ ). Nel caso dei semigruppi commutativi è molto usata anche la notazione *additiva*; in questo caso l'operazione si chiama *addizione*, la si denota con  $+$ , e  $a + b$  si dice la *somma* di  $a$  e  $b$ .

Dato che in un semigrupp  $(S, \cdot)$  vale la proprietà associativa, scriveremo spesso  $abc$ , senza le parentesi, per indicare l'elemento  $(ab)c$  di  $S$ .

Sia  $A$  un insieme e  $*$  un'operazione su  $A$ , cioè  $*$  :  $A \times A \rightarrow A$  sia un'applicazione. Dato un qualunque sottoinsieme  $B$  di  $A$  possiamo considerare l'applicazione  $B \times B \rightarrow A$  ottenuta da  $*$  :  $A \times A \rightarrow A$  restringendo il dominio a  $B \times B$ . (Volendo essere più precisi possiamo dire che dati l'insieme  $A$ , l'operazione  $*$  :  $A \times A \rightarrow A$  e  $B \subseteq A$ , possiamo definire l'applicazione  $\circ$  :  $B \times B \rightarrow A$  ponendo  $\circ(x, y) = *(x, y)$  per ogni  $(x, y) \in B \times B$ . Oppure possiamo dire che dati l'insieme  $A$ , l'operazione  $*$  :  $A \times A \rightarrow A$  e  $B \subseteq A$ , possiamo definire l'applicazione  $\circ$  :  $B \times B \rightarrow A$  come l'applicazione composta dell'applicazione di inclusione  $B \times B \rightarrow A \times A$ —vedi esercizio 2.19—e dell'applicazione  $*$  :  $A \times A \rightarrow A$ .) All'applicazione  $\circ$  :  $B \times B \rightarrow A$  così ottenuta non è possibile in generale restringere

il codominio a  $B$  ottenendo un'applicazione  $B \times B \rightarrow B$ , ossia un'operazione su  $B$ , perché non è detto che in generale  $b * b' \in B$  per ogni  $b, b' \in B$ . Si vede così che l'operazione  $*$  su  $A$  induce un'operazione su un sottoinsieme  $B$  di  $A$  se e solo se  $B$  è un sottoinsieme di  $A$  chiuso per l'operazione  $*$ , cioè se e solo se  $b * b' \in B$  per ogni  $b, b' \in B$ . Per non introdurre troppi simboli si preferisce indicare l'operazione indotta su un sottoinsieme chiuso  $B$  di  $A$  con lo stesso simbolo  $*$  usato per denotare l'operazione su  $A$ .

ESEMPIO 5. Se  $\mathbb{R}$  è l'insieme dei numeri reali e  $-$  indica la differenza tra i numeri reali, allora  $(\mathbb{R}, -)$  non è un semigrupp ed  $\mathbb{N}$  non è un sottoinsieme di  $\mathbb{R}$  chiuso per l'operazione  $-$ . Invece se  $+$  è l'addizione tra numeri reali abbiamo già visto che  $(\mathbb{R}, +)$  è un semigrupp ed  $\mathbb{N}$  è ovviamente un sottoinsieme additivamente chiuso di  $\mathbb{R}$ , cioè un sottoinsieme di  $\mathbb{R}$  chiuso per l'operazione  $+$ . Se  $\cdot$  denota la moltiplicazione tra numeri reali e  $\mathbb{Z}_{\leq 0} = \{z \mid z \in \mathbb{Z}, z \leq 0\}$ , allora  $(\mathbb{R}, \cdot)$  è un semigrupp, ma  $\mathbb{Z}_{\leq 0}$  non è un sottoinsieme di  $\mathbb{R}$  chiuso per l'operazione  $\cdot$ .  $\square$

Se  $S$  è un semigrupp e  $T$  è un sottoinsieme chiuso di  $S$ , allora  $T$  con l'operazione indotta dall'operazione di  $S$  è a sua volta un semigrupp (perché se la proprietà associativa vale per ogni  $a, b, c \in S$ , a maggior ragione essa vale per ogni  $a, b, c \in T$ ). Si dice in questo caso che  $T$  è un *sottosemigrupp* di  $S$ .

ESEMPIO 6. Il semigrupp  $(\mathbb{N}, +)$  è un sottosemigrupp di  $(\mathbb{Z}, +)$ . Se  $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ ,  $(\mathbb{Z}^*, \cdot)$  è un sottosemigrupp di  $(\mathbb{Z}, \cdot)$ . Se  $A \subseteq B$ , allora  $(\mathcal{P}(A), \cup)$  è un sottosemigrupp di  $(\mathcal{P}(B), \cup)$  perché per ogni  $X, Y \in \mathcal{P}(A)$ , da  $X \subseteq A$  e  $Y \subseteq A$  segue che  $X \cup Y \subseteq A$ , cioè che  $X \cup Y \in \mathcal{P}(A)$ . Quindi  $\mathcal{P}(A)$  è un sottoinsieme di  $\mathcal{P}(B)$  chiuso per l'operazione  $\cup$ .  $\square$

Se  $(S, \cdot)$  è un semigrupp moltiplicativo ed  $a$  è un suo elemento, per ogni intero positivo  $n$  si definisce per induzione la *potenza  $n$ -esima*  $a^n$  di  $a$  ponendo

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

per ogni intero positivo  $n$ .

Invece in un semigrupp  $(S, +)$ , scritto in notazione additiva, per ogni  $a \in S$  ed ogni intero positivo  $n$  si definisce il *multiplo  $n$ -esimo*  $na$  di  $a$  ponendo

$$1a = a, \quad (n+1)a = na + a$$

per ogni  $n \geq 1$ .

PROPOSIZIONE 17.1. Sia  $(S, \cdot)$  un semigrupp. Se  $a \in S$  ed  $m, n$  sono interi positivi, allora

$$a^n a^m = a^{n+m} \quad \text{e} \quad (a^n)^m = a^{nm}.$$

Se  $a, b \in S$ ,  $ab = ba$  ed  $n$  è un intero positivo, allora

$$(ab)^n = a^n b^n.$$

**Dimostrazione.** Dimostriamo che  $a^n a^m = a^{n+m}$  per induzione su  $m$  (quindi per ogni numero intero  $m \geq 1$  l'asserzione  $P$  sul numero intero  $m$  che stiamo dimostrando è "per ogni intero positivo  $n$  si ha  $a^n a^m = a^{n+m}$ "). Se  $m = 1$  si ha  $a^n a^1 = a^n a = a^{n+1}$ , e quindi l'asserzione è vera in questo caso. Inoltre se è vera per  $m$ , essa è vera anche per  $m+1$  in quanto  $a^n a^{m+1} = a^n (a^m a) = (a^n a^m) a = a^{n+m} a = a^{n+m+1}$ . Quindi l'asserzione è vera per ogni  $m$ .

Dimostriamo poi per induzione su  $m$  che  $(a^n)^m = a^{nm}$ . Per  $m = 1$  si ha  $(a^n)^1 = a^n = a^{n \cdot 1}$ , e quindi l'asserzione è vera in questo caso. Supponiamo che sia vera per  $m$ , e dimostriamo che è vera anche per  $m+1$ : si ha  $(a^n)^{m+1} = (a^n)^m (a^n) = a^{nm} a^n = a^{nm+n}$  (quest'ultima uguaglianza vale perché è stata dimostrata nel paragrafo precedente), e quindi  $(a^n)^{m+1} = a^{nm+n} = a^{n(m+1)}$ , ossia l'asserzione è vera anche per  $m+1$ .

Per dimostrare che da  $ab = ba$  segue  $(ab)^n = a^n b^n$ , facciamo vedere innanzi tutto che se  $ab = ba$  allora  $ab^n = b^n a$  per induzione su  $n$ . Per  $n = 1$  si ha  $ab^1 = ab = ba = b^1 a$ ; inoltre se  $ab^n = b^n a$ , allora  $ab^{n+1} = ab^n b = b^n a b = b^n b a = b^{n+1} a$ . Questo dimostra che se  $ab = ba$ , allora  $ab^n = b^n a$  per ogni  $n \geq 1$ .

Dimostriamo infine per induzione su  $n$  che se  $ab = ba$ , allora  $(ab)^n = a^n b^n$ . Per  $n = 1$  si ha  $(ab)^1 = ab = a^1 b^1$ . Supposto di sapere che l'asserzione vale per  $n$ , cioè che  $(ab)^n = a^n b^n$ , dimostriamola per  $n+1$ : si ha  $(ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^n ab^n = a^{n+1} b^{n+1}$ . Questo conclude la dimostrazione.  $\square$

### Esercizi svolti

**17.1.** Siano  $A$  un insieme e  $A^A$  l'insieme di tutte le applicazioni di  $A$  in  $A$ . Date due applicazioni  $f, g \in A^A$ , l'applicazione composta  $f \circ g : A \rightarrow A$  è ancora un elemento di  $A^A$ . Questo significa che la composizione di applicazioni può essere vista come un'applicazione  $\circ : A^A \times A^A \rightarrow A^A$ , vale a dire che la composizione di applicazioni è un'operazione su  $A^A$ . Si dimostri che

- $(A^A, \circ)$  è un semigruppato;
- se  $B \subseteq A$ , l'insieme delle applicazioni  $f : A \rightarrow A$  tali che  $f(B) \subseteq B$  è un sottosemigruppato  $S_B$  di  $(A^A, \circ)$ ;
- se  $a_0 \in A$  ed  $f : A \rightarrow A$  è definita da  $f(a) = a_0$  per ogni  $a \in A$ , si calcolino le potenze  $n$ -esime dell'elemento  $f$  del semigruppato  $A^A$  per ogni intero  $n \geq 1$ ;
- se  $(A, \leq)$  è un insieme parzialmente ordinato, sia  $\text{End}(A)$  l'insieme di tutti gli omomorfismi di insieme parzialmente ordinato di  $A$  in  $A$ . Si dimostri che  $\text{End}(A)$  è un sottosemigruppato di  $(A^A, \circ)$ .

**Soluzione.** (a) Si è visto nel capitolo 3 che la composizione di applicazioni è associativa. Quindi  $(f \circ g) \circ h = f \circ (g \circ h)$  per ogni  $f, g, h \in A^A$ .

(b) Si deve dimostrare che se  $f, g \in S_B$  allora  $f \circ g \in S_B$ . Se  $f, g \in S_B$ , allora  $f \circ g$  è un'applicazione di  $A$  in  $A$  e si ha  $(f \circ g)(B) = f(g(B)) \subseteq f(B) \subseteq B$ . Quindi  $f \circ g \in S_B$ .

(c) Dimostriamo per induzione che si ha  $f^n = f$  per ogni intero  $n \geq 1$ . Per  $n = 1$  questo è ovvio. Si osservi poi che  $f \circ f = f$  in quanto per ogni  $a \in A$  si ha  $(f \circ f)(a) = f(f(a)) = f(a_0) = a_0 = f(a)$ . Supposto quindi che  $f^{n-1} = f$ , si ha  $f^n = f^{n-1} \circ f = f \circ f = f$ . Per il principio di induzione ne segue che  $f^n = f$  per ogni intero  $n \geq 1$ .

(d) Si deve dimostrare che se  $f, g \in \text{End}(A)$  allora  $f \circ g \in \text{End}(A)$ . Se  $f, g \in \text{End}(A)$ , allora  $f \circ g$  è un'applicazione di  $A$  in  $A$ ; inoltre per ogni  $a, b \in A$  con  $a \leq b$  si ha  $g(a) \leq g(b)$  (perché  $g$  è un omomorfismo di insiemi ordinati), e quindi  $f(g(a)) \leq f(g(b))$  (perché  $f$  è un omomorfismo), vale a dire  $(f \circ g)(a) \leq (f \circ g)(b)$ . Questo dimostra che  $f \circ g$  è un omomorfismo di insiemi ordinati, e quindi  $f \circ g \in \text{End}(A)$ .  $\square$

**17.2.** Siano  $(S, \cdot)$  un semigruppato e  $T_1, T_2$  due suoi sottosemigruppato. Si supponga che  $t_1 t_2 = t_2 t_1$  per ogni  $t_1 \in T_1$  e ogni  $t_2 \in T_2$ . Si dimostri che l'insieme  $T_1 T_2 = \{t_1 t_2 \mid t_1 \in T_1, t_2 \in T_2\}$  è un sottosemigruppato di  $S$ .

**Soluzione.** Si deve dimostrare che se  $x, y \in T_1 T_2$  allora  $xy \in T_1 T_2$ . Se  $x, y \in T_1 T_2$ , si ha  $x = t_1 t_2$  e  $y = t'_1 t'_2$  per qualche  $t_1, t'_1 \in T_1, t_2, t'_2 \in T_2$ . Ne segue che  $xy = (t_1 t_2)(t'_1 t'_2) = t_1(t_2(t'_1 t'_2)) = t_1((t_2 t'_1)t'_2) = t_1(t'_1(t_2 t'_2)) = (t_1 t'_1)(t_2 t'_2) \in T_1 T_2$ .  $\square$

**17.3.** Siano  $(S, \cdot)$  un semigruppato e  $T_1, T_2$  due suoi sottosemigruppato. Si dimostri che  $T_1 \cap T_2$  è un sottosemigruppato di  $S$ .

**Soluzione.** Si deve dimostrare che se  $x, y \in T_1 \cap T_2$  allora  $xy \in T_1 \cap T_2$ . Se  $x, y \in T_1 \cap T_2$ , si ha che  $x, y \in T_1$  e  $x, y \in T_2$ . Ma  $T_1$  e  $T_2$  sono sottosemigruppato di  $S$ , e quindi  $xy \in T_1$  e  $xy \in T_2$ . Se ne conclude che  $xy \in T_1 \cap T_2$ .  $\square$

### Altri esercizi

**17.4.** Si osservi che se  $\alpha$  e  $\beta$  sono numeri reali positivi, il quoziente  $\alpha/\beta$  è ancora un numero reale positivo. Quindi la divisione  $/$  è un'operazione sull'insieme  $\mathbb{R}^+$  dei numeri reali positivi. L'insieme  $\mathbb{R}^+$  munito della divisione è un semigruppato?

**17.5.** Sia  $\circ$  l'operazione su  $\mathbb{N}$  definita da  $a \circ b = a + b + ab$  per ogni  $a, b \in \mathbb{N}$ . Si dimostri che  $(\mathbb{N}, \circ)$  è un semigruppato commutativo.

**17.6.** Sia  $(S, \cdot)$  un semigruppato e  $X$  un insieme. Sull'insieme  $S^X$  di tutte le applicazioni di  $X$  in  $S$  si definisca un'operazione  $*$  ponendo, per ogni  $f, g \in S^X$ ,  $(f * g)(x) = f(x) \cdot g(x)$  per ogni  $x \in X$ .

- (a) Si dimostri che  $(S^X, *)$  è un semigruppato.  
 (b) Si dimostri che se  $(S, \cdot)$  è un semigruppato commutativo allora anche  $(S^X, *)$  è un semigruppato commutativo.

17.7. Si dimostri che  $Z + iZ = \{a + ib \mid a, b \in Z\}$  è un sottosemigruppato sia di  $(C, +)$  che di  $(C, \cdot)$ .

17.8. Sul prodotto cartesiano  $R \times R$  si definisca un'operazione  $*$  ponendo, per ogni  $(a, b), (a', b') \in R \times R$ ,  $(a, b) * (a', b') = (aa', ab' + b)$ .

- (a) Si dimostri che  $(R \times R, *)$  è un semigruppato.  
 (b) Il semigruppato  $(R \times R, *)$  è commutativo?  
 (c) Si dimostri che  $\{1\} \times R$  e  $R \times \{0\}$  sono due sottosemigruppato di  $(R \times R, *)$ .  
 (d) Si dimostri per induzione sul numero intero positivo  $n$  che  $(1, b)^n = (1, nb)$  e  $(a, 0)^n = (a^n, 0)$  per ogni  $a, b \in R$ .

17.9. Sia  $\{0, 1\}^R$  l'insieme di tutte le applicazioni di  $R$  nell'insieme con due elementi  $\{0, 1\}$ . Sull'insieme  $\{0, 1\}^R$  si definisca, per ogni  $f, g \in \{0, 1\}^R$ ,  $(f * g)(x) = f(x) + g(x) - f(x)g(x)$  per ogni  $x \in R$ .

- (a) Si dimostri che  $f * g \in \{0, 1\}^R$  per ogni  $f, g \in \{0, 1\}^R$ , e che  $(\{0, 1\}^R, *)$  è un semigruppato.  
 (b) Per ogni sottoinsieme  $A$  di  $R$  sia

$$S_A = \{f \mid f \in \{0, 1\}^R, f(a) = 0 \text{ per ogni } a \in A\}.$$

Si dimostri che  $S_A$  è un sottosemigruppato di  $\{0, 1\}^R$ .

- (c) Si dimostri che se  $A \subseteq B \subseteq R$  allora  $S_A \supseteq S_B$ , e che  $S_\emptyset = \{0, 1\}^R$ .  
 (d) Si dimostri che nel semigruppato  $(\{0, 1\}^R, *)$  si ha  $f^2 = f$  per ogni  $f \in \{0, 1\}^R$ .  
 (e) Si deduca da (d) che nel semigruppato  $(\{0, 1\}^R, *)$  si ha  $f^n = f$  per ogni  $f \in \{0, 1\}^R$  e ogni intero  $n \geq 1$ .

17.10. Se  $M_n(R)$  è l'insieme delle matrici  $n \times n$  e  $\cdot$  è il prodotto righe per colonne,  $(M_n(R), \cdot)$  è un semigruppato per l'esercizio 6.2. Si considerino le matrici  $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$  e  $B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ . Si calcolino  $A^2$  e  $B^2$ , e si dimostri che  $(AB)^2 \neq A^2B^2$ .

[Questo dimostra che l'ipotesi  $ab = ba$  nell'ultima parte della proposizione 17.1 è essenziale per la validità della proposizione stessa.]

17.11. Sia  $S$  il prodotto cartesiano  $R^* \times N$ . Si definisca un'operazione su  $S$  ponendo  $(\alpha, n)(\beta, m) = (\alpha\beta^n, nm)$  per ogni  $(\alpha, n), (\beta, m) \in S$ .

- (a) Si provi che  $S$  è un semigruppato.  
 (b) Il semigruppato  $S$  è commutativo?

- (c) Se  $a = (2, 2)$  e  $b = (1, 2)$  si calcolino  $(ab)^2$  e  $a^2b^2$  dimostrando che  $(ab)^2 \neq a^2b^2$ .

17.12. Si ripeta l'enunciato della proposizione 17.1 per un semigruppato additivo  $(S, +)$ .

## Capitolo 18. Monoidi

Siano  $(S, \cdot)$  un semigruppato,  $e \in S$ . L'elemento  $e$  si dice un'identità sinistra se  $ea = a$  per ogni  $a \in S$ , un'identità destra se  $ae = a$  per ogni  $a \in S$ , un'identità (o un elemento neutro) se è sia un'identità sinistra che un'identità destra.

ESEMPIO 1. Sia  $S = R \times R$  il semigruppato in cui l'operazione  $*$  è definita ponendo, per ogni  $(a, b), (c, d) \in S$ ,  $(a, b) * (c, d) = (bc, bd)$ . Non è difficile dimostrare che  $S$  è un semigruppato. Cerchiamo le identità destre di  $S$ : l'elemento  $(x, y)$  di  $S$  è un'identità destra se e solo se  $(a, b) * (x, y) = (a, b)$  per ogni  $(a, b) \in S$ , cioè se e solo se  $(bx, by) = (a, b)$  per ogni  $a, b \in R$ . Ovviamente non esiste alcun numero reale  $x$  tale che  $bx = a$  per ogni  $a, b \in R$ . Quindi il semigruppato  $S$  non ha identità destre. Cerchiamo le identità sinistre di  $S$ : l'elemento  $(x, y)$  di  $S$  è un'identità sinistra se e solo se  $(x, y) * (c, d) = (c, d)$  per ogni  $(c, d) \in S$ , cioè se e solo se  $(yc, yd) = (c, d)$  per ogni  $c, d \in R$ , ossia se e solo se  $yc = c$  per ogni  $c \in R$  e  $yd = d$  per ogni  $d \in R$ . Questo accade se e solo se  $y = 1$ . Abbiamo così dimostrato che  $(x, y)$  è un'identità sinistra di  $S$  se e solo se  $y = 1$ . Quindi le identità sinistre di  $S$  sono tutti e soli gli elementi di  $S$  del tipo  $(x, 1)$  con  $x \in R$ . In particolare  $S$  ha infinite identità sinistre.  $\square$

LEMMA 18.1. Se in semigruppato ci sono un'identità sinistra e un'identità destra  $e'$ , allora  $e = e'$ .

COROLLARIO 18.2. In un semigruppato l'identità, se esiste, è unica.

Un monoido è un semigruppato dotato di identità. In un monoido moltiplicativo  $(M, \cdot)$  l'identità viene usualmente denotata con 1 o con  $1_M$ ; in un monoido additivo  $(M, +)$  l'identità viene usualmente indicata con 0 o con  $0_M$ , e viene detta lo zero del monoido.

ESEMPIO 2. I semigruppato  $(N, +)$ ,  $(Z, +)$ ,  $(Q, +)$ ,  $(R, +)$ ,  $(C, +)$  sono monoidi; la loro identità è il numero 0.

I semigruppato  $(N, \cdot)$ ,  $(Z, \cdot)$ ,  $(Q, \cdot)$ ,  $(R, \cdot)$ ,  $(C, \cdot)$  sono monoidi; la loro identità è il numero 1.  $\square$

ESEMPIO 3. Consideriamo sull'insieme  $\mathbb{Z}$  l'operazione  $*$  definita da

$$a * b = ab - a - b + 2$$

per ogni  $a, b \in \mathbb{Z}$ . Allora  $(\mathbb{Z}, *)$  è un semigruppato in quanto per ogni  $a, b, c \in \mathbb{Z}$  si ha  $(a * b) * c = (ab - a - b + 2) * c = abc - ac - bc + 2c - ab + a + b - 2 - c + 2 = abc - ac - bc - ab + a + b + c$  e  $a * (b * c) = a * (bc - b - c + 2) = abc - ab - ac - ac - bc - ab + a + b + c = abc - ab - ac - bc - ab + a + b + c$ . Si noti che  $ac + 2a - a - bc + b + c - 2 + 2 = abc - ab - ac - bc + a + b + c$ . Si noti che  $(\mathbb{Z}, *)$  è commutativo in quanto  $a * b = b * a$  per ogni  $a, b \in \mathbb{Z}$ . Il numero intero  $2$  è l'identità di  $(\mathbb{Z}, *)$ , in quanto per ogni  $a \in \mathbb{Z}$  si ha  $2 * a = 2a - 2 - a + 2 = a$ ; questo prova che  $2$  è un'identità sinistra, ma abbiamo già fatto osservare che il semigruppato è commutativo, e ovviamente in un semigruppato commutativo un'identità sinistra è un'identità. Quindi  $(\mathbb{Z}, *)$  è un monoide avente  $2$  come identità.  $\square$

ESEMPIO 4. Sia  $(A, \leq)$  un reticolo. Se come di consueto  $a \vee b$  denota l'estremo superiore di  $\{a, b\}$ , allora  $\vee$  può essere vista come un'applicazione  $A \times A \rightarrow A$ , ossia come un'operazione su  $A$ . In base alla proposizione 11.1  $(A, \vee)$  è un semigruppato commutativo. Vediamo se nel semigruppato commutativo  $(A, \vee)$  vi sono identità. Un elemento  $e \in A$  è un'identità di  $(A, \vee)$  se e solo se  $e \vee a = a$  per ogni  $a \in A$ , cioè (vedi l'esempio 1 del capitolo 11) se e solo se  $e \leq a$  per ogni  $a \in A$ , ossia se  $e$  è il minimo di  $A$ . Quindi  $(A, \vee)$  è un monoide se e solo se  $(A, \leq)$  ha minimo, e in tal caso l'identità di  $(A, \vee)$  è proprio il minimo di  $(A, \leq)$ .

Accade una cosa simile partendo sempre da un reticolo  $(A, \leq)$  ma considerando il semigruppato commutativo  $(A, \wedge)$ . In questo caso si conclude che  $(A, \wedge)$  è un monoide se e solo se  $(A, \leq)$  ha massimo, e se questo avviene l'identità di  $(A, \wedge)$  è esattamente il massimo di  $(A, \leq)$ .  $\square$

Se  $(M, \cdot)$  è un monoide e  $a \in M$ , per ogni  $n \in \mathbb{N}$  si definisce la *potenza n-esima* di  $a$  ponendo  $a^0 = 1_M$  e  $a^{n+1} = a^n a$  per ogni  $n \geq 0$ .

ESEMPIO 5. Sia  $A$  un insieme. È facile verificare che se  $\mathcal{P}(A)$  denota l'insieme delle parti di  $A$  e  $\cap$  denota l'intersezione di insiemi allora  $(\mathcal{P}(A), \cap)$  è un monoide la cui identità è  $1_{\mathcal{P}(A)} = A$ . Se  $B \in \mathcal{P}(A)$ , cioè  $B \subseteq A$ , allora si ha

$$B^0 = 1_{\mathcal{P}(A)} = A \quad \text{e} \quad B^n = B \quad \text{per ogni } n \geq 1.$$

Questo può essere dimostrato per induzione su  $n \geq 1$ , in quanto  $B^1 = B$  e  $B^{n+1} = B^n \cap B = B \cap B = B$  se  $n \geq 1$ .  $\square$

ESEMPIO 6. Sia  $A$  un insieme. È facile verificare (si veda l'esercizio 17.1) che se  $A^A$  denota l'insieme di tutte le applicazioni di  $A$  in  $A$  e  $\circ$  denota la composizione di applicazioni allora  $(A^A, \circ)$  è un monoide la cui identità è l'applicazione identica  $\iota_A : A \rightarrow A$ .

Nel caso particolare in cui  $A = \{1, 2, 3, 4\}$  e  $f \in A^A$  è l'applicazione definita da  $f(1) = 1$ ,  $f(2) = 1$ ,  $f(3) = 2$ ,  $f(4) = 3$ , allora  $f^0 = \iota_A$ ,  $f^1 = f$ ,  $f^2 = f \circ f$ , e per ogni  $n \geq 3$   $f^n$  è l'applicazione definita da  $f^n(a) = 1$  per ogni  $a \in A = \{1, 2, 3, 4\}$ .  $\square$

Se  $M$  è un monoide, un *sottomonoido*  $N$  di  $M$  è un sottoinsieme di  $M$  tale che  $1_M \in N$ , e se  $a, b \in N$  allora  $ab \in N$ . Ad esempio, per ogni monoide  $M$  i suoi sottoinsiemi  $\{1_M\}$  ed  $M$  sono sottomonoidi.

ESEMPIO 7. Fissato  $n \in \mathbb{N}$  poniamo  $N_{\geq n} = \{a \in \mathbb{N}, a \geq n\}$ ; è facile verificare che  $N_{\geq n} \cup \{0\}$  è un sottomonoido di  $(\mathbb{N}, +)$  e che  $N_{\geq n} \cup \{1\}$  è un sottomonoido di  $(\mathbb{N}, \cdot)$ . Infatti  $N_{\geq n} \cup \{0\}$  è un sottomonoido di  $(\mathbb{N}, +)$  perché  $0 \in N_{\geq n} \cup \{0\}$  e perché se  $a, b \in N_{\geq n} \cup \{0\}$  anche  $a + b \in N_{\geq n} \cup \{0\}$ ; analogamente  $N_{\geq n} \cup \{1\}$  è un sottomonoido di  $(\mathbb{N}, \cdot)$  perché  $1 \in N_{\geq n} \cup \{1\}$  e perché se  $a, b \in N_{\geq n} \cup \{1\}$  anche  $ab \in N_{\geq n} \cup \{1\}$ .  $\square$

ESEMPIO 8. Se  $a \in \mathbb{Z}$  e  $a\mathbb{Z} = \{az \mid z \in \mathbb{Z}\}$ , è facile verificare che  $a\mathbb{Z}$  è un sottomonoido di  $(\mathbb{Z}, +)$  e che  $a\mathbb{Z} \cup \{1\}$  è un sottomonoido di  $(\mathbb{Z}, \cdot)$ .  $\square$

ESEMPIO 9. Sia  $M$  un monoide e per ogni  $\lambda \in \Lambda$  sia  $M_\lambda$  un sottomonoido di  $M$ . Allora  $\bigcap_{\lambda \in \Lambda} M_\lambda$  è un sottomonoido di  $M$  perché:

- (1)  $1_M \in M_\lambda$  per ogni  $\lambda \in \Lambda$ , e quindi  $1_M \in \bigcap_{\lambda \in \Lambda} M_\lambda$ ;
- (2) se  $a, b \in \bigcap_{\lambda \in \Lambda} M_\lambda$ , allora  $a, b \in M_\lambda$  per ogni  $\lambda \in \Lambda$ , e quindi, dato che ogni  $M_\lambda$  è un sottomonoido di  $M$ ,  $ab \in M_\lambda$  per ogni  $\lambda \in \Lambda$ . Se ne deduce che  $ab \in \bigcap_{\lambda \in \Lambda} M_\lambda$ .  $\square$

Se  $X$  è un sottoinsieme di  $M$ , l'intersezione di tutti i sottomonoidi di  $M$  che contengono  $X$  è un sottomonoido di  $M$  (vedi esempio 9), ed è ovviamente il più piccolo sottomonoido di  $M$  che contiene  $X$ . Si chiama *sottomonoido di  $M$  generato da  $X$* , e lo si denota con  $[X]$ . Ad esempio dato che  $\{1_M\}$  è il più piccolo di tutti i sottomonoidi di  $M$ , si ha  $[0] = \{1_M\}$  e  $[1_M] = \{1_M\}$ .

Se  $X = \{a\}$  ha un solo elemento si scrive  $[a]$  in luogo di  $[\{a\}]$  e si dice che  $[a]$  è il *sottomonoido di  $M$  generato da  $a$* . Un monoide  $M$  si dice *ciclico* se esiste un elemento  $a \in M$  tale che  $M = [a]$ . In tal caso  $a$  si dice un *generatore* del monoide ciclico  $M$ .

PROPOSIZIONE 18.3. Se  $M$  è un monoide e  $X$  è un suo sottoinsieme non vuoto, allora  $[X] = \{1_M, x_1 x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X\}$ . In particolare, se  $X = \{a\}$ , allora  $[a] = \{a^n \mid n \in \mathbb{N}\}$ .

ESEMPIO 10. Si consideri il monoide  $(\mathbb{N}, \cdot)$ . Sia  $X = \{2, 3, 4\}$ . Il sottomonoido di  $(\mathbb{N}, \cdot)$  generato da  $X$  è

$$[X] = \{1, x_1 x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{2, 3, 4\}\} =$$



$$= \{1, 2^a 3^b 4^c \mid a, b, c \in \mathbb{N}\} = \{2^a 3^b 4^c \mid a, b, c \in \mathbb{N}\} = \\ = \{2^a 3^b \mid a, b \in \mathbb{N}\}.$$

(Per convincersi dell'ultima uguaglianza si osservi che l'inclusione  $\supseteq$  è ovvia, mentre l'inclusione  $\subseteq$  vale in quanto  $2^a 3^b 4^c = 2^{a+2c} 3^b$ .)  $\square$

ESEMPIO 11. Si consideri il monoide  $(\mathbb{N}, +)$ . Sia  $X = \{2, 3, 4\}$ . Il sottomonoide di  $(\mathbb{N}, +)$  generato da  $X$  è

$$[X] = \{0, x_1 + x_2 + \dots + x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{2, 3, 4\}\} = \\ = \{0, 2a + 3b + 4c \mid a, b, c \in \mathbb{N}\} = \mathbb{N} \setminus \{1\}.$$

Dimostriamo l'ultima uguaglianza: per l'inclusione  $\subseteq$  si osservi che se uno tra  $a, b$  o  $c$  è diverso da zero allora  $2a + 3b + 4c \geq 2$ ; per l'inclusione  $\supseteq$  si prenda un  $x \in \mathbb{N} \setminus \{1\}$  e si distinguano i tre casi  $x = 0$ ,  $x \geq 2$  pari, e  $x \geq 2$  dispari; se  $x = 0$  non c'è niente da dimostrare; se  $x \geq 2$  è pari allora  $x = 2a$  per qualche  $a \in \mathbb{N}$ ; se infine  $x \geq 2$  è dispari allora  $x = 2a + 3$  per qualche  $a \in \mathbb{N}$ .  $\square$

ESEMPIO 12. Sia  $A$  un insieme e si consideri il monoide  $(A^A, \circ)$  (vedi l'esempio 6 e l'esercizio 17.1). Per ogni  $a \in A$  sia  $\varphi_a : A \rightarrow A$  l'applicazione definita da  $\varphi_a(t) = a$  per ogni  $t \in A$ . Si ponga  $X = \{\varphi_a \mid a \in A\}$ . Il sottomonoide di  $(A^A, \circ)$  generato da  $X$  è

$$[X] = \{\iota_A, \xi_1 \circ \xi_2 \circ \dots \circ \xi_n \mid n \in \mathbb{N}^*, \xi_1, \xi_2, \dots, \xi_n \in X\} = \\ = \{\iota_A, \varphi_{a_1} \circ \varphi_{a_2} \circ \dots \circ \varphi_{a_n} \mid n \in \mathbb{N}^*, a_1, a_2, \dots, a_n \in A\} = \\ = \{\iota_A, \varphi_a \mid a \in A\} = \{\iota_A\} \cup X.$$

La penultima uguaglianza segue dal fatto che ovviamente  $\varphi_{a_1} \circ \varphi_{a_2} \circ \dots \circ \varphi_{a_n} = \varphi_{a_1}$ .  $\square$

Se  $(S, *)$ ,  $(S', \circ)$  sono due semigrupp, un omomorfismo di semigrupp  $\varphi$  di  $S$  in  $S'$  è un'applicazione  $\varphi : S \rightarrow S'$  tale che  $\varphi(x * y) = \varphi(x) \circ \varphi(y)$  per ogni  $x, y \in S$ . Se  $(S, *)$ ,  $(S', \circ)$  sono due monoidi, un omomorfismo di monoidi  $\varphi$  di  $S$  in  $S'$  è un omomorfismo di semigrupp tale che  $\varphi(1_S) = 1_{S'}$ .

Un isomorfismo (di semigrupp o di monoidi) è un omomorfismo biiettivo. Un endomorfismo di  $S$  è un omomorfismo di  $S$  in  $S$ . Un automorfismo di  $S$  è un endomorfismo biiettivo di  $S$  (o, equivalentemente, un isomorfismo di  $S$  in  $S$ ). Due semigrupp (o due monoidi)  $S$  ed  $S'$  si dicono isomorfi se esiste un isomorfismo di  $S$  in  $S'$ . Per indicare che due semigrupp o due monoidi  $S$ ,  $S'$  sono isomorfi scriveremo  $S \cong S'$ .

ESEMPIO 13. L'applicazione  $\pi : \mathbb{Z} \rightarrow \{1, -1\}$  definita da  $\pi(z) = (-1)^z$  per ogni  $z \in \mathbb{Z}$ , cioè l'applicazione definita da  $\pi(z) = 1$  se  $z$  è pari e  $\pi(z) = -1$  se  $z$  è dispari, è un omomorfismo di monoidi di  $(\mathbb{Z}, +)$  in  $(\{1, -1\}, \cdot)$ . Infatti  $\pi(z + z') =$

$(-1)^{z+z'} = (-1)^z (-1)^{z'} = \pi(z) \pi(z')$  per ogni  $z, z' \in \mathbb{Z}$ , e inoltre, osservato che 0 è l'identità di  $(\mathbb{Z}, +)$  e 1 è l'identità di  $(\{1, -1\}, \cdot)$ , si ha  $\pi(0) = (-1)^0 = 1$ .  $\square$

ESEMPIO 14. Sia  $(\mathbb{Z}^*, \cdot)$  il monoide moltiplicativo di tutti i numeri interi diversi da zero. L'applicazione  $\sigma : \mathbb{Z}^* \rightarrow \{1, -1\}$  definita da  $\sigma(z) = z/|z|$  per ogni  $z \in \mathbb{Z}^*$ , cioè l'applicazione definita da  $\sigma(z) = 1$  se  $z > 0$  e  $\sigma(z) = -1$  se  $z < 0$ , è un omomorfismo di monoidi di  $(\mathbb{Z}^*, \cdot)$  in  $(\{1, -1\}, \cdot)$ . Infatti  $\sigma(z z') = z z' / |z z'| = (z/|z|)(z'/|z'|) = \sigma(z) \sigma(z')$  per ogni  $z, z' \in \mathbb{Z}^*$ , e inoltre, osservato che 1 è sia l'identità di  $(\mathbb{Z}^*, \cdot)$  che l'identità di  $(\{1, -1\}, \cdot)$ , si ha  $\sigma(1) = 1/|1| = 1$ .  $\square$

ESEMPIO 15. Fissiamo un numero razionale  $k$ . Consideriamo l'applicazione  $\varphi_k : \mathbb{Q} \rightarrow \mathbb{Q}$  definita da  $\varphi_k(x) = kx$  per ogni  $x \in \mathbb{Q}$ . Allora  $\varphi_k$  è un endomorfismo del monoide  $(\mathbb{Q}, +)$ , in quanto per ogni  $x, y \in \mathbb{Q}$  si ha  $\varphi_k(x + y) = k(x + y) = kx + ky = \varphi_k(x) + \varphi_k(y)$  e, osservato che 0 è l'identità di  $(\mathbb{Q}, +)$ , si ha  $\varphi_k(0) = k \cdot 0 = 0$ . Se  $k \neq 0$  l'applicazione  $\varphi_k$  è un automorfismo di  $(\mathbb{Q}, +)$  in quanto:

- (1)  $\varphi_k$  è iniettiva, perché se  $x, y \in \mathbb{Q}$  e  $\varphi_k(x) = \varphi_k(y)$ , allora  $kx = ky$ , da cui  $x = y$  perché  $k \neq 0$ ;
- (2)  $\varphi_k$  è suriettiva, perché se  $x \in \mathbb{Q}$ , allora  $k^{-1}x \in \mathbb{Q}$  (si osservi che  $k^{-1} \in \mathbb{Q}$  perché  $k \neq 0$ ) e si ha  $\varphi_k(k^{-1}x) = k k^{-1}x = x$ .  $\square$

ESEMPIO 16. Sia  $\mu : \mathbb{C} \rightarrow \mathbb{R}$  l'applicazione definita da  $\mu(z) = |z|$  per ogni  $z \in \mathbb{C}$ . Allora  $\mu$  è un omomorfismo del monoide  $(\mathbb{C}, \cdot)$  nel monoide  $(\mathbb{R}, \cdot)$ , come è facile verificare.  $\square$

ESEMPIO 17. Siano  $A \subseteq B$  insiemi. Definiamo l'applicazione

$$\psi : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$$

ponendo  $\psi(X) = X$  per ogni  $X \in \mathcal{P}(A)$ . Allora:

- (a) l'applicazione  $\psi$  è un omomorfismo di monoidi di  $(\mathcal{P}(A), \cup)$  in  $(\mathcal{P}(B), \cup)$  in quanto per ogni  $X, Y \in \mathcal{P}(A)$  si ha  $\psi(X \cup Y) = X \cup Y = \psi(X) \cup \psi(Y)$  e  $\psi(\emptyset) = \emptyset$ ;
- (b) l'applicazione  $\psi$  è un omomorfismo di semigrupp di  $(\mathcal{P}(A), \cap)$  in  $(\mathcal{P}(B), \cap)$  in quanto per ogni  $X, Y \in \mathcal{P}(A)$  si ha  $\psi(X \cap Y) = X \cap Y = \psi(X) \cap \psi(Y)$ ;
- (c) se  $A \subset B$  l'applicazione  $\psi$  non è un omomorfismo di monoidi di  $(\mathcal{P}(A), \cap)$  in  $(\mathcal{P}(B), \cap)$  in quanto le identità di  $(\mathcal{P}(A), \cap)$  e  $(\mathcal{P}(B), \cap)$  sono  $A$  e  $B$  rispettivamente, mentre  $\psi(A) = A \subset B$ .  $\square$

### Esercizi svolti

18.1. Siano  $S$  e  $T$  due semigrupp. Sul prodotto cartesiano  $S \times T$  si definisca un'operazione di moltiplicazione ponendo  $(s, t)(s', t') = (ss', tt')$  per ogni  $(s, t), (s', t') \in S \times T$ .

- (a) Si dimostri che  $S \times T$  con questa operazione è un semigrupp (detto il prodotto diretto di  $S$  per  $T$ ).
- (b) Si dimostri che se  $S$  e  $T$  sono monoidi, il loro prodotto diretto  $S \times T$  è un monoide, che  $S \times \{1_T\}$  e  $\{1_S\} \times T$  sono sottomonoidi di  $S \times T$ , che i monoidi  $S$  e  $S \times \{1_T\}$  sono isomorfi, e che i monoidi  $T$  e  $\{1_S\} \times T$  sono isomorfi.
- (c) Sia  $S \times S$  il prodotto diretto di un semigrupp commutativo  $S$  per sé stesso. Si dimostri che l'applicazione  $\mu : S \times S \rightarrow S$  definita da  $\mu(s, t) = st$  per ogni  $(s, t) \in S \times S$  è un omomorfismo di semigrupp.
- (d) Si dimostri che se  $S$  è un monoide commutativo l'applicazione  $\mu : S \times S \rightarrow S$  è un omomorfismo suriettivo di monoidi.

*Soluzione.* (a) Si deve solamente dimostrare che l'operazione di moltiplicazione su  $S \times T$  è associativa. Per ogni  $(s, t), (s', t'), (s'', t'') \in S \times T$  si ha

$$\begin{aligned} ((s, t)(s', t'))(s'', t'') &= (ss', tt')(s'', t'') = ((ss')s'', (tt')t'') = \\ &= (s(ss''), t(t't'')) = (s, t)(s's'', t't'') = \\ &= (s, t)((s', t')(s'', t'')). \end{aligned}$$

(b) Abbiamo visto in (a) che  $S \times T$  è un semigrupp. Dimostriamo che è un monoide facendo vedere che la coppia  $(1_S, 1_T)$  è la sua identità: si ha  $(s, t)(1_S, 1_T) = (s1_S, t1_T) = (s, t)$  e  $(1_S, 1_T)(s, t) = (1_Ss, 1_Tt) = (s, t)$  per ogni  $(s, t) \in S \times T$ . Quindi  $S \times T$  è un monoide.

Dimostriamo che  $S \times \{1_T\}$  è un sottomonoide di  $S \times T$ . Si ha  $1_{S \times T} = (1_S, 1_T) \in S \times \{1_T\}$ . Inoltre se  $(s, 1_T), (s', 1_T) \in S \times \{1_T\}$ , allora  $(s, 1_T)(s', 1_T) = (ss', 1_T) \in S \times \{1_T\}$ . Quindi  $S \times \{1_T\}$  è un sottomonoide di  $S \times T$ . Analogamente si vede che  $\{1_S\} \times T$  è un sottomonoide di  $S \times T$ .

Per dimostrare che i monoidi  $S$  e  $S \times \{1_T\}$  sono isomorfi consideriamo l'applicazione  $\varphi : S \rightarrow S \times \{1_T\}$  definita da  $\varphi(s) = (s, 1_T)$  per ogni  $s \in S$ . È evidente che  $\varphi$  è una biiezione. Inoltre per ogni  $s, s' \in S$  si ha  $\varphi(s)\varphi(s') = (s, 1_T)(s', 1_T) = (ss', 1_T) = \varphi(ss')$  e  $\varphi(1_S) = (1_S, 1_T) = 1_{S \times T}$ . Quindi  $\varphi$  è un isomorfismo di monoidi. In modo analogo si vede che i monoidi  $T$  e  $\{1_S\} \times T$  sono isomorfi.

(c) Per ogni  $(s, t), (s', t') \in S \times S$  si ha

$$\begin{aligned} \mu((s, t)(s', t')) &= \mu(ss', tt') = (ss')(tt') = \\ &= s(s't')t' = s(ts')t' = \\ &= (st)(s't') = \mu(s, t)\mu(s', t'). \end{aligned}$$

(d) Si osservi intanto che da (b) segue che se  $S$  è un monoide con identità  $1_S$ , anche  $S \times S$  è un monoide con identità  $1_{S \times S} = (1_S, 1_S)$ . In (c) si è già dimostrato che  $\mu$  è un omomorfismo di semigrupp. Per far vedere che  $\mu$  è un omomorfismo

di monoidi ci resta da osservare che  $\mu(1_{S \times S}) = \mu(1_S, 1_S) = 1_S \cdot 1_S = 1_S$ . Infine l'applicazione  $\mu : S \times S \rightarrow S$  è suriettiva, perché per ogni  $a \in S$  si ha che  $(a, 1_S) \in S \times S$  e  $\mu(a, 1_S) = a \cdot 1_S = a$ . □

**18.2.** Si dimostri che se  $M$  è un monoide ciclico, allora  $M$  è commutativo.

*Soluzione.* Se  $M$  è un monoide ciclico, esiste un elemento  $a \in M$  tale che  $M = \langle a \rangle$ , cioè tale che  $M = \{a^n \mid n \in \mathbb{N}\}$ . Mostriamo che  $M$  è commutativo, cioè che per ogni  $x, y \in M$  si ha  $xy = yx$ . Se  $x, y \in M$ , esistono  $n, m \in \mathbb{N}$  tali che  $x = a^n$  e  $y = a^m$ . Pertanto

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx. \quad \square$$

**18.3.** Sia  $A$  un insieme e sia  $(\mathcal{P}(A), \cup)$  il monoide delle parti di  $A$  dotato dell'operazione di unione. Si consideri il sottoinsieme  $X = \{\{a\} \mid a \in A\}$  di  $\mathcal{P}(A)$ .

- (a) Si determini il sottomonoide  $[X]$  di  $\mathcal{P}(A)$  generato da  $X$ .
- (b) Se  $a_0 \in A$  è un elemento fissato, si determini il sottomonoide ciclico  $\langle \{a_0\} \rangle$  di  $\mathcal{P}(A)$  generato da  $\{a_0\}$ .

*Soluzione.* (a) Si osservi intanto che  $1_{\mathcal{P}(A)} = \emptyset$ , perché per ogni  $B \in \mathcal{P}(A)$  si ha  $B \cup \emptyset = \emptyset \cup B = B$ . Pertanto

$$\begin{aligned} [X] &= \{1_{\mathcal{P}(A)}, x_1 \cup x_2 \cup \dots \cup x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X\} = \\ &= \{\emptyset, \{a_1\} \cup \{a_2\} \cup \dots \cup \{a_n\} \mid n \in \mathbb{N}^*, a_1, a_2, \dots, a_n \in A\} = \\ &= \{\emptyset, \{a_1, a_2, \dots, a_n\} \mid n \in \mathbb{N}^*, a_1, a_2, \dots, a_n \in A\} = \\ &= \{F \mid F \subseteq A, F \text{ finito}\}. \end{aligned}$$

Quindi il sottomonoide di  $(\mathcal{P}(A), \cup)$  generato da  $X$  è l'insieme dei sottoinsiemi finiti di  $A$ .

(b) Per quanto riguarda  $\langle \{a_0\} \rangle$  si osservi che si ha  $\{a_0\}^0 = 1_{\mathcal{P}(A)} = \emptyset$  e

$$\{a_0\}^n = \underbrace{\{a_0\} \cup \{a_0\} \cup \dots \cup \{a_0\}}_{n \text{ volte}} = \{a_0\}$$

per ogni numero intero  $n > 0$ . Quindi  $\langle \{a_0\} \rangle = \{\{a_0\}^n \mid n \in \mathbb{N}\} = \{\emptyset, \{a_0\}\}$  è il sottomonoide di  $(\mathcal{P}(A), \cup)$  avente come soli elementi  $\emptyset$  e  $\{a_0\}$ . □

### Altri esercizi

**18.4.** Sia  $A$  un insieme non vuoto. Quali sono le identità sinistre e le identità destre nel semigrupp  $(A, *)$  dell'esempio 4 del capitolo 17? Si dimostri che  $(A, *)$  è un monoide se e solo se  $|A| = 1$ .

**18.5.** Si dimostri che il semigrupp  $(\mathbb{R} \times \mathbb{R}, *)$  dell'esercizio 17.8 è un monoide. Quale elemento di  $\mathbb{R} \times \mathbb{R}$  è l'identità del monoide?

18.6. Si dimostri che il semigruppò  $(\{0, 1\}^{\mathbb{R}}, *)$  dell'esercizio 17.9 è un monoide. Quale applicazione di  $\mathbb{R}$  in  $\{0, 1\}$  è l'identità di questo monoide?

18.7. Si fissi un numero intero positivo  $n$ . Sia  $M_n(\mathbb{R})$  l'insieme delle matrici  $n \times n$  ad elementi reali:

$$M_n(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \mid a_{ij} \in \mathbb{R} \text{ per ogni } i, j \right\}.$$

Si provi che  $M_n(\mathbb{R})$  con la moltiplicazione righe per colonne è un monoide.

18.8. Siano  $A = \{0, 1, 2, 3, 4, 5\}$  e  $(A^A, \circ)$  il monoide di tutte le applicazioni di  $A$  in  $A$  con la composizione di applicazioni.

- (a) Quanti elementi ha  $A^A$ ?  
 (b) Sia  $f: A \rightarrow A$  l'applicazione definita da  $f(a) = \min\{a^2, 5\}$ , e sia  $[f]$  il sottomonoido di  $A^A$  generato da  $f$ . Quanti elementi ha  $[f]$ ? Quali sono?

[Suggerimento: si dimostri per induzione che  $f^n = f^2$  per ogni  $n \geq 2$ .]

18.9. Sia  $M = \mathbb{N} \times \mathbb{N}$  il prodotto diretto del monoide  $(\mathbb{N}, +)$  per sé stesso (vedi esercizio 18.1). Siano  $a, b$  due numeri naturali positivi fissati. Si definisca un'applicazione  $f: M \rightarrow \mathbb{N}$  ponendo  $f(x, y) = a^x b^y$  per ogni  $(x, y) \in M$ .

- (a) Si dimostri che  $f$  è un omomorfismo di monoidi di  $M$  nel monoide moltiplicativo  $(\mathbb{N}, \cdot)$ .  
 (b) Se  $a > 1$  e  $b = a^2$ , si calcoli  $f^{-1}(1)$ .  
 (c) Se  $a > 1$  e  $b = a^2$ , si dimostri che  $f$  non è iniettiva.  
 (d) Se  $a$  e  $b$  sono numeri primi distinti, si dimostri che  $f$  è iniettiva.

18.10. Si consideri il monoide moltiplicativo  $(\mathbb{R}, \cdot)$ . Sia  $S = \{-1, 0\}$  il sottomonoido di  $\mathbb{R}$  generato dal sottoinsieme  $\{-1, 0\}$  di  $\mathbb{R}$ .

- (a) Quali e quanti sono gli elementi di  $S$ ?  
 (b) Si dimostri che esiste un unico endomorfismo  $\varphi$  del monoide  $(\mathbb{R}, \cdot)$  tale che  $\varphi(0) = 0$  e  $\varphi(a) = -1$  per ogni numero reale negativo  $a$ .  
 (c) Si provi che  $\varphi(\mathbb{R}) = S$ .

[Suggerimento per la parte (b): Per capire come deve essere definito  $\varphi$  si osservi che ogni numero reale positivo è il quadrato di un numero reale negativo. Una volta definita opportunamente l'applicazione  $\varphi$  si faccia vedere che è un endomorfismo di monoidi, cioè che  $\varphi(1) = 1$  e che  $\varphi(xy) = \varphi(x)\varphi(y)$ , distinguendo i quattro casi  $xy = 0$ ,  $x$  e  $y$  entrambi positivi,  $x$  e  $y$  entrambi negativi,  $x$  e  $y$  uno positivo e l'altro negativo].

18.11. Si consideri il monoide  $(\mathbb{Q}, +)$ . Sia  $M = \mathbb{N} \setminus \{1\}$ .

- (a) Si dimostri che  $M$  è un sottomonoido di  $\mathbb{Q}$ .  
 (b) Si dimostri che il monoide  $M$  non è ciclico.

## Capitolo 19. Quozienti

Se  $(S, \cdot)$  è un semigruppò e  $\sim$  è un'equivalenza sull'insieme  $S$ , diciamo che l'operazione  $\cdot$  e l'equivalenza  $\sim$  sono tra loro compatibili se  $a \sim b$  e  $c \sim d$  implicano  $ac \sim bd$  per ogni  $a, b, c, d \in S$ .

Ad esempio se  $(S, \cdot)$ ,  $(S', \cdot)$  sono due semigruppò ed  $f: S \rightarrow S'$  è un omomorfismo di semigruppò è facile verificare che la relazione di equivalenza  $\sim_f$  su  $S$  associata ad  $f$  (definita, per ogni  $a, b \in S$ , da  $a \sim_f b$  se  $f(a) = f(b)$  — vedi l'esempio 8 del capitolo 7) e l'operazione su  $S$  sono tra loro compatibili.

Dato un qualunque semigruppò  $(S, \cdot)$  e una relazione di equivalenza  $\sim$  su  $S$  compatibile con l'operazione di  $S$ , è possibile definire sull'insieme quoziente un'operazione (che denoteremo ancora con  $\cdot$ ) ponendo  $[a] \cdot [b] = [ab]$  per ogni  $[a], [b] \in S/\sim$ , ed  $S/\sim$  con questa operazione risulta essere un semigruppò (detto il semigruppò quoziente di  $S$  modulo  $\sim$ ). Inoltre se il semigruppò  $S$  è commutativo anche  $S/\sim$  è un semigruppò commutativo, e se  $S$  è un monoide con identità  $1_S$  anche  $S/\sim$  è un monoide con identità  $1_{S/\sim} = [1_S]$  (detto il monoide quoziente di  $S$  modulo  $\sim$ ). La proiezione canonica  $\pi: S \rightarrow S/\sim$  definita da  $\pi(a) = [a]$  per ogni  $a \in S$  risulta essere un omomorfismo di semigruppò (rispettivamente, di monoidi).

ESEMPIO 1. Sia  $n \geq 1$  un numero naturale fissato. Sappiamo che la moltiplicazione su  $\mathbb{Z}$  e la congruenza modulo  $n$  sono tra loro compatibili (esercizio 8.3). Sull'insieme quoziente  $\mathbb{Z}/\equiv_n$  è pertanto definita un'operazione di moltiplicazione, che verrà denotata ancora con  $\cdot$ , nel modo seguente:

$$[a] \cdot [b] = [ab] \text{ per ogni } a, b \in \mathbb{Z}.$$

Con questa operazione  $\mathbb{Z}/\equiv_n$  diventa un monoide con  $n$  elementi nel quale l'identità è la classe di equivalenza  $[1]$ . La proiezione canonica  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/\equiv_n$ , definita da  $\pi(a) = [a]$  per ogni  $a \in \mathbb{Z}$ , è un omomorfismo del monoide  $(\mathbb{Z}, \cdot)$  nel monoide  $(\mathbb{Z}/\equiv_n, \cdot)$ .  $\square$

ESEMPIO 2. Come nell'esempio precedente si fissi un numero naturale  $n \geq 1$ . Anche l'addizione su  $\mathbb{Z}$  e la congruenza modulo  $n$  sono tra loro compatibili (esercizio 8.3). Sull'insieme quoziente  $\mathbb{Z}/\equiv_n$  c'è pertanto un'ulteriore operazione, che

verrà denotata ancora con  $+$ , definita nel modo seguente:

$$[a] + [b] = [a + b] \text{ per ogni } a, b \in \mathbb{Z}.$$

Con questa operazione  $\mathbb{Z}/\equiv_n$  diventa un monoide con  $n$  elementi, diverso ovviamente da quello dell'esempio 1 perché l'operazione è diversa, in cui l'identità è la classe di equivalenza  $[0]$ . La proiezione canonica  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/\equiv_n$ , definita da  $\pi(a) = [a]$  per ogni  $a \in \mathbb{Z}$ , è un omomorfismo del monoide  $(\mathbb{Z}, +)$  nel monoide  $(\mathbb{Z}/\equiv_n, +)$ .  $\square$

**TEOREMA 19.1.** (TEOREMA FONDAMENTALE DI OMOMORFISMO PER I SEMIGRUPPI E I MONOIDI). Siano  $S, S'$  semigrupp (monoidi) ed  $f: S \rightarrow S'$  un omomorfismo di semigrupp (monoidi). Se  $\sim_f$  è la relazione di equivalenza associata ad  $f$  (definita, per ogni  $a, b \in S$ , da  $a \sim_f b$  se  $f(a) = f(b)$ ) e  $\pi: S \rightarrow S/\sim_f$  è la proiezione canonica, allora:

- (a) esiste un'unica applicazione  $\tilde{f}: S/\sim_f \rightarrow S'$  che rende commutativo il diagramma

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ \pi \searrow & & \nearrow \tilde{f} \\ & S/\sim_f & \end{array}$$

cioè tale che  $\tilde{f} \circ \pi = f$ ;

- (b)  $\tilde{f}$  è un omomorfismo iniettivo di semigrupp (monoidi);  
(c)  $\tilde{f}$  è un isomorfismo se e solo se  $f$  è suriettivo.

### Esercizi svolti

**19.1.** Siano  $S$  un insieme e  $*$  l'operazione su  $S$  definita da  $x * y = x$  per ogni  $x, y \in S$ . Se  $T$  è un sottoinsieme di  $S$  si definisca una relazione  $\sim_T$  su  $S$  ponendo, per ogni  $x, y \in S$ ,

$$x \sim_T y \text{ se } \begin{cases} x = y \\ \text{oppure} \\ x \in T \text{ e } y \in T. \end{cases}$$

- (a) Si dimostri che  $\sim_T$  è un'equivalenza su  $S$  e si determini  $S/\sim_T$ .  
(b) Si dimostri che  $(S, *)$  è un semigrupp.  
(c) Si dimostri che  $*$  e  $\sim_T$  sono tra loro compatibili.  
(d) Si dimostri che ogni sottoinsieme di  $S$  è un sottosemigrupp di  $S$ .  
(e) Si dimostri che se  $t_0 \in T$ , allora il semigrupp quoziente  $S/\sim_T$  e il sottosemigrupp  $\{t_0\} \cup (S \setminus T)$  di  $S$  sono isomorfi.

**Soluzione.** (a) Conviene innanzitutto osservare che fissato un qualunque elemento  $y \in S$  si hanno due casi: se  $y \in T$  gli elementi che stanno nella relazione  $\sim_T$  con  $y$  sono tutti e soli gli elementi di  $T$ ; se invece  $y \notin T$ , l'unico elemento che sta nella relazione  $\sim_T$  con  $y$  è  $y$  stesso. Dimostriamo che  $\sim_T$  è una relazione di equivalenza su  $S$ . La riflessività di  $\sim_T$  segue immediatamente da come è stata definita  $\sim_T$  (perché se  $x = y$  allora  $x \sim_T y$ ). Lo stesso vale per la simmetria. Transitività: Siano  $x, y, z \in S$  tali che  $x \sim_T y$  e  $y \sim_T z$ . Se  $y \notin T$ , allora si deve avere che  $x = y$  e  $y = z$ , e quindi in questo caso  $x \sim_T z$ . Se invece  $y \in T$ , allora da  $x \sim_T y$  segue che  $x \in T$ , e da  $y \sim_T z$  segue che  $z \in T$ . Quindi  $x$  e  $z$  appartengono entrambi a  $T$ , da cui  $x \sim_T z$  anche in quest'altro caso. Questo dimostra che  $\sim_T$  è un'equivalenza su  $S$ . Determiniamo  $S/\sim_T$ . Sia  $s \in S$ . Se  $s \in T$  si ha  $[s]_{\sim_T} = \{x \mid x \in S, x \sim_T s\} = \{x \mid x \in T\} = T$ . Se invece  $s \notin T$  si ha  $[s]_{\sim_T} = \{x \mid x \in S, x \sim_T s\} = \{x \mid x = s\} = \{s\}$ . Quindi

$$\begin{aligned} S/\sim_T &= \{[s]_{\sim_T} \mid s \in S\} = \\ &= \{[s]_{\sim_T} \mid s \in T\} \cup \{[s]_{\sim_T} \mid s \in S \setminus T\} = \{T\} \cup \{[s]_{\sim_T} \mid s \in S \setminus T\}. \end{aligned}$$

- (b) Siano  $x, x', x'' \in S$ . Allora  $(x * x') * x'' = x * x' = x$  e  $x * (x' * x'') = x * x' = x$ , da cui  $(x * x') * x'' = x * (x' * x'')$ .  
(c) Siano  $x, y, x', y' \in S$  tali che  $x \sim_T y$  e  $x' \sim_T y'$ . Allora  $x * x' = x \sim_T y = y * y'$ .  
(d) Sia  $S'$  un qualunque sottoinsieme di  $S$ . Da  $x, y \in S'$  segue che  $x * y = x \in S'$ . Quindi  $S'$  è un sottosemigrupp di  $S$ .  
(e) Sia  $t_0 \in T$ . Si consideri l'applicazione  $f: S \rightarrow \{t_0\} \cup (S \setminus T)$  definita da

$$f(s) = \begin{cases} t_0 & \text{se } s \in T, \\ s & \text{se } s \in S \setminus T. \end{cases}$$

L'applicazione  $f$  è un omomorfismo del semigrupp  $S$  nel suo sottosemigrupp  $\{t_0\} \cup (S \setminus T)$ , in quanto per ogni  $s, s' \in S$  si ha  $f(s * s') = f(s) = f(s) * f(s')$ . È facile verificare che  $f$  è suriettivo. Per il teorema fondamentale di omomorfismo per i semigrupp c'è un isomorfismo di semigrupp  $\tilde{f}: S/\sim_f \rightarrow \{t_0\} \cup (S \setminus T)$ . Mostriamo che le equivalenze  $\sim_f$  e  $\sim_T$  coincidono. Per ogni  $x, y \in S$  si ha  $x \sim_f y$  se e solo se  $f(x) = f(y)$ , ossia, per come è definita  $f$ , se e solo se  $x$  e  $y$  appartengono entrambi a  $T$  oppure  $x = y$ . Quindi  $x \sim_f y$  se e solo se  $x \sim_T y$ , e pertanto le due equivalenze  $\sim_f$  e  $\sim_T$  su  $S$  coincidono. Si conclude quindi che i semigrupp  $S/\sim_T = S/\sim_f$  e  $\{t_0\} \cup (S \setminus T)$  sono isomorfi.  $\square$

**19.2.** Si consideri il monoide moltiplicativo dei numeri complessi  $(\mathbb{C}, \cdot)$ . Sia  $f: \mathbb{C} \rightarrow \mathbb{C}$  l'applicazione definita da  $f(z) = z^2$  per ogni  $z \in \mathbb{C}$ .

- (a) Si dimostri che  $f$  è un omomorfismo suriettivo di monoidi.  
(b) Si dimostri che l'equivalenza  $\sim_f$  è definita, per ogni  $z, z' \in \mathbb{C}$ , da  $z \sim_f z'$  se e solo se  $z = z'$  oppure  $z = -z'$ .

- (c) Per ogni  $z \in \mathbb{C}$  si determini  $[z]_{\sim_f}$  e la cardinalità di  $[z]_{\sim_f}$ .  
 (d) Si dimostri che i monoidi moltiplicativi  $\mathbb{C}/\sim_f$  e  $\mathbb{C}$  sono isomorfi.

*Soluzione.* (a) Per dimostrare che  $f$  è un omomorfismo di monoidi è sufficiente osservare che  $f(zz') = (zz')^2 = z^2 z'^2 = f(z)f(z')$  per ogni  $z, z' \in \mathbb{C}$ , e che  $f(1) = 1^2 = 1$ . Per dimostrare che  $f$  è suriettivo si fissi un qualunque elemento  $z \in \mathbb{C}$ . Scrivendo  $z$  in forma trigonometrica si ha che  $z = \varrho(\cos \varphi + i \sin \varphi)$  per qualche  $\varphi, \varrho \in \mathbb{R}, \varrho \geq 0$ . Allora  $z' = \sqrt{\varrho}(\cos(\varphi/2) + i \sin(\varphi/2))$  è un numero complesso tale che  $z'^2 = z$ , cioè tale che  $f(z') = z$ . Quindi l'omomorfismo  $f$  è suriettivo.

(b) Dati  $z, z' \in \mathbb{C}$ , si ha  $z \sim_f z'$  se e solo se  $f(z) = f(z')$ , cioè se e solo se  $z^2 = z'^2$ , vale a dire se e solo se  $z^2 - z'^2 = 0$ . Quindi  $z \sim_f z'$  se e solo se  $(z - z')(z + z') = 0$ , cioè se e solo se  $z - z' = 0$  oppure  $z + z' = 0$ , ossia se e solo se  $z = z'$  oppure  $z = -z'$ .

(c) Dato  $z \in \mathbb{C}$  si ha  $[z]_{\sim_f} = \{x \in \mathbb{C} \mid x \sim_f z\} = \{x \in \mathbb{C} \mid x = z \text{ oppure } x = -z\} = \{z, -z\}$ . In particolare  $[z]_{\sim_f}$  ha cardinalità 2 se  $z \neq 0$ , e ha cardinalità 1 se  $z = 0$ .

(d) Applicando il teorema fondamentale di omomorfismo per i monoidi all'omomorfismo suriettivo  $f: \mathbb{C} \rightarrow \mathbb{C}$  si vede che esiste un isomorfismo di monoidi  $\tilde{f}: \mathbb{C}/\sim_f \rightarrow \mathbb{C}$ . Pertanto i monoidi moltiplicativi  $\mathbb{C}/\sim_f$  e  $\mathbb{C}$  sono isomorfi.  $\square$

**19.3.** Si consideri il monoide moltiplicativo dei numeri complessi  $(\mathbb{C}, \cdot)$ . Siano  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$  e  $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ .

- (a) Si dimostri che  $\mathbb{C}^*$  e  $\mathbb{T}$  sono sottomonoidi di  $(\mathbb{C}, \cdot)$ .  
 (b) Si consideri l'applicazione  $f: \mathbb{C}^* \rightarrow \mathbb{T}$  definita da  $f(z) = \frac{z}{|z|}$  per ogni  $z \in \mathbb{C}^*$ . Si dimostri che  $f$  è un omomorfismo suriettivo di monoidi.  
 (c) Siano  $z, z' \in \mathbb{C}^*$ . Si dimostri che  $z \sim_f z'$  se e solo se esiste  $\alpha \in \mathbb{R}$  tale che  $\alpha > 0$  e  $z = \alpha z'$ .  
 (d) Per ogni  $z \in \mathbb{C}^*$  si determini  $[z]_{\sim_f}$ .  
 (e) Si dimostri che i monoidi moltiplicativi  $\mathbb{C}^*/\sim_f$  e  $\mathbb{T}$  sono isomorfi.

*Soluzione.* (a)  $\mathbb{C}^*$  è un sottomonoido di  $(\mathbb{C}, \cdot)$  perché  $1 \in \mathbb{C}^*$  e se  $z, z' \in \mathbb{C}^*$ , allora  $z \neq 0$  e  $z' \neq 0$ , da cui  $zz' \neq 0$ , ossia  $zz' \in \mathbb{C}^*$ . Analogamente  $\mathbb{T}$  è un sottomonoido di  $(\mathbb{C}, \cdot)$ , perché  $1 \in \mathbb{T}$  (in quanto  $|1| = 1$ ) e se  $z, z' \in \mathbb{T}$ , allora  $|z| = 1$  e  $|z'| = 1$ , da cui  $|zz'| = |z||z'| = 1 \cdot 1 = 1$ , e quindi  $zz' \in \mathbb{T}$ .

(b) Si ha  $f(zz') = \frac{zz'}{|zz'|} = \frac{z}{|z|} \frac{z'}{|z'|} = f(z)f(z')$  per ogni  $z, z' \in \mathbb{C}^*$  e  $f(1) = \frac{1}{|1|} = 1$ . Quindi  $f$  è un omomorfismo di monoidi. Per dimostrare che  $f$  è suriettivo basta osservare che per ogni  $z \in \mathbb{T}$  si ha

$$f(z) = \frac{z}{|z|} = \frac{z}{1} = z.$$

- (c) Siano  $z, z' \in \mathbb{C}^*$ . Se  $z \sim_f z'$ , si ha  $f(z) = f(z')$ , cioè  $\frac{z}{|z|} = \frac{z'}{|z'|}$ . Ne segue che  $z = \frac{|z|}{|z'|} z'$  con  $\frac{|z|}{|z'|} \in \mathbb{R}$  e  $\frac{|z|}{|z'|} > 0$ .

Viceversa supponiamo che esista  $\alpha \in \mathbb{R}$  tale che  $\alpha > 0$  e  $z = \alpha z'$ . Allora  $f(z) = f(\alpha z') = \frac{\alpha z'}{|\alpha z'|} = \frac{\alpha z'}{\alpha |z'|} = \frac{z'}{|z'|} = f(z')$ . Quindi  $z \sim_f z'$ .

- (d) Dato  $z \in \mathbb{C}^*$  si ha

$$\begin{aligned} [z]_{\sim_f} &= \{x \in \mathbb{C}^* \mid x \sim_f z\} = \\ &= \{x \in \mathbb{C}^* \mid \text{esiste } \alpha \in \mathbb{R}, \alpha > 0 \text{ tale che } x = \alpha z\} = \\ &= \{\alpha z \mid \alpha \in \mathbb{R}, \alpha > 0\}. \end{aligned}$$

Quindi  $[z]_{\sim_f}$  è l'insieme dei numeri complessi che nel piano di Argand-Gauss stanno sulla semiretta aperta passante per il punto  $z$  e avente l'origine nel punto 0.

- (e) Applicando il teorema fondamentale di omomorfismo per i monoidi all'omomorfismo suriettivo  $f: \mathbb{C}^* \rightarrow \mathbb{T}$  si vede che esiste un isomorfismo di monoidi  $\tilde{f}: \mathbb{C}^*/\sim_f \rightarrow \mathbb{T}$ . Pertanto i monoidi moltiplicativi  $\mathbb{C}^*/\sim_f$  e  $\mathbb{T}$  sono isomorfi.  $\square$

### Altri esercizi

**19.4.** Sia  $\sim$  la relazione su  $\mathbb{C}$  definita, per ogni  $a, b \in \mathbb{C}$ , da  $a \sim b$  se  $a - b \in \mathbb{Z}$ .

- (a) Si dimostri che  $\sim$  è un'equivalenza su  $\mathbb{C}$ .  
 (b) Si dimostri che  $\sim$  è compatibile con l'addizione tra numeri complessi.

**19.5.** Sia  $(M, \cdot)$  un monoide. Se  $x, y \in M$  poniamo  $x \sim y$  se esiste  $n \in \mathbb{N}^*$  tale che  $x^n = y^n$ .

- (a) Si provi che la relazione  $\sim$  è un'equivalenza sull'insieme  $M$ .  
 (b) Se  $M$  è un monoide commutativo, si provi che l'equivalenza  $\sim$  è compatibile con l'operazione di  $M$ .  
 (c) Si provi che se  $x \in M$ ,  $n \in \mathbb{N}^*$  e  $x^n \sim 1_M$ , allora  $x \sim 1_M$ .

**19.6.** Sia  $f: S \rightarrow S'$  un omomorfismo di semigrupp. Allora:

- (a) se  $T$  è un sottosemigruppo di  $S$ ,  $f(T)$  è un sottosemigruppo di  $S'$ ;  
 (b) se  $T'$  è un sottosemigruppo di  $S'$ ,  $f^{-1}(T')$  è un sottosemigruppo di  $S$ .

**19.7.** Sia  $f: M \rightarrow M'$  un omomorfismo di monoidi. Allora:

- (a) se  $N$  è un sottomonoido di  $M$ ,  $f(N)$  è un sottomonoido di  $M'$ ;  
 (b) se  $N'$  è un sottomonoido di  $M'$ ,  $f^{-1}(N')$  è un sottomonoido di  $M$ .

**19.8.** Nell'insieme  $\mathbb{Z}$  sia  $\sim$  la relazione definita, per ogni  $a, b \in \mathbb{Z}$ , da  $a \sim b$  se esistono  $n, m \in \mathbb{N}$  tali che  $2^n a = 2^m b$ .



- (a) Si dimostri che  $\sim$  è un'equivalenza su  $\mathbb{Z}$ .  
 (b) Si dimostri che  $\sim$  è compatibile con la moltiplicazione  $\cdot$  in  $\mathbb{Z}$ . È quindi possibile definire il monoide quoziente  $\mathbb{Z}/\sim$ .  
 (c) Si dimostri che se  $D$  è l'insieme dei numeri interi dispari, allora  $D \cup \{0\}$  è un sottomonoide di  $(\mathbb{Z}, \cdot)$ .  
 (d) Sia  $\varphi: D \cup \{0\} \rightarrow \mathbb{Z}/\sim$  l'applicazione definita da  $\varphi(a) = [a]_\sim$  per ogni  $a \in D \cup \{0\}$ . Si dimostri che  $\varphi$  è un isomorfismo di monoidei.
- 19.9. (a) Si dimostri che se  $f: S \rightarrow S'$  è un omomorfismo di semigrupp, allora  $S/\sim_f$  ed  $f(S)$  sono semigrupp isomorfi.  
 (b) Si dimostri che se  $f: M \rightarrow M'$  è un omomorfismo di monoidei, allora  $M/\sim_f$  ed  $f(M)$  sono monoidei isomorfi.

19.10. Sia  $(\mathbb{R} \times \mathbb{R}, \star)$  il monoide dell'esercizio 17.8.

- (a) Si dimostri che la prima proiezione  $\pi_1: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , definita per ogni  $(a, b) \in \mathbb{R} \times \mathbb{R}$  da  $\pi_1(a, b) = a$ , è un omomorfismo suriettivo del monoide  $(\mathbb{R} \times \mathbb{R}, \star)$  nel monoide  $(\mathbb{R}, \cdot)$ .  
 (b) Si dimostri che la seconda proiezione  $\pi_2: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , definita per ogni  $(a, b) \in \mathbb{R} \times \mathbb{R}$  da  $\pi_2(a, b) = b$ , non è un omomorfismo del monoide  $(\mathbb{R} \times \mathbb{R}, \star)$  nel monoide  $(\mathbb{R}, \cdot)$ .  
 (c) Sia  $\sim$  l'equivalenza su  $\mathbb{R} \times \mathbb{R}$  definita, per ogni  $(a, b), (a', b') \in \mathbb{R} \times \mathbb{R}$ , da  $(a, b) \sim (a', b')$  se  $a = a'$ . Si dimostri che l'equivalenza  $\sim$  e l'equivalenza  $\sim_{\pi_1}$  associata a  $\pi_1$  coincidono.  
 (d) Si dimostri che il monoide quoziente  $\mathbb{R} \times \mathbb{R}/\sim$  e il monoide  $(\mathbb{R}, \cdot)$  sono isomorfi.  
 (e) Per ogni  $(a, b) \in \mathbb{R} \times \mathbb{R}$  sia  $f_{(a,b)}: \mathbb{R} \rightarrow \mathbb{R}$  l'applicazione definita da  $f_{(a,b)}(x) = ax + b$  per ogni  $x \in \mathbb{R}$ . Sia  $\varphi: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}^{\mathbb{R}}$  l'applicazione definita da  $\varphi(a, b) = f_{(a,b)}$  per ogni  $(a, b) \in \mathbb{R} \times \mathbb{R}$ . Si dimostri che  $\varphi$  è un omomorfismo iniettivo del monoide  $(\mathbb{R} \times \mathbb{R}, \star)$  nel monoide  $(\mathbb{R}^{\mathbb{R}}, \circ)$  di tutte le applicazioni di  $\mathbb{R}$  in  $\mathbb{R}$  dotato della composizione di applicazioni.

19.11. Sia  $(\mathbb{R}, \cdot)$  il monoide moltiplicativo dei numeri reali.

- (a) Si dimostri che  $\mathbb{R}_{\geq 0} = \{\alpha \mid \alpha \in \mathbb{R}, \alpha \geq 0\}$  è un sottomonoide di  $(\mathbb{R}, \cdot)$ .  
 (b) Si consideri l'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $\varphi(x) = x^2$  per ogni  $x \in \mathbb{R}$ . Si dimostri che  $\varphi$  è un endomorfismo del monoide  $(\mathbb{R}, \cdot)$ .  
 (c) Sia  $\sim$  l'equivalenza su  $\mathbb{R}$  definita, per ogni  $a, b \in \mathbb{R}$ , da  $a \sim b$  se  $|a| = |b|$ . Si dimostri che l'equivalenza  $\sim$  e l'equivalenza  $\sim_\varphi$  associata a  $\varphi$  coincidono.  
 (d) Si dimostri che i monoide moltiplicativi  $\mathbb{R}/\sim$  e  $\mathbb{R}_{\geq 0}$  sono isomorfi.

19.12. Siano  $A$  un insieme e  $(A^A, \circ)$  il monoide di tutte le applicazioni di  $A$  in  $A$ . Sia  $B \subseteq A$ .

- (a) Si dimostri che  $S = \{f \mid f \in A^A, f(B) \subseteq B\}$  è un sottomonoide di  $A^A$ .  
 (b) Per ogni  $f \in S$  sia  $f|_B$  la restrizione di  $f$  a  $B$ , cioè l'applicazione  $f|_B: B \rightarrow B$  definita da  $f|_B(b) = f(b)$  per ogni  $b \in B$ . Si consideri l'applicazione  $\varphi: S \rightarrow B^B$  definita da  $\varphi(f) = f|_B$  per ogni  $f \in S$ . Si dimostri che  $\varphi$  è un omomorfismo suriettivo di monoidei di  $S$  nel monoide  $(B^B, \circ)$ .  
 (c) Si definisca un'equivalenza  $\sim$  su  $S$  ponendo, per ogni  $f, g \in S$ ,  $f \sim g$  se  $f|_B = g|_B$  per ogni  $b \in B$ . Si dimostri che l'equivalenza  $\sim$  e l'equivalenza  $\sim_\varphi$  associata all'applicazione  $\varphi$  coincidono.  
 (d) Si dimostri che i monoide  $S/\sim$  e  $B^B$  sono isomorfi.

## Capitolo 20. Monoide liberi

Sia  $A$  un insieme fissato. Se  $n \in \mathbb{N}$  chiameremo *parola di lunghezza  $n$  nell'alfabeto  $A$*  una qualunque sequenza  $a_1 a_2 \dots a_n$  di  $n$  elementi di  $A$ . C'è un'unica parola di lunghezza 0, detta la *parola vuota*; la indicheremo con  $w_0$ . Per ogni  $n \in \mathbb{N}$  sia

$$W_n = \{a_1 a_2 \dots a_n \mid a_1, a_2, \dots, a_n \in A\}$$

l'insieme delle parole di lunghezza  $n$ . Allora:

- (1)  $W_0 = \{w_0\}$ .  
 (2) c'è una corrispondenza biunivoca  $\varphi_1: A \rightarrow W_1$  data da  $\varphi_1(a) = a$  per ogni  $a \in A$  ( $\varphi_1$  associa ad ogni  $a \in A$  la parola di un'unica lettera  $a$ ), e  
 (3) per ogni  $n \geq 2$  c'è una corrispondenza biunivoca

$$\varphi_n: \underbrace{A \times A \times \dots \times A}_{n \text{ volte}} \rightarrow W_n$$

data da

$$\varphi_n(a_1, a_2, \dots, a_n) = a_1 a_2 \dots a_n$$

$$\text{per ogni } (a_1, a_2, \dots, a_n) \in \underbrace{A \times A \times \dots \times A}_{n \text{ volte}}.$$

Sia  $W = \bigcup_{n \in \mathbb{N}} W_n$  l'insieme di tutte le parole nell'alfabeto  $A$ . Date due parole  $w = a_1 a_2 \dots a_n$ ,  $w' = b_1 b_2 \dots b_m \in W$  di lunghezza  $n$  ed  $m$  rispettivamente, possiamo formare la parola

$$w \circ w' = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$$

di lunghezza  $n + m$  ottenuta *giustapponendo* le due parole  $w$  e  $w'$ . Ovviamente la *giustapposizione* (o *concatenazione*)  $\circ$  è un'operazione sull'insieme  $W$ , ed

anzi  $(W, \circ)$  risulta essere un monoide avente come identità la parola vuota  $w_0$ . Chiameremo  $(W, \circ)$  il *monoide delle parole nell'alfabeto A* o il *monoide libero su A*.

Dato che  $W_1 \subseteq W$ , possiamo considerare l'applicazione di inclusione  $\varepsilon: W_1 \rightarrow W$  data da  $\varepsilon(w) = w$  per ogni  $w \in W_1$ . Sia  $\varphi: A \rightarrow W$  l'applicazione composta di  $\varphi_1: A \rightarrow W_1$  e di  $\varepsilon: W_1 \rightarrow W$ ; l'applicazione  $\varphi = \varepsilon \circ \varphi_1$  associa ad ogni elemento  $a \in A$  la parola  $a \in W$  avente lunghezza 1. Chiameremo  $\varphi: A \rightarrow W$  l'applicazione canonica di  $A$  in  $W$ .

**TEOREMA 20.1 (PROPRIETÀ UNIVERSALE DEI MONOIDI LIBERI).** *Siano  $A$  un insieme,  $(W, \circ)$  il monoide libero su  $A$ , e  $\varphi: A \rightarrow W$  l'applicazione canonica di  $A$  in  $W$ . Allora per ogni monoide  $M$  e per ogni applicazione  $f: A \rightarrow M$  esiste un unico omomorfismo di monoidi  $\hat{f}: W \rightarrow M$  che rende commutativo il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{f} & M \\ \varphi \searrow & & \nearrow \hat{f} \\ & W & \end{array}$$

cioè tale che  $\hat{f} \circ \varphi = f$ .

*Dimostrazione. Esistenza:* Sia  $f: A \rightarrow M$  un'applicazione dell'insieme  $A$  nel monoide  $M$ . Mostriamo che esiste un omomorfismo di monoidi  $\hat{f}: W \rightarrow M$  tale che  $\hat{f} \circ \varphi = f$ . Poniamo  $\hat{f}(w_0) = 1_M$  e, per ogni parola  $w = a_1 a_2 \dots a_n \in W$  di lunghezza  $n \geq 1$ , poniamo

$$\hat{f}(w) = f(a_1) f(a_2) \dots f(a_n).$$

Verifichiamo che  $\hat{f}: W \rightarrow M$  è un omomorfismo di monoidi. Siano  $w, w' \in W$ . Se  $w$  ha lunghezza zero allora

$$\hat{f}(w \circ w') = \hat{f}(w') = 1_M \cdot \hat{f}(w') = \hat{f}(w) \hat{f}(w');$$

similmente se  $w'$  ha lunghezza zero; se invece le parole  $w$  e  $w'$  hanno entrambe lunghezza maggiore di zero, diciamo  $w = a_1 a_2 \dots a_n$  e  $w' = b_1 b_2 \dots b_m$ , allora  $w \circ w' = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$  e

$$\hat{f}(w \circ w') = f(a_1) f(a_2) \dots f(a_n) f(b_1) f(b_2) \dots f(b_m) = \hat{f}(w) \hat{f}(w').$$

Quindi  $\hat{f}$  è un omomorfismo di monoidi, e per ogni  $a \in A$  si ha  $(\hat{f} \circ \varphi)(a) = \hat{f}(a) = f(a)$ , cioè  $\hat{f} \circ \varphi = f$ .

*Unicità.* Mostriamo che c'è un *unico* omomorfismo  $\hat{f}: W \rightarrow M$  tale che  $\hat{f} \circ \varphi = f$ . Sia  $f': W \rightarrow M$  un altro omomorfismo di monoidi tale che  $f' \circ \varphi = f$ . Allora  $f'(w_0) = 1_M = \hat{f}(w_0)$ , e per ogni parola  $w = a_1 a_2 \dots a_n$  di lunghezza  $n \geq 1$  si ha  $w = \varphi(a_1) \circ \varphi(a_2) \circ \dots \circ \varphi(a_n)$ , e quindi

$$f'(w) = f'(\varphi(a_1) \circ \varphi(a_2) \circ \dots \circ \varphi(a_n)) =$$

$$\begin{aligned} &= f'(\varphi(a_1)) f'(\varphi(a_2)) \dots f'(\varphi(a_n)) = \\ &= (f' \circ \varphi)(a_1) (f' \circ \varphi)(a_2) \dots (f' \circ \varphi)(a_n) = \\ &= f(a_1) f(a_2) \dots f(a_n) = \hat{f}(w). \end{aligned}$$

Quindi  $f' = \hat{f}$ . Questo prova che  $\hat{f}$  è l'unico omomorfismo con le proprietà richieste.  $\square$

Consideriamo l'applicazione  $\lambda: W \rightarrow \mathbb{N}$  che associa ad ogni parola nell'alfabeto  $A$  di lunghezza  $n$  il numero naturale  $n$ . (Quindi ogni parola  $w \in W$  ha lunghezza  $\lambda(w)$ .) L'applicazione  $\lambda$  è un omomorfismo del monoide  $(W, \circ)$  nel monoide  $(\mathbb{N}, +)$ , in quanto  $\lambda(w_0) = 0$  e una parola ottenuta giustapponendo due parole di lunghezza  $n$  ed  $m$  rispettivamente ha lunghezza  $n + m$ , cioè  $\lambda(w \circ w') = \lambda(w) + \lambda(w')$  per ogni  $w, w' \in W$ .

**LEMMA 20.2.** *Se l'insieme  $A = \{a\}$  ha un unico elemento, l'applicazione  $\lambda: W \rightarrow \mathbb{N}$  che associa ad ogni parola  $w \in W$  nell'alfabeto  $A$  la sua lunghezza è un isomorfismo del monoide  $(W, \circ)$  nel monoide  $(\mathbb{N}, +)$ .*

*Dimostrazione.* Abbiamo già visto che  $\lambda: W \rightarrow \mathbb{N}$  è un omomorfismo. Dato che  $w_0$  è l'unica parola di lunghezza 0, e che per ogni  $n \in \mathbb{N}$ ,  $n \geq 1$ ,  $\underbrace{aa \dots a}_n$  è l'unica parola di lunghezza  $n$  nell'alfabeto  $A$ , si conclude che  $\lambda$  è sia iniettiva che suriettiva, e dunque è una biiezione.  $\square$

Quindi se  $|A| = 1$  il monoide  $(W, \circ)$ , essendo isomorfo a  $(\mathbb{N}, +)$ , è un monoide commutativo. Se invece  $|A| > 1$  il monoide libero su  $A$  non è commutativo.

Un *alfabeto valutato* è una coppia ordinata  $(A, \tau)$ , dove  $A$  è un insieme finito e  $\tau: A \rightarrow \mathbb{N}$  è un'applicazione. Per ogni  $a \in A$  il numero naturale  $\tau(a)$  si dice la *valutazione* di  $a$ .

**ESEMPIO 1.** Sia  $A = \mathbb{Z} \cup \{+, -, \cdot\}$  l'insieme dei numeri interi a cui sono stati aggiunti i tre simboli ulteriori  $+$ ,  $-$  e  $\cdot$ . Poniamo  $\tau(z) = 0$  per ogni  $z \in \mathbb{Z}$ ,  $\tau(+)=2$ ,  $\tau(-)=1$ ,  $\tau(\cdot)=2$ . Allora  $(A, \tau)$  è un alfabeto valutato. Come si può intravedere in questo esempio, nell'alfabeto valutato  $(A, \tau)$  converrà pensare  $\tau(a)$  come il "numero di simboli a cui si può applicare  $a$ ".  $\square$

Se  $(A, \tau)$  è un alfabeto valutato e  $n \in \mathbb{N}$ , poniamo  $A_n = \tau^{-1}(n)$ . Gli elementi di  $A_0$  si dicono *costanti*.

Siano ora dati un alfabeto valutato  $(A, \tau)$  ed un insieme  $X$  (i cui elementi saranno detti *variabili*). Le *parole generate da  $(A, \tau)$  e  $X$*  sono definite nel modo seguente:

- gli elementi di  $A \cup X$  sono parole;
- se  $a \in A_n$  e  $w_1, w_2, \dots, w_n$  sono parole, anche  $aw_1 w_2 \dots w_n$  è una parola;

- (c) sono parole solo le espressioni che si ottengono applicando un numero finito di volte (a) e (b).

ESEMPIO 2. Sia  $(A, \tau)$  l'alfabeto valutato dell'esempio 1 e sia  $X = \{x, y, z\}$ . Sono parole  $x, +xy, 2, -+xy, -2-+xy$ . Le parole generate da  $(A, \tau)$  e  $X$  sono quindi tutte le espressioni polinomiali in  $x, y, z$  a coefficienti in  $\mathbb{Z}$  in notazione polacca.  $\square$

Il concetto di valutazione in un alfabeto valutato è strettamente collegato a quello di arietà di un'operazione. Ricordiamo che se  $X$  è un insieme ed  $n \geq 1$  è un intero, un'operazione  $n$ -aria su  $X$  è un'applicazione  $\underbrace{X \times X \times \dots \times X}_{n \text{ volte}} \rightarrow X$ . Ecco

quindi che quelle che finora abbiamo chiamato semplicemente operazioni si chiamano in questa terminologia più precisa operazioni 2-arie (o più frequentemente, come abbiamo già detto, operazioni binarie). Un'operazione 1-aria (operazione unaria) su  $X$  non è altro che un'applicazione  $X \rightarrow X$ .

Si noti che abbiamo volutamente introdotto una differenza tra quanto visto nella capitolo 14 (capitolo in cui spiegando la notazione polacca denotavamo con  $-$  la sottrazione che è un'operazione binaria) e gli esempi 1 e 2 di questo capitolo (in cui con  $-$  abbiamo denotato il passaggio all'opposto che è un'operazione unaria). Questo diverso uso del simbolo  $-$ , per denotare un'operazione binaria prima, e per denotare un'operazione unaria poi, mostra che a volte, nell'uso corrente, si possono denotare mediante lo stesso simbolo operazioni distinte con arietà distinte.

### Esercizi svolti

20.1. Si dimostri che ogni monoide è isomorfo ad un quoziente di un monoide libero. Più precisamente si dimostri che dato un qualunque monoide  $M$  esiste un insieme  $A$  e una relazione di equivalenza  $\sim$  sul monoide libero  $W$  su  $A$ , compatibile con l'operazione  $\circ$  di  $W$ , tale che  $M$  sia isomorfo al monoide  $W/\sim$ .

*Soluzione.* Dato un monoide  $M$ , si fissi come insieme  $A$  lo stesso insieme  $M$ , e sia  $W$  il monoide libero su  $A = M$ . Sia  $\varphi: M \rightarrow W$  l'applicazione canonica di  $M$  in  $W$ , e si applichi la proprietà universale dei monoidi liberi (teorema 20.1) all'applicazione identica  $i: M \rightarrow M$ . Si ottiene così che esiste un omomorfismo di monoidi  $\hat{i}: W \rightarrow M$  che rende commutativo il diagramma

$$\begin{array}{ccc} M & \xrightarrow{i} & M \\ \varphi \searrow & & \nearrow \hat{i} \\ & W & \end{array}$$

cioè tale che  $\hat{i} \circ \varphi = i$ . Dato che  $\hat{i} \circ \varphi = i$  è suriettiva, per la parte (b) dell'esercizio 3.2 anche l'omomorfismo  $\hat{i}$  è suriettivo. Si applichi ora il teorema fondamentale di omomorfismo per i monoidi all'omomorfismo suriettivo  $\hat{i}: W \rightarrow M$ . Denotata con  $\sim$  l'equivalenza su  $W$  associata a  $\hat{i}$ , equivalenza che sappiamo essere compatibile con l'operazione di  $W$  perché  $\hat{i}$  è un omomorfismo di monoidi, se ne ricava che esiste un isomorfismo  $\bar{i}: W/\sim \rightarrow M$ . Pertanto i monoidi  $W/\sim$  ed  $M$  sono isomorfi.  $\square$

! 20.2. Sia  $A$  un insieme non vuoto,  $\sim$  una relazione di equivalenza su  $A$ ,  $\pi: A \rightarrow A/\sim$  la proiezione canonica,  $W$  il monoide libero su  $A$ , e  $\varphi: A \rightarrow W$  l'applicazione canonica di  $A$  in  $W$ . Sull'insieme  $W$  si definisca una relazione  $\equiv$  ponendo, per ogni  $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in W$ ,

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_m \text{ se } n = m, a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n.$$

- (a) Si provi che la relazione  $\equiv$  è un'equivalenza sull'insieme  $W$ .  
 (b) Si provi che l'equivalenza  $\equiv$  e l'operazione  $\circ$  di  $W$  sono tra loro compatibili.  
 (c) Siano  $(\bar{W}, \circ)$  il monoide libero sull'insieme quoziente  $A/\sim$  e  $\bar{\varphi}: A/\sim \rightarrow \bar{W}$  l'applicazione canonica di  $A/\sim$  in  $\bar{W}$ . Si consideri l'applicazione composta  $f = \bar{\varphi} \circ \pi: A \rightarrow \bar{W}$ . Tale applicazione composta associa ad ogni lettera  $a \in A$  la parola di un'unica lettera  $[a]_\sim$  nell'alfabeto  $A/\sim$ . Per la proprietà universale dei monoidi liberi in corrispondenza all'applicazione  $f = \bar{\varphi} \circ \pi: A \rightarrow \bar{W}$  esiste un unico omomorfismo di monoidi  $\hat{f}: W \rightarrow \bar{W}$  che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\sim \\ \varphi \downarrow & & \downarrow \bar{\varphi} \\ W & \xrightarrow{\hat{f}} & \bar{W} \end{array}$$

cioè tale che  $(\hat{f}) \circ \varphi = \bar{\varphi} \circ \pi$ . Si dimostri che l'omomorfismo  $\hat{f}$  è suriettivo.

- (d) Si dimostri che l'equivalenza  $\equiv$  e l'equivalenza  $\sim_{\hat{f}}$  associata all'applicazione  $\hat{f}$  coincidono.  
 (e) Si dimostri che i monoidi  $W/\equiv$  e  $\bar{W}$  sono isomorfi.

*Soluzione.* (a) *Riflessività di  $\equiv$ .* Sia  $a_1 a_2 \dots a_n \in W$ . Per la riflessività di  $\sim$  e di  $\sim$  si ha che  $n = n$  e  $a_1 \sim a_1, a_2 \sim a_2, \dots, a_n \sim a_n$ . Quindi

$$a_1 a_2 \dots a_n \equiv a_1 a_2 \dots a_n.$$

*Simmetria di  $\equiv$ .* Siano  $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in W$  tali che

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_m.$$

Allora  $n = m$  e  $a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n$ . Dato che  $\sim$  è simmetrico, ne segue che  $m = n$  e  $b_1 \sim a_1, b_2 \sim a_2, \dots, b_n \sim a_n$ . Quindi  $b_1 b_2 \dots b_m \equiv a_1 a_2 \dots a_n$ .

Transitività di  $\equiv$ . Siano  $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m, c_1 c_2 \dots c_p \in W$  tali che

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_m \quad \text{e} \quad b_1 b_2 \dots b_m \equiv c_1 c_2 \dots c_p.$$

Allora  $n = m, m = p, a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n, b_1 \sim c_1, b_2 \sim c_2, \dots, b_m \sim c_m$ . Dalla transitività di  $\sim$  si deduce che  $n = m = p$  e che  $a_1 \sim c_1, a_2 \sim c_2, \dots, a_n \sim c_n$ . Quindi  $a_1 a_2 \dots a_n \equiv c_1 c_2 \dots c_p$ .

(b) Siano  $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m, c_1 c_2 \dots c_p, d_1 d_2 \dots d_q \in W$  tali che  $a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_m$  e  $c_1 c_2 \dots c_p \equiv d_1 d_2 \dots d_q$ . Allora  $n = m, p = q, a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n, c_1 \sim d_1, c_2 \sim d_2, \dots, c_p \sim d_p$ . Ne segue che  $n + p = m + q$  e che  $a_1 a_2 \dots a_n c_1 c_2 \dots c_p \equiv b_1 b_2 \dots b_m d_1 d_2 \dots d_q$ .

(c) Vediamo innanzitutto come è definito l'omomorfismo di monoidi  $\hat{f}: W \rightarrow \bar{W}$ . Se  $a \in W$  è una parola di lunghezza 1 si ha  $\hat{f}(a) = \hat{f}(\varphi(a)) = (\hat{f} \circ \varphi)(a) = f(a) = (\varphi \circ \pi)(a) = \varphi(\pi(a)) = \varphi([a]_{\sim}) = [a]_{\sim}$ . Quindi  $\hat{f}$  fa corrispondere alla parola  $a \in W$  di lunghezza 1 la parola  $[a]_{\sim} \in \bar{W}$  di lunghezza 1. Più in generale data una parola di lunghezza arbitraria  $a_1 a_2 \dots a_n \in W$ , applicando ad essa l'omomorfismo di monoidi  $\hat{f}$  si ottiene  $\hat{f}(a_1 a_2 \dots a_n) = \hat{f}(a_1 \circ a_2 \circ \dots \circ a_n) = \hat{f}(a_1) \circ \hat{f}(a_2) \circ \dots \circ \hat{f}(a_n) = [a_1]_{\sim} \circ [a_2]_{\sim} \circ \dots \circ [a_n]_{\sim} = [a_1]_{\sim} [a_2]_{\sim} \dots [a_n]_{\sim}$ . Quindi  $\hat{f}: W \rightarrow \bar{W}$  fa corrispondere alla parola  $a_1 a_2 \dots a_n \in W$  la parola  $[a_1]_{\sim} [a_2]_{\sim} \dots [a_n]_{\sim} \in \bar{W}$ . È ora evidente che l'applicazione  $\hat{f}$  è suriettiva.

(d) Siano  $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in W$ . Si ha

$$a_1 a_2 \dots a_n \sim_{\hat{f}} b_1 b_2 \dots b_m$$

se e solo se  $\hat{f}(a_1 a_2 \dots a_n) = \hat{f}(b_1 b_2 \dots b_m)$ , cioè se e solo se

$$[a_1]_{\sim} [a_2]_{\sim} \dots [a_n]_{\sim} = [b_1]_{\sim} [b_2]_{\sim} \dots [b_m]_{\sim}.$$

Questo accade se e solo se  $n = m, [a_1]_{\sim} = [b_1]_{\sim}, [a_2]_{\sim} = [b_2]_{\sim}, \dots, [a_n]_{\sim} = [b_n]_{\sim}$ . Quindi  $a_1 a_2 \dots a_n \sim_{\hat{f}} b_1 b_2 \dots b_m$  se e solo se  $n = m, a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n$ . Pertanto le due equivalenze  $\equiv$  e  $\sim_{\hat{f}}$  coincidono.

(e) Applicando il teorema fondamentale di omomorfismo per i monoidi all'omomorfismo suriettivo  $\hat{f}: W \rightarrow \bar{W}$ , si vede che esiste un isomorfismo di monoidi  $\bar{f}: W/\sim_{\hat{f}} \rightarrow \bar{W}$ . Si è visto in (d) che le due equivalenze  $\equiv$  e  $\sim_{\hat{f}}$  coincidono. Pertanto i monoidi  $W/\equiv$  e  $\bar{W}$  sono isomorfi.  $\square$

20.3. Si dimostri il seguente corollario al teorema 20.1: Siano  $A, B$  insiemi,  $(W_A, \circ), (W_B, \circ)$  i monoidi liberi su  $A$  e  $B$  rispettivamente, e  $\varphi_A: A \rightarrow W_A, \varphi_B: B \rightarrow W_B$  le applicazioni canoniche. Allora per ogni applicazione  $f: A \rightarrow B$

esiste un unico omomorfismo di monoidi  $\bar{f}: W_A \rightarrow W_B$  che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \varphi_A \downarrow & & \downarrow \varphi_B \\ W_A & \xrightarrow{\bar{f}} & W_B \end{array}$$

Soluzione. Si applichi la proprietà universale dei monoidi liberi (teorema 20.1) al monoido  $W_B$  e all'applicazione  $\varphi_B \circ f: A \rightarrow W_B$ . Se ne ricava che esiste un unico omomorfismo di monoidi  $\bar{f}: W_A \rightarrow W_B$  tale che  $\bar{f} \circ \varphi_A = \varphi_B \circ f$ .  $\square$

### Altri esercizi

20.4. Se  $A$  è l'insieme vuoto, cos'è il monoido libero su  $A$ ? Quanti elementi ha?

20.5. Siano  $M$  un monoido,  $A$  un insieme,  $(W, \circ)$  il monoido libero su  $A$  e  $\varphi: A \rightarrow W$  l'applicazione canonica di  $A$  in  $W$ . Si denoti con  $\text{Hom}(W, M)$  l'insieme degli omomorfismi di monoidi di  $W$  in  $M$  e con  $M^A$  l'insieme delle applicazioni di  $A$  in  $M$ . Si dimostri che l'applicazione  $\Phi: \text{Hom}(W, M) \rightarrow M^A$  definita da  $\Phi(h) = h \circ \varphi$  per ogni  $h \in \text{Hom}(W, M)$  è una biiezione.

20.6. Siano  $M$  un monoido,  $X$  un suo sottoinsieme, ed  $\varepsilon: X \rightarrow M$  l'applicazione di inclusione definita da  $\varepsilon(x) = x$  per ogni  $x \in X$  (vedi esercizio 2.19). Si denoti con  $W$  il monoido libero sull'insieme  $X$  e con  $\varphi: X \rightarrow W$  l'applicazione canonica. Per la proprietà universale dei monoidi liberi, in corrispondenza all'applicazione di inclusione  $\varepsilon: X \rightarrow M$  esiste un unico omomorfismo di monoidi  $\bar{\varepsilon}: W \rightarrow M$  tale che  $\bar{\varepsilon} \circ \varphi = \varepsilon$ . Si dimostri che l'immagine  $\bar{\varepsilon}(W)$  dell'omomorfismo  $\bar{\varepsilon}$  coincide con il sottomonoido  $[X]$  di  $M$  generato da  $X$ .

20.7. Sia  $A$  un insieme fissato e sia  $W' = \bigcup_{n \geq 1} W_n$  l'insieme di tutte le parole di lunghezza  $\geq 1$  nell'alfabeto  $A$ . Allora  $W'$  è un semigruppato rispetto alla concatenazione di parole, detto il *semigruppato libero* su  $A$ . Anche in questo caso si ha l'applicazione canonica  $\varphi: A \rightarrow W'$  che associa ad ogni elemento  $a \in A$  la parola  $a \in W'$  di lunghezza 1.

Si dimostri la seguente proprietà universale dei semigruppati liberi:

Siano  $A$  un insieme,  $(W', \circ)$  il semigruppato libero su  $A$ , e  $\varphi: A \rightarrow W'$  l'applicazione canonica di  $A$  in  $W'$ . Allora per ogni semigruppato  $S$  e ogni applicazione  $f: A \rightarrow S$  esiste un unico omomorfismo di semigruppati  $\bar{f}: W' \rightarrow S$  che rende

commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{f} & S \\ \varphi \searrow & & \nearrow \hat{f} \\ & W' & \end{array}$$

cioè tale che  $\hat{f} \circ \varphi = f$ .

**20.8.** Si dimostri che se  $|A| = 1$ , il semigruppso libero  $W'$  su  $A$  (vedi esercizio 20.7) è isomorfo al semigruppso  $(N^*, +)$ .

## Capitolo 21. Gruppi

Se  $(M, \cdot)$  è un monoide con identità  $1_M$  e  $a$  è un elemento di  $M$ ,  $a$  si dice *invertibile a sinistra* se esiste  $b \in M$  tale che  $ba = 1$ . L'elemento  $a$  si dice invece *invertibile a destra* se esiste  $c \in M$  tale che  $ac = 1$ , e si dice *invertibile* (o un'unità) se è sia invertibile a sinistra che invertibile a destra.

**ESEMPIO 1.** Se  $A$  è un insieme e  $(A^A, \circ)$  è il monoide delle applicazioni di  $A$  in  $A$ , allora l'identità del monoide è l'applicazione identica  $\iota_A : A \rightarrow A$ . Un elemento  $\varphi$  di  $A^A$  è invertibile a sinistra se e solo se esiste  $\psi \in A^A$  tale che  $\psi \circ \varphi = \iota_A$ , ossia, per l'esercizio 3.5, se e solo se l'applicazione  $\varphi$  è iniettiva. Analogamente, per l'esercizio 3.6, un elemento  $\varphi$  di  $A^A$  è invertibile a destra se e solo se è un'applicazione suriettiva. Se ne conclude che gli elementi invertibili del monoide  $(A^A, \circ)$  sono esattamente le biezioni  $A \rightarrow A$ .  $\square$

**LEMMA 21.1.** Se  $M$  è un monoide,  $a \in M$  è un elemento invertibile e  $b, c \in M$  sono tali che  $ba = ac = 1_M$ , allora  $b = c$ .

Per il lemma 21.1 un elemento invertibile  $a \in M$  ha un'unico *inverso* sia a sinistra che a destra; denoteremo tale inverso con  $a^{-1}$ .

**LEMMA 21.2.** Sia  $M$  un monoide e siano  $a, b$  elementi invertibili di  $M$ . Allora  $ab$  e  $a^{-1}$  sono elementi invertibili; in particolare  $(ab)^{-1} = b^{-1}a^{-1}$  e  $(a^{-1})^{-1} = a$ .

Se nel monoide  $M$  l'operazione è denotata con la notazione additiva, l'inverso di un elemento invertibile  $a$  si preferisce chiamarlo l'*opposto* di  $a$ , e denotarlo con  $-a$ .

Un *gruppo* è un monoide in cui ogni elemento è invertibile. Quindi un gruppo  $(G, \cdot)$  è un insieme  $G$  dotato di un'operazione  $\cdot$  associativa, con un'identità, e in cui ogni elemento è invertibile.

Un gruppo  $(G, \cdot)$  tale che  $ab = ba$  per ogni  $a, b \in G$  si dice un *gruppo abeliano* (o *commutativo*). Generalmente nei gruppi l'operazione è indicata come addizione solo nel caso di gruppi abeliani; la notazione moltiplicativa è invece usata sia per i gruppi abeliani che per quelli non abeliani. La cardinalità di un gruppo  $G$ , cioè  $|G|$ , si chiama di solito l'*ordine* di  $G$ .

**ESEMPIO 2.** I monoidi  $(N, +)$ ,  $(N, \cdot)$ ,  $(Z, \cdot)$ ,  $(Q, \cdot)$ ,  $(R, \cdot)$ ,  $(C, \cdot)$  non sono gruppi; infatti in  $(N, +)$  l'unico elemento invertibile è lo 0, in  $(N, \cdot)$  l'unico elemento invertibile è 1, in  $(Z, \cdot)$  gli unici elementi invertibili sono 1 e -1, in  $(Q, \cdot)$ ,  $(R, \cdot)$ ,  $(C, \cdot)$  tutti gli elementi sono invertibili eccetto lo 0.  $\square$

**ESEMPIO 3.** I monoidi  $(Z, +)$ ,  $(Q, +)$ ,  $(R, +)$ ,  $(C, +)$  sono gruppi. Se  $Q^* = Q \setminus \{0\}$ ,  $R^* = R \setminus \{0\}$ ,  $C^* = C \setminus \{0\}$ , allora i monoidi  $(Q^*, \cdot)$ ,  $(R^*, \cdot)$ ,  $(C^*, \cdot)$  sono gruppi.  $\square$

**ESEMPIO 4.** Se  $(M, \cdot)$  è un monoide e  $U(M)$  è l'insieme degli elementi invertibili di  $M$ , mostriamo che  $U(M)$  è un sotto-monoide di  $M$  e che il monoide  $(U(M), \cdot)$  è un gruppo.

Si noti intanto che il prodotto di due elementi invertibili è invertibile per il lemma 21.2. Quindi  $U(M)$  è un sottoinsieme moltiplicativamente chiuso di  $M$ . Inoltre  $1_M \in U(M)$  perché  $1_M \cdot 1_M = 1_M$ . Questo dimostra che  $U(M)$  è un sotto-monoide di  $M$ . Per mostrare che il monoide  $(U(M), \cdot)$  è un gruppo resta da dimostrare che ogni elemento di  $U(M)$  è invertibile in  $U(M)$ , cioè che per ogni  $a \in U(M)$  esiste  $b \in U(M)$  tale che  $ab = ba = 1_M$ . Ma  $a \in U(M)$  è invertibile in  $M$ , e se  $a^{-1}$  è il suo inverso in  $M$ , allora per il lemma 21.2 anche  $a^{-1}$  è invertibile in  $M$ , ossia  $a^{-1} \in U(M)$ . Dato che  $aa^{-1} = a^{-1}a = 1_M$ , se ne conclude che ogni elemento di  $U(M)$  è invertibile in  $U(M)$ .  $\square$

**ESEMPIO 5.** Applicando quanto abbiamo dimostrato nell'esempio 4 (cioè che se  $M$  è un monoide  $U(M)$  risulta essere un gruppo) ai monoidi visti nell'esempio 2 troviamo che i gruppi degli elementi invertibili dei monoidi  $(N, +)$ ,  $(N, \cdot)$ ,  $(Z, \cdot)$ ,  $(Q, \cdot)$ ,  $(R, \cdot)$ ,  $(C, \cdot)$  sono rispettivamente i gruppi  $(\{0\}, +)$ ,  $(\{1\}, \cdot)$ ,  $(\{1, -1\}, \cdot)$ ,  $(Q^*, \cdot)$ ,  $(R^*, \cdot)$ ,  $(C^*, \cdot)$ .  $\square$

Se  $(G, \cdot)$  è un gruppo e  $g \in G$ , la *potenza  $n$ -esima* di  $g$ , dove  $n \in Z$ , si definisce ponendo

$$g^n = \begin{cases} 1_G & \text{se } n = 0, \\ (g^{n-1})g & \text{se } n > 0, \\ (g^{-1})^{-n} & \text{se } n < 0. \end{cases}$$



PROPOSIZIONE 21.3. Siano  $(G, \cdot)$  un gruppo,  $g \in G$  ed  $n, m \in \mathbb{Z}$ . Allora  $g^n g^m = g^{n+m}$  e  $(g^n)^m = g^{nm}$ . Inoltre se  $g, h \in G$ ,  $gh = hg$  ed  $n \in \mathbb{Z}$ , allora  $(gh)^n = g^n h^n$ .

Sia  $(G, \cdot)$  un gruppo e sia  $H$  un sottoinsieme chiuso di  $G$ . Se  $(H, \cdot)$  è un gruppo, diremo che  $H$  è un sottogruppo di  $G$ , e scriveremo  $H \leq G$ . Quindi se  $G$  è un gruppo e  $H \subseteq G$ ,  $H$  è un sottogruppo di  $G$  se e solo se

- (1) chiusura:  $ab \in H$  per ogni  $a, b \in H$ ;
- (2) identità:  $1_G \in H$ ;
- (3) inversa:  $a^{-1} \in H$  per ogni  $a \in H$ .

Tra i sottogruppi di un qualunque gruppo  $(G, \cdot)$  vi sono sempre lo stesso gruppo  $G$  (detto il sottogruppo improprio di  $G$ ) e  $\{1_G\}$  (detto il sottogruppo identico o banale). Chiaramente ogni sottogruppo di un sottogruppo abeliano è abeliano.

ESEMPIO 6. Per ogni numero intero  $n \geq 0$  sia  $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ . Dimostriamo che se  $H$  è un sottoinsieme di  $\mathbb{Z}$ ,  $H$  è un sottogruppo di  $(\mathbb{Z}, +)$  se e solo se esiste  $n \in \mathbb{N}$  tale che  $H = n\mathbb{Z}$ . In altre parole, i sottogruppi di  $(\mathbb{Z}, +)$  sono tutti e soli del tipo  $n\mathbb{Z}$ .

È facile dimostrare che se  $H = n\mathbb{Z}$  per qualche  $n \in \mathbb{N}$  allora  $H$  è un sottogruppo di  $\mathbb{Z}$ . Infatti si ha

- (1) (chiusura): se  $a, b \in H$ , allora  $a = nz$  e  $b = nz'$  per opportuni  $z, z' \in \mathbb{Z}$ , da cui  $a + b = nz + nz' = n(z + z') \in n\mathbb{Z} = H$ ;
- (2) (identità):  $0_{\mathbb{Z}} = 0 = 0 \cdot n \in n\mathbb{Z} = H$ ;
- (3) (inverso): se  $a \in H$ , allora  $a = nz$  per qualche  $z \in \mathbb{Z}$ , da cui  $-a = n(-z) \in n\mathbb{Z} = H$ .

Viceversa sia  $H$  un sottogruppo del gruppo additivo  $(\mathbb{Z}, +)$ . Allora  $H \supseteq \{0\}$ . Se  $H = \{0\}$ , allora  $H = 0\mathbb{Z}$ . Supponiamo quindi che  $H \supset \{0\}$ . Si osservi che essendo  $H$  un sottogruppo, da  $a \in H$  segue che anche  $-a \in H$ . Quindi  $H$  deve contenere dei numeri interi positivi. Sia  $n$  il più piccolo intero positivo appartenente ad  $H$ . Dimostriamo che  $H = n\mathbb{Z}$  verificando la doppia inclusione.

Se  $x \in n\mathbb{Z}$ , allora  $x = nz$  per qualche  $z \in \mathbb{Z}$ . Se  $z = 0$  allora  $x = 0 \in H$  perché  $H$  è un sottogruppo di  $\mathbb{Z}$ . Se  $z > 0$  allora  $x = \underbrace{n + n + \dots + n}_{z \text{ volte}} \in H$  perché

$n \in H$  e  $H$  è chiuso per l'addizione. Se infine  $z < 0$  allora  $-n \in H$  perché  $H$  è un sottogruppo, da cui  $x = nz = \underbrace{(-n) + (-n) + \dots + (-n)}_{-z \text{ volte}} \in H$ . Abbiamo così dimostrato che  $H \supseteq n\mathbb{Z}$ .

Per l'inclusione opposta supponiamo che  $x \in H$ , e dividiamo  $x$  per  $n$ . Si trovano allora degli interi  $q$  ed  $r$  tali che  $x = nq + r$  e  $0 \leq r < n$ . Ne segue che  $r = x - nq \in H$  perché  $x$  e  $nq$  appartengono entrambi ad  $H$ . Per la minimalità

di  $n$  non può essere  $r > 0$ , ma deve essere  $r = 0$ . Se ne conclude che  $x = nq \in n\mathbb{Z}$ .  $\square$

LEMMA 21.4. Sia  $G$  un gruppo e sia  $H$  un suo sottoinsieme. Allora  $H$  è sottogruppo di  $G$  se e solo se  $H \neq \emptyset$  e  $ab^{-1} \in H$  per ogni  $a, b \in H$ .

ESEMPIO 7. Abbiamo già visto nell'esempio 3 che  $C^* = \mathbb{C} \setminus \{0\}$  è un gruppo rispetto alla moltiplicazione. Consideriamo il sottoinsieme  $T$  di  $C^*$  costituito dai numeri complessi di modulo 1:

$$T = \{z \mid z \in C^*, |z| = 1\}.$$

Mostriamo che  $T$  è un sottogruppo di  $(C^*, \cdot)$  facendo uso del lemma 21.4. Osserviamo intanto che  $T \neq \emptyset$  perché ad esempio  $1 \in T$ . Poi se  $z, z' \in T$  allora  $zz'^{-1} \in C$  e  $|zz'^{-1}| = |z||z'|^{-1} = 1/1 = 1$ , e quindi  $zz'^{-1} \in T$ . Pertanto  $T$  è sottogruppo di  $C^*$ .  $\square$

ESEMPIO 8. Sia  $n \geq 1$  un numero naturale fissato. Osserviamo che se  $z \in C$  è una radice  $n$ -esima dell'unità allora  $z \neq 0$  (perché  $0^n = 0 \neq 1$ ). Quindi se

$$C_n = \{z \mid z \in C, z^n = 1\}$$

è l'insieme delle radici  $n$ -esime dell'unità, allora  $C_n \subseteq C^*$ . Mostriamo che  $C_n$  è un sottogruppo di  $(C^*, \cdot)$ . Intanto  $C_n \neq \emptyset$ , anzi abbiamo visto nel capitolo 5 che  $|C_n| = n$ . Poi se  $z, z' \in C_n$ , allora  $zz'^{-1} \in C$  e si ha  $(zz'^{-1})^n = z^n(z'^n)^{-1} = 1 \cdot 1^{-1} = 1$ . Quindi  $zz'^{-1} \in C_n$ . Pertanto per il lemma 21.4  $C_n$  è un sottogruppo di  $(C^*, \cdot)$ . Si noti che l'ordine del gruppo  $C_n$ , detto il gruppo delle radici  $n$ -esime dell'unità, è proprio  $n$ .  $\square$

Se  $G$  e  $H$  sono gruppi, un omomorfismo di gruppi  $\varphi: G \rightarrow H$  è un'applicazione tale che  $\varphi(ab) = \varphi(a)\varphi(b)$  per ogni  $a, b \in G$ .

LEMMA 21.5. Sia  $\varphi: G \rightarrow H$  un omomorfismo di gruppi. Allora:

- (a)  $\varphi(1_G) = 1_H$ ;
- (b)  $\varphi(g^{-1}) = (\varphi(g))^{-1}$  per ogni  $g \in G$ ;
- (c)  $\varphi(g^z) = (\varphi(g))^z$  per ogni  $g \in G$  e ogni  $z \in \mathbb{Z}$ .

Dimostrazione. (a) Si ha  $1_G = 1_G \cdot 1_G$ , e quindi  $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G)$  perché  $\varphi$  è un omomorfismo. Moltiplicando questa uguaglianza a destra per l'inverso  $(\varphi(1_G))^{-1}$  dell'elemento  $\varphi(1_G) \in H$  si ha  $\varphi(1_G)(\varphi(1_G))^{-1} = \varphi(1_G)\varphi(1_G)(\varphi(1_G))^{-1}$ , cioè  $1_H = \varphi(1_G) \cdot 1_H = \varphi(1_G)$ .

(b) Per dimostrare che  $\varphi(g^{-1}) = (\varphi(g))^{-1}$ , cioè che  $\varphi(g^{-1})$  è l'inverso di  $\varphi(g)$  in  $H$ , si deve far vedere che moltiplicando a sinistra e a destra  $\varphi(g)$  per  $\varphi(g^{-1})$  si ottiene  $1_H$ . Questo è molto facile, in quanto

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H$$

$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1_G) = 1_H.$$

(c) Dimostriamo che  $\varphi(g^z) = (\varphi(g))^z$  per ogni  $g \in G$  e per ogni  $z \in \mathbb{Z}$ ,  $z \geq 0$ , per induzione su  $z$ . Se  $z = 0$ , allora  $\varphi(g^0) = \varphi(1_G) = 1_H$  e  $(\varphi(g))^0 = 1_H$ . Quindi il caso  $z = 0$  è verificato. Se per l'ipotesi induttiva  $\varphi(g^{z-1}) = (\varphi(g))^{z-1}$ , allora  $\varphi(g^z) = \varphi(g^{z-1}g) = \varphi(g^{z-1})\varphi(g) = (\varphi(g))^{z-1}\varphi(g) = (\varphi(g))^z$ . Questo dimostra che la (c) è vera per ogni  $z \geq 0$  e per ogni  $g \in G$ .

Se poi  $z < 0$ , allora  $-z > 0$  e quindi  $\varphi((g^{-1})^{-z}) = (\varphi(g^{-1}))^{-z}$  per quanto dimostrato nel paragrafo precedente. Pertanto

$$\begin{aligned}\varphi(g^z) &= \varphi((g^{-1})^{-z}) = (\varphi(g^{-1}))^{-z} = \\ &= ((\varphi(g))^{-1})^{-z} = (\varphi(g))^z. \quad \square\end{aligned}$$

Un omomorfismo di gruppi biiettivo si dice un *isomorfismo*, un omomorfismo  $G \rightarrow G$  si dice un *endomorfismo* di  $G$ , e un endomorfismo biiettivo di  $G$ , cioè un isomorfismo  $G \rightarrow G$ , si dice un *automorfismo* di  $G$ . Due gruppi  $G$  e  $H$  si dicono *isomorfi* se esiste un isomorfismo di  $G$  in  $H$ ; scriveremo in tal caso  $G \cong H$ .

### Esercizi svolti

**21.1.** Sull'insieme  $\mathbb{R}^* \times \mathbb{R} = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{R}, \alpha \neq 0\}$  si definisca un'operazione ponendo  $(\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \alpha\beta' + \frac{\beta}{\alpha'})$  per ogni  $(\alpha, \beta), (\alpha', \beta') \in \mathbb{R}^* \times \mathbb{R}$ . Si dimostri che  $\mathbb{R}^* \times \mathbb{R}$  con questa operazione è un gruppo.

*Soluzione.* Si osservi intanto che  $\cdot$  è un'operazione in  $\mathbb{R}^* \times \mathbb{R}$  in quanto se  $\alpha, \beta, \alpha', \beta' \in \mathbb{R}$  e  $\alpha, \alpha' \neq 0$ , allora  $\alpha\alpha', \alpha\beta' + \frac{\beta}{\alpha'} \in \mathbb{R}$  e  $\alpha\alpha' \neq 0$ .

Mostriamo che l'operazione è associativa. Siano  $(\alpha, \beta), (\alpha', \beta'), (\alpha'', \beta'') \in \mathbb{R}^* \times \mathbb{R}$ . Allora

$$\begin{aligned}((\alpha, \beta)(\alpha', \beta'))(\alpha'', \beta'') &= \left(\alpha\alpha', \alpha\beta' + \frac{\beta}{\alpha'}\right)(\alpha'', \beta'') = \\ &= \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \left(\alpha\beta' + \frac{\beta}{\alpha'}\right)\frac{\alpha''}{\alpha''}\right) = \\ &= \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \frac{\alpha\beta'\alpha''}{\alpha''} + \frac{\beta\alpha''}{\alpha'\alpha''}\right)\end{aligned}$$

e

$$\begin{aligned}(\alpha, \beta)((\alpha', \beta')(\alpha'', \beta'')) &= (\alpha, \beta)\left(\alpha'\alpha'', \alpha'\beta'' + \frac{\beta'}{\alpha''}\right) = \\ &= \left(\alpha\alpha'\alpha'', \alpha\left(\alpha'\beta'' + \frac{\beta'}{\alpha''}\right) + \frac{\beta}{\alpha'\alpha''}\right) =\end{aligned}$$

$$= \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \frac{\alpha\beta'}{\alpha''} + \frac{\beta}{\alpha'\alpha''}\right).$$

Quindi l'operazione in questione è associativa.

Cerchiamo l'identità. Se l'elemento  $(x, y) \in \mathbb{R}^* \times \mathbb{R}$  è l'identità, allora  $(x, y)(\alpha, \beta) = (\alpha, \beta)$  per ogni  $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$ , cioè  $(x\alpha, x\beta + \frac{y}{\alpha}) = (\alpha, \beta)$  per ogni  $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$ . Questo accade se e solo se  $x\alpha = \alpha$  e  $x\beta + \frac{y}{\alpha} = \beta$  per ogni  $\alpha \in \mathbb{R}^*$  e ogni  $\beta \in \mathbb{R}$ , vale a dire se e solo se  $x = 1$  e  $y = 0$ . Abbiamo così dimostrato che se in  $(\mathbb{R}^* \times \mathbb{R}, \cdot)$  c'è un'identità, questa deve essere  $(1, 0)$ .

Mostriamo che  $(1, 0)$  è proprio l'identità di  $\mathbb{R}^* \times \mathbb{R}$ . Per ogni  $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$  si ha  $(1, 0)(\alpha, \beta) = (1 \cdot \alpha, 1 \cdot \beta + \frac{0}{\alpha}) = (\alpha, \beta)$  e  $(\alpha, \beta)(1, 0) = (\alpha \cdot 1, \alpha \cdot 0 + \frac{\beta}{1}) = (\alpha, \beta)$ . Quindi  $(1, 0)$  è proprio l'identità di  $\mathbb{R}^* \times \mathbb{R}$ .

Cerchiamo l'inverso di un generico elemento  $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$ . Supponiamo che  $(x, y) \in \mathbb{R}^* \times \mathbb{R}$  sia un inverso di  $(\alpha, \beta)$ . Allora si deve avere  $(x, y)(\alpha, \beta) = (1, 0)$ , cioè  $(x\alpha, x\beta + \frac{y}{\alpha}) = (1, 0)$ , vale a dire  $x\alpha = 1$  e  $x\beta + \frac{y}{\alpha} = 0$ . Quindi se  $(x, y)$  è l'inverso di  $(\alpha, \beta)$  si deve avere  $x = 1/\alpha$  e  $y = -\beta$ . Questo dimostra che l'inverso di  $(\alpha, \beta)$ , se esiste, deve essere  $(1/\alpha, -\beta)$ .

Mostriamo che  $(1/\alpha, -\beta)$  è proprio l'inverso di  $(\alpha, \beta)$ : si ha

$$(\alpha, \beta)(1/\alpha, -\beta) = (\alpha(1/\alpha), \alpha(-\beta) + \beta) = (1, 0)$$

e

$$(1/\alpha, -\beta)(\alpha, \beta) = ((1/\alpha)\alpha, (1/\alpha)\beta + (-\beta)/\alpha) = (1, 0). \quad \square$$

**21.2.** Si dimostri che tutti i gruppi con un solo elemento sono tra loro isomorfi. (Un gruppo con un solo elemento è detto *gruppo identico* o *gruppo banale*.)

*Soluzione.* Siano  $(G_1, *)$ ,  $(G_2, \cdot)$  due gruppi con un solo elemento. Supponiamo  $G_1 = \{e_1\}$  e  $G_2 = \{e_2\}$ . Dato che  $G_1$  e  $G_2$  sono insieme moltiplicativamente chiusi, si deve avere  $e_1 * e_1 = e_1$  ed  $e_2 \cdot e_2 = e_2$ . Sia  $\varphi: G_1 \rightarrow G_2$  l'applicazione definita da  $\varphi(e_1) = e_2$ . Allora  $\varphi$  è una biiezione e per ogni  $g, h \in G_1$  si ha  $g = h = e_1$ , e quindi  $\varphi(g * h) = \varphi(e_1 * e_1) = \varphi(e_1) = e_2 = e_2 \cdot e_2 = \varphi(e_1) \cdot \varphi(e_1) = \varphi(g) \cdot \varphi(h)$ . Pertanto  $\varphi$  è un isomorfismo tra  $G_1$  e  $G_2$ .  $\square$

**21.3.** Siano  $\mathbb{R}$  il gruppo additivo dei numeri reali,

$$T = \{z \mid z \in \mathbb{C}, |z| = 1\}$$

il gruppo moltiplicativo dei numeri complessi di modulo 1,  $\varphi: \mathbb{R} \rightarrow T$  l'applicazione definita da  $\varphi(x) = \cos x + i \sin x$  per ogni  $x \in \mathbb{R}$ . Si dimostri che  $\varphi$  è un omomorfismo di gruppi.

*Soluzione.* Per ogni  $x, y \in \mathbb{R}$  si ha  $\varphi(x)\varphi(y) = (\cos x + i \sin x)(\cos y + i \sin y) = (\cos x \cos y - \sin x \sin y) + i(\cos x \sin y + \sin x \cos y) = \cos(x+y) + i \sin(x+y) = \varphi(x+y)$ .  $\square$

### Altri esercizi

**21.4.** Si dimostri che il semigruppato  $(\mathbb{R} \times \mathbb{R}, *)$  dell'esercizio 17.8 è un monoide e se ne determinino gli elementi invertibili.

**21.5.** Se  $W$  è il monoide libero su un insieme  $A$ , quali sono gli elementi invertibili di  $W$ ? invertibili a destra? invertibili a sinistra?

**21.6.** Sia  $G$  il prodotto cartesiano  $\mathbb{Z} \times \{1, -1\}$ . Si definisca un'operazione su  $G$  ponendo  $(m, \alpha)(n, \beta) = (m + \alpha n, \alpha\beta)$  per ogni  $(m, \alpha), (n, \beta) \in G$ .

- (a) Si provi che  $G$  è un gruppo.
- (b) Il gruppo  $G$  è abeliano?

**21.7.** Siano  $m, n$  numeri naturali. Si dimostri che  $m\mathbb{Z} \supseteq n\mathbb{Z}$  se e solo se  $m \mid n$ .

**21.8.** Sia  $(G, +)$  un gruppo abeliano. Per ogni  $n \in \mathbb{N}$  si definisca  $G[n] = \{g \in G \mid ng = 0_G\}$ .

- (a) Si dimostri che  $G[n]$  è un sottogruppo di  $G$ .
- (b) Si dimostri che se  $m, n \geq 1$  sono primi tra loro, allora

$$G[mn] = \{g + h \mid g \in G[m], h \in G[n]\} \quad \text{e} \quad G[m] \cap G[n] = \{0_G\}.$$

[Suggerimento per (b): corollario 4.2.]

**21.9.** Un elemento  $e$  di un semigruppato  $(S, \cdot)$  si dice *idempotente* se  $e^2 = e$ .

- (a) Si dimostri che se  $A$  è un insieme, nel semigruppato  $(A, *)$  studiato nell'esempio 4 del capitolo 17 ogni elemento è idempotente.
- (b) Si dimostri che se  $(G, \cdot)$  è un gruppo ed  $e \in G$  è un elemento idempotente, allora  $e = 1_G$ .
- (c) Si dimostri che se  $(M, \cdot)$  è un monoide ed  $e \in M$  è un elemento idempotente, allora  $eMe = \{eme \mid m \in M\}$  è un sottosemigruppato di  $M$  e che  $eMe$  è un monoide.

**21.10.** Siano  $(G, +)$  un gruppo abeliano e  $P$  un sottoinsieme di  $G$  con le seguenti proprietà:

- (a)  $0_G \notin P$ ;
- (b)  $P$  è *additivamente chiuso*, cioè se  $x, y \in P$  allora  $x + y \in P$ ;
- (c) se  $x \in G, x \neq 0_G$  e  $x \notin P$ , allora  $-x \in P$ .

Si definisca sull'insieme  $G$  una relazione  $\leq$  ponendo, per ogni  $x, y \in G, x \leq y$  se  $y - x \in P \cup \{0_G\}$ . Si dimostri che la relazione  $\leq$  è un ordinamento totale sull'insieme  $G$ .

**21.11.** Sia  $(G, \cdot)$  un gruppo. Per ogni  $x \in G$  poniamo  $K(x) = \{y^{-1}xy \mid y \in G\}$ . Si dimostri che  $\mathcal{F} = \{K(x) \mid x \in G\}$  è una partizione di  $G$ .

**21.12.** Si consideri la seguente proprietà di un gruppo  $(G, \cdot)$ : per ogni  $x \in G$  ed ogni intero positivo  $n$ , se  $x^n = 1_G$  allora  $x = 1_G$ .

- (a) I gruppi  $(\mathbb{C}^*, \cdot)$  e  $(\mathbb{C}, +)$  hanno tale proprietà?

Nel seguito dell'esercizio supporremo sempre che  $(G, \cdot)$  sia un gruppo con la proprietà in questione.

- (b) Si provi che se  $x \in G, x \neq 1_G, n$  ed  $m$  sono interi positivi e  $x^n = x^m$ , allora  $n = m$ .

Si definisca sull'insieme  $G$  una relazione  $\leq$  ponendo, per ogni  $x, y \in G, x \leq y$  se esiste un numero naturale  $n$  tale che  $x = y^n$ .

- (c) Si dimostri che  $\leq$  è un ordinamento parziale sull'insieme  $G$ .
- (d) Si dimostri che  $\leq$  è un ordinamento totale sull'insieme  $G$  se e solo se  $G = \{1_G\}$ .

[Suggerimento per (d): se  $x$  è un elemento di  $G$  e  $x \neq 1_G$ , considerare  $x^2$  e  $x^3$ .]

**21.13.** (a) Sia  $X$  un insieme. Ricordiamo che le *relazioni* su  $X$  sono i sottoinsiemi di  $X \times X$ . Sia  $\mathcal{R}_X = \{\varrho \mid \varrho \subseteq X \times X\} = \mathcal{P}(X \times X)$  l'insieme di tutte le relazioni su  $X$ . Date  $\varrho, \sigma \in \mathcal{R}_X$  definiamo  $\varrho \circ \sigma \in \mathcal{R}_X$  ponendo

$$\varrho \circ \sigma = \{(x, y) \in X \times X \mid \text{esiste } z \in X \text{ tale che } (x, z) \in \varrho \text{ e } (z, y) \in \sigma\}.$$

Si dimostri che  $(\mathcal{R}_X, \circ)$  è un monoide; l'operazione  $\circ$  di questo monoide è detta la *composizione di relazioni*. Se ne determini l'identità. Dato che le applicazioni di  $X$  in  $X$  sono particolari corrispondenze di  $X$  in  $X$ , cioè particolari relazioni su  $X$ , si ha che  $X^X$  è un sottoinsieme di  $\mathcal{R}_X$ . Si dimostri che  $X^X$  è un sottomonoido di  $\mathcal{R}_X$ . Si osservi che l'operazione indotta su  $X^X$  dall'operazione di  $\mathcal{R}_X$ , cioè dalla composizione di relazioni, è la composizione di applicazioni. Si determinino gli elementi invertibili a destra nel monoide  $(\mathcal{R}_X, \circ)$  e quelli invertibili a sinistra.

- (b) Una matrice  $A = (a_{ij})$  in cui si ha  $a_{ij} = 0$  oppure  $a_{ij} = 1$  per ogni  $i$  e ogni  $j$  si dice una *matrice*  $(0, 1)$ . Sia  $M_n(0, 1)$  l'insieme di tutte le matrici  $(0, 1)$ . Si definisca un'applicazione  $\nu: M_n(\mathbb{R}) \rightarrow M_n(0, 1)$  ponendo  $\nu((a_{ij})) = (a'_{ij})$ , ove  $a'_{ij} = 1$  se  $a_{ij} \neq 0$  e  $a'_{ij} = 0$  se  $a_{ij} = 0$ . È possibile definire un'operazione  $*$  in  $M_n(0, 1)$  ponendo, per ogni  $A, B \in M_n(0, 1), A * B = \nu(AB)$ , dove  $AB$  è il prodotto righe per colonne di  $A$  e di  $B$ .

Sia  $X = \{x_1, x_2, \dots, x_n\}$  un insieme finito con  $n$  elementi. Se  $\varrho \subseteq X \times X$  è una relazione su  $X$ , la matrice della corrispondenza  $\varrho$  (esercizio 6.1) è la matrice  $A_\varrho = (\varrho_{ij})$  definita da  $\varrho_{ij} = 1$  se  $x_i \varrho x_j$  e  $\varrho_{ij} = 0$  altrimenti. Si definisca un'applicazione  $\varphi: \mathcal{R}_X \rightarrow M_n(0, 1)$  ponendo  $\varphi(\varrho) = A_\varrho$  per ogni  $\varrho \in \mathcal{R}_X$ . Si provi che  $\varphi(\varrho) * \varphi(\varrho') = \varphi(\varrho \circ \varrho')$  per ogni  $\varrho, \varrho' \in \mathcal{R}_X$ . Se ne deduca che  $(M_n(0, 1), *)$  è un monoide e che  $\varphi: \mathcal{R}_X \rightarrow M_n(0, 1)$  è un isomorfismo del monoide  $(\mathcal{R}_X, \circ)$  nel monoide  $(M_n(0, 1), *)$ .

## Capitolo 22. Equivalenze compatibili con l'addizione in $\mathbb{N}$ e in $\mathbb{Z}$

**PROPOSIZIONE 22.1.** *Nel monoide  $(\mathbb{Z}, +)$  le relazioni di equivalenza compatibili con l'addizione sono tutte e sole le congruenze modulo  $n$ ,  $n \in \mathbb{N}$ .*

*Dimostrazione.* Si è già visto nell'esercizio 8.3 che le congruenze modulo  $n$  sono compatibili con l'addizione.

Mostriamo, viceversa, che se  $\sim$  è un'equivalenza sull'insieme  $\mathbb{Z}$  compatibile con l'addizione  $+$ , allora esiste un numero naturale  $n$  tale che  $\sim$  coincide con la congruenza modulo  $n$ . Se l'equivalenza  $\sim$  coincide con l'uguaglianza  $=$ , allora  $\sim$  è la congruenza modulo 0. Quindi dobbiamo solo dimostrare che se  $\sim$  è un'equivalenza sull'insieme  $\mathbb{Z}$  compatibile con l'addizione e diversa dall'uguaglianza, allora esiste un numero naturale  $n$  tale che  $\sim$  coincide con la congruenza modulo  $n$ . Dato che  $\sim$  è diversa dall'uguaglianza, esistono  $a, b \in \mathbb{Z}$ ,  $a \neq b$ , tali che  $a \sim b$ . Per la simmetria dell'equivalenza  $\sim$  possiamo supporre  $a > b$ . Essendo  $a \sim b$  e  $-b \sim -b$  (per la riflessività di  $\sim$ ), otteniamo dalla compatibilità di  $\sim$  che  $a - b \sim 0$ . Inoltre  $a - b > 0$ , e quindi l'insieme  $A = \{x \in \mathbb{Z} \mid x \sim 0 \text{ e } x > 0\}$  è un sottoinsieme non vuoto di  $\mathbb{N}$ . Sia  $n$  il minimo di  $A$ . Mostriamo che  $\sim$  coincide proprio con la congruenza modulo  $n$ , cioè che per ogni  $x, y \in \mathbb{Z}$  si ha che  $x \sim y$  se e solo se  $x \equiv y \pmod{n}$ . Dato che le relazioni  $\sim$  e la congruenza modulo  $n$  sono entrambe simmetriche per dimostrare che  $x \sim y$  se e solo se  $x \equiv y \pmod{n}$  possiamo supporre  $x \leq y$ .

Ora se  $x \sim y$ , dividiamo  $y - x$  per  $n$ ; si ha  $y - x = nq + r$  con  $q, r \in \mathbb{Z}$ ,  $0 \leq r < n$  e  $q \geq 0$  (perché  $y \geq x$ ). Da  $x \sim y$ ,  $-y \sim -y$ ,  $n \sim 0$ ,  $\dots$ ,  $n \sim 0$  ( $q$  volte) e  $r \sim r$ , si ha, sommando,  $x - y + nq + r \sim -y + r$ , cioè  $0 \sim r$ , e quindi  $r \sim 0$ . Se fosse  $r \neq 0$ , allora  $r \in A$  e  $r < n$ , assurdo per la minimalità di  $n$ . Quindi  $r = 0$ ,  $y - x = nq$ , e pertanto  $x \equiv y \pmod{n}$ .

Viceversa sia  $x \equiv y \pmod{n}$  e  $x \leq y$ . Allora  $y - x = nq$  per qualche  $q \in \mathbb{Z}$ ,  $q \geq 0$ . Da  $x \sim x$ ,  $n \sim 0$ ,  $\dots$ ,  $n \sim 0$  ( $q$  volte), sommando si ottiene che  $x + nq \sim x$ , cioè  $y \sim x$ . Per la simmetria si conclude che  $x \sim y$ .  $\square$

Consideriamo il monoide additivo dei numeri naturali  $(\mathbb{N}, +)$ . Fissiamo  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , e definiamo la relazione  $\sim_{k,n}$  su  $\mathbb{N}$  ponendo per ogni  $x, y \in \mathbb{N}$

$$x \sim_{k,n} y \text{ se } \begin{cases} x = y \\ \text{oppure} \\ x \geq k, y \geq k \text{ e } x \equiv y \pmod{n}. \end{cases}$$

**ESEMPIO 1.** Si ha

$$\begin{array}{llll} 0 \not\sim_{4,9} 9, & 2 \not\sim_{4,9} 11, & 3 \not\sim_{4,9} 12, & 4 \sim_{4,9} 13, \\ 5 \sim_{4,9} 14, & 100 \sim_{4,9} 10. & \square \end{array}$$

La relazione  $\sim_{k,n}$  è un'equivalenza su  $\mathbb{N}$ : verificare che  $\sim_{k,n}$  è riflessiva e simmetrica è immediato; per la transitività si supponga che  $x, y, z \in \mathbb{N}$  e che  $x \sim_{k,n} y$  e  $y \sim_{k,n} z$ . Se si ha  $x = y$  oppure  $y = z$ , allora ovviamente  $x \sim_{k,n} z$ . Si può supporre quindi  $x \neq y$  e  $y \neq z$ . Da  $x \sim_{k,n} y$  e  $y \sim_{k,n} z$  segue quindi che  $x \geq k$ ,  $y \geq k$ ,  $z \geq k$ ,  $x \equiv y \pmod{n}$  e  $y \equiv z \pmod{n}$ . Ma allora  $x \equiv z \pmod{n}$ , da cui  $x \sim_{k,n} z$ .

È quindi possibile costruire l'insieme quoziente

$$\mathbb{N}/\sim_{k,n} = \{[x]_{\sim_{k,n}} \mid x \in \mathbb{N}\}.$$

**LEMMA 22.2.** *Se  $k$  ed  $n \geq 1$  sono numeri naturali fissati, allora*

$$\mathbb{N}/\sim_{k,n} = \{[0]_{\sim_{k,n}}, [1]_{\sim_{k,n}}, \dots, [k+n-1]_{\sim_{k,n}}\},$$

*e gli elementi  $[0]_{\sim_{k,n}}, [1]_{\sim_{k,n}}, \dots, [k+n-1]_{\sim_{k,n}}$  di  $\mathbb{N}/\sim_{k,n}$  sono tutti distinti tra loro. In particolare  $\mathbb{N}/\sim_{k,n}$  è un insieme avente esattamente  $k+n$  elementi.*

*Dimostrazione.* Ovviamente l'insieme  $\mathbb{N}/\sim_{k,n} = \{[x] \mid x \in \mathbb{N}\}$  contiene  $\{[0], [1], \dots, [k+n-1]\}$ . Viceversa mostriamo che se  $[a] \in \mathbb{N}/\sim_{k,n}$ , ove  $a$  è un numero naturale, allora  $[a] \in \{[0], [1], \dots, [k+n-1]\}$ . Se  $a < k$ , allora  $a \leq k-1 \leq k+n-1$ , e quindi  $[a] \in \{[0], [1], \dots, [k+n-1]\}$ . Se invece  $a \geq k$ , dividiamo  $a-k$  per  $n$ ; si ha  $a-k = nq + r$  con  $q, r \in \mathbb{Z}$  e  $0 \leq r \leq n-1$ . Allora  $k \leq k+r \leq k+n-1$  e  $a \equiv k+r \pmod{n}$ . Ne segue che  $a \sim_{k,n} k+r$ , e quindi  $[a] = [k+r]$ . Inoltre  $k+r \leq k+n-1$  e quindi  $[a] = [k+r] \in \{[0], [1], \dots, [k+n-1]\}$ . Abbiamo così dimostrato che  $\mathbb{N}/\sim_{k,n} = \{[0], [1], \dots, [k+n-1]\}$ .

Mostriamo che gli elementi  $[0], [1], [2], \dots, [k+n-1]$  di  $\mathbb{N}/\sim_{k,n}$  sono tutti  $k+n$  distinti tra loro. Supponiamo che  $i$  e  $j$  siano due numeri interi con  $0 \leq i < j \leq k+n-1$  e dimostriamo che  $[i] \neq [j]$ . Se per assurdo si avesse  $[i] = [j]$ , allora  $i \sim_{k,n} j$ . Dato che  $i \neq j$ , deve essere quindi  $i \geq k$ ,  $j \geq k$  e  $i \equiv j \pmod{n}$ .

(mod  $n$ ). Da  $i \geq k$  segue che  $-i \leq -k$ , e da questo e  $j \leq k+n-1$  segue che  $0 < j-i \leq (k+n-1)-k = n-1$ . Ma  $j-i \equiv 0 \pmod{n}$ , e abbiamo visto che  $0 < j-i \leq n-1$ . Questo è ovviamente assurdo. Abbiamo così dimostrato che gli elementi  $[0], [1], [2], \dots, [k+n-1]$  di  $\mathbb{N}/\sim_{k,n}$  sono tutti distinti tra loro. Pertanto  $\mathbb{N}/\sim_{k,n}$  ha esattamente  $k+n$  elementi.  $\square$

Gli elementi di  $\mathbb{N}/\sim_{k,n}$  sono quindi:

$$\begin{aligned} [0]_{\sim_{k,n}} &= \{0\}, \\ [1]_{\sim_{k,n}} &= \{1\}, \\ [2]_{\sim_{k,n}} &= \{2\}, \\ &\dots \\ [k-2]_{\sim_{k,n}} &= \{k-2\}, \\ [k-1]_{\sim_{k,n}} &= \{k-1\}, \\ [k]_{\sim_{k,n}} &= \{k, k+n, k+2n, k+3n, \dots\}, \\ [k+1]_{\sim_{k,n}} &= \{k+1, k+1+n, k+1+2n, k+1+3n, \dots\}, \\ &\dots \\ [k+n-2]_{\sim_{k,n}} &= \{k+n-2, k+n-2+n, k+n-2+2n, k+n-2+3n, \dots\}, \\ [k+n-1]_{\sim_{k,n}} &= \{k+n-1, k+n-1+n, k+n-1+2n, k+n-1+3n, \dots\}. \end{aligned}$$

Nel capitolo 8 avevamo visto che una possibile rappresentazione di  $\mathbb{Z}/\equiv_n$  poteva essere quella della figura 8.1. Il lettore dovrebbe convincersi facilmente che l'analoga rappresentazione di  $\mathbb{N}/\sim_{k,n}$  è quella della figura 22.1.

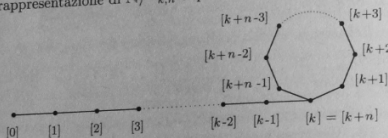


Figura 22.1

**PROPOSIZIONE 22.3.** Nel monoide  $(\mathbb{N}, +)$  le relazioni di equivalenza compatibili con l'addizione sono tutte e sole le relazioni  $\sim_{k,n}$  (dove  $k \geq 0$  e  $n \geq 1$ ) e l'uguaglianza  $=$ .

Anche la dimostrazione della proposizione 22.3 viene omessa per brevità. In base a tale proposizione l'addizione su  $\mathbb{N}$  induce un'operazione  $+$  su  $\mathbb{N}/\sim_{k,n}$  definita da  $[x]_{\sim_{k,n}} + [y]_{\sim_{k,n}} = [x+y]_{\sim_{k,n}}$  per ogni  $x, y \in \mathbb{N}$ , e rispetto a tale operazione  $\mathbb{N}/\sim_{k,n}$  è un monoide. Si noti che tale monoide è ciclico generato da

$[1]_{\sim_{k,n}}$ , in quanto per la proposizione 18.3 si ha  $[1]_{\sim_{k,n}} = \{t[1]_{\sim_{k,n}} \mid t \in \mathbb{N}\} = \{[t]_{\sim_{k,n}} \mid t \in \mathbb{N}\} = \mathbb{N}/\sim_{k,n}$ .

**PROPOSIZIONE 22.4.** Ogni monoide ciclico  $(M, \cdot)$  è isomorfo a  $(\mathbb{N}, +)$  oppure a  $(\mathbb{N}/\sim_{k,n}, +)$  per qualche  $k, n \in \mathbb{N}$ ,  $n \geq 1$ .

**Dimostrazione.** Sia  $(M, \cdot)$  un monoide ciclico. Allora esiste  $a \in M$  tale che  $M = \{a^t \mid t \in \mathbb{N}\}$ . Consideriamo l'applicazione  $\varphi: \mathbb{N} \rightarrow M$  definita da  $\varphi(t) = a^t$  per ogni  $t \in \mathbb{N}$ . L'applicazione  $\varphi$  è un omomorfismo suriettivo del monoide  $(\mathbb{N}, +)$  nel monoide  $(M, \cdot)$ . Per il teorema fondamentale di omomorfismo si ha che esiste un isomorfismo di monoidi  $\tilde{\varphi}: \mathbb{N}/\sim_{\varphi} \rightarrow M$ , ove  $\sim_{\varphi}$  è la relazione di equivalenza su  $\mathbb{N}$  associata a  $\varphi$ . Tale equivalenza è compatibile con l'addizione di  $\mathbb{N}$  perché  $\varphi$  è un omomorfismo di monoidi (capitolo 19), e quindi per la proposizione 22.3 la relazione  $\sim_{\varphi}$  è una delle relazioni  $\sim_{k,n}$  per qualche  $k \geq 0$  e qualche  $n \geq 1$  oppure è l'uguaglianza  $=$ . Se  $\sim_{\varphi}$  è una delle relazioni  $\sim_{k,n}$ , allora  $M \cong \mathbb{N}/\sim_{\varphi} = \mathbb{N}/\sim_{k,n}$ . Se invece  $\sim_{\varphi}$  è la relazione di uguaglianza, allora  $\varphi$  è iniettiva, perché se  $x, y \in \mathbb{N}$  e  $\varphi(x) = \varphi(y)$ , allora  $x \sim_{\varphi} y$ , e quindi  $x = y$  dato che  $\sim_{\varphi} = =$  coincidono. Quindi in questo caso  $\varphi$  è una biiezione. Ma allora in questo caso  $(\mathbb{N}, +)$  e  $(M, \cdot)$  sono isomorfi.  $\square$

### Esercizi svolti

**22.1.** Si dimostri che i monoidi  $(\mathbb{N}/\sim_{0,n}, +)$  e  $(\mathbb{Z}/\equiv_n, +)$  sono isomorfi per ogni numero naturale  $n \geq 1$  fissato.

**Soluzione.** Si consideri l'applicazione  $f: \mathbb{N} \rightarrow \mathbb{Z}/\equiv_n$  definita da  $f(x) = [x]_{\equiv_n}$  per ogni  $x \in \mathbb{N}$ . L'applicazione  $f$  è un omomorfismo del monoide  $(\mathbb{N}, +)$  nel monoide  $(\mathbb{Z}/\equiv_n, +)$  perché per ogni  $x, y \in \mathbb{N}$  si ha  $f(x+y) = [x+y]_{\equiv_n} = [x]_{\equiv_n} + [y]_{\equiv_n} = f(x) + f(y)$  e  $f(0) = [0]_{\equiv_n} = 0_{\mathbb{Z}/\equiv_n}$ . Inoltre l'omomorfismo  $f$  è suriettivo perché  $\mathbb{Z}/\equiv_n = \{[0]_{\equiv_n}, [1]_{\equiv_n}, \dots, [n-1]_{\equiv_n}\}$  per il lemma 8.1. Per il teorema fondamentale di omomorfismo per i monoidi (teorema 19.1) esiste un isomorfismo di monoidi  $\tilde{f}: \mathbb{N}/\sim_f \rightarrow \mathbb{Z}/\equiv_n$ , ove  $\sim_f$  è la relazione di equivalenza su  $\mathbb{N}$  associata ad  $f$ . Per concludere è quindi sufficiente dimostrare che le due equivalenze  $\sim_f$  e  $\sim_{0,n}$  su  $\mathbb{N}$  coincidono. Ora se  $x, y \in \mathbb{N}$  si ha  $x \sim_f y$  se e solo se  $f(x) = f(y)$ , cioè se e solo se  $[x]_{\equiv_n} = [y]_{\equiv_n}$ , ossia se e solo se  $x \equiv y \pmod{n}$ . Questo accade se e solo se  $x \sim_{0,n} y$ . Abbiamo così dimostrato che  $\sim_f$  e  $\sim_{0,n}$  coincidono.  $\square$

**22.2.** Si dimostri che se  $(G, \cdot)$  è un gruppo e  $\sim$  è un'equivalenza su  $G$  compatibile con l'operazione  $\cdot$ , allora il monoide quoziente  $(G/\sim, \cdot)$  è un gruppo.

**Soluzione.** Si deve dimostrare che ogni elemento di  $G/\sim$  è invertibile. Gli elementi di  $G/\sim$  sono del tipo  $[g]_{\sim}$ , con  $g \in G$ . Dato che  $G$  è un gruppo,  $g$  ha un inverso  $g^{-1} \in G$ . Ma allora  $[g^{-1}]_{\sim}$  appartiene a  $G$  e si ha  $[g]_{\sim} [g^{-1}]_{\sim} = [gg^{-1}]_{\sim} =$





(c) Se ne deduca che se  $m$  è un intero positivo, il gruppo  $(\mathbb{Z}/\equiv_m, +)$  ha un sottogruppo isomorfo a  $(\mathbb{Z}/\equiv_n, +)$  per ogni divisore positivo  $n$  di  $m$ .

22.11. Si dimostri che i monoidi  $(\mathbb{N}, +)$  e  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , sono tutti a due a due non isomorfi tra loro.

22.12. Dimostrare che se  $k > 1$  ed  $n \geq 1$ , allora  $[1]_{\sim_{k,n}} \in \mathbb{N}/\sim_{k,n}$  è l'unico generatore del monoide ciclico  $(\mathbb{N}/\sim_{k,n}, +)$ .

22.13. Sia  $(G, \cdot)$  un gruppo con la proprietà che per ogni  $g \in G$  e ogni numero intero  $n > 0$  si abbia che  $g^n = 1$  implica  $g = 1$ . Si dimostri che tutti i sottomonoidi ciclici di  $G$  eccetto il sottomonoido  $\{1\}$  sono isomorfi ad  $(\mathbb{N}, +)$ .

**Isomorfismi tra monoidi ciclici.** Se  $(M, \cdot)$  è un monoide ciclico, sappiamo che  $M$  è isomorfo a  $(\mathbb{N}, +)$  oppure a  $(\mathbb{N}/\sim_{k,n}, +)$  per qualche  $k \in \mathbb{N}$  e qualche  $n \in \mathbb{N}$ ,  $n \geq 1$  (proposizione 22.4). Per determinare a quale di questi monoidi è isomorfo  $M$  si può procedere nel modo seguente. Si fissa innanzitutto un generatore  $a$  di  $M$ . Se  $a^p \neq a^q$  per ogni  $p, q \in \mathbb{N}$ ,  $p \neq q$ , allora  $M \cong \mathbb{N}$ . Se invece esistono  $p, q \in \mathbb{N}$ ,  $p \neq q$ , tali che  $a^p = a^q$ , allora  $M \cong \mathbb{N}/\sim_{k,n}$  dove  $k$  è il minimo tra i numeri naturali  $p$  con questa proprietà:

$$k = \min\{p \in \mathbb{N} \mid \text{esiste } q \in \mathbb{N}, q \neq p, \text{ tale che } a^p = a^q\}.$$

Una volta trovato  $k$ , per determinare  $n$  si può procedere in due modi:

- (1) calcolare  $|M|$ ; infatti deve essere  $k + n = |M|$ ;
- (2) far uso della formula  $k + n = \min\{q \mid q \in \mathbb{N}, q > k, a^q = a^k\}$ .

Il  $k$  e l' $n$  così trovati sono i numeri naturali per i quali  $M \cong \mathbb{N}/\sim_{k,n}$ .

22.14. Siano  $Y \subseteq X$  due insiemi non vuoti. Si consideri il monoide  $(\mathcal{P}(X), \cap)$  e l'elemento  $Y \in \mathcal{P}(X)$ . Determinare a quale tra i monoidi  $(\mathbb{N}, +)$  o  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , è isomorfo il sottomonoido ciclico  $[Y]$  di  $\mathcal{P}(X)$  generato da  $Y$ .

22.15. Sia  $(\mathbb{C}, \cdot)$  il monoide moltiplicativo dei numeri complessi. Determinare a quale tra i monoidi  $(\mathbb{N}, +)$  o  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , è isomorfo il sottomonoido ciclico  $[i]$  di  $(\mathbb{C}, \cdot)$  generato da  $i$ .

22.16. Sia  $(\mathbb{C}, +)$  il monoide additivo dei numeri complessi. Determinare a quale tra i monoidi  $(\mathbb{N}, +)$  o  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , è isomorfo il sottomonoido ciclico  $[i]$  di  $(\mathbb{C}, +)$  generato da  $i$ .

22.17. Siano  $X = \{0, 1, 2, 3, 4\}$  ed  $X^X$  il monoide delle applicazioni di  $X$  in  $X$ . Si consideri l'applicazione  $f: X \rightarrow X$  definita da  $f(0) = 0$  e  $f(x) = x - 1$  per ogni  $x = 1, 2, 3, 4$ . Determinare a quale tra i monoidi  $(\mathbb{N}, +)$  o  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , è isomorfo il sottomonoido ciclico  $[f]$  di  $X^X$  generato da  $f$ .

22.18. Nell'insieme  $\mathbb{C}^*$  dei numeri complessi non nulli si definisca una relazione  $\sim$  ponendo, per ogni  $a, b \in \mathbb{C}^*$ ,  $a \sim b$  se  $\frac{a}{b} \in \mathbb{R}$ .

- (a) Si dimostri che  $\sim$  è un'equivalenza su  $\mathbb{C}^*$ .
- (b) Si dimostri che l'equivalenza  $\sim$  su  $\mathbb{C}^*$  è compatibile con la moltiplicazione tra numeri complessi.
- (c) Si dimostri che il monoide quoziente  $(\mathbb{C}^*/\sim, \cdot)$  e il suo elemento  $[i\sqrt{2}]_{\sim}$ . Quanti elementi ha il sottomonoido ciclico  $[i\sqrt{2}]_{\sim}$  di  $(\mathbb{C}^*/\sim, \cdot)$  generato da  $[i\sqrt{2}]_{\sim}$ ?
- (d) Determinare a quale tra i monoidi  $(\mathbb{N}, +)$  o  $(\mathbb{N}/\sim_{k,n}, +)$ ,  $k, n \in \mathbb{N}$ ,  $n \geq 1$ , è isomorfo  $[i\sqrt{2}]_{\sim}$ .

## Capitolo 23. Permutazioni

Sia  $n \geq 1$  un numero intero fissato e sia  $X_n = \{1, 2, \dots, n\}$ . Il gruppo  $S_n$ , i cui elementi sono tutte le biezioni  $X_n \rightarrow X_n$  e in cui l'operazione  $\circ$  è la composizione di applicazioni, è detto il *gruppo simmetrico su  $n$  oggetti* o il *gruppo delle permutazioni di  $n$  oggetti*. Le biezioni  $X_n \rightarrow X_n$  si chiamano anche *permutazioni*.

Se  $f \in S_n$  denoteremo  $f$  con il simbolo

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

ESEMPIO 1. Se  $f: X_5 \rightarrow X_5$  è l'applicazione definita da  $f(1) = 2$ ,  $f(2) = 5$ ,  $f(3) = 3$ ,  $f(4) = 1$ ,  $f(5) = 4$ , allora  $f$  viene denotata con il simbolo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}. \quad \square$$

In questa notazione:

- (1) l'identità del gruppo  $S_n$ , che è l'applicazione identica  $\iota_{X_n}: X_n \rightarrow X_n$ , viene denotata con

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix};$$

- (2) data

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix},$$

l'inversa  $f^{-1}$  di  $f$  si ottiene scambiando le due righe e poi riordinando le colonne in modo che la prima riga diventi la riga  $1 \ 2 \ 3 \ \dots \ n$ .

ESEMPIO 2. Se

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix},$$

scambiando le righe si ottiene  $\begin{pmatrix} 2 & 5 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ , e riordinando le colonne si

$$\text{ricava } f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}. \quad \square$$

ESEMPIO 3. Se  $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$  e  $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$  calcoliamo  $f \circ g$ .

Si ha

$$\begin{aligned} (f \circ g)(1) &= f(g(1)) = f(5) = 5, \\ (f \circ g)(2) &= f(g(2)) = f(4) = 3, \\ (f \circ g)(3) &= f(g(3)) = f(3) = 1, \\ (f \circ g)(4) &= f(g(4)) = f(1) = 2, \\ (f \circ g)(5) &= f(g(5)) = f(2) = 4. \end{aligned}$$

Quindi  $f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$ . In modo analogo è facile dimostrare che, scambiando  $f$  e  $g$ , si ha  $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$ . In particolare il gruppo  $S_5$  non è abeliano.  $\square$

Si osservi che quando si denota una permutazione  $f$  con il simbolo

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix},$$

allora nella seconda riga  $f(1) \ f(2) \ f(3) \ \dots \ f(n)$  compaiono una ed una sola volta tutti i numeri tra 1 ed  $n$ : compaiono una volta perché l'applicazione  $f: X_n \rightarrow X_n$  è suriettiva; compaiono una sola volta perché l'applicazione  $f$  è iniettiva.

LEMMA 23.1. *L'ordine di  $S_n$  è  $n!$ .*

Sia  $d$  un numero naturale,  $1 \leq d \leq n$ . Un ciclo di lunghezza  $d$  in  $S_n$  è una permutazione  $f \in S_n$  con la seguente proprietà: esistono  $d$  elementi distinti  $a_1, a_2, \dots, a_d \in \{1, 2, \dots, n\}$  tali che  $f(a_i) = a_{i+1}$  per ogni  $i = 1, 2, \dots, d-1$ ,  $f(a_d) = a_1$ ,  $f(k) = k$  per ogni  $k \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_d\}$ . Denoteremo tale ciclo con il simbolo  $(a_1 \ a_2 \ \dots \ a_d)$ .

ESEMPIO 4. In  $S_6$  il ciclo  $(3 \ 1 \ 2 \ 6)$  (di lunghezza 4) è la permutazione  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$ . Quindi

$$(3 \ 1 \ 2 \ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

Si noti che si ha anche

$$(1 \ 2 \ 6 \ 3) = (2 \ 6 \ 3 \ 1) = (6 \ 3 \ 1 \ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}. \quad \square$$

Il lettore osservi che i cicli di lunghezza 1 sono tutti uguali all'identità, e che, viceversa, l'identità può essere considerata un ciclo di lunghezza 1.

Due cicli  $(a_1 \ a_2 \ \dots \ a_d)$ ,  $(b_1 \ b_2 \ \dots \ b_t)$  di  $S_n$  si dicono *disgiunti* se  $\{a_1, a_2, \dots, a_d\} \cap \{b_1, b_2, \dots, b_t\} = \emptyset$ .

LEMMA 23.2. Se  $f = (a_1 \ a_2 \ \dots \ a_d)$  e  $g = (b_1 \ b_2 \ \dots \ b_t)$  sono cicli disgiunti, allora  $f \circ g = g \circ f$ .

TEOREMA 23.3. Ogni permutazione può essere scritta come prodotto di cicli disgiunti. Tale scrittura è unica a meno dell'ordine dei fattori.

ESEMPIO 5. Vediamo il procedimento per scrivere la permutazione

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix}$$

come prodotto di cicli disgiunti.

Scriviamo intanto il numero 1:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1$$

Dato che  $f$  manda 1 in 5 si ha

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5$$

Ma  $f$  manda 5 in 2 e quindi scriviamo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2$$

e 2 viene mandato in 1 che è il primo numero con cui avevamo cominciato il ciclo. Quindi il primo ciclo è concluso e si può scrivere

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ$$

Iniziamo il secondo ciclo con il primo numero che non abbiamo ancora incontrato (1 e 2 li abbiamo già trovati, e quindi il primo numero non ancora trovato è il 3); quindi

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3)$$

La permutazione  $f$  manda 3 in 7:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7)$$

e manda 7 in 3. Quindi anche il secondo ciclo è concluso:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7) \circ \dots$$

Il primo numero che non abbiamo ancora incontrato è 4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7) \circ (4 \dots)$$

La  $f$  manda 4 in 6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7) \circ (4 \ 6)$$

e manda 6 in 8

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7) \circ (4 \ 6 \ 8)$$

e 8 in 4, che è il primo numero con cui avevamo iniziato questo ciclo. Quindi

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \ 5 \ 2) \circ (3 \ 7) \circ (4 \ 6 \ 8).$$

La scrittura della decomposizione in cicli disgiunti della permutazione  $f$  è così completata. Si noti che tale scrittura è unica a meno dell'ordine dei fattori; per il lemma 23.2 si ha infatti anche

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (3 \ 7) \circ (1 \ 5 \ 2) \circ (4 \ 6 \ 8)$$

o anche

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (3 \ 7) \circ (4 \ 6 \ 8) \circ (1 \ 5 \ 2),$$

eccetera.

ESEMPIO 6. Il lettore decomponga in prodotto di cicli disgiunti la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 5 & 2 & 1 & 4 \end{pmatrix}.$$

Il risultato è

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 5 & 2 & 1 & 4 \end{pmatrix} = (1 \ 6) \circ (2 \ 7 \ 4 \ 5) \circ (3).$$

Si noti che il ciclo (3) è un ciclo di lunghezza 1, cioè è l'applicazione identica, e ovviamente comporre con l'applicazione identica non modifica il risultato. Quindi possiamo scrivere anche

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 5 & 2 & 1 & 4 \end{pmatrix} = (1 \ 6) \circ (2 \ 7 \ 4 \ 5). \quad \square$$

I cicli di lunghezza 2 si chiamano anche trasposizioni.

TEOREMA 23.4. Ogni permutazione può essere scritta come prodotto di trasposizioni.

Il teorema 23.4 segue dal teorema 23.3 osservando che ogni ciclo

$$(a_1 \ a_2 \ \dots \ a_d)$$

è prodotto di trasposizioni in quanto

$$(a_1 \ a_2 \ \dots \ a_d) = (a_1 \ a_d)(a_1 \ a_{d-1}) \dots (a_1 \ a_3)(a_1 \ a_2).$$

ESEMPIO 7. In  $S_8$  si ha

$$(2 \ 4 \ 5 \ 6 \ 7) = (2 \ 7) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 4). \quad \square$$

COROLLARIO 23.5. Sia  $(S_n, \circ)$  il monoide di tutte le permutazioni di  $n$  oggetti,  $C_n \subseteq S_n$  il sottoinsieme dei cicli e  $T_n \subseteq C_n$  il sottoinsieme delle trasposizioni. Se  $[C_n]$  e  $[T_n]$  denotano rispettivamente i sottoinsiemi di  $S_n$  generati da  $C_n$  e  $T_n$ , allora  $[C_n] = [T_n] = S_n$ .

Definiamo un'applicazione  $\lambda: S_n \rightarrow \mathbb{N}$  nel modo seguente: data  $f \in S_n$  decomponiamo  $f$  come prodotto di cicli disgiunti,

$$f = (a_{11} a_{12} \dots a_{1d_1}) \circ (a_{21} a_{22} a_{2d_2}) \circ \dots \circ (a_{k1} a_{k2} a_{kd_k});$$

se  $f$  è prodotto di  $k$  cicli di lunghezza  $d_1, d_2, \dots, d_k$  rispettivamente, poniamo

$$\lambda(f) = \left( \sum_{i=1}^k d_i \right) - k.$$

TEOREMA 23.6. L'applicazione  $\text{sgn}: S_n \rightarrow \{1, -1\}$  definita da  $\text{sgn}(f) = (-1)^{\lambda(f)}$  per ogni  $f \in S_n$  è un omomorfismo del gruppo  $(S_n, \circ)$  nel gruppo  $(\{1, -1\}, \cdot)$ .

Per ogni  $f \in S_n$  diremo che  $\text{sgn}(f)$  è la *segnatura* di  $f$ . Non è difficile dimostrare che  $\text{sgn}(f) = 1$  se e solo se tutte le decomposizioni di  $f$  come prodotto di trasposizioni hanno un numero pari di fattori, e che  $\text{sgn}(f) = -1$  se e solo se tutte le decomposizioni di  $f$  come prodotto di trasposizioni hanno un numero dispari di fattori. In particolare le rappresentazioni di una fissata permutazione  $f$  come prodotto di trasposizioni hanno tutte un numero pari o tutte un numero dispari di fattori. Distingueremo pertanto le permutazioni in permutazioni di *classe pari* e permutazioni di *classe dispari*.

### Esercizi svolti

**23.1.** Sia  $n \geq 1$  un numero naturale. Si provi che il gruppo  $S_n$  è abeliano se e solo se  $n = 1$  oppure  $n = 2$ .

*Soluzione.* Per  $n = 1$  c'è una sola biiezione  $\{1\} \rightarrow \{1\}$ , che è la  $\iota_{\{1\}}$ , cioè  $S_1$  contiene un unico elemento che è l'unico ciclo (1) di lunghezza 1. Quindi in questo caso  $S_1 = \{(1)\}$  è il gruppo banale con un solo elemento, e questo è certamente un gruppo abeliano.

Per  $n = 2$  ci sono due biiezioni  $\{1, 2\} \rightarrow \{1, 2\}$ , l'applicazione identica  $\iota_{\{1,2\}}$  e lo scambio  $\sigma : \{1, 2\} \rightarrow \{1, 2\}$  definito da  $\sigma(1) = 2$  e  $\sigma(2) = 1$ . Ma  $\iota_{\{1,2\}} = (1)$  e  $\sigma = (1\ 2)$ . Quindi in questo caso  $S_2 = \{(1), (1\ 2)\}$  ha due elementi, e anche questo è un gruppo abeliano.

Per  $n \geq 3$  si ha che  $(1\ 2)$  e  $(1\ 2\ 3)$  appartengono a  $S_n$ , e

$$(1\ 2) \circ (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix},$$

$$(1\ 2\ 3) \circ (1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}.$$

Quindi  $(1\ 2) \circ (1\ 2\ 3) \neq (1\ 2\ 3) \circ (1\ 2)$ , e pertanto il gruppo  $S_n$  non è abeliano per  $n \geq 3$ .  $\square$

**23.2.** Si scriva la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 3 & 8 & 7 \end{pmatrix}$$

come prodotto di trasposizioni.

*Soluzione.* Come prodotto di cicli disgiunti si ha

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 3 & 8 & 7 \end{pmatrix} = (1\ 2\ 4\ 6\ 3\ 5)(7\ 8),$$

e quindi, come si vede facendo uso della formula scritta subito dopo il teorema 23.4, questa permutazione è uguale a

$$(1\ 5)(1\ 3)(1\ 6)(1\ 4)(1\ 2)(7\ 8). \quad \square$$

**23.3.** La permutazione

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

è di classe pari o di classe dispari?

*Soluzione.* Decomponendo la permutazione  $f$  in prodotto di cicli disgiunti si ottiene  $f = (1\ 9\ 2\ 8)(3\ 7)(4\ 6)$ . Per vedere se è di classe pari o di classe dispari si può ora procedere in due modi:

(1) calcolarne la segnatura. Si ha  $\lambda(f) = 4 + 2 + 2 - 3 = 5$ , e quindi  $\text{sgn}(f) = (-1)^5 = -1$ . Pertanto  $f$  è di classe dispari.

(2) scomporla come prodotto di trasposizioni. Si ha

$$f = (1\ 8)(1\ 2)(1\ 9)(3\ 7)(4\ 6),$$

e quindi  $f$  è esprimibile come prodotto di cinque trasposizioni. Dato che il numero 5 è dispari, anche in questo caso si conclude che la permutazione  $f$  è di classe dispari.  $\square$

### Altri esercizi

**23.4.** (a) Si scrivano tutti gli elementi del gruppo  $S_4$ .

(b) Sia  $f \in S_4$  la biiezione

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Si determinino tutti gli elementi  $g \in S_4$  tali che  $f \circ g = f$ .

**23.5.** Sia  $f : \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$  l'applicazione definita da

$$f(1) = 3, \quad f(2) = 5, \quad f(3) = 4, \quad f(4) = 1, \quad f(5) = 2.$$

Si dica se la permutazione  $f \in S_5$  è un ciclo.

**23.6.** In  $S_7$  si considerino i cicli  $f = (1\ 3\ 4\ 5\ 6)$  e  $g = (1\ 4\ 6\ 3\ 5)$ . Tali cicli sono disgiunti? Si ha  $f \circ g = g \circ f$ ?



23.7. Si scriva la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 2 & 8 & 3 & 7 & 1 & 5 & 4 & 6 & 10 \end{pmatrix}$$

come prodotto di cicli disgiunti.

23.8. Sia  $S_8$  il gruppo simmetrico su 8 oggetti e sia

$$g = (1 \ 3 \ 5 \ 7) \circ (2 \ 3 \ 7) \in S_8.$$

- (a) Si scriva  $g$  come prodotto di cicli disgiunti.  
(b) Si calcoli  $g^{-1}$ .

23.9. Si consideri la seguente permutazione  $f \in S_{13}$ :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 13 & 10 & 7 & 8 & 9 & 6 & 3 & 1 & 12 & 5 & 11 & 2 & 4 \end{pmatrix}.$$

- (a) Si scriva  $f$  come prodotto di cicli disgiunti.  
(b) Si scriva  $f$  come prodotto di trasposizioni.  
(c) Si calcoli la segnatura di  $f$ .

23.10. Si dica se la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 5 & 4 & 10 & 8 & 11 & 1 & 2 & 9 \end{pmatrix}$$

è di classe pari o di classe dispari.

23.11. Sia  $E = \{z \mid z \in \mathbb{C}, z^8 = 1\}$  l'insieme delle radici ottave dell'unità e sia  $i \in \mathbb{C}$  l'unità immaginaria. Si definisca un'applicazione  $\varphi: E \rightarrow E$  ponendo  $\varphi(z) = iz$  per ogni  $z \in E$ .

- (a) Si provi che  $\varphi$  è una biiezione.  
(b) Sia  $z_h = \cos(\pi h/4) + i \sin(\pi h/4)$  per ogni  $h \in \mathbb{Z}$ . Si ponga

$$X_8 = \{1, 2, 3, 4, 5, 6, 7, 8\},$$

e si consideri l'applicazione  $\psi: X_8 \rightarrow E$  definita da  $\psi(h) = z_h$  per ogni  $h \in X_8$ . Allora  $f = \psi^{-1} \circ \varphi \circ \psi$  è una permutazione di  $X_8$ . Si scriva  $f$  come prodotto di cicli disgiunti e se ne determini la classe.

23.12. Siano  $2 \leq d \leq n$  numeri interi. Sia  $f \in S_n$  un ciclo di lunghezza  $d$ . Si dimostri che:

- (a) se  $d = 2$ ,  $f^2$  è l'identità del gruppo  $S_n$ ;  
(b) se  $d$  è dispari,  $f^2$  è un ciclo di lunghezza  $d$ ;  
(c) se  $d \geq 4$  è pari,  $f^2$  è il prodotto di due cicli disgiunti di lunghezza  $d/2$ .

## Capitolo 24. Sottogruppi normali e classi laterali

Se  $(G, \cdot)$  è un gruppo,  $H$  è un sottogruppo di  $G$  e  $g \in G$ , l'insieme  $gH = \{gh \mid h \in H\} \subseteq G$  si dice la *classe laterale sinistra* di  $G$  modulo  $H$  di rappresentante  $g$ . Analogamente  $Hg = \{hg \mid h \in H\}$  si dice la *classe laterale destra*.

ESEMPIO 1. Sia  $G = \mathbb{R}^*$  il gruppo moltiplicativo dei reali non nulli. Se  $H = \mathbb{R}^+ = \{\alpha \mid \alpha \in \mathbb{R}, \alpha > 0\}$ , è facile verificare che  $\mathbb{R}^+$  è un sottogruppo di  $\mathbb{R}^*$ . Fissato  $g \in \mathbb{R}^*$ , calcoliamo la classe laterale sinistra di  $\mathbb{R}^*$  modulo  $\mathbb{R}^+$  di rappresentante  $g$ . Distinguiamo i due casi  $g > 0$  e  $g < 0$ .

Se  $g > 0$  si ha  $g\mathbb{R}^+ = \mathbb{R}^+$  (questo lo si verifica con la doppia inclusione; l'inclusione  $\subseteq$  è ovvia; viceversa se  $\alpha \in \mathbb{R}^+$ , allora  $\alpha = g \cdot \frac{\alpha}{g}$  e  $\frac{\alpha}{g} \in \mathbb{R}^+$ ). Quindi

$$\alpha = g \cdot \frac{\alpha}{g} \in g\mathbb{R}^+.$$

Se invece  $g < 0$ , allora  $g\mathbb{R}^+ = \mathbb{R}^-$ , dove con  $\mathbb{R}^-$  abbiamo indicato l'insieme dei numeri reali negativi:  $\mathbb{R}^- = \{\alpha \mid \alpha \in \mathbb{R}, \alpha < 0\}$ . Verifichiamo anche l'uguaglianza  $g\mathbb{R}^+ = \mathbb{R}^-$  con la doppia inclusione. Dato che  $g < 0$ , è evidente che  $g\mathbb{R}^+ \subseteq \mathbb{R}^-$ . Viceversa se  $\alpha \in \mathbb{R}^-$ , allora  $\frac{\alpha}{g} \in \mathbb{R}^+$ , e quindi  $\alpha = g \cdot \frac{\alpha}{g} \in g\mathbb{R}^+$ . Pertanto  $\mathbb{R}^- \subseteq g\mathbb{R}^+$ .  $\square$

ESEMPIO 2. Può ovviamente capitare che  $g_1H = g_2H$  anche quando  $g_1 \neq g_2$ . Dimostriamo che se  $G$  è un gruppo,  $H \leq G$ , e  $g_1, g_2 \in G$ , allora  $g_1H = g_2H$  se e solo se  $g_1^{-1}g_2 \in H$ .

Se  $g_1H = g_2H$ , allora  $g_2 = g_2 \cdot 1_G \in g_2H = g_1H$ . Quindi esiste un elemento  $h \in H$  tale che  $g_2 = g_1h$ . Moltiplichiamo questa uguaglianza a sinistra per  $g_1^{-1}$ . Si ottiene che  $g_1^{-1}g_2 = g_1^{-1}g_1h$ , e pertanto  $g_1^{-1}g_2 = 1_Gh = h \in H$ .

Viceversa supponiamo che  $g_1^{-1}g_2 \in H$ . Allora  $g_1^{-1}g_2 = h$  per qualche  $h \in H$ , da cui, moltiplicando a sinistra per  $g_1$ , si ottiene che  $g_2 = g_1h$ . Da quest'ultima uguaglianza, moltiplicando a destra per  $h^{-1}$ , si ottiene poi anche che  $g_2h^{-1} = g_1$ . Dimostriamo che  $g_1H = g_2H$  verificando la doppia inclusione.

Se  $x \in g_1H$ , allora  $x = g_1k$  per qualche  $k \in H$ , da cui  $x = g_2h^{-1}k$ . Essendo  $H$  un sottogruppo di  $G$  si ha che  $h^{-1}k \in H$ , e quindi  $x = g_2h^{-1}k \in g_2H$ . Se invece  $y \in g_2H$ , allora  $y = g_2k'$  per qualche  $k' \in H$ , da cui  $y = g_2k' = g_1hk'$ . Ma  $hk' \in H$  perché  $H$  è un sottogruppo di  $G$ ; ne segue che  $y = g_1hk' \in g_1H$ .  $\square$



modulo  $N$ , i cui elementi sono le classi laterali sinistre (o destre)  $gN = Ng$ , cioè

$$G/N = \{gN \mid g \in G\},$$

e nel quale l'operazione è definita da

$$gN \cdot g'N = gg'N$$

per ogni  $gN, g'N \in G/N$ . L'identità di  $G/N$  è  $1_G/N = 1_G \cdot N = N$ , e l'inverso dell'elemento  $gN \in G/N$  è  $(gN)^{-1} = g^{-1}N$ . La proiezione canonica  $\pi: G \rightarrow G/N$  è definita da  $\pi(g) = gN$  per ogni  $g \in G$ . Tale applicazione è un omomorfismo suriettivo di gruppi, perché per ogni  $g, g' \in G$  si ha  $\pi(g) \cdot \pi(g') = gN \cdot g'N = gg'N = \pi(gg')$ .

**ESEMPIO 5.** Sia  $G = \mathbb{C}^*$  il gruppo moltiplicativo dei numeri complessi non nulli e sia  $N = \mathbb{R}^+$  il sottogruppo di  $G$  i cui elementi sono i numeri reali positivi. Per ogni  $\theta \in \mathbb{R}$  ed ogni numero complesso  $z = \rho(\cos \theta + i \sin \theta)$  avente argomento  $\theta$ , la classe laterale sinistra  $z\mathbb{R}^+$  è l'insieme degli elementi del tipo  $\rho(\cos \theta + i \sin \theta)t$  con  $t \in \mathbb{R}^+$ , ossia  $z\mathbb{R}^+ = \{\rho t(\cos \theta + i \sin \theta) \mid t \in \mathbb{R}^+\} = \{r(\cos \theta + i \sin \theta) \mid r \in \mathbb{R}^+\}$ . Quindi gli elementi di  $z\mathbb{R}^+$  sono tutti i numeri complessi aventi argomento  $\theta$ , vale a dire tutti i punti del piano di Argand-Gauss che stanno sulla semiretta  $\theta$ , vale a dire tutti i punti del piano di Argand-Gauss che stanno sulla semiretta  $\theta$ , vale a dire tutti i punti del piano di Argand-Gauss che stanno sulla semiretta  $\theta$ , vale a dire tutti i punti del piano di Argand-Gauss che stanno sulla semiretta  $\theta$ . Il gruppo quoziente di queste classi laterali formano una partizione di  $\mathbb{C}^*$ . Il gruppo quoziente di  $\mathbb{C}^*$  modulo  $\mathbb{R}^+$  è  $\mathbb{C}^*/\mathbb{R}^+ = \{z\mathbb{R}^+ \mid z \in \mathbb{C}^*\}$  e si ha  $z\mathbb{R}^+ \cdot z'\mathbb{R}^+ = zz'\mathbb{R}^+$  per ogni  $z, z' \in \mathbb{C}^*$ . L'identità di  $\mathbb{C}^*/\mathbb{R}^+$  è  $1_{\mathbb{C}^*}/\mathbb{R}^+ = \mathbb{R}^+$ , che è l'insieme dei numeri complessi di argomento 0. Per ogni  $z \in \mathbb{C}^*$  si ha  $(z\mathbb{R}^+)^{-1} = z^{-1}\mathbb{R}^+$ .  $\square$

### Esercizi svolti

**24.1.** Sia  $S(\mathbb{R})$  il gruppo di tutte le biezioni  $f: \mathbb{R} \rightarrow \mathbb{R}$  dotato come operazione della composizione di applicazioni  $\circ$ . Si consideri il sottogruppo

$$H = \{f \in S(\mathbb{R}) \mid f(0) = 0\}$$

di  $S(\mathbb{R})$ , e sia  $u: \mathbb{R} \rightarrow \mathbb{R}$  la biezione definita da  $u(x) = x + 1$  per ogni  $x \in \mathbb{R}$ . Si determinino le classi laterali  $uH$  e  $Hu$ . Il sottogruppo  $H$  di  $S(\mathbb{R})$  è normale?

**Soluzione.** Si ha  $uH = \{uf \mid f \in S(\mathbb{R}), f(0) = 0\}$ . Mostriamo che questo insieme coincide con  $\{g \mid g \in S(\mathbb{R}), g(0) = 1\}$  verificando la doppia inclusione. Se  $f \in S(\mathbb{R})$  e  $f(0) = 0$  allora  $uf(0) = u(0) = 1$ . Viceversa se  $g \in S(\mathbb{R})$  e  $g(0) = 1$ , consideriamo l'elemento  $f = u^{-1}g$  di  $S(\mathbb{R})$ . (Si potrebbe dimostrare che  $f$  è l'applicazione di  $\mathbb{R}$  in  $\mathbb{R}$  definita da  $f(x) = g(x) - 1$  per ogni  $x \in \mathbb{R}$ , ma questo non è indispensabile per risolvere l'esercizio.) Dato che  $u(0) = 1$ , deve essere  $u^{-1}(1) = 0$ , e quindi  $f(0) = (u^{-1}g)(0) = u^{-1}(g(0)) = u^{-1}(1) = 0$ . Pertanto  $f \in H$  e  $g = (uu^{-1})g = u(u^{-1}g) = uf \in uH$ .

Analogamente si ha che  $Hu = \{fu \mid f \in S(\mathbb{R}), f(0) = 0\}$  coincide con l'insieme  $\{g \mid g \in S(\mathbb{R}), g(-1) = 0\}$ . Infatti se  $fu \in Hu$ , con  $f \in S(\mathbb{R})$  e  $f(0) = 0$ , allora  $fu(-1) = f(0) = 0$ . Viceversa sia  $g \in S(\mathbb{R})$  tale che  $g(-1) = 0$ . Si osservi che dato che  $u(-1) = 0$ , si deve avere  $u^{-1}(0) = -1$ , e quindi  $gu^{-1}(0) = g(-1) = 0$ . Pertanto  $gu^{-1} \in H$ , da cui  $g = gu^{-1}u \in Hu$ .

Abbiamo così dimostrato che  $uH = \{g \mid g \in S(\mathbb{R}), g(0) = 1\}$  e  $Hu = \{g \mid g \in S(\mathbb{R}), g(-1) = 0\}$ . Ne segue che  $uH \neq Hu$ . Ad esempio la funzione  $g: \mathbb{R} \rightarrow \mathbb{R}$  definita da  $g(x) = -x + 1$  per ogni  $x \in \mathbb{R}$  appartiene a  $uH$  (perché  $g(0) = 1$ ), ma non appartiene ad  $Hu$  (perché  $g(-1) = 2$ ). In particolare  $H$  non è un sottogruppo normale di  $S(\mathbb{R})$ .  $\square$

**24.2.** Siano  $n$  ed  $m$  interi positivi e siano  $C_n$  e  $C_m$  i gruppi delle radici  $n$ -esime e delle radici  $m$ -esime dell'unità rispettivamente (si veda l'esempio 8 del capitolo 21). Si dimostri che  $C_n \subseteq C_m$  se e solo se  $n \mid m$ . Se  $C_n \subseteq C_m$  si calcoli l'indice  $[C_m : C_n]$ .

**Soluzione.** Si ha  $C_n \subseteq C_m$  se e solo se i vertici dell' $n$ -agone regolare inscritto nella circonferenza  $\mathcal{C}$  di centro 0 e raggio 1 e avente un vertice nel punto  $(1, 0)$  sono anche vertici dell' $m$ -agone regolare inscritto in  $\mathcal{C}$  e con un vertice nel punto  $(1, 0)$ . Ovviamente questo può accadere se e solo se  $n \mid m$ . In tal caso, cioè se  $C_n \subseteq C_m$ , si ha che  $[C_m] = [C_m : C_n][C_n]$ , e quindi  $[C_m : C_n] = \frac{[C_m]}{[C_n]} = \frac{m}{n}$ .  $\square$

### Altri esercizi

**24.3.** Sia  $\mathbb{C}^*$  il gruppo moltiplicativo dei numeri complessi non nulli e sia  $T$  il sottogruppo di  $\mathbb{C}^*$  i cui elementi sono i numeri complessi di modulo 1. Si dimostri che per ogni numero complesso  $z \in \mathbb{C}^*$ , la classe laterale sinistra  $zT$  è l'insieme dei numeri complessi aventi modulo uguale al modulo di  $z$ , cioè è l'insieme dei numeri complessi che rappresentano nel piano di Argand-Gauss stanno sulla circonferenza avente come centro l'origine e passante per  $z$ . Si noti che le classi laterali formano una partizione di  $\mathbb{C}^*$ .

**24.4.** Sia  $\mathbb{R}^*$  il gruppo moltiplicativo dei numeri complessi non nulli; si consideri il sottogruppo  $H = \{1, -1\}$  di  $\mathbb{R}^*$ . Si dimostri che per ogni numero reale  $\alpha \in \mathbb{R}^*$ , la classe laterale sinistra  $\alpha H$  è l'insieme  $\{\alpha, -\alpha\}$ . Si noti che anche in questo caso le classi laterali sinistre formano una partizione di  $\mathbb{R}^*$ .

**24.5.** Sia  $f: G \rightarrow G'$  un omomorfismo di gruppi e sia  $H'$  un sottogruppo di  $G'$ .

- Può essere che  $f^{-1}(H') = \emptyset$ ?
- Se  $C$  è una classe laterale sinistra di  $G'$  modulo  $H'$ , può essere che  $f^{-1}(C) = \emptyset$ ?

24.6. Sia  $S_{10}$  il gruppo simmetrico su dieci oggetti e

$$H = \{ f \mid f \in S_{10}, f(10) = 10 \}.$$

- Si dimostri che  $H$  è un sottogruppo di  $S_{10}$ .
- Si dimostri che il gruppo  $H$  è isomorfo al gruppo simmetrico su nove oggetti  $S_9$ .
- Si calcoli l'indice  $[S_{10} : H]$ .

24.7. Sia  $S_8$  il gruppo simmetrico su 8 oggetti e sia

$$H = \{ f \in S_8 \mid f(4) = 4 \}.$$

- Si verifichi che  $H$  è un sottogruppo di  $S_8$ .
  - Il sottogruppo  $H$  è un sottogruppo normale di  $S_8$ ?
- 24.8. Siano  $n \geq 2$  un numero intero,  $S_n$  il gruppo delle permutazioni dell'insieme  $X_n = \{1, 2, 3, \dots, n\}$ , e  $G = \{ f \mid f \in S_n, f(\{1, 2\}) \subseteq \{1, 2\} \}$ .
- Si dimostri che  $G$  è un sottogruppo di  $S_n$ .
  - Si calcoli l'ordine di  $G$ .
  - Se  $H$  è un sottogruppo di  $G$  di ordine 2, si calcoli l'indice  $[G : H]$ .

24.9. Sia  $G$  un gruppo e sia  $H_n$  un sottogruppo di  $G$  per ogni  $n \in \mathbb{N}$ . Supponiamo che  $H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots$ . Sia  $H = \bigcup_{n \in \mathbb{N}} H_n$ . Si dimostri che:

- $H$  è un sottogruppo di  $G$ ;
- se  $H_n$  è un sottogruppo normale di  $G$  per ogni  $n \in \mathbb{N}$ , allora  $H$  è un sottogruppo normale di  $G$ .

24.10. Sia  $G = \mathbb{Q}^* \times \mathbb{Q}$  il prodotto cartesiano degli insiemi  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  e  $\mathbb{Q}$ . Su  $G$  si definisca un'operazione ponendo

$$(\alpha, x)(\beta, y) = (\alpha\beta, x\beta + y) \quad \text{per ogni } (\alpha, x), (\beta, y) \in \mathbb{Q}^* \times \mathbb{Q}.$$

- Si provi che  $G$  è un gruppo.
- Il gruppo  $G$  è abeliano?
- La proiezione sul secondo fattore  $\pi_2 : \mathbb{Q}^* \times \mathbb{Q} \rightarrow \mathbb{Q}$  definita da  $\pi_2(\alpha, x) = x$  per ogni  $(\alpha, x) \in G$  è un omomorfismo del gruppo  $G$  nel gruppo  $(\mathbb{Q}, +)$ ?
- Il sottoinsieme  $H = \mathbb{Q}^* \times \{0\}$  di  $G$  è un sottogruppo normale di  $G$ ?

24.11. Sia  $G$  un gruppo. Per ogni  $x \in G$  si ponga

$$C(x) = \{ g \mid g \in G, gx = xg \}.$$

- Si dimostri che  $C(x)$  è un sottogruppo di  $G$  per ogni  $x \in G$ .

- Nell'insieme  $G$  si definisca una relazione  $\sim$  ponendo, per ogni  $x, y \in G$ ,  $x \sim y$  se esiste  $g \in G$  ( $g$  dipendente da  $x$  e da  $y$ ) tale che  $g^{-1}xg = y$ . Si provi che  $\sim$  è una relazione di equivalenza in  $G$ .
- Per ogni elemento  $x \in G$  si denoti con  $[x]_{\sim}$  la classe di equivalenza di  $x$ . Sia  $D_x = \{ C(x)g \mid g \in G \}$  l'insieme di tutte le classi laterali destre di  $G$  modulo  $C(x)$ , e si definisca  $\varphi : D_x \rightarrow [x]_{\sim}$  ponendo  $\varphi(C(x)g) = g^{-1}xg$  per ogni  $g \in G$ . Si provi che l'applicazione  $\varphi$  è ben definita.
- Si dimostri che  $\varphi$  è una biiezione.
- Si dimostri che se  $G$  è un gruppo finito e  $x \in G$ , allora  $[x]_{\sim}$  divide  $|G|$ .
- Si dimostri che se  $G$  è un gruppo finito e  $x \in G$ , allora  $[x]_{\sim}$  divide  $|G|$ .

[Suggerimento: dedurre (e) da (d) e dalla dimostrazione del teorema di Lagrange.]

24.12. Si consideri il gruppo abeliano additivo  $\mathbb{Z}$ .

- Se  $\sim$  è una relazione di equivalenza su  $\mathbb{Z}$  compatibile con l'operazione  $+$ , allora per la proposizione 22.1  $\sim$  deve essere la congruenza  $\equiv$  modulo  $n$  per qualche  $n \in \mathbb{N}$ . Si determini il sottogruppo  $[0]_{\equiv}$  di  $\mathbb{Z}$  corrispondente a  $\equiv$ .
- Se  $N$  è un sottogruppo di  $\mathbb{Z}$ , allora come si è visto nell'esempio 6 del capitolo 21 esiste  $n \in \mathbb{N}$  tale che  $N = n\mathbb{Z}$ . Se  $\sim_N$  è definita per ogni  $a, b \in \mathbb{Z}$  da  $a \sim_N b$  se  $b - a \in N$ , qual è la relazione di equivalenza  $\sim_N$  su  $\mathbb{Z}$  compatibile con l'addizione?

24.13. Si dimostri che se  $G$  è un gruppo ed  $N$  è un sottogruppo normale di  $G$ , allora  $|G/N| = [G : N]$ .

24.14. Si consideri il gruppo  $(\mathbb{Q}/\mathbb{Z}, +)$ .

- Si dimostri che per ogni elemento  $x \in \mathbb{Q}/\mathbb{Z}$  esiste  $t \in \mathbb{N}^*$  tale che  $tx = 0$ .
- Siano  $a, b$  due numeri interi non nulli primi tra loro. Se  $x$  è l'elemento  $\frac{a}{b} + \mathbb{Z}$  di  $\mathbb{Q}/\mathbb{Z}$ , si calcoli il più piccolo numero naturale  $t \in \mathbb{N}^*$  tale che  $tx = 0$ .

## Capitolo 25. Omomorfismi di gruppi

Se  $f: G \rightarrow G'$  è un omomorfismo di gruppi, il nucleo di  $f$  è l'insieme  $f^{-1}(1_{G'}) = \{g \in G, f(g) = 1_{G'}\}$ . Lo si indica con  $\ker f$ .

LEMMA 25.1. Il nucleo  $\ker f$  di un omomorfismo di gruppi  $f: G \rightarrow G'$  è un sottogruppo normale di  $G$ .

ESEMPIO 1. Consideriamo l'applicazione  $\mu: C^* \rightarrow \mathbb{R}^*$  definita da  $\mu(z) = |z|$  per ogni  $z \in C^*$ . L'applicazione  $\mu$  è un omomorfismo del gruppo  $(C^*, \cdot)$  nel gruppo  $(\mathbb{R}^*, \cdot)$ , perché per ogni  $z, z' \in C^*$  si ha  $\mu(zz') = |zz'| = |z||z'| = \mu(z)\mu(z')$ . Il nucleo di  $\mu$  è

$$\ker \mu = \{z \in C^*, \mu(z) = 1\} = \{z \in C^*, |z| = 1\},$$

che è il sottogruppo di  $C^*$  che avevamo già incontrato nell'esempio 7 del capitolo 21, dove era stato indicato con  $T$ .  $\square$

ESEMPIO 2. Sia  $G$  un gruppo,  $N$  un sottogruppo normale di  $G$  e  $\pi: G \rightarrow G/N$  la proiezione canonica di  $G$  nel gruppo quoziente  $G/N$ . Abbiamo già osservato che  $\pi$  è un omomorfismo di gruppi. Calcoliamone il nucleo. Si ha

$$\begin{aligned} \ker \pi &= \{g \in G, \pi(g) = 1_{G/N}\} = \\ &= \{g \in G, gN = N\} = \{g \in G, g \in N\} \end{aligned}$$

(si veda l'osservazione dopo l'esempio 2 del capitolo 24). Quindi  $\ker \pi = N$ .  $\square$

LEMMA 25.2. Un omomorfismo di gruppi  $f: G \rightarrow G'$  è iniettivo se e solo se  $\ker f = \{1_G\}$ .

TEOREMA 25.3 (TEOREMA FONDAMENTALE DI OMOMORFISMO PER I GRUPPI). Siano  $G, G'$  gruppi ed  $f: G \rightarrow G'$  un omomorfismo di gruppi. Se  $\ker f$  è il nucleo di  $f$  e  $\pi: G \rightarrow G/\ker f$  è la proiezione canonica, allora:

- (a) esiste un'unica applicazione  $\tilde{f}: G/\ker f \rightarrow G'$  che rende commutativo il diagramma

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \searrow & & \nearrow \tilde{f} \\ & G/\ker f & \end{array}$$

- cioè tale che  $\tilde{f} \circ \pi = f$ ;
- (b)  $\tilde{f}$  è un omomorfismo iniettivo di gruppi;
- (c)  $\tilde{f}$  è un isomorfismo se e solo se  $f$  è suriettivo.

PROPOSIZIONE 25.4. Sia  $f: G \rightarrow G'$  un omomorfismo di gruppi. Allora:

- (a) se  $H$  è un sottogruppo di  $G$ ,  $f(H)$  è un sottogruppo di  $G'$ ;
- (b) se  $H'$  è un sottogruppo di  $G'$ ,  $f^{-1}(H')$  è un sottogruppo di  $G$ ;
- (c) se  $H$  è un sottogruppo di  $G$ , allora

$$f^{-1}(f(H)) = H \cdot \ker(f) = \{ab \mid a \in H, b \in \ker(f)\};$$

- (d) se  $H'$  è un sottogruppo di  $G'$ , allora  $f(f^{-1}(H')) = H' \cap f(G)$ .

Dimostrazione. (a) Esercizio lasciato al lettore.

(b) Dato che  $f(1_G) = 1_{G'} \in H'$ , si ha che  $1_G \in f^{-1}(H')$ . Quindi  $f^{-1}(H') \neq \emptyset$ . Se poi  $a, b \in f^{-1}(H')$ , allora  $f(a), f(b) \in H'$ , da cui  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} \in H'$ , e quindi  $ab^{-1} \in f^{-1}(H')$ . Per il lemma 21.4 questo dimostra che  $f^{-1}(H') \leq G$ .

(c) Sia  $x \in f^{-1}(f(H))$ . Allora  $f(x) \in f(H)$ , e quindi  $f(x) = f(h)$  per qualche  $h \in H$ . Ma allora  $f(h^{-1}x) = f(h^{-1})f(x) = (f(h))^{-1}f(x) = (f(h))^{-1}f(h) = 1_{G'}$ , e quindi  $h^{-1}x \in \ker f$ . Quindi  $h^{-1}x = k$  per qualche  $k \in \ker f$ . Moltiplicando a sinistra per  $h$  si ottiene che  $x = hk$  appartiene a  $H \cdot \ker f$ .

Viceversa sia  $x \in H \cdot \ker f$ . Allora  $x = hk$  per opportuni elementi  $h \in H$ ,  $k \in \ker f$ . Ne segue che  $f(x) = f(hk) = f(h)f(k) = f(h) \cdot 1_{G'} = f(h) \in f(H)$ , e quindi  $x \in f^{-1}(f(H))$ .

(d) Questa uguaglianza vale per ogni applicazione  $f: G \rightarrow G'$  tra due insiemi arbitrari  $G$  e  $G'$  e ogni sottoinsieme  $H'$  di  $G'$ . Questo è stato visto nell'esercizio 2.13, la cui soluzione si trova nell'Appendice B.  $\square$

COROLLARIO 25.5. Se  $f: G \rightarrow G'$  è un omomorfismo di gruppi, allora  $G/\ker(f)$  ed  $f(G)$  sono gruppi isomorfi.

ESEMPIO 3. Consideriamo l'omomorfismo  $\text{sgn}: S_n \rightarrow \{1, -1\}$ . Il nucleo di  $\text{sgn}$  è  $\ker \text{sgn} = \{f \in S_n \mid \text{sgn}(f) = 1\}$ , ossia il sottogruppo di tutte le permutazioni di  $S_n$  di classe pari. Tale sottogruppo è detto il sottogruppo alterno di  $S_n$ , e in genere lo si denota con  $A_n$ . Essendo  $A_n$  il nucleo dell'omomorfismo  $\text{sgn}$ , il sottogruppo  $A_n$  è normale in  $S_n$  per il lemma 25.1. Inoltre osservato che per  $n \geq 2$  l'omomorfismo  $\text{sgn}$  è suriettivo, ossia  $\text{sgn}(S_n) = \{1, -1\}$ , dal corollario 25.5 si deduce che i gruppi  $S_n/A_n$  e  $\{1, -1\}$  sono isomorfi per ogni  $n \geq 2$ .  $\square$





Sia  $\langle X \rangle$  il sottogruppo di  $G$  generato da  $X$ , e  $[X \cup X^{-1}]$  il sottomonoido di  $G$  generato da  $X \cup X^{-1}$ . Si dimostri che  $\langle X \rangle = [X \cup X^{-1}]$ . (Quindi gli elementi di  $\langle X \rangle$  sono i prodotti di un numero finito di elementi che o stanno in  $X$  oppure i cui inversi stanno in  $X$ .)

- (c) Se  $g$  è un elemento di un gruppo  $G$ , si dimostri che il sottogruppo ciclico di  $G$  generato da  $g$  è l'insieme delle potenze di  $g$  a esponente intero, cioè  $\langle g \rangle = \{g^z \mid z \in \mathbb{Z}\}$ .

**Soluzione.** (a) Si ha che  $1_G \in G_\lambda$  per ogni  $\lambda \in \Lambda$ , e quindi  $1_G \in \bigcap_{\lambda \in \Lambda} G_\lambda$ . In particolare  $\bigcap_{\lambda \in \Lambda} G_\lambda \neq \emptyset$ .

Siano  $x, y \in \bigcap_{\lambda \in \Lambda} G_\lambda$ . Allora  $x, y \in G_\lambda$  per ogni  $\lambda \in \Lambda$ . Dato che tutti i  $G_\lambda$  sono sottogruppi di  $G$  ne segue che  $xy^{-1} \in G_\lambda$  per ogni  $\lambda \in \Lambda$ . Quindi  $xy^{-1} \in \bigcap_{\lambda \in \Lambda} G_\lambda$ . Abbiamo così dimostrato che  $\bigcap_{\lambda \in \Lambda} G_\lambda$  è un sottogruppo di  $G$  (lemma 21.4).

(b) Per dimostrare che  $\langle X \rangle = [X \cup X^{-1}]$  si deve dimostrare che  $[X \cup X^{-1}]$  è il più piccolo sottogruppo di  $G$  che contiene  $X$ . Questo è ovvio se  $X = \emptyset$  (in questo caso sia  $\langle X \rangle$  che  $[X \cup X^{-1}]$  sono uguali a  $\{1_G\}$ ), e quindi supporremo  $X \neq \emptyset$ . Si osservi che

$$[X \cup X^{-1}] = \{1_G, x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X \cup X^{-1}\} = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\}.$$

Per far vedere che questo è il più piccolo sottogruppo di  $G$  che contiene  $X$  dobbiamo dimostrare (1) che  $[X \cup X^{-1}]$  è un sottogruppo di  $G$ , (2) che  $[X \cup X^{-1}]$  contiene  $X$ , (3) che se  $H$  è un qualunque sottogruppo di  $G$  e  $H \supseteq X$  allora  $H \supseteq [X \cup X^{-1}]$ .

(1) Per mostrare che  $[X \cup X^{-1}]$  è un sottogruppo di  $G$ , si osservi intanto che  $[X \cup X^{-1}] \neq \emptyset$ . Inoltre se  $x, y$  sono due elementi di  $[X \cup X^{-1}]$ , allora  $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$  e  $y = y_1^{\eta_1} y_2^{\eta_2} \dots y_m^{\eta_m}$ , dove  $x_i, y_j \in X$  ed  $\varepsilon_i, \eta_j$  sono 1 o -1 per tutti gli  $i$  e tutti i  $j$ . Pertanto anche

$$xy^{-1} = (x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}) (y_1^{\eta_1} y_2^{\eta_2} \dots y_m^{\eta_m})^{-1} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} y_m^{-\eta_m} y_{m-1}^{-\eta_{m-1}} \dots y_2^{-\eta_2} y_1^{-\eta_1}$$

è un elemento di  $[X \cup X^{-1}]$ . Questo dimostra che  $[X \cup X^{-1}]$  è un sottogruppo di  $G$ .

(2) è evidente.

(3) Sia  $H$  un qualunque sottogruppo di  $G$  tale che  $H \supseteq X$ . Dimostriamo che  $H \supseteq [X \cup X^{-1}]$ . Sia  $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$  un qualunque elemento di  $[X \cup X^{-1}]$  con gli  $x_i \in X$  e gli  $\varepsilon_i$  uguali a 1 o a -1. Dato che  $X \subseteq H$ , si ha  $x_i \in H$  per ogni  $i$ , e dato che  $H$  è un sottogruppo di  $G$  si ha che  $x_i^{\varepsilon_i} \in H$  sia se  $\varepsilon_i = 1$  che se  $\varepsilon_i = -1$ . Ne segue che il loro prodotto  $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$  appartiene ad  $H$ . Abbiamo così

dimostrato che  $[X \cup X^{-1}]$  è contenuto in ogni sottogruppo  $H$  di  $G$  che contiene  $X$ . Quindi  $[X \cup X^{-1}]$  è il più piccolo sottogruppo di  $G$  che contiene  $X$ .

(c) Per quanto visto in (b) si ha

$$\begin{aligned} \langle g \rangle &= \langle \{g\} \rangle = \{ \{g\} \cup \{g\}^{-1} \} = \{ \{g, g^{-1}\} \} = \\ &= \{1_G, x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{g, g^{-1}\}\} = \\ &= \{1_G, g^{\varepsilon_1} g^{\varepsilon_2} \dots g^{\varepsilon_n} \mid n \in \mathbb{N}^*, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\} = \\ &= \{1_G, g^{\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_n} \mid n \in \mathbb{N}^*, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\} = \\ &= \{g^z \mid z \in \mathbb{Z}\}. \quad \square \end{aligned}$$

**25.3.** Sia  $C_n$  il gruppo delle radici  $n$ -esime dell'unità, sottogruppo del gruppo moltiplicativo  $C^*$  dei numeri complessi non nulli. Facendo uso dell'applicazione  $\varphi_n : C^* \rightarrow C^*$  definita da  $\varphi_n(x) = x^n$  per ogni  $x \in C^*$ , e applicando ad essa il teorema fondamentale di omomorfismo per i gruppi, si dimostri che  $C^*/C_n \cong C^*$  qualunque sia il numero naturale  $n \geq 1$ .

**Soluzione.** L'applicazione  $\varphi_n : C^* \rightarrow C^*$  definita da  $\varphi_n(x) = x^n$  per ogni  $x \in C^*$  è un endomorfismo del gruppo moltiplicativo  $C^*$ , in quanto per ogni  $x, y \in C^*$  si ha  $\varphi_n(xy) = (xy)^n = x^n y^n = \varphi_n(x) \varphi_n(y)$ .

Mostriamo che  $\varphi_n$  è suriettiva. Sia  $y \in C^*$ . Scrivendo  $y$  in forma trigonometrica si ha che  $y = \rho(\cos \alpha + i \sin \alpha)$  per opportuni  $\rho, \alpha \in \mathbb{R}$ ,  $\rho > 0$ . È facile verificare che per il numero complesso  $x = \sqrt[n]{\rho}(\cos(\alpha/n) + i \sin(\alpha/n))$  si ha allora  $\varphi_n(x) = x^n = (\sqrt[n]{\rho}(\cos(\alpha/n) + i \sin(\alpha/n)))^n = \rho(\cos \alpha + i \sin \alpha) = y$ . Quindi  $\varphi_n$  è suriettiva.

Applicando il teorema fondamentale di omomorfismo per i gruppi all'omomorfismo suriettivo  $\varphi_n : C^* \rightarrow C^*$  si ottiene che esiste un isomorfismo di gruppi  $\tilde{\varphi}_n : C^*/\ker \varphi_n \rightarrow C^*$ . Ma

$$\ker \varphi_n = \{x \in C^* \mid \varphi_n(x) = 1\} = \{x \in C^* \mid x^n = 1\} = C_n.$$

Quindi  $C^*/C_n = C^*/\ker \varphi_n \cong C^*$ .  $\square$

### Altri esercizi

**25.4.** Sia  $(G, \cdot)$  un gruppo e sia  $(\text{Aut}(G), \circ)$  il gruppo degli automorfismi di  $G$ , cioè l'insieme di tutti gli automorfismi di  $G$  dotato, come operazione, della composizione di applicazioni  $\circ$ . Osservato che l'identità del gruppo  $\text{Aut}(G)$  è l'applicazione identica  $\iota_G$  di  $G$ , si consideri il prodotto cartesiano  $L = G \times \text{Aut}(G)$  e si definisca un'operazione  $*$  in  $L$  ponendo  $(x, \varphi) * (y, \psi) = (x\varphi(y), \varphi \circ \psi)$  per ogni  $(x, \varphi), (y, \psi) \in L$ . Si provi che:

- (a) l'insieme  $L$  è un gruppo rispetto all'operazione  $*$ ;  
(b) il sottoinsieme  $G \times \{\iota_G\}$  di  $L$  è un sottogruppo normale di  $L$ ;

(c) la proiezione canonica  $\pi_2 : L \rightarrow \text{Aut}(G)$ , definita da  $\pi_2(x, \varphi) = \varphi$  per ogni  $(x, \varphi) \in L$ , è un omomorfismo di gruppi avente come nucleo  $G \times \{1_G\}$ .  
[Suggerimento per (a): dimostrare che  $1_L = (1_G, 1_G)$  e che  $(x, \varphi)^{-1} = ((\varphi^{-1}(x))^{-1}, \varphi^{-1})$ .]

25.5. Sia  $(Q, +)$  il gruppo dei numeri razionali,  $Z$  il sottogruppo dei numeri interi e  $Q/Z$  il gruppo quoziente. Si definisca  $\varphi : Q \rightarrow Q/Z$  ponendo  $\varphi(x) = 3x + Z$  per ogni  $x \in Q$ . Si dimostri che

- (a) l'applicazione  $\varphi$  è un omomorfismo di gruppi;
- (b) l'applicazione  $\varphi$  è suriettiva;
- (c) il nucleo di  $\varphi$  è un sottogruppo di  $Q$  contenente  $Z$ ;
- (d) il gruppo  $\ker \varphi / Z$  ha ordine 3.

25.6. Siano  $(R^*, \cdot)$  il gruppo moltiplicativo dei numeri reali non nulli,  $H$  il suo sottogruppo  $\{\frac{1}{2^z} \mid z \in \mathbb{Z}\}$  e  $R^*/H$  il gruppo quoziente. Si ponga  $\varphi(xH) = x^2H$  per ogni  $x \in R^*$ . Si dimostri che

- (a) l'applicazione  $\varphi : R^*/H \rightarrow R^*/H$  è ben definita;
- (b) l'applicazione  $\varphi$  è un endomorfismo del gruppo  $R^*/H$ ;
- (c) il nucleo di  $\varphi$  è un sottogruppo di  $R^*/H$  di ordine 2.

25.7. Per ogni gruppo  $G$  e ogni sottoinsieme  $X$  di  $G$  si ponga

$$C_G(X) = \{g \in G \mid gx = xg \text{ per ogni } x \in X\}.$$

- (a) Si dimostri che  $C_G(X)$  è un sottogruppo normale di  $G$ .  
Se  $N$  è un sottogruppo di  $G$  e  $g$  è un elemento di  $G$ , si ponga  $\sigma_g(a) = g^{-1}ag$  per ogni  $a \in N$ .
- (b) Tale posizione definisce un'applicazione  $\sigma_g : N \rightarrow N$  per ogni  $g \in G$  se e solo se il sottogruppo  $N$  di  $G$  è normale. Si spieghi il perché.

Nel seguito dell'esercizio supporremo sempre  $N$  sottogruppo normale di  $G$ .

- (c) Si provi che  $\sigma_g$  è un automorfismo di  $N$ .
- (d) Sia  $\text{Aut}(N)$  il gruppo degli automorfismi di  $N$  con l'operazione di composizione di applicazioni o. Si provi che l'applicazione  $\varphi : G \rightarrow \text{Aut}(N)$  definita da  $\varphi(g) = \sigma_g$  per ogni  $g \in G$  è un omomorfismo di gruppi.
- (e) Si dimostri che  $\ker \varphi = C_G(N)$ .

25.8. Siano  $G$  un gruppo e  $\iota_G : G \rightarrow G$  l'applicazione identica di  $G$ . Qual è il nucleo di  $\iota_G$ ? Nella notazione dell'enunciato del teorema fondamentale di omomorfismo per i gruppi, come è definito l'omomorfismo  $\tilde{\iota}_G : G/\{1_G\} \rightarrow G$ ? L'omomorfismo  $\tilde{\iota}_G : G/\{1_G\} \rightarrow G$  è un isomorfismo? Se ne deduca che  $G/\{1_G\} \cong G$ .

25.9. Per ogni gruppo abeliano  $(G, \cdot)$  si definisca

$$t(G) = \{x \in G \mid \text{esiste } n \in \mathbb{N}, n > 0 \text{ tale che } x^n = 1_G\}.$$

- (a) Si dimostri che  $t(G)$  è un sottogruppo di  $G$ .
- (b) Si dimostri che  $t(G/t(G)) = \{1_{G/t(G)}\}$  per ogni gruppo abeliano  $G$ .
- (c) Se  $Q^*$  è il gruppo moltiplicativo dei numeri razionali non nulli si calcoli  $t(Q^*)$ .
- (d) Se  $R$  è il gruppo additivo dei numeri reali si calcoli  $t(R)$ .
- (e) Si dimostri che  $Q^*/t(Q^*) \cong Q^+$ , ove  $Q^+$  è il gruppo moltiplicativo dei numeri razionali positivi.

[Suggerimento per (e): Applicare il teorema fondamentale di omomorfismo per i gruppi all'omomorfismo  $\varphi : Q^* \rightarrow Q^+$  definito da  $\varphi(x) = |x|$  per ogni  $x \in Q^*$ .]

25.10. Sia  $z_h = \cos(\pi h/6) + i \sin(\pi h/6)$  per ogni  $h \in \mathbb{Z}$ . Sia

$$C_{12} = \{z \in \mathbb{C} \mid z^{12} = 1\} = \{z_h \mid h \in \mathbb{Z}\}$$

il gruppo moltiplicativo delle radici dodicesime dell'unità. Si consideri l'applicazione  $\varphi : \mathbb{Z} \rightarrow C_{12}$  definita da  $\varphi(h) = z_h$  per ogni  $h \in \mathbb{Z}$ .

- (a) Si provi che l'applicazione  $\varphi$  è un omomorfismo del gruppo  $(\mathbb{Z}, +)$  nel gruppo  $(C_{12}, \cdot)$ .
- (b) Si calcoli il nucleo di  $\varphi$ .
- (c) Si dimostri che i gruppi  $C_{12}$  e  $\mathbb{Z}/12\mathbb{Z}$  sono isomorfi.

25.11. Sia  $C_4 = \{z \in \mathbb{C} \mid z^4 = 1\}$  il gruppo moltiplicativo delle radici quarte dell'unità. Si consideri l'applicazione  $\varphi : \mathbb{Z} \rightarrow C_4$  definita da  $\varphi(t) = i^t$  per ogni  $t \in \mathbb{Z}$ .

- (a) Si dimostri che l'applicazione  $\varphi$  è un omomorfismo suriettivo del gruppo  $(\mathbb{Z}, +)$  nel gruppo  $(C_4, \cdot)$ .
- (b) Si determini  $n \in \mathbb{N}$  tale che  $\ker \varphi = n\mathbb{Z}$ .
- (c) Se  $n$  è il numero naturale determinato in (b) si dimostri che i gruppi  $C_4$  e  $\mathbb{Z}/n\mathbb{Z}$  sono isomorfi.

25.12. Siano  $G$  un gruppo ed  $M \supseteq N$  due sottogruppi normali di  $G$ . Si dimostri che  $M/N$  è un sottogruppo normale di  $G/N$  e che i gruppi  $G/M$  e  $(G/N)/(M/N)$  sono isomorfi.

[Suggerimento: applicare il teorema fondamentale di omomorfismo all'applicazione  $\pi : G/N \rightarrow G/M$  definita da  $\pi(gN) = gM$  per ogni  $g \in G$ .]

25.13. Siano  $S_n$  e  $A_n$  il gruppo simmetrico su  $n$  oggetti e il sottogruppo alterno rispettivamente.

- (a) Si dimostri che se  $n \geq 2$  allora  $S_n/A_n \cong \{1, -1\}$ .

- (b) Si calcoli l'ordine di  $A_n$ .  
 (c) Si calcoli l'indice  $[S_n : A_n]$ .

[Suggerimento: in (b) e (c) distinguere i casi  $n = 1$  e  $n \geq 2$ .]

- 25.14. Si dimostri che se  $G$  e  $H$  sono gruppi ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora  $[G : \ker f] = |f(G)|$ .  
 25.15. Si dimostri che se  $G$  e  $H$  sono gruppi,  $H$  è finito ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora  $[G : \ker f]$  è finito e divide  $|H|$ .  
 25.16. Si dimostri che se  $G$  e  $H$  sono gruppi,  $G$  è finito ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora  $[G : \ker f]$  divide  $|G|$ .  
 25.17. Si dimostri che se  $G$  e  $H$  sono gruppi finiti,  $|G|$  e  $|H|$  sono primi tra loro, ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora  $f(x) = 1_H$  per ogni  $x \in G$ .  
 25.18. Si dimostri che se  $G$  e  $H$  sono gruppi,  $G$  è finito ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora  $|f(G)|$  è finito e divide  $|G|$ .  
 25.19. Si dimostri che se  $G$  e  $H$  sono gruppi finiti,  $|H|$  è un numero primo, ed  $f : G \rightarrow H$  è un omomorfismo di gruppi, allora si ha uno dei seguenti due casi:  
 (a)  $f(x) = 1_H$  per ogni  $x \in G$ , oppure  
 (b) l'omomorfismo  $f$  è suriettivo e  $|H|$  è un fattore primo di  $|G|$ .  
 25.20. Si dimostri che ogni gruppo ciclico (vedi esercizio 25.2) è isomorfo a  $\mathbb{Z}/n\mathbb{Z}$  per qualche  $n \in \mathbb{N}$ .  
 [Suggerimento: ragionare come nella proposizione 22.4 sostituendo il gruppo  $(\mathbb{Z}, +)$  al monoide  $(\mathbb{N}, +)$ .]  
 25.21. È possibile dimostrare che l'insieme  $\mathbb{Z}^{\mathbb{N}}$  delle applicazioni di  $\mathbb{N}$  in  $\mathbb{Z}$  è un gruppo rispetto all'operazione  $+$  definita ponendo, per ogni  $f, g \in \mathbb{Z}^{\mathbb{N}}$  e ogni  $n \in \mathbb{N}$ ,  $(f+g)(n) = f(n) + g(n)$ . Sia  $H$  l'insieme degli  $f \in \mathbb{Z}^{\mathbb{N}}$  che sono omomorfismi di insiemi ordinati di  $(\mathbb{N}, \leq)$  in  $(\mathbb{Z}, \leq)$ , cioè l'insieme delle applicazioni  $f : \mathbb{N} \rightarrow \mathbb{Z}$  tali che  $f(n) \leq f(m)$  per ogni  $n, m \in \mathbb{N}$  con  $n \leq m$ .  
 (a) Si dica se  $H$  è un sottogruppo di  $(\mathbb{Z}^{\mathbb{N}}, +)$ .  
 (b) Si dica se  $H$  è un sottomonoide di  $(\mathbb{Z}^{\mathbb{N}}, +)$ .

Si consideri l'applicazione  $\varphi : \mathbb{Z}^{\mathbb{N}} \rightarrow \mathbb{Z}^{\mathbb{N}}$  definita da

$$\varphi(f)(n) = \sum_{i=0}^n f(i)$$

per ogni  $f \in \mathbb{Z}^{\mathbb{N}}$  e ogni  $n \in \mathbb{N}$ .

- (c) Si dimostri che  $\varphi$  è un endomorfismo del gruppo  $\mathbb{Z}^{\mathbb{N}}$ .  
 (d) Si dica se  $\varphi$  è un automorfismo di  $\mathbb{Z}^{\mathbb{N}}$ .

25.22. Sia  $\mathbb{Z}$  l'insieme dei numeri interi. Sull'insieme  $G = \mathbb{Z} \times \{1, -1\}$  si definisca un'operazione  $*$  ponendo, per ogni  $(a, x), (b, y) \in \mathbb{Z} \times \{1, -1\}$ ,

$$(a, x) * (b, y) = (a + xb, xy).$$

- (a) Si dimostri che  $G$  con questa operazione è un gruppo.  
 (b) Si dimostri che la proiezione canonica sul secondo fattore  $\pi_2 : \mathbb{Z} \times \{1, -1\} \rightarrow \{1, -1\}$  è un omomorfismo del gruppo  $G$  nel gruppo moltiplicativo  $\{1, -1\}$ .  
 (c) Si dimostri che  $H = \{(a, 1) \mid a \in \mathbb{Z}\}$  è un sottogruppo normale di  $G$ .  
 (d) Si calcoli l'indice  $[G : H]$ .

PARTE QUINTA  
INSIEMI DOTATI DI PIÙ OPERAZIONI

Capitolo 26. Anelli

Un insieme  $R$  dotato di due operazioni  $+$  e  $\cdot$  si dice un *anello* se sono soddisfatte le seguenti condizioni:

(a) (*associatività dell'addizione*):

$$(a + b) + c = a + (b + c) \quad \text{per ogni } a, b, c \in R;$$

(b) (*elemento neutro per l'addizione*): esiste un elemento  $z \in R$  tale che  $a + z = a$  per ogni  $a \in R$ ;

(c) (*inverso per l'addizione*): per ogni  $a \in R$  esiste  $b \in R$  tale che

$$a + b = z;$$

(d) (*commutatività dell'addizione*):  $a + b = b + a$  per ogni  $a, b \in R$ ;

(e) (*associatività della moltiplicazione*):

$$(ab)c = a(bc) \quad \text{per ogni } a, b, c \in R;$$

(f) (*distributività*): per ogni  $a, b, c \in R$  si ha

$$a(b + c) = ab + ac \quad \text{e} \quad (b + c)a = ba + ca.$$

Le operazioni  $+$  e  $\cdot$  si dicono *addizione* e *moltiplicazione* rispettivamente, e se  $a, b \in R$ ,  $a + b$  e  $ab$  si dicono la *somma* e il *prodotto* di  $a$  e  $b$ . Quando vorremo evidenziare le operazioni di addizione e di moltiplicazione su un anello scriveremo  $(R, +, \cdot)$ ; questo ci permetterà di essere più precisi quando su uno stesso insieme  $R$  saranno definite varie strutture d'anello, e quindi varie operazioni di addizione e moltiplicazione.



ESEMPIO 1. Gli insiemi  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$ , dotati delle operazioni usuali di addizione e moltiplicazione, sono anelli.  $\square$

ESEMPIO 2. Sia  $Z \times Z$  il prodotto cartesiano di  $Z$  per  $Z$ ; definiamo in  $Z \times Z$  l'addizione  $+$  e la moltiplicazione  $\circ$  ponendo  $(a, b) + (c, d) = (a + c, b + d)$  e  $(a, b) \circ (c, d) = (ac, ad + bc)$  per ogni  $(a, b), (c, d) \in Z \times Z$ . È facile verificare che sono soddisfatte le sei condizioni da (a) ad (f) sopra riportate. Ad esempio per ogni  $(a, b), (c, d), (e, f) \in Z \times Z$  si ha

$$\begin{aligned} (a, b) \circ ((c, d) + (e, f)) &= (a, b) \circ (c + e, d + f) = \\ &= (a(c + e), a(d + f) + b(c + e)) = \\ &= (ac + ae, ad + af + bc + be) \end{aligned}$$

$$\text{e} \quad (a, b) \circ (c, d) + (a, b) \circ (e, f) = (ac, ad + bc) + (ae, af + be) = (ac + ae, ad + af + bc + be),$$

da cui

$$(a, b) \circ ((c, d) + (e, f)) = (a, b) \circ (c, d) + (a, b) \circ (e, f),$$

che è la prima delle due proprietà distributive descritte in (f). Quindi  $(Z \times Z, +, \circ)$  è un anello.  $\square$

ESEMPIO 3. Come nell'esempio 2 sia  $Z \times Z$  il prodotto cartesiano di  $Z$  per  $Z$  e definiamo in  $Z \times Z$  l'addizione  $+$  ponendo  $(a, b) + (c, d) = (a + c, b + d)$ . Definiamo invece la moltiplicazione  $*$  ponendo  $(a, b) * (c, d) = (ac, bc)$ . Anche in questo caso è facile verificare che sono soddisfatte le condizioni (a)-(f). Quindi anche  $(Z \times Z, +, *)$  è un anello. L'anello  $(Z \times Z, +, *)$  è però diverso dall'anello  $(Z \times Z, +, \circ)$  descritto nell'esempio 2, in quanto le loro moltiplicazioni sono diverse.  $\square$

Si noti che se  $(R, +, \cdot)$  è un anello, allora  $(R, +)$  è un gruppo abeliano e  $(R, \cdot)$  è un semigruppato. Un anello  $(R, +, \cdot)$  si dice *commutativo* se  $ab = ba$  per ogni  $a, b \in R$ . (Si noti che l'addizione è sempre commutativa, qualunque sia l'anello  $R$ .) L'elemento  $z \in R$  tale che  $a + z = a$  per ogni  $a \in R$  è detto lo *zero* dell'anello, e lo si indica con  $0$  o con  $0_R$ ; naturalmente  $0_R$  è l'identità del gruppo additivo  $(R, +)$ . Se il semigruppato  $(R, \cdot)$  ha un'identità  $e_R \neq 0$ , allora  $e_R$  si dice l'*identità* dell'anello. Si osservi che affinché  $e_R$  sia l'identità dell'anello  $R$  sono necessarie due condizioni: che  $e_R a = a e_R = a$  per ogni  $a \in R$  (ossia che  $e_R$  sia l'identità del semigruppato moltiplicativo  $(R, \cdot)$ ) e che  $e_R \neq 0$ . Quindi ogni anello  $R$  con identità ha almeno due elementi distinti  $0_R$  ed  $e_R$ . L'identità dell'anello  $R$  viene denotata di solito con  $1$  o con  $1_R$ .

LEMMA 26.1. Sia  $R$  un anello, e siano  $a, b \in R$ . Allora

$$0a = a0 = 0 \quad \text{e} \quad (-a)b = a(-b) = -(ab).$$

Quindi l'opposto dell'elemento  $a$  moltiplicato per un elemento  $b$  è uguale all'opposto dell'elemento  $ab$ .

Dato che ogni anello è un gruppo abeliano rispetto all'addizione ed è un semigruppato rispetto alla moltiplicazione, per ogni elemento  $a$  di un anello è possibile definire il multiplo  $n$ -esimo  $na$  per ogni intero  $n$  e la potenza  $n$ -esima  $a^n$  per ogni intero positivo  $n$ .

ESEMPIO 4. Nell'anello  $(Z \times Z, +, *)$  dell'esempio 3 si ha

$$\begin{aligned} 3(2, 1) &= (2, 1) + (2, 1) + (2, 1) = (6, 3), \\ (-3)(2, 1) &= -(2, 1) + -(2, 1) + -(2, 1) = \\ &= (-2, -1) + (-2, -1) + (-2, -1) = (-6, -3) \end{aligned}$$

e

$$(2, 1)^3 = (2, 1) * (2, 1) * (2, 1) = (4, 2) * (2, 1) = (8, 4). \quad \square$$

ESEMPIO 5. Dimostriamo che l'anello  $(Z \times Z, +, \circ)$  dell'esempio 2 è commutativo: per ogni  $(a, b), (c, d) \in Z \times Z$  si ha  $(a, b) \circ (c, d) = (ac, ad + bc) = (ca, cb + da) = (c, d) \circ (a, b)$ . Invece l'anello  $(Z \times Z, +, *)$  dell'esempio 3 non è commutativo, in quanto  $(1, 1) * (0, 1) = (0, 0)$ , mentre  $(0, 1) * (1, 1) = (0, 1)$ .  $\square$

ESEMPIO 6. Tutti gli anelli dell'esempio 1 sono commutativi.  $\square$

ESEMPIO 7. Tutti gli anelli degli esempi 1 e 2 sono anelli con identità. L'identità degli anelli dell'esempio 1 è sempre il numero 1. L'identità dell'anello  $(Z \times Z, +, \circ)$  dell'esempio 2 è l'elemento  $(1, 0)$ , perché per ogni  $(a, b) \in Z \times Z$  si ha  $(a, b) \circ (1, 0) = (a \cdot 1, a \cdot 0 + b \cdot 1) = (a, b)$ . (Questo basta a dire che  $(1, 0)$  è l'identità dell'anello perché abbiamo già visto nell'esempio 5 che la moltiplicazione  $\circ$  è commutativa).  $\square$

Se  $R$  è un anello, un *sottoanello*  $S$  di  $R$  è un sottoinsieme  $S$  di  $R$  tale che  $(S, +)$  sia un sottogruppo di  $(R, +)$  ed  $(S, \cdot)$  sia un sottosemigruppato di  $(R, \cdot)$ . In tal caso  $S$ , con le operazioni indotte dalle operazioni di  $R$ , è un anello. Se  $R$  è un anello con identità  $1_R$ , si richiede anche che  $1_R$  appartenga ad  $S$  affinché  $S$  sia sottoanello di  $R$ . Quindi:

se  $R$  è un anello, un sottoinsieme  $S$  di  $R$  è un sottoanello di  $R$  se e solo se  $S \neq \emptyset$  e inoltre  $a - b, ab \in S$  per ogni  $a, b \in S$ ;

se  $R$  è un anello con identità, un sottoinsieme  $S$  di  $R$  è un sottoanello di  $R$  se e solo se  $1_R \in S$  e inoltre  $a - b, ab \in S$  per ogni  $a, b \in S$ .

ESEMPIO 8. Se si considerano gli anelli  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  dell'esempio 1, si ha che  $\mathbb{Z}$  è un sottoanello di  $\mathbb{Q}$ , di  $\mathbb{R}$  e di  $\mathbb{C}$ , l'anello  $\mathbb{Q}$  è un sottoanello di  $\mathbb{R}$  e di  $\mathbb{C}$ , e l'anello  $\mathbb{R}$  è un sottoanello di  $\mathbb{C}$ .  $\square$

ESEMPIO 9. Sia  $R = \mathbb{Z} \times \mathbb{Z}$  l'anello dell'esempio 2. Abbiamo visto nell'esempio 7 che  $R$  è un anello con identità  $1_R = (1, 0)$ . Si consideri il sottoinsieme  $S = \{(x, 0) \mid x \in \mathbb{Z}\} \subseteq R$ . Allora  $S$  è un sottoanello di  $R$  perché:

- (i)  $1_R = (0, 1) \in S$ ;
- (ii) per ogni  $(x, 0), (y, 0) \in S$  si ha  $(x, 0) - (y, 0) = (x - y, 0) \in S$ ;
- (iii) per ogni  $(x, 0), (y, 0) \in S$  si ha  $(x, 0) \circ (y, 0) = (xy, 0 + 0 \cdot y) = (xy, 0) \in S$ .  $\square$

Un elemento  $a \neq 0$  di un anello  $R$  è un *divisore dello zero* in  $R$  se esiste  $b \in R$ ,  $b \neq 0$  tale che  $ab = 0$  oppure  $ba = 0$ . Un *dominio di integrità* (o *dominio*, o *anello integro*) è un anello commutativo con identità privo di divisori dello zero. Quindi un anello commutativo  $R$  con identità è un dominio se e solo se per ogni  $a, b \in R$  si ha che  $ab = 0$  implica  $a = 0$  oppure  $b = 0$ .

ESEMPIO 10. Gli anelli  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  dell'esempio 1 sono tutti anelli commutativi con identità nei quali da  $ab = 0$  segue che  $a = 0$  oppure  $b = 0$ . Quindi  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  sono tutti domini di integrità.  $\square$

ESEMPIO 11. Nell'anello commutativo con identità  $\mathbb{Z} \times \mathbb{Z}$  dell'esempio 2 si ha  $(0, 1) \neq (0, 0)$  e  $(0, 1) \circ (0, 1) = (0, 0)$ . Quindi  $(0, 1)$  è un divisore dello zero in  $\mathbb{Z} \times \mathbb{Z}$  e  $\mathbb{Z} \times \mathbb{Z}$  non è un dominio di integrità. Mostriamo, più in generale che un elemento  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  è un divisore dello zero in  $\mathbb{Z} \times \mathbb{Z}$  se e solo se  $a = 0$  e  $b \neq 0$ . Se  $(a, b)$  è un divisore dello zero in  $\mathbb{Z} \times \mathbb{Z}$ , con  $a, b \in \mathbb{Z}$ , allora  $(a, b) \neq (0, 0)$  ed esiste  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  tale che  $(x, y) \neq (0, 0)$  e  $(a, b) \circ (x, y) = (0, 0)$  oppure  $(x, y) \circ (a, b) = (0, 0)$ . Dato che  $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$  è un anello commutativo, si ha quindi  $(a, b) \circ (x, y) = (0, 0)$ , ossia  $(ax, ay + bx) = (0, 0)$ . Abbiamo così ricavato il sistema

$$\begin{cases} (a, b) \neq (0, 0) \\ (x, y) \neq (0, 0) \\ ax = 0 \\ ay + bx = 0. \end{cases}$$

Se  $a \neq 0$  si ha quindi

$$\begin{cases} (x, y) \neq (0, 0) \\ x = 0 \\ ay + bx = 0, \end{cases}$$

da cui

$$\begin{cases} x = 0 \\ y \neq 0 \\ ay = 0. \end{cases}$$

Questa è una contraddizione, perché in  $\mathbb{Z}$  non si può avere  $a \neq 0$ ,  $y \neq 0$  e  $ay = 0$ . Quindi deve essere  $a = 0$ , e allora da  $(a, b) \neq (0, 0)$  si ottiene  $b \neq 0$ .

Viceversa se  $a = 0$  e  $b \neq 0$ , allora  $(a, b) \circ (0, 1) = (0, b) \circ (0, 1) = (0, 0)$ ,  $(a, b) \neq (0, 0)$  e  $(0, 1) \neq (0, 0)$ . Quindi  $(a, b)$  è un divisore dello zero in  $\mathbb{Z} \times \mathbb{Z}$ .  $\square$

Se  $R$  è un anello commutativo con identità, gli elementi invertibili del monoide  $(R, \cdot)$  si dicono gli elementi *invertibili* (o le *unità*) dell'anello  $R$ . Come abbiamo già visto nell'esempio 4 del capitolo 21, tali elementi formano un gruppo  $U(R)$ , detto il *gruppo degli elementi invertibili* (o *delle unità*) dell'anello  $R$ . Se  $a \in R$  è invertibile, il suo inverso si denota, come già visto per i monoidi, con  $a^{-1}$ .

Un *campo* (o *corpo*) è un anello commutativo con identità in cui ogni elemento *non nullo* è invertibile. Quindi un anello  $R$  commutativo con identità è un campo se e solo se  $U(R) = R \setminus \{0\}$ . Si osservi che  $0_R$  non è mai invertibile in nessun anello  $R$  con identità  $1_R$  (perché se  $0_R$  fosse invertibile e  $a \in R$  fosse il suo inverso allora  $0_R = 0_R \cdot a = 1_R$ , assurdo.)

LEMMA 26.2. Ogni campo è un dominio di integrità.

ESEMPIO 12. Consideriamo l'anello  $\mathbb{Z}$  degli interi. In  $\mathbb{Z}$  gli elementi invertibili sono solo 1 e -1, perché questi sono gli unici numeri interi  $x$  per i quali esiste un numero intero  $y$  tale che  $xy = 1$ . Quindi  $U(\mathbb{Z}) = \{1, -1\}$ ; in particolare  $\mathbb{Z}$  non è un campo. Avevamo però visto nell'esempio 10 che  $\mathbb{Z}$  è un dominio di integrità. Quindi  $\mathbb{Z}$  è un dominio di integrità che non è un campo.  $\square$

ESEMPIO 13. Gli anelli  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  sono campi.  $\square$

### Esercizi svolti

26.1. Sia  $(G, +)$  un gruppo abeliano, e sia  $\text{End}(G)$  l'insieme di tutti gli endomorfismi di  $G$ . Se  $f, f' \in \text{End}(G)$  definiamo

$$(f + f')(x) = f(x) + f'(x), \quad (f \circ f')(x) = f(f'(x)) \quad \text{per ogni } x \in G.$$

Si provi che  $(\text{End}(G), +, \circ)$  è un anello (detto l'anello degli endomorfismi di  $G$ ). Qual è l'identità di questo anello?

*Soluzione.* Si osservi innanzitutto che  $+$  e  $\circ$  sono effettivamente delle operazioni in  $\text{End}(G)$ , ossia che se  $f, f' \in \text{End}(G)$ , anche  $f + f', f \circ f' \in \text{End}(G)$ . Per dimostrare questo è sufficiente osservare che  $f + f'$  ed  $f \circ f'$  sono applicazioni di  $G$  in  $G$  e che per ogni  $x, y \in G$  si ha

$$\begin{aligned}(f + f')(x + y) &= f(x + y) + f'(x + y) = f(x) + f(y) + f'(x) + f'(y) = \\ &= f(x) + f'(x) + f(y) + f'(y) = (f + f')(x) + (f + f')(y)\end{aligned}$$

e

$$\begin{aligned}(f \circ f')(x + y) &= f(f'(x + y)) = f(f'(x) + f'(y)) = \\ &= f(f'(x)) + f(f'(y)) = (f \circ f')(x) + (f \circ f')(y).\end{aligned}$$

Quindi  $f + f'$  ed  $f \circ f'$  appartengono a  $\text{End}(G)$ .

Si deve poi dimostrare che tutte le condizioni dalla (a) alla (f) della definizione di anello sono soddisfatte. Mostriamolo per le ultime tre, lasciando la verifica delle altre al lettore:

(d) (commutatività dell'addizione): per ogni  $f, g \in \text{End}(G)$  e per ogni  $x \in G$  si ha  $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$ . Dato che questo vale per ogni  $x$  nel dominio  $G$  delle due applicazioni  $f + g$  e  $g + f$ , se ne deduce che  $f + g = g + f$ .

(e) (associatività della moltiplicazione): abbiamo già visto nel capitolo 3 che la composizione di applicazioni  $\circ$  è sempre associativa. La condizione (e) ne è un caso particolare.

(f) (distributività): per ogni  $f, g, h \in \text{End}(G)$  e per ogni  $x \in G$  si ha

$$\begin{aligned}(f \circ (g + h))(x) &= f((g + h)(x)) = f(g(x) + h(x)) = \\ &= f(g(x)) + f(h(x)) = (f \circ g)(x) + (f \circ h)(x) = \\ &= (f \circ g + f \circ h)(x).\end{aligned}$$

Dato che questo vale per ogni  $x$  nel dominio  $G$  delle due applicazioni  $f \circ (g + h)$  e  $f \circ g + f \circ h$ , se ne deduce che  $f \circ (g + h) = f \circ g + f \circ h$ . Analogamente  $(g + h) \circ f = g \circ f + h \circ f$ .

L'identità dell'anello  $(\text{End}(G), +, \circ)$  è l'applicazione identica  $\iota_G : G \rightarrow G$ . Infatti si ha  $\iota_G \in \text{End}(G)$  e  $\iota_G \circ f = f \circ \iota_G = f$  per ogni  $f \in \text{End}(G)$ .  $\square$

**26.2.** Si provi che se  $R$  è un anello e  $a, b \in R$ , allora  $(-a)(-b) = ab$ .

*Soluzione.* Applicando due volte il lemma 26.1 si ha  $(-a)(-b) = -(a(-b)) = -(-(ab))$ , e questo è uguale ad  $ab$  perché in un gruppo additivo si ha  $-(-x) = x$  (lemma 21.2).  $\square$

**26.3.** Si provi che ogni dominio di integrità finito, ossia ogni dominio di integrità con un numero finito di elementi, è un campo.

*Soluzione.* Sia  $R$  un dominio di integrità finito. Dobbiamo dimostrare che  $R$  è un campo, cioè che ogni elemento non nullo di  $R$  è invertibile in  $R$ . Sia  $a \in R$ ,  $a \neq 0$ ; si consideri l'applicazione  $\tau_a : R \rightarrow R$  definita da  $\tau_a(x) = ax$  per ogni  $x \in R$ . Mostriamo che  $\tau_a$  è iniettiva: se  $x, y \in R$  e  $\tau_a(x) = \tau_a(y)$ , allora  $ax = ay$ , da cui  $ax - ay = 0$ , e quindi, per la distributività,  $a(x - y) = 0$ . Ma  $R$  è un dominio di integrità ed  $a \neq 0$ , e quindi  $x - y = 0$ , ossia  $x = y$ . Questo dimostra che  $\tau_a : R \rightarrow R$  è iniettiva. Ma  $R$  è un insieme finito, e quindi  $\tau_a : R \rightarrow R$  è biiettiva. In particolare esiste  $b \in R$  tale che  $\tau_a(b) = 1_R$ , ove  $1_R$  denota l'identità di  $R$ . Ma allora  $ab = \tau_a(b) = 1_R$ , ed essendo  $R$  commutativo si ha anche che  $ba = 1_R$ . Quindi  $a$  è invertibile e  $b \in R$  è il suo inverso.  $\square$

**26.4.** Sia  $R$  un anello commutativo con identità. Si provi che  $R$  è un dominio di integrità se e solo se in  $R$  vale la proprietà di cancellazione, ossia per ogni  $a, b, c \in R$ ,  $ab = ac$  e  $a \neq 0$  implicano  $b = c$ .

*Soluzione.* Supponiamo che  $R$  sia un dominio di integrità. Siano  $a, b, c \in R$ , tali che  $ab = ac$  e  $a \neq 0$ . Allora  $ab - ac = 0$ , e quindi per la distributività  $a(b - c) = 0$ . Ma  $R$  è un dominio di integrità ed  $a \neq 0$ , e pertanto  $b - c = 0$ , ossia  $b = c$ .

Viceversa supponiamo che in  $R$  valga la proprietà di cancellazione, ossia che per ogni  $a, b, c \in R$ ,  $ab = ac$  e  $a \neq 0$  implicano  $b = c$ . Per dimostrare che  $R$  è un dominio si deve far vedere che  $ab = 0$  implica  $a = 0$  oppure  $b = 0$  per ogni  $a, b \in R$ . Sia  $ab = 0$ . Allora si ha  $0 \neq a$  oppure  $a = 0$ . Se  $a \neq 0$ , per la proprietà di cancellazione da  $ab = 0 = a \cdot 0$  si ricava  $b = 0$ . Se invece  $a = 0$  non c'è nulla da dimostrare. Quindi  $0 \neq a$  oppure  $b = 0$ .  $\square$

### Altri esercizi

**26.5.** Sia  $X$  un insieme non vuoto e sia  $R$  il campo dei numeri reali. Nell'insieme  $R^X = \{f \mid f : X \rightarrow R \text{ è un'applicazione}\}$  si definiscano l'addizione e la moltiplicazione ponendo per ogni  $f, g \in R^X$  e per ogni  $x \in X$

$$(f + g)(x) = f(x) + g(x) \quad \text{e} \quad (fg)(x) = f(x)g(x).$$

Si provi che  $(R^X, +, \cdot)$  è un anello commutativo con identità. L'identità è l'applicazione  $e : X \rightarrow R$  definita da  $e(x) = 1$  per ogni  $x \in X$ .

**26.6.** Sia  $Z^n = \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{Z}\}$  l'insieme di tutte le  $n$ -uple di numeri interi. In  $Z^n$  si definiscano un'operazione di addizione ed un'operazione di moltiplicazione ponendo

$$\begin{aligned}(x_1, x_2, \dots, x_n) + (x'_1, x'_2, \dots, x'_n) &= (x_1 + x'_1, x_2 + x'_2, \dots, x_n + x'_n) \\ (x_1, x_2, \dots, x_n)(x'_1, x'_2, \dots, x'_n) &= (x_1 x'_1, x_2 x'_2, \dots, x_n x'_n).\end{aligned}$$

Si dimostri che  $Z^n$  con queste operazioni è un anello commutativo con identità.

26.7. Si dimostri che  $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$  è un anello rispetto alle usuali operazioni di addizione e moltiplicazione tra numeri interi.

26.8. Sia  $(\mathbb{Z} \times \mathbb{Z}, +, *)$  l'anello dell'esempio 3 e sia  $S = \{(z, 0) \mid z \in \mathbb{Z}\}$ . Si provi che  $S$  è un sottoanello di  $\mathbb{Z} \times \mathbb{Z}$ .

26.9. Sia  $A = \{a + b\sqrt[3]{5} + c\sqrt[3]{5}^2 \mid a, b, c \in \mathbb{Z}\}$ . Si dimostri che  $A$  è un sottoanello dell'anello  $\mathbb{R}$  dei numeri reali.

26.10. Sia  $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ . Si dimostri che  $\mathbb{Z}[i]$  è un sottoanello dell'anello  $\mathbb{C}$  dei numeri complessi.

26.11. Sia  $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ . Si dimostri che  $\mathbb{Q}[i]$  è un sottoanello dell'anello  $\mathbb{C}$  dei numeri complessi. Si dimostri poi che  $\mathbb{Q}[i]$  è un campo.

26.12. Sia  $(\mathbb{Q}, +, \cdot)$  il campo dei numeri razionali. Si definisca un'ulteriore operazione  $*$  in  $\mathbb{Q}$  ponendo  $x * y = \frac{3}{4}xy$  per ogni  $x, y \in \mathbb{Q}$ . Si dimostri che  $(\mathbb{Q}, +, *)$  è un campo.

[Suggerimento: Si provi innanzitutto che  $(\mathbb{Q}, +, *)$  è un anello commutativo, poi se ne determini l'identità, e infine nel dimostrare che ogni elemento non nullo è invertibile si faccia attenzione a non confondere il numero razionale 1 con l'identità dell'anello  $(\mathbb{Q}, +, *)$ .]

26.13. Sia  $\mathbb{Z} \times 2\mathbb{Z} = \{(x, 2y) \mid x, y \in \mathbb{Z}\}$ . Si dimostri che  $\mathbb{Z} \times 2\mathbb{Z}$  è un sottoanello dell'anello  $\mathbb{Z} \times \mathbb{Z}$  dell'esempio 2.

26.14. Sia  $R$  un anello e sia  $R_\lambda$  un sottoanello di  $R$  per ogni  $\lambda \in \Lambda$ . Si dimostri che  $\bigcap_{\lambda \in \Lambda} R_\lambda$  è un sottoanello di  $R$ .

26.15. Calcolare  $U(R)$  dove  $R$  è l'anello dell'esempio 2.

26.16. Sia  $(R, +, \cdot)$  l'anello dei numeri reali. Nell'insieme  $R$  si definiscano due operazioni  $\oplus$  e  $\otimes$  ponendo  $x \oplus y = x + y - 2$ ,  $x \otimes y = xy - 2x - 2y + 6$  per ogni  $x, y \in R$ . Allora  $(R, \oplus, \otimes)$  è un anello commutativo con identità.

- Si dica qual è lo zero dell'anello  $(R, \oplus, \otimes)$  (cioè l'elemento neutro per l'operazione  $\oplus$ ).
- Si dica qual è l'identità dell'anello  $(R, \oplus, \otimes)$ .
- Si dica se  $(R, \oplus, \otimes)$  è un campo.

26.17. Si provi per induzione su  $n \geq 0$  che se  $a, b \in R$  ed  $R$  è un anello commutativo, allora  $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ .

[Suggerimento: si ragioni come nell'esercizio 9.17.]

## Capitolo 27. Ideali

Sia  $R$  un anello. Un sottoinsieme non vuoto  $I$  di  $R$  si dice un *ideale* di  $R$  se sono soddisfatte le seguenti due condizioni:

- $x - y \in I$  per ogni  $x, y \in I$ ;
- $rx \in I$  e  $xr \in I$  per ogni  $r \in R$  e ogni  $x \in I$ .

Se  $I$  è ideale di  $R$  scriveremo  $I \trianglelefteq R$ . Si noti che per la condizione (a) ogni ideale di  $R$  è in particolare un sottogruppo del gruppo additivo  $(R, +)$ .

ESEMPIO 1. Consideriamo l'anello  $\mathbb{Z}$  degli interi e cerchiamone gli ideali. Ogni ideale  $I$  di  $\mathbb{Z}$  deve essere in particolare un sottogruppo di  $(\mathbb{Z}, +)$ . Quindi per l'esempio 6 del capitolo 21 gli ideali di  $\mathbb{Z}$  sono tutti del tipo  $n\mathbb{Z}$  con  $n \geq 0$  intero. Si noti poi che viceversa ogni  $n\mathbb{Z}$  è un ideale di  $\mathbb{Z}$ , in quanto

- il sottoinsieme  $n\mathbb{Z}$  di  $\mathbb{Z}$  è non vuoto,
- la condizione (a) della definizione di ideale è soddisfatta perché  $n\mathbb{Z}$  è un sottogruppo del gruppo  $(\mathbb{Z}, +)$ , e
- la condizione (b) è soddisfatta perché se  $r \in \mathbb{Z}$  e  $x \in n\mathbb{Z}$ , allora  $x = nz$  per qualche  $z \in \mathbb{Z}$ , e quindi  $rx = r(nz) = n(rz) \in n\mathbb{Z}$ ; infine anche  $xr \in n\mathbb{Z}$  perché  $\mathbb{Z}$  è commutativo.

Abbiamo così dimostrato che gli ideali dell'anello  $\mathbb{Z}$  sono tutti e soli gli  $n\mathbb{Z}$  con  $n \geq 0$  intero.  $\square$

ESEMPIO 2. Sia  $R$  un anello commutativo con identità. Un polinomio nell'indeterminata  $x$  a coefficienti in  $R$  è un'espressione del tipo  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  dove  $n$  è un numero naturale e  $a_0, a_1, a_2, \dots, a_n \in R$ . Due polinomi  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  e  $b_0 + b_1x + b_2x^2 + \dots + b_mx^m$  a coefficienti in  $R$  sono uguali se  $a_i = b_i$  per ogni  $i \geq 0$ ; qui si suppone che gli  $a_i$  e  $b_i$  non scritti siano tutti uguali a zero, cioè che  $a_i = 0$  per ogni  $i > n$  e  $b_i = 0$  per ogni  $i > m$ . Si noti infatti che dati due polinomi  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  e  $b_0 + b_1x + b_2x^2 + \dots + b_mx^m$  è possibile supporre  $n = m$ , in quanto è sufficiente aggiungere eventualmente ulteriori termini tutti con il coefficiente nullo.

A partire da un anello  $R$ , commutativo con identità, costruiamo l'insieme  $R[x]$  di tutti i polinomi nell'indeterminata  $x$  a coefficienti in  $R$ . Quindi

$$R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid$$

$$n \in \mathbb{N}, a_i \in R \text{ per ogni } i = 0, 1, 2, \dots, n\}.$$

Sull'insieme  $R[x]$  definiamo due operazioni  $+$  e  $\cdot$  ponendo

$$(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \dots + b_nx^n) = \\ = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n$$

$$(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) = \\ = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots + (a_nb_m)x^{n+m}.$$

È allora possibile dimostrare che  $R[x]$  con queste due operazioni è a sua volta un anello commutativo con identità, detto l'anello dei polinomi nell'indeterminata  $x$  a coefficienti in  $R$ . Lo zero di questo anello è  $0_{R[x]} = 0_R$  e la sua identità è  $1_{R[x]} = 1_R$ . Si noti che  $R$  è un sottoanello di  $R[x]$ .

L'insieme

$$I = \{a_1x + a_2x^2 + \dots + a_nx^n \mid n \in \mathbb{N}^*, a_i \in R \text{ per ogni } i = 1, 2, \dots, n\},$$

cioè l'insieme di tutti gli elementi di  $R[x]$  con "termine noto" nullo, è un ideale di  $R[x]$ , come è facile verificare. Più in generale se  $t$  è un numero naturale fissato e

$$I_t = \{a_{t+1}x^{t+1} + a_{t+2}x^{t+2} + \dots + a_nx^n \mid n \in \mathbb{N}, n > t, \\ a_i \in R \text{ per ogni } i = t+1, t+2, \dots, n\},$$

cioè  $I_t$  è l'insieme di tutti i polinomi  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$  con  $a_0 = a_1 = \dots = a_t = 0$ , allora  $I_t$  è un ideale di  $R[x]$ . Questo può essere verificato facilmente o in modo diretto oppure osservando che  $I_t = \{x^{t+1}f \mid f \in R[x]\}$ . □

ESEMPIO 3. Dato un qualunque anello  $R$  è immediato verificare che  $R$  ha sempre almeno i due ideali  $I$  (detto l'ideale improprio) e  $\{0_R\}$  (detto l'ideale nullo). □

TEOREMA 27.1. Sia  $(R, +, \cdot)$  un anello. Se  $\sim$  è una relazione di equivalenza su  $R$  compatibile con le operazioni  $+$  e  $\cdot$ , allora  $[0_R]_{\sim}$ , la classe di equivalenza di  $0_R$ , è un ideale di  $R$ . Viceversa, se  $I$  è un ideale di  $R$  e  $\sim_I$  è definita per ogni  $a, b \in R$  da  $a \sim_I b$  se  $a - b \in I$ , allora  $\sim_I$  è una relazione di equivalenza su  $R$  compatibile con entrambe le operazioni  $+$  e  $\cdot$ , e  $[0_R]_{\sim_I} = I$ .

Siano  $R$  un anello e  $I$  un suo ideale. Dato che  $I$  è in particolare un sottogruppo del gruppo additivo  $(R, +)$ , è possibile costruire il gruppo quoziente  $(R/I, +)$ , i cui elementi sono le classi laterali  $r + I$  di  $R$  modulo  $I$  (le classi laterali destre e sinistre coincidono perché il gruppo additivo  $R$  è abeliano). Non è difficile dimostrare che se si definisce su  $R/I$  un'ulteriore operazione  $\cdot$  ponendo  $(r + I) \cdot (r' + I) = rr' + I$  per ogni  $r, r' \in R$  si ottiene su  $R/I$  una struttura d'anello

$(R/I, +, \cdot)$ . Quindi, riassumendo, per ogni anello  $R$  e ogni suo ideale  $I$  abbiamo costruito un anello  $R/I$ , detto l'anello quoziente di  $R$  modulo  $I$ , i cui elementi sono le classi laterali  $r + I$ , cioè

$$R/I = \{r + I \mid r \in R\},$$

e in cui le operazioni sono definite da

$$(r + I) + (r' + I) = (r + r') + I$$

$$(r + I) \cdot (r' + I) = rr' + I$$

per ogni  $r + I, r' + I \in R/I$ . Lo zero di  $R/I$  è  $0_{R/I} = 0_R + I = I$ , l'opposto di  $r + I$  è  $-r + I$  per ogni  $r \in R$ , e se  $R$  è un anello con identità  $1_R$  e  $I$  è un ideale proprio di  $R$ , anche  $R/I$  è un anello con identità e la sua identità è  $1_{R/I} = 1_R + I$ .

Se  $R, S$  sono anelli, un omomorfismo d'anello  $\varphi: R \rightarrow S$  è un'applicazione di  $R$  in  $S$  tale che  $\varphi(a + b) = \varphi(a) + \varphi(b)$  e  $\varphi(ab) = \varphi(a)\varphi(b)$  per ogni  $a, b \in R$ . Se  $R$  ed  $S$  sono anelli con identità supporremo inoltre che ogni omomorfismo d'anello  $\varphi: R \rightarrow S$  abbia l'ulteriore proprietà che  $\varphi(1_R) = 1_S$ . (Quindi se  $R$  ed  $S$  hanno l'identità, un'applicazione  $\varphi: R \rightarrow S$  è un omomorfismo d'anello se e solo se  $f$  è un omomorfismo del gruppo  $(R, +)$  nel gruppo  $(S, +)$  e del monoide  $(R, \cdot)$  nel monoide  $(S, \cdot)$ .)

Un omomorfismo biiettivo si dice un isomorfismo, un omomorfismo  $R \rightarrow R$  si dice un endomorfismo di  $R$ , e un endomorfismo biiettivo di  $R$ , cioè un isomorfismo  $R \rightarrow R$ , si dice un automorfismo di  $R$ . Due anelli  $R$  ed  $S$  si dicono isomorfi se esiste un isomorfismo di  $R$  in  $S$ ; scriveremo in tal caso  $R \cong S$ .

ESEMPIO 4. Dato un anello  $R$  commutativo e con identità, consideriamo l'applicazione  $\varphi: R[x] \rightarrow R$  definita da

$$\varphi(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) = a_0$$

per ogni  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$ . Allora  $\varphi$  è un omomorfismo di anelli con identità in quanto si ha

$$\begin{aligned} \varphi((a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \dots + b_nx^n)) &= \\ = \varphi((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n) &= \\ = a_0 + b_0 &= \\ = \varphi(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + \varphi(b_0 + b_1x + b_2x^2 + \dots + b_nx^n), & \\ \varphi((a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m)) &= \\ = \varphi((a_0b_0) + (a_0b_1 + a_1b_0)x + & \\ + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots + (a_nb_m)x^{n+m}) &= a_0b_0 = \\ = \varphi(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)\varphi(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) & \end{aligned}$$



e

$$\varphi(1) = 1. \quad \square$$

ESEMPIO 5. Se  $R$  è un anello e  $I$  è un suo ideale, la proiezione canonica  $\pi: R \rightarrow R/I$ , definita da  $\pi(r) = r + I$  per ogni  $r \in R$ , è un omomorfismo suriettivo d'anelli, perché per ogni  $r, r' \in R$  si ha

$$\pi(r) + \pi(r') = (r + I) + (r' + I) = (r + r') + I = \pi(r + r')$$

e

$$\pi(r) \cdot \pi(r') = (r + I) \cdot (r' + I) = rr' + I = \pi(rr'). \quad \square$$

Se  $f: R \rightarrow S$  è un omomorfismo d'anelli, il nucleo di  $f$  è

$$\ker f = \{r \in R, f(r) = 0_S\}.$$

LEMMA 27.2. Se  $f: R \rightarrow S$  è un omomorfismo di anelli, il nucleo di  $f$  è un ideale di  $R$ .

TEOREMA 27.3. (TEOREMA FONDAMENTALE DI OMOMORFISMO PER GLI ANELLI). Siano  $R, R'$  anelli ed  $f: R \rightarrow R'$  un omomorfismo di anelli. Se  $\ker f$  è il nucleo di  $f$ ,  $R/\ker f$  è l'anello quoziente di  $R$  modulo  $\ker f$  e  $\pi: R \rightarrow R/\ker f$  è la proiezione canonica, allora:

- (a) esiste un'unica applicazione  $\tilde{f}: R/\ker f \rightarrow R'$  che rende commutativo il diagramma

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \pi \searrow & & \nearrow \tilde{f} \\ R/\ker f & & \end{array}$$

cioè tale che  $\tilde{f} \circ \pi = f$ ;

- (b)  $\tilde{f}$  è un omomorfismo iniettivo di anelli;  
(c)  $\tilde{f}$  è un isomorfismo se e solo se  $f$  è suriettivo.

COROLLARIO 27.4. Siano  $R, R'$  anelli ed  $f: R \rightarrow R'$  un omomorfismo di anelli. Allora  $f(R)$  è un sottoanello di  $R'$  e gli anelli  $R/\ker f$  ed  $f(R)$  sono isomorfi.

TEOREMA 27.5 (TEOREMA DI CORRISPONDENZA PER GLI IDEALI). Siano  $R, R'$  anelli ed  $f: R \rightarrow R'$  un omomorfismo di anelli. Siano poi  $\mathcal{L} = \{I \mid I \trianglelefteq R, I \supseteq \ker f\}$  l'insieme degli ideali di  $R$  che contengono il nucleo di  $f$  ed  $\mathcal{L}' = \{J \mid J \trianglelefteq f(R)\}$  l'insieme degli ideali di  $f(R)$ . Allora c'è una biiezione  $\Phi: \mathcal{L} \rightarrow \mathcal{L}'$  definita da  $\Phi(I) = f(I)$  per ogni  $I \in \mathcal{L}$ , la cui inversa è la biiezione  $\Psi: \mathcal{L}' \rightarrow \mathcal{L}$  definita da  $\Psi(J) = f^{-1}(J)$  per ogni  $J \in \mathcal{L}'$ .

ESEMPIO 6. Dato un qualunque anello  $R$  sia  $M_n(R)$  l'insieme delle matrici quadrate di ordine  $n$  ad elementi in  $R$ : gli elementi di  $M_n(R)$  sono le matrici quadrate  $n \times n$  definite come le matrici ad elementi reali da noi incontrate nel capitolo 6 con la sola differenza che gli elementi  $a_{ij}$  delle matrici sono ora non più numeri reali bensì elementi dell'anello  $R$ . In  $M_n(R)$  si definiscono due operazioni di addizione e moltiplicazione con le stesse formule del capitolo 6: la somma di due matrici si ottiene sommando gli elementi delle due matrici elemento per elemento, mentre il prodotto è quello righe per colonne. È allora possibile verificare che  $M_n(R)$  con queste operazioni diventa un anello. Lo zero di questo anello è la matrice  $n \times n$  avente tutti i suoi  $n^2$  elementi uguali a  $0_R$ . Se l'anello  $R$  ha identità  $1_R$ , allora  $M_n(R)$  è un anello con identità  $1_{M_n(R)} = (\delta_{ij})$ , dove  $(\delta_{ij})$  è la matrice  $n \times n$  con  $\delta_{ij} = 1_R$  se  $i = j$  e  $\delta_{ij} = 0_R$  se  $i \neq j$ .

Se  $\varphi: R \rightarrow M_n(R)$  è l'applicazione definita per ogni  $r \in R$  da

$$\varphi(r) = \begin{pmatrix} r & 0 & 0 & \dots & 0 \\ 0 & r & 0 & \dots & 0 \\ 0 & 0 & r & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & r \end{pmatrix},$$

è possibile verificare che  $\varphi$  è un omomorfismo iniettivo di anelli.  $\square$

### Esercizi svolti

27.1. Sia  $R$  un anello commutativo con identità e sia  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$  un polinomio a coefficienti in  $R$  nell'indeterminata  $x$ . Gli  $a_i$  si dicono i coefficienti di  $f$ , e se  $a_n \neq 0$  si dice che il polinomio  $f$  ha grado  $n$  (in simboli  $\delta(f) = n$ ). In tal caso  $a_n$  è detto il coefficiente direttivo del polinomio  $f$ . Il polinomio nullo è per definizione di grado  $-\infty$ .

Si provi che se  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ,  $g = b_0 + b_1x + b_2x^2 + \dots + b_mx^m \in R[x]$ , allora

- (a)  $\delta(f+g) \leq \max\{\delta(f), \delta(g)\}$ ;  
(b)  $\delta(fg) \leq \delta(f) + \delta(g)$ ;  
(c) se  $R$  è un dominio di integrità, allora  $\delta(fg) = \delta(f) + \delta(g)$ .

Soluzione. Si osservi innanzitutto che (a), (b) e (c) sono vere se  $f = 0$  oppure  $g = 0$ . Quindi si può supporre che  $f \neq 0$  e  $g \neq 0$ .

- (a) Se per assurdo fosse  $d = \delta(f+g) > \max\{\delta(f), \delta(g)\}$ , allora  $d > \delta(f)$  e  $d > \delta(g)$ , e quindi  $a_d = b_d = 0$ . Ma allora il coefficiente di  $x^d$  in  $f+g$  sarebbe  $a_d + b_d = 0$ , e questo contraddice il fatto che  $\delta(f+g) = d$ .

(b) e (c) Se  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  ha grado  $n$  e  $g = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$  ha grado  $m$ , allora  $fg = (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots + (a_nb_m)x^{n+m}$  ha grado  $\leq n+m$ . Se poi  $R$  è anche un dominio di integrità, dato che  $\delta(f) = n$  e  $\delta(g) = m$ , e quindi  $a_n \neq 0$  e  $b_m \neq 0$ , possiamo dedurre anche che  $a_nb_m \neq 0$ . Quindi in questo caso il coefficiente di  $x^{n+m}$  è  $\neq 0$ , e quindi  $\delta(fg) = n+m$ .  $\square$

Si osservi che affinché queste formule siano tutte valide è necessario supporre che  $\delta(0) = -\infty$ . Se prendiamo ad esempio  $f = 0$  e  $g = x$  nella (c), allora la  $\delta(fg) = \delta(f) + \delta(g)$  diventa  $-\infty = -\infty + 1$  se si pone  $\delta(0) = -\infty$ , mentre sarebbe diventata  $0 = 0 + 1$  se si fosse posto  $\delta(0) = 0$ .

27.2. Sia  $R$  un anello commutativo con identità. Si dimostri che  $R[x]$  è un dominio d'integrità se e solo se  $R$  è un dominio d'integrità.

*Soluzione.* Se  $R[x]$  è un dominio d'integrità, cioè in  $R[x]$  il prodotto di due elementi non nulli è non nullo, anche  $R$ , che è un sottoanello di  $R[x]$ , è un dominio d'integrità.

Viceversa supponiamo che  $R$  sia un dominio d'integrità. Siano  $f, g \in R[x]$  due polinomi tali che  $f \neq 0$  e  $g \neq 0$ , cioè tali che  $\delta(f) \geq 0$  e  $\delta(g) \geq 0$ . Possiamo allora applicare la formula (c) dell'esercizio 27.2 ottenendo che  $\delta(fg) = \delta(f) + \delta(g) \geq 0 + 0 = 0$ . Quindi  $fg \neq 0$ . Questo dimostra che  $R[x]$  è un dominio d'integrità.  $\square$

27.3. Sia  $\mathbb{Q}[x]$  l'anello dei polinomi nell'indeterminata  $x$  a coefficienti razionali e sia  $\alpha \in \mathbb{C}$  un numero complesso fissato. Per ogni  $f \in \mathbb{Q}[x]$  sia  $f(\alpha) \in \mathbb{C}$  il valore del polinomio  $f$  calcolato in  $\alpha$ . Si dimostri che

- l'applicazione  $\varphi_\alpha : \mathbb{Q}[x] \rightarrow \mathbb{C}$  definita da  $\varphi_\alpha(f) = f(\alpha)$  per ogni polinomio  $f \in \mathbb{Q}[x]$  è un omomorfismo di anelli;
- il nucleo di  $\varphi_\alpha$  è l'insieme  $I_\alpha$  di tutti i polinomi a coefficienti razionali di cui  $\alpha$  è una radice;
- l'insieme  $I_\alpha$  è un ideale di  $\mathbb{Q}[x]$ .

*Soluzione.* (a) Si ha, per ogni  $f, g \in \mathbb{Q}[x]$ ,

$$\begin{aligned}\varphi_\alpha(f+g) &= (f+g)(\alpha) = f(\alpha) + g(\alpha) = \varphi_\alpha(f) + \varphi_\alpha(g) \\ \varphi_\alpha(fg) &= (fg)(\alpha) = f(\alpha)g(\alpha) = \varphi_\alpha(f)\varphi_\alpha(g) \\ \varphi_\alpha(1) &= 1.\end{aligned}$$

Quindi  $\varphi_\alpha : \mathbb{Q}[x] \rightarrow \mathbb{C}$  è un omomorfismo di anelli.

(b) Si ha

$$\ker(\varphi_\alpha) = \{f \mid f \in \mathbb{Q}[x], \varphi_\alpha(f) = 0\} = \{f \mid f \in \mathbb{Q}[x], f(\alpha) = 0\},$$

e quindi  $\ker(\varphi_\alpha)$  è proprio l'insieme di tutti gli  $f \in \mathbb{Q}[x]$  di cui  $\alpha$  è radice.

(c) Segue da (b) e dal lemma 27.2.  $\square$

### Altri esercizi

27.4. Siano  $X$  un insieme non vuoto ed  $R$  il campo dei numeri reali. Nell'insieme  $R^X$  di tutte le applicazioni di  $X$  in  $R$  si definiscano un'operazione di addizione e un'operazione di moltiplicazione ponendo, per ogni  $f, g \in R^X$ ,  $(f+g)(x) = f(x) + g(x)$  e  $(fg)(x) = f(x)g(x)$  per ogni  $x \in X$ . Non sarebbe difficile dimostrare che  $(R^X, +, \cdot)$  è un anello commutativo con identità.

- Si determini l'identità dell'anello  $R^X$ .
- Si determinino i divisori dello zero nell'anello  $R^X$ .
- Si determinino gli elementi invertibili nell'anello  $R^X$ .
- Per ogni sottoinsieme  $Y$  di  $X$  sia

$$I_Y = \{f \in R^X \mid f(y) = 0 \text{ per ogni } y \in Y\}.$$

Si dimostri che  $I_Y$  è un ideale di  $R^X$  per ogni  $Y \subseteq X$ .

27.5. Per ogni anello  $R$  sia  $Z(R) = \{z \in R \mid zr = rz \text{ per ogni } r \in R\}$ .

- Si dimostri che  $Z(R)$  è un sottoanello di  $R$  e che  $Z(R)$  è commutativo.
- Si dimostri che se  $I$  è un ideale di  $R$  allora  $I \cap Z(R)$  è un ideale di  $Z(R)$ .
- Si dimostri che se  $J$  è un ideale di  $Z(R)$  e

$$JR = \left\{ \sum_{i=1}^n j_i r_i \mid n \in \mathbb{N}^*, j_1, j_2, \dots, j_n \in J, r_1, r_2, \dots, r_n \in R \right\},$$

allora  $JR$  è un ideale di  $R$ .

27.6. Si provi che se  $I$  è un ideale di un anello  $R$  con identità  $1_R$  e  $1_R \in I$ , allora  $I = R$ . Si provi che se  $I$  è un ideale di un anello  $R$  con identità ed  $I$  contiene un elemento invertibile di  $R$ , allora  $I = R$ .

27.7. Sia  $(R, +, \cdot)$  un anello commutativo con identità e sia  $a$  un elemento di  $R$ . Si ponga  $I(a) = \{x \in R \mid xa = 0\}$ .

- Si dimostri che  $I(a)$  è un ideale di  $R$ .
- Si dimostri che se  $f : R \rightarrow R$  è l'applicazione definita da  $f(x) = xa$  per ogni  $x \in R$ , allora  $f$  è un endomorfismo del gruppo abeliano  $(R, +)$  il cui nucleo è  $I(a)$ .
- Si determini  $I(a)$  quando  $R = \mathbb{Z} \times \mathbb{Z}$  è l'anello delle coppie ordinate di numeri interi con le operazioni definite da  $(x, y) + (x', y') = (x + x', y + y')$  e  $(x, y)(x', y') = (xx', yy')$  per ogni  $(x, y), (x', y') \in R$ , e  $a = (0, 2)$ .

27.8. Si dimostri che se  $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$  sono ideali di un anello  $R$ , allora anche  $I = \bigcup_{n \in \mathbb{N}} I_n$  è un ideale di  $R$ .

27.9. Sia  $R$  un anello commutativo con identità. Si dimostri che l'anello dei polinomi  $R[x]$  nell'indeterminata  $x$  non è un campo.

27.10. Siano  $\alpha \in \mathbb{C}$  e  $n \in \mathbb{Z}$  due numeri fissati. Sia  $\mathbb{Z}[x]$  l'anello dei polinomi a coefficienti interi nell'indeterminata  $x$  e

$$I_{n,\alpha} = \{f \in \mathbb{Z}[x] \mid f(\alpha) = 0 \text{ ed } n \mid f(0)\}.$$

Si dimostri che  $I_{n,\alpha}$  è un ideale di  $\mathbb{Z}[x]$ .

27.11. Sia  $R$  il campo dei numeri reali. Si determinino tutte le equivalenze  $\sim$  sull'insieme  $R$  compatibili sia con l'operazione di addizione che con l'operazione di moltiplicazione tra numeri reali.

27.12. Si consideri il sottoanello  $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$  dell'anello dei numeri complessi  $\mathbb{C}$  ( $\mathbb{Z}[i]$  è detto l'anello degli interi di Gauss). Si consideri l'applicazione  $\nu: \mathbb{Z}[i] \rightarrow \mathbb{Z}$  definita da  $\nu(a + ib) = a^2 + b^2$  per ogni  $a, b \in \mathbb{Z}$ .

- Si dimostri che  $\nu$  è un omomorfismo del monoide  $(\mathbb{Z}[i], \cdot)$  nel monoide  $(\mathbb{Z}, \cdot)$ .
- Si deduca da (a) che se  $z \in \mathbb{Z}[i]$  è un elemento invertibile dell'anello  $\mathbb{Z}[i]$ , allora  $\nu(z) = 1$ .
- Si deduca da (b) che gli elementi invertibili dell'anello  $\mathbb{Z}[i]$  sono tutti e soli gli elementi  $1, -1, i, -i$ .

27.13. Sia  $R$  un anello e  $\iota_R: R \rightarrow R$  l'applicazione identica di  $R$ . Qual è il nucleo di  $\iota_R$ ? Nella notazione dell'enunciato del teorema fondamentale di omomorfismo per gli anelli come è definito l'omomorfismo  $\bar{\iota}_R: R/\{0_R\} \rightarrow R$ ? L'omomorfismo  $\bar{\iota}_R: R/\{0_R\} \rightarrow R$  è un isomorfismo? Se ne deduca che  $R/\{0_R\} \cong R$ .

## Capitolo 28. L'anello delle classi resto e la caratteristica di un anello

Fissiamo un intero  $n \geq 0$ . Abbiamo già osservato nell'esempio 1 del capitolo 27 che  $n\mathbb{Z}$  è un ideale di  $\mathbb{Z}$  (anzi avevamo dimostrato che gli ideali di  $\mathbb{Z}$  sono tutti e soli gli  $n\mathbb{Z}$  per qualche  $n \in \mathbb{N}$ ). È possibile quindi costruire l'anello quoziente  $\mathbb{Z}/n\mathbb{Z}$ . Si osservi che l'equivalenza  $\sim_{n\mathbb{Z}}$  su  $\mathbb{Z}$  associata all'ideale  $n\mathbb{Z}$  è definita, per ogni  $x, y \in \mathbb{Z}$ , da  $x \sim_{n\mathbb{Z}} y$  se e solo se  $x - y \in n\mathbb{Z}$ , cioè se e solo se  $n \mid (x - y)$ , vale a dire se e solo se  $x \equiv y \pmod{n}$ . Quindi l'equivalenza

$\sim_{n\mathbb{Z}}$  e la congruenza  $\equiv_n$  sull'insieme  $\mathbb{Z}$  coincidono. Per  $n = 0$  la congruenza  $\equiv_0$  sull'insieme  $\mathbb{Z}$  è l'eguaglianza (esempio 2 del capitolo 8), e per  $n = 1$  la congruenza  $\equiv_1$  è l'equivalenza banale sull'insieme  $\mathbb{Z}$  in cui tutti gli elementi sono equivalenti tra loro. In questi due casi gli insiemi quozienti sono rispettivamente  $\mathbb{Z}/\equiv_0 = \{\{a\} \mid a \in \mathbb{Z}\}$  e  $\mathbb{Z}/\equiv_1 = \{\mathbb{Z}\}$ . Supponiamo quindi d'ora in poi  $n > 1$ . L'insieme  $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim_{n\mathbb{Z}} = \mathbb{Z}/\equiv_n$  è l'insieme delle classi resto modulo  $n$ , cioè  $\mathbb{Z}/n\mathbb{Z} = \{[a]_{\equiv_n} \mid a \in \mathbb{Z}\} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ . Denoteremo talvolta  $\mathbb{Z}/n\mathbb{Z}$  con  $\mathbb{Z}_n$ , e i suoi elementi  $[a]_{\equiv_n} = a + n\mathbb{Z}$  verranno denotati con  $\bar{a}$ , sottintendendo il numero fissato  $n$ . Quindi  $\mathbb{Z}_n$  è un anello con  $n$  elementi,  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ , e le operazioni di addizione e moltiplicazione in  $\mathbb{Z}_n$  sono definite da

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a+b} \\ \bar{a} \cdot \bar{b} &= \overline{ab}\end{aligned}$$

per ogni  $a, b \in \mathbb{Z}$ . Ovviamente si ha  $\bar{a} = \bar{b}$  se e solo se  $a \equiv b \pmod{n}$ . In particolare  $\bar{a} = \bar{0}$  se e solo se  $n \mid a$ . L'anello  $\mathbb{Z}_n$  è un anello commutativo con identità; il suo zero è  $\bar{0}$ , la sua identità è  $\bar{1}$ .

### PROPOSIZIONE 28.1.

- Sia  $R$  un anello commutativo con identità e sia  $a \in R$ . Se  $a$  è invertibile, allora  $a$  non è divisore dello zero.
- Sia  $R$  un anello finito, commutativo e con identità e sia  $a \in R$ . Allora  $a$  è invertibile se e solo se  $a \neq 0$  e  $a$  non è divisore dello zero.

*Dimostrazione.* (a) Supponiamo per assurdo che  $a \in R$  sia un elemento invertibile che sia anche un divisore dello zero. Dato che  $a$  è invertibile esiste  $b \in R$  tale che  $ab = 1$ . Dato che  $a$  è divisore dello zero esiste  $c \in R$ ,  $c \neq 0$ , tale che  $ca = 0$ . Ma allora  $c = c \cdot 1 = c(ab) = (ca)b = 0b = 0$ , e questo è assurdo.

(b) Abbiamo già osservato che lo zero non è mai invertibile (capitolo 26). In vista di (a) dobbiamo quindi dimostrare solamente che se  $R$  è un anello commutativo, finito e con identità ed  $a \in R$  non è invertibile, allora  $a$  è divisore dello zero. Consideriamo l'applicazione  $\varphi: R \rightarrow R$  definita da  $\varphi(r) = ar$  per ogni  $r \in R$ . Questa  $\varphi$  è un endomorfismo del gruppo additivo  $R$ , perché  $\varphi(r+r') = a(r+r') = ar + ar' = \varphi(r) + \varphi(r')$ . Dato che  $a$  non è invertibile, non esiste nessun  $r \in R$  tale che  $1_R = ar$ ; quindi  $1_R \notin \varphi(R)$ . In particolare l'applicazione  $\varphi$  non è suriettiva. Dato che  $R$  è un insieme finito, l'applicazione  $\varphi$  non è nemmeno iniettiva (perché se fosse iniettiva, sarebbe una biiezione, e quindi sarebbe suriettiva). Ma  $\varphi$  è un omomorfismo di gruppi additivi, e quindi  $\ker \varphi \neq \{0_R\}$  per il lemma 25.2. Se ne deduce che esiste  $r \in \ker \varphi$ ,  $r \neq 0_R$ . Quindi  $a \neq 0$ ,  $r \neq 0$  e  $ar = 0$ . Pertanto  $a$  è un divisore dello zero.  $\square$

**COROLLARIO 28.2.** Se  $R$  è un anello commutativo con identità e con un numero finito di elementi, allora  $R$  è un campo se e solo se  $R$  è un dominio d'integrità.

*Dimostrazione.* Se  $R$  è un campo,  $R$  è un dominio d'integrità per il lemma 26.2.

Viceversa se  $R$  è un dominio d'integrità,  $R$  non ha divisori dello zero. Per la proposizione 28.1 ogni elemento  $a \neq 0$  di  $R$  è invertibile. Quindi  $R$  è un campo.  $\square$

**PROPOSIZIONE 28.3.** Sia  $a$  un numero intero. L'elemento  $\bar{a}$  è invertibile in  $\mathbb{Z}_n$  se e solo se  $a$  ed  $n$  sono primi tra loro.

*Dimostrazione.* Sia  $\bar{a}$  invertibile in  $\mathbb{Z}_n$ . Allora esiste  $\alpha \in \mathbb{Z}$  tale che  $\bar{a} \cdot \bar{\alpha} = \bar{1}$ . Quindi  $n \mid (1 - \alpha a)$ , ossia esiste  $\beta \in \mathbb{Z}$  tale che  $1 - \alpha a = \beta n$ . Da  $\alpha a + \beta n = 1$  e dal corollario 4.2 segue che  $a$  ed  $n$  sono primi tra loro.

Viceversa supponiamo che  $a$  ed  $n$  siano primi tra loro. Per il corollario 4.2 esistono  $\alpha, \beta \in \mathbb{Z}$  tali che  $\alpha a + \beta n = 1$ . Ma allora  $\bar{1} = \bar{\alpha a + \beta n} = \bar{\alpha} \cdot \bar{a} + \bar{\beta} \cdot \bar{n} = \bar{\alpha} \cdot \bar{a} + \bar{\beta} \cdot \bar{0} = \bar{\alpha} \cdot \bar{a} + \bar{0} = \bar{\alpha} \cdot \bar{a}$ , e quindi  $\bar{\alpha} \in \mathbb{Z}_n$  è l'inverso di  $\bar{a}$ . In particolare  $\bar{a} \in \mathbb{Z}_n$  è invertibile.  $\square$

Dalle proposizioni 28.1 e 28.3 segue che se  $a \in \mathbb{Z}$ , allora  $\bar{a}$  è un divisore dello zero in  $\mathbb{Z}_n$  se e solo se  $n$  non divide  $a$  e  $(a, n) \neq 1$ .

**COROLLARIO 28.4.** Sia  $n > 1$  un intero. Le seguenti affermazioni sono equivalenti:

- (a) l'anello  $\mathbb{Z}_n$  è un campo;
- (b) l'anello  $\mathbb{Z}_n$  è un dominio d'integrità;
- (c)  $n$  è un numero primo.

*Dimostrazione.* Le condizioni (a) e (b) sono equivalenti per il corollario 28.2. Inoltre  $\mathbb{Z}_n$  è un campo se e solo se i suoi elementi  $\bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-1}$  sono tutti invertibili, ossia, per la proposizione 28.3, se e solo se gli interi  $1, 2, 3, \dots, n-1$  sono tutti primi con  $n$ . Questo avviene se e solo se  $n$  è un numero primo. Quindi anche le condizioni (a) e (c) sono equivalenti tra loro.  $\square$

**ESEMPIO 1.** L'anello  $\mathbb{Z}_2$  è un campo (perché 2 è un numero primo) con solo due elementi,  $\bar{0}$  e  $\bar{1}$ , che sono proprio lo zero e l'identità dell'anello.  $\square$

**ESEMPIO 2.** L'anello  $\mathbb{Z}_3$  è un campo (perché 3 è primo) con tre elementi,  $\bar{0}, \bar{1}$  e  $\bar{2}$ . Ovviamente  $\bar{0}$  non è invertibile. L'elemento  $\bar{1}$  è invertibile e il suo inverso  $(\bar{1})^{-1}$  è  $\bar{1}$  perché  $\bar{1} \cdot \bar{1} = \bar{1}$ . Anche l'inverso  $(\bar{2})^{-1}$  di  $\bar{2}$  coincide con  $\bar{2}$  stesso perché  $\bar{2} \cdot \bar{2} = \bar{4} = \bar{1}$ .  $\square$

**ESEMPIO 3.** L'anello  $\mathbb{Z}_6$  non è un campo (perché 6 non è un numero primo). L'elemento  $\bar{0}$  è lo zero di  $\mathbb{Z}_6$ , e  $\bar{1}$  è la sua identità. Gli elementi  $\bar{2}, \bar{3}$  e  $\bar{4}$  sono divisori dello zero perché si ha  $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$  e  $\bar{4} \cdot \bar{3} = \bar{12} = \bar{0}$ ; in particolare  $\bar{2}, \bar{3}$  e  $\bar{4}$  non sono invertibili in  $\mathbb{Z}_6$ . Invece  $\bar{5}$  è invertibile, perché  $\bar{5} \cdot \bar{5} = \bar{25} = \bar{1}$ ; si ha pertanto  $(\bar{5})^{-1} = \bar{5}$ .  $\square$

**ESEMPIO 4.** Nel campo  $\mathbb{Z}_5$  si ha  $(\bar{1})^{-1} = \bar{1}, (\bar{2})^{-1} = \bar{3}, (\bar{3})^{-1} = \bar{2}, (\bar{4})^{-1} = \bar{4}$ .  $\square$

**DEFINIZIONE.** Sia  $R$  un anello con identità  $1_R$ . Se esiste un intero positivo  $n$  tale che

$$\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} = 0_R,$$

il più piccolo intero  $n$  con tale proprietà si dice la caratteristica dell'anello  $R$ ; se invece

$$\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} \neq 0_R$$

per ogni  $n > 0$ , diremo che l'anello  $R$  ha caratteristica zero.

La caratteristica dell'anello  $R$  verrà denotata con  $\text{char } R$ .

**ESEMPIO 5.** Per il campo  $\mathbb{C}$  dei numeri complessi si ha  $\text{char } \mathbb{C} = 0$ .  $\square$

**ESEMPIO 6.** Se  $S$  è un sottoanello di un anello con identità  $R$  (e quindi  $1_S = 1_R$ ), allora  $\text{char } S = \text{char } R$ . In particolare  $\text{char } \mathbb{Z} = \text{char } \mathbb{Q} = \text{char } \mathbb{R} = 0$ .  $\square$

**ESEMPIO 7.** Per ogni  $n > 1$  si ha  $\text{char } \mathbb{Z}_n = n$ .  $\square$

Si osservi che esistono anelli con identità di caratteristica  $n$  per ogni  $n \in \mathbb{N}$ ,  $n \neq 1$ . Non esistono invece anelli di caratteristica 1. Infatti se  $R$  fosse un anello di caratteristica 1,  $R$  dovrebbe essere un anello con identità per il quale  $1_R = 0_R$ , mentre avevamo supposto che per ogni anello con identità si avesse sempre  $1_R \neq 0_R$ .

**PROPOSIZIONE 28.5.** Sia  $R$  un anello con identità  $1_R$  e sia

$$P = \{z 1_R \mid z \in \mathbb{Z}\}$$

l'insieme di tutti i multipli interi dell'elemento  $1_R$ . Allora  $P$  è un sottoanello di  $R$  (detto il sottoanello fondamentale di  $R$ ). Se  $R$  ha caratteristica 0, allora  $P \cong \mathbb{Z}$ . Se invece  $R$  ha caratteristica  $n > 0$ , allora  $P \cong \mathbb{Z}_n$ .

Per la proposizione 28.5 ogni anello  $R$  con identità ha un sottoanello isomorfo a  $\mathbb{Z}$  (se  $\text{char } R = 0$ ) o a  $\mathbb{Z}_n$  (se  $\text{char } R = n > 0$ ).

**COROLLARIO 28.6.** Ogni dominio di integrità ha caratteristica 0 oppure un numero primo. In particolare ogni campo ha caratteristica 0 oppure un numero primo.

ESEMPIO 8. Fissato un numero intero  $t > 1$  si consideri l'anello  $Z_t \times Z_t = \{(a, b) \mid a, b \in Z_t\}$  con le operazioni definite da

$$(a, b) + (a', b') = (a + a', b + b') \\ (a, b)(a', b') = (aa', bb')$$

per ogni  $(a, b), (a', b') \in Z_t \times Z_t$ . L'anello  $Z_t \times Z_t$  è un anello commutativo con identità. L'identità è  $(\bar{1}, \bar{1})$ , lo zero è  $(\bar{0}, \bar{0})$ . Si ha

$$\underbrace{(\bar{1}, \bar{1}) + \dots + (\bar{1}, \bar{1})}_{n \text{ volte}} = \underbrace{(\bar{1} + \dots + \bar{1}, \bar{1} + \dots + \bar{1})}_{n \text{ volte}} = (\bar{n}, \bar{n}),$$

e  $(\bar{n}, \bar{n}) = (\bar{0}, \bar{0})$  se e solo se  $t \mid n$ . Dato che  $t$  è il più piccolo intero positivo  $n$  tale che  $t \mid n$ , si ha che  $\text{char}(Z_t \times Z_t) = t$ . In particolare se  $t$  è primo  $Z_t \times Z_t$  è un anello la cui caratteristica è un numero primo che però non è un dominio d'integrità (e quindi tantomeno un campo) perché  $(\bar{0}, \bar{1})(\bar{1}, \bar{0}) = (\bar{0}, \bar{0})$ .  $\square$

Sia  $R$  un anello commutativo con identità. Un ideale  $I$  di  $R$  si dice un ideale massimale se  $I \neq R$  e per ogni ideale  $J$  di  $R$  tale che  $J \supseteq I$  si ha  $J = I$  oppure  $J = R$ . Un ideale  $I$  di  $R$  si dice invece un ideale primo se  $I \neq R$  e per ogni  $x, y \in R$  tale che  $xy \in I$  si ha che  $x \in I$  oppure  $y \in I$ .

ESEMPIO 9. Se  $R$  è un anello commutativo con identità, l'ideale nullo  $\{0\}$  è un ideale primo di  $R$  se e solo se  $R$  è un dominio d'integrità. Infatti l'ideale nullo  $\{0\}$  è sempre un ideale proprio, e quindi  $\{0\}$  è primo se e solo se per ogni  $x, y \in R$  tale che  $xy \in \{0\}$  si ha  $x \in \{0\}$  oppure  $y \in \{0\}$ . Questo è equivalente a dire che per ogni  $x, y \in R$  con  $xy = 0$  si ha  $x = 0$  oppure  $y = 0$ , cioè che  $R$  è un dominio d'integrità.  $\square$

ESEMPIO 10. Sarebbe possibile dimostrare che in un anello commutativo con identità, l'ideale nullo  $\{0\}$  è un ideale massimale se e solo se  $R$  è un campo.  $\square$

PROPOSIZIONE 28.7. Sia  $I$  un ideale di un anello commutativo con identità  $R$ . Allora

- (a)  $I$  è un ideale primo di  $R$  se e solo se l'anello quoziente  $R/I$  è un dominio d'integrità;  
(b)  $I$  è un ideale massimale di  $R$  se e solo se l'anello quoziente  $R/I$  è un campo.

COROLLARIO 28.8. Ogni ideale massimale è primo.

ESEMPIO 11. L'anello  $Z$  degli interi è un dominio d'integrità e non è un campo. Quindi il suo ideale nullo  $\{0\}$  è primo e non è massimale (esempi 9 e 10). Per l'esempio 1 del capitolo 27 gli altri ideali di  $Z$  sono gli  $nZ$  con  $n \geq 1$  intero. Per  $n = 1$  si ha l'ideale improprio. Per  $n \geq 2$  si ha che  $Z/nZ = Z_n$  è un dominio d'integrità se e solo se  $Z/nZ = Z_n$  è un campo, e questo avviene se e solo se  $n$

è un numero primo (corollario 28.4). Dalla proposizione 28.7 segue che per ogni intero  $n \geq 1$  l'ideale  $nZ$  di  $Z$  è un ideale primo se e solo se è massimale, e questo accade se e solo se  $n$  è un numero primo. Abbiamo così dedotto che:

- (a) gli ideali primi di  $Z$  sono l'ideale nullo e gli ideali  $nZ$  con  $n$  numero primo;  
(b) gli ideali massimali di  $Z$  sono gli ideali  $nZ$  con  $n$  numero primo.  $\square$

### Esercizi svolti

28.1. Si dimostri che ogni sottoanello finito con identità di un campo è un campo. Si dia un esempio di un sottoanello infinito con identità di un campo che non è un campo.

Soluzione. Se  $F$  è un campo,  $F$  è un dominio d'integrità. Ma allora se  $R$  è un suo sottoanello,  $R$  è pure un dominio d'integrità. Per il corollario 28.2  $R$  è un campo.

Per risolvere la seconda parte dell'esercizio basta prendere invece come esempio il campo  $R$  e il suo sottoanello  $Z$ , che è un dominio d'integrità ma non è un campo.  $\square$

28.2. Si calcoli la caratteristica dell'anello  $(Z \times Z, +, \circ)$  dell'esempio 2 del capitolo 26.

Soluzione. Si osservi intanto che  $(Z \times Z, +, \circ)$  è un anello con identità, e che si ha  $0_{Z \times Z} = (0, 0)$  e  $1_{Z \times Z} = (1, 0)$  (perché  $(0, 0) + (a, b) = (a, b)$ ,  $(a, b) + (0, 0) = (a, b)$ ,  $(1, 0) \circ (a, b) = (a, b)$ ,  $(a, b) \circ (1, 0) = (a, b)$  per ogni  $(a, b) \in Z \times Z$ ). Inoltre per ogni numero naturale  $n > 0$  si ha

$$\underbrace{(1, 0) + (1, 0) + \dots + (1, 0)}_{n \text{ volte}} = (n, 0) \neq 0_{Z \times Z} = (0, 0).$$

Quindi  $(Z \times Z, +, \circ)$  ha caratteristica 0.  $\square$

28.3. Siano  $n, m \geq 2$  numeri naturali. Sia  $R$  un anello con  $m$  elementi e sia  $M_n(R)$  l'anello delle matrici quadrate di ordine  $n$  ad elementi in  $R$  (vedi esempio 6 del capitolo 27). Si dimostri che l'anello  $M_n(R)$  ha  $m^{(n^2)}$  elementi e che la sua caratteristica è uguale alla caratteristica di  $R$ .

Soluzione. Gli elementi di  $M_n(R)$  sono le matrici

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$



dove gli  $a_{ij} \in R$ . Ciascun  $a_{ij}$  può essere scelto in  $m$  modi diversi e gli  $a_{ij}$  in una matrice sono  $n^2$ . Quindi le matrici

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

possono essere costruite in  $\underbrace{m \cdot m \cdot \dots \cdot m}_{n^2 \text{ volte}} = m^{(n^2)}$  modi diversi. Se ne deduce che

$$|M_n(R)| = m^{(n^2)}.$$

Per quanto riguarda la caratteristica si osservi invece che nell'esempio 6 del capitolo 27 abbiamo dimostrato che lo zero di  $M_n(R)$  è la matrice quadrata di ordine  $n$

$$\begin{pmatrix} 0_R & 0_R & \dots & 0_R \\ 0_R & 0_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 0_R \end{pmatrix}$$

e che l'identità dell'anello è la matrice

$$\begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 1_R \end{pmatrix}.$$

Quindi

$$\begin{aligned} n \cdot \begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 1_R \end{pmatrix} &= \\ &= \underbrace{\begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 1_R \end{pmatrix} + \dots + \begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 1_R \end{pmatrix}}_{n \text{ volte}} = \\ &= \begin{pmatrix} n \cdot 1_R & 0_R & \dots & 0_R \\ 0_R & n \cdot 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & n \cdot 1_R \end{pmatrix}, \end{aligned}$$

e pertanto

$$n \cdot \begin{pmatrix} 1_R & 0_R & \dots & 0_R \\ 0_R & 1_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 1_R \end{pmatrix} = \begin{pmatrix} 0_R & 0_R & \dots & 0_R \\ 0_R & 0_R & \dots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \dots & 0_R \end{pmatrix}$$

se e solo se  $n \cdot 1_R = 0_R$ . Se ne deduce che  $M_n(R)$  ed  $R$  hanno la stessa caratteristica.  $\square$

### Altri esercizi

**28.4.** Sia  $Z_4$  l'anello delle classi resto modulo 4 ed  $R = Z_4 \times Z_4 \times Z_4$  l'insieme di tutte le terne di elementi di  $Z_4$ . Si definiscano su  $R$  le operazioni  $+$  e  $\cdot$  ponendo  $(a, b, c) + (a', b', c') = (a+a', b+b', c+c')$  e  $(a, b, c)(a', b', c') = (aa', ab'+ba', ac'+ca')$  per ogni  $(a, b, c), (a', b', c') \in R$ . È allora possibile dimostrare che  $R$  con queste operazioni è un anello commutativo con identità.

(a) Quanti elementi ha  $R$ ?

(b) Si determini l'identità di  $R$ .

(c) Si dimostri che  $\{0\} \times Z_4 \times Z_4$  è un ideale di  $R$  e che tutti gli elementi non nulli di  $\{0\} \times Z_4 \times Z_4$  sono divisori dello zero in  $R$ .

(d) Si determini la caratteristica di  $R$ .

**28.5.** Siano  $n \geq 2$  un numero intero,  $X$  un insieme non vuoto e  $Z_n$  l'anello delle classi resto degli interi modulo  $n$ . L'insieme

$$Z_n^X = \{f \mid f: X \rightarrow Z_n\}$$

è un anello se si definiscono le operazioni di addizione e di moltiplicazione ponendo  $(f+g)(x) = f(x) + g(x)$  e  $(fg)(x) = f(x)g(x)$  per ogni  $f, g \in Z_n^X$  e ogni  $x \in X$ .

(a) Qual è il sottoanello fondamentale di  $Z_n^X$ ?

(b) Qual è la caratteristica di  $Z_n^X$ ?

(c) Si dimostri che  $Z_n^X$  è un campo se e solo se  $X$  ha cardinalità 1 ed  $n$  è un numero primo.

**28.6.** Si dimostri che se  $R$  è un anello con identità finito con  $|R|$  elementi, allora la caratteristica di  $R$  è un divisore di  $|R|$ .

**28.7.** Si dimostri che in ogni anello  $R$  di caratteristica 2 si ha  $a = -a$  per ogni  $a \in R$ , cioè ogni elemento coincide col suo opposto.

**28.8.** Si dimostri che se  $R$  è un anello con identità avente un numero primo  $p$  di elementi, allora  $R$  è isomorfo al campo  $Z_p$ .

[Suggerimento: si consideri il gruppo additivo  $(R, +)$  e il suo sottogruppo  $(P_R, +)$ , ove  $P_R$  è il sottoanello fondamentale di  $R$ . Si applichi il teorema di Lagrange al gruppo  $R$  e al suo sottogruppo  $P_R$ .]

28.9. Si dimostri che ogni campo finito ha per caratteristica un numero primo.

28.10. Siano  $R$  ed  $S$  anelli con identità ed  $f: R \rightarrow S$  un omomorfismo di anelli con identità, cioè un omomorfismo d'anello tale che  $f(1_R) = 1_S$ .

- Si dimostri che se  $S$  ha caratteristica zero, allora anche l'anello  $R$  ha caratteristica zero.
- Si dimostri che se  $P_R$  e  $P_S$  sono il sottoanello fondamentale di  $R$  e di  $S$  rispettivamente, allora  $f(P_R) = P_S$ .
- Si dimostri che se  $R$  ha caratteristica  $n > 0$ , allora la caratteristica di  $S$  è un divisore di  $n$ .

28.11. Sia  $(Q, +)$  il gruppo additivo dei numeri razionali. Si definisca un'operazione  $*$  in  $Q$  ponendo  $x * y = \frac{5}{3}xy$  per ogni  $x, y \in Q$ . È allora possibile dimostrare che  $(Q, +, *)$  è un anello commutativo con identità.

- Si determini l'identità di  $(Q, +, *)$ .
- Si calcoli la caratteristica di  $(Q, +, *)$ .
- Si determini il sottoanello fondamentale di  $(Q, +, *)$  dei numeri razionali.
- Si dimostri che  $(Q, +, *)$  è un campo isomorfo al campo  $(Q, +, \cdot)$  dei numeri razionali. Qui  $\cdot$  denota la moltiplicazione usuale tra numeri razionali.

28.12. Sia  $A = \mathbb{R} \times \mathbb{Z}_8$ , dove  $\mathbb{R}$  denota l'insieme dei numeri reali e  $\mathbb{Z}_8$  denota l'insieme delle classi resto degli interi modulo 8. Su  $A$  si definiscano due operazioni  $+$  e  $\cdot$  ponendo  $(a, b) + (a', b') = (a + a', b + b')$  e  $(a, b)(a', b') = (aa', bb')$  per ogni  $(a, b), (a', b') \in A$ . È allora possibile dimostrare che  $A$  con queste operazioni diventa un anello commutativo con identità.

- L'anello  $A$  è un dominio d'integrità?
- Si dimostri che  $\{0\} \times \mathbb{Z}_8$  è un ideale massimale di  $A$ .
- Si dimostri che l'ideale  $\mathbb{R} \times \{0\}$  di  $A$  non è un ideale primo.
- Si calcoli la caratteristica di  $A$ .

[Suggerimento per (b): applicare il teorema fondamentale di omomorfismo per gli anelli alla proiezione canonica sul primo fattore  $\pi_R: \mathbb{R} \times \mathbb{Z}_8 \rightarrow \mathbb{R}$ .]

28.13. Siano  $R$  un anello commutativo con identità,  $M$  un suo ideale massimale e  $A$  un sottoanello di  $R$ . Si dimostri che:

- il sottoinsieme  $A + M = \{a + m \mid a \in A, m \in M\}$  di  $R$  è un sottoanello di  $R$ ;
- il sottoinsieme  $M$  di  $A + M$  è un ideale primo di  $A + M$ .

## Capitolo 29. Anelli booleani

Se  $R$  è un anello ed  $e \in R$ , diremo che  $e$  è *idempotente* se  $e^2 = e$ . Un anello booleano (o anello di Boole) è un anello con identità in cui ogni elemento è idempotente.

LEMMA 29.1. Ogni anello booleano è un anello commutativo di caratteristica 2.

ESEMPIO 1. Sia  $X$  un insieme,  $\mathcal{P}(X)$  l'insieme delle parti di  $X$ ,  $\Delta$  la differenza simmetrica e  $\cap$  l'intersezione. Si noti che se  $A, B \in \mathcal{P}(X)$  allora  $A \Delta B \in \mathcal{P}(X)$  (perché  $A \Delta B \subseteq A \cup B \subseteq X$ ) e  $A \cap B \in \mathcal{P}(X)$ . Quindi  $\Delta$  e  $\cap$  sono due operazioni su  $\mathcal{P}(X)$ , e non è difficile verificare che  $(\mathcal{P}(X), \Delta, \cap)$  è un anello commutativo con identità, detto l'anello delle parti di  $X$ . Lo zero dell'anello è  $0_{\mathcal{P}(X)} = \emptyset$ , l'identità è  $1_{\mathcal{P}(X)} = X$ , l'opposto di un elemento  $A \in \mathcal{P}(X)$  è  $A$  stesso perché  $A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$ , e ogni elemento di  $\mathcal{P}(X)$  è idempotente perché  $A^2 = A \cap A = A$ . Quindi  $\mathcal{P}(X)$  è un anello booleano.  $\square$

ESEMPIO 2. Il campo  $\mathbb{Z}_2$  è un anello booleano. Viceversa per il lemma 29.1 e la proposizione 28.5, dato un qualunque anello booleano  $R$  il suo sottoinsieme  $P = \{0_R, 1_R\}$  è un sottoanello di  $R$  isomorfo a  $\mathbb{Z}_2$ . Quindi ogni anello booleano contiene un sottoanello isomorfo a  $\mathbb{Z}_2$ .  $\square$

TEOREMA 29.2. Sia  $(R, +, \cdot)$  un anello booleano. Definiamo una relazione  $\leq$  in  $R$  ponendo, per ogni  $a, b \in R$ ,  $a \leq b$  se  $ab = a$ . Allora  $(R, \leq)$  è un reticolo booleano con almeno due elementi.

Viceversa sia  $(L, \leq)$  un reticolo booleano con almeno due elementi. Definiamo due operazioni  $+$  e  $\cdot$  nell'insieme  $L$  ponendo, per ogni  $a, b \in L$ ,  $a + b = (a \wedge b') \vee (a' \wedge b)$  e  $ab = a \wedge b$ . Allora  $(L, +, \cdot)$  è un anello booleano.

Si potrebbe dimostrare che nel reticolo booleano  $(R, \leq)$  costruito a partire dall'anello booleano  $(R, +, \cdot)$  nel modo descritto nell'enunciato del teorema 29.2, gli estremi superiori e inferiori di  $\{a, b\}$  sono dati, per ogni  $a, b \in R$ , dalle formule

$$a \vee b = a + b + ab \quad \text{e} \quad a \wedge b = ab.$$

Le due costruzioni descritte nel teorema precedente, ossia la costruzione del reticolo booleano con almeno due elementi  $(R, \leq)$  a partire dall'anello booleano  $(R, +, \cdot)$  e la costruzione dall'anello booleano  $(L, +, \cdot)$  a partire dal reticolo

booleano con almeno due elementi  $(L, \leq)$ , sono una l'inversa dell'altra. Questo significa che partendo da un reticolo booleano  $(L, \leq)$ , costruendo l'anello booleano ad esso associato  $(L, +, \cdot)$ , e poi costruendo il reticolo booleano a partire dall'anello  $(L, +, \cdot)$ , si ritrova esattamente il reticolo booleano associato. Analogamente se si parte da un anello booleano, si costruisce l'anello booleano associato, e poi si costruisce l'anello booleano associato a questo reticolo, si ritrova esattamente l'anello booleano di partenza. Verifichiamo la prima di queste due asserzioni. Partendo dal reticolo booleano  $(L, \leq)$ , costruiamo l'anello booleano  $(L, +, \cdot)$ ; quindi definiamo su  $L$  le due operazioni di addizione e di moltiplicazione ponendo  $a + b = (a \wedge b') \vee (a' \wedge b)$  e  $ab = a \wedge b$ ; qui con  $\vee, \wedge$  e  $'$  si denotano le due relazioni  $\leq$  e  $\leq$  su  $L$  coincidenti. In base al teorema 29.2 la relazione  $\leq$  è l'ordine parziale sull'insieme  $L$  definito, per ogni  $a, b \in L$ , da  $a \leq b$  se e solo se  $ab = a$ . Quindi  $a \leq b$  se e solo se  $a \wedge b = a$  nel reticolo  $(L, \leq)$ , cioè, per quanto visto nell'esempio 1 del capitolo 11, se e solo se  $a \leq b$ . Quindi le due relazioni  $\leq$  e  $\leq$  su  $L$  coincidono, ossia  $(L, \leq)$  è proprio il reticolo  $(L, \leq)$  da cui si era partiti.

ESEMPIO 3. Se  $X \neq \emptyset$  è un insieme, l'anello booleano associato al reticolo booleano  $(\mathcal{P}(X), \subseteq)$  (che ha almeno due elementi) è l'anello  $(\mathcal{P}(X), \Delta, \cap)$  delle parti di  $X$  dell'esempio 1. Infatti l'addizione nell'anello  $\mathcal{P}(X)$  è definita, per ogni  $A, B \in \mathcal{P}(X)$  da  $A + B = (A \wedge B') \vee (A' \wedge B) = (A \cap (X \setminus B)) \cup ((X \setminus A) \cap B) = (A \setminus B) \cup (B \setminus A) = A \Delta B$ , e quindi l'addizione  $+$  in  $\mathcal{P}(X)$  è proprio la differenza simmetrica  $\Delta$ . Per quanto riguarda la moltiplicazione in  $\mathcal{P}(X)$  si ha  $AB = A \wedge B = A \cap B$ , e pertanto la moltiplicazione in  $\mathcal{P}(X)$  è proprio l'intersezione  $\cap$  tra insiemi.  $\square$

TEOREMA 29.3. Ogni anello booleano è isomorfo a un sottoanello dell'anello  $(\mathcal{P}(X), \Delta, \cap)$  per un opportuno insieme non vuoto  $X$ . Ogni anello booleano finito è isomorfo all'anello  $(\mathcal{P}(X), \Delta, \cap)$  per un opportuno insieme finito non vuoto  $X$ .

COROLLARIO 29.4. Ogni reticolo booleano è isomorfo a un sottoreticolo del reticolo  $(\mathcal{P}(X), \subseteq)$  per un opportuno insieme  $X$ . Ogni reticolo booleano finito è isomorfo al reticolo  $(\mathcal{P}(X), \subseteq)$  per un opportuno insieme finito  $X$ .

COROLLARIO 29.5. Esiste un anello booleano finito con  $n$  elementi se e solo se  $n = 2^m$  per qualche intero  $m \geq 1$ . Esiste un reticolo booleano finito con  $n$  elementi se e solo se  $n = 2^m$  per qualche intero  $m \geq 0$ .

COROLLARIO 29.6. Due anelli booleani finiti sono isomorfi se e solo se sono equipotenti. Due reticoli booleani finiti sono isomorfi se e solo se sono equipotenti.

### I reticoli come strutture algebriche.

TEOREMA 29.7. Sia  $(L, \leq)$  un reticolo. Nell'insieme  $L$  si definiscano due operazioni  $\vee : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \vee y$  per ogni  $x, y \in L$ , e  $\wedge : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \wedge y$  per ogni  $x, y \in L$ . Allora le operazioni  $\vee$  e  $\wedge$  soddisfano alle seguenti proprietà:

- commutatività:  $x \vee y = y \vee x$ ,  $x \wedge y = y \wedge x$  per ogni  $x, y \in L$ ;
- associatività:  $x \vee (y \vee z) = (x \vee y) \vee z$ ,  $x \wedge (y \wedge z) = (x \wedge y) \wedge z$  per ogni  $x, y, z \in L$ ;
- proprietà di assorbimento:  $x \vee (x \wedge y) = x$ ,  $x \wedge (x \vee y) = x$  per ogni  $x, y \in L$ .

Viceversa sia  $(L, \vee, \wedge)$  un insieme  $L$  su cui sono definite due operazioni  $\vee$  e  $\wedge$  che soddisfano alle tre proprietà (a), (b), (c) precedenti. Nell'insieme  $L$  si definisca una relazione  $\leq$  ponendo, per ogni  $x, y \in L$ ,  $x \leq y$  se  $x \wedge y = x$ . Allora  $(L, \leq)$  è un reticolo.

In base al teorema 29.7 i reticoli possono essere visti indifferentemente o come insiemi  $L$  parzialmente ordinati in cui  $\{x, y\}$  ha estremo superiore ed estremo inferiore per ogni  $x, y \in L$  oppure come strutture algebriche, ossia come insiemi  $L$  con due operazioni binarie  $\vee$  e  $\wedge$  entrambe soddisfacenti alle proprietà commutativa, associativa e di assorbimento.

ESEMPIO 4. Nel reticolo  $(\mathbb{R}, \leq)$ , dove  $\leq$  è l'ordinamento usuale nell'insieme  $\mathbb{R}$  dei numeri reali, per ogni  $x, y \in \mathbb{R}$  si ha  $x \vee y = \max\{x, y\}$  e  $x \wedge y = \min\{x, y\}$ , dove  $\max$  e  $\min$  denotano rispettivamente il maggiore e il minore tra  $x$  e  $y$ . Quindi la struttura algebrica corrispondente al reticolo  $(\mathbb{R}, \leq)$  è  $(\mathbb{R}, \max, \min)$ .  $\square$

COROLLARIO 29.8. Sia  $(L, \leq)$  un reticolo distributivo. Nell'insieme  $L$  si definiscano due operazioni  $\vee : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \vee y$  per ogni  $x, y \in L$ , e  $\wedge : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \wedge y$  per ogni  $x, y \in L$ . Allora le operazioni  $\vee$  e  $\wedge$  soddisfano alle seguenti proprietà:

- commutatività:  $x \vee y = y \vee x$ ,  $x \wedge y = y \wedge x$  per ogni  $x, y \in L$ ;
- associatività:  $x \vee (y \vee z) = (x \vee y) \vee z$ ,  $x \wedge (y \wedge z) = (x \wedge y) \wedge z$  per ogni  $x, y, z \in L$ ;
- proprietà di assorbimento:  $x \vee (x \wedge y) = x$ ,  $x \wedge (x \vee y) = x$  per ogni  $x, y \in L$ ;
- distributività:  $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ ,  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$  per ogni  $x, y, z \in L$ .

Viceversa sia  $(L, \vee, \wedge)$  un insieme  $L$  su cui sono definite due operazioni  $\vee$  e  $\wedge$  che soddisfano alle quattro proprietà (a), (b), (c), (d) precedenti. Nell'insieme  $L$  si definisca una relazione  $\leq$  ponendo, per ogni  $x, y \in L$ ,  $x \leq y$  se  $x \wedge y = x$ . Allora  $(L, \leq)$  è un reticolo distributivo.

**COROLLARIO 29.9.** Sia  $(L, \leq)$  un reticolo limitato. Nell'insieme  $L$  si definiscano due operazioni  $\vee : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \vee y$  per ogni  $x, y \in L$ , e  $\wedge : L \times L \rightarrow L$  definita da  $(x, y) \mapsto x \wedge y$  per ogni  $x, y \in L$ . Allora le operazioni  $\vee$  e  $\wedge$  soddisfano alle seguenti proprietà:

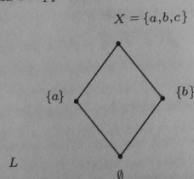
- (a) *commutatività*:  $x \vee y = y \vee x$ ,  $x \wedge y = y \wedge x$  per ogni  $x, y \in L$ ;
- (b) *associatività*:  $x \vee (y \vee z) = (x \vee y) \vee z$ ,  $x \wedge (y \wedge z) = (x \wedge y) \wedge z$  per ogni  $x, y, z \in L$ ;
- (c) *proprietà di assorbimento*:  $x \vee (x \wedge y) = x$ ,  $x \wedge (x \vee y) = x$  per ogni  $x, y \in L$ ;
- (d) *elementi neutri*: esistono  $0, 1 \in L$  tali che  $x \vee 0 = x$ ,  $x \wedge 1 = x$  per ogni  $x \in L$ .

Viceversa sia  $(L, \vee, \wedge)$  un insieme  $L$  su cui sono definite due operazioni  $\vee$  e  $\wedge$  che soddisfano alle quattro proprietà (a), (b), (c), (d) precedenti. Nell'insieme  $L$  si definisca una relazione  $\leq$  ponendo, per ogni  $x, y \in L$ ,  $x \leq y$  se  $x \wedge y = x$ . Allora  $(L, \leq)$  è un reticolo limitato.

Siano  $L, L'$  due reticoli. Un'applicazione  $\varphi : L \rightarrow L'$  si dice un *omomorfismo di reticoli* se per ogni  $x, y \in L$  si ha  $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$  e  $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$ . Un *isomorfismo di reticoli* è un omomorfismo biiettivo di reticoli.

**ESEMPIO 5.** Se  $(L, \leq)$ ,  $(L', \leq)$  sono reticoli, ogni omomorfismo di reticoli  $\varphi : L \rightarrow L'$  è anche un omomorfismo di insiemi ordinati. Per dimostrarlo è sufficiente osservare che se  $\varphi$  è un omomorfismo di reticoli,  $x, y \in L$  e  $x \leq y$ , allora  $x \wedge y = x$ , e quindi  $\varphi(x) \wedge \varphi(y) = \varphi(x \wedge y) = \varphi(x)$ , da cui si deduce che  $\varphi(x) \leq \varphi(y)$ . Pertanto  $\varphi$  è un omomorfismo di insiemi ordinati.

Però non vale il viceversa, cioè esistono reticoli  $(L, \leq)$ ,  $(L', \leq)$  e omomorfismi di insiemi ordinati  $\varphi : L \rightarrow L'$  che non sono omomorfismi di reticoli. Ad esempio sia  $X = \{a, b, c\}$  un insieme di cardinalità 3 e sia  $L = \{\emptyset, \{a\}, \{b\}, X\}$ . Si ordini parzialmente  $L$  mediante l'inclusione  $\subseteq$ . Allora  $(L, \subseteq)$  è l'insieme parzialmente ordinato il cui diagramma è rappresentato nella figura:



In particolare  $L$  è un reticolo; anzi,  $L$  è addirittura un reticolo booleano, perché è isomorfo a  $(\mathcal{P}(Y), \subseteq)$  dove  $Y$  denota un qualunque insieme di cardina-

lità 2. Consideriamo l'applicazione  $\varepsilon : L \rightarrow \mathcal{P}(X)$  definita da  $\varepsilon(A) = A$  per ogni  $A \in L$ ; l'applicazione  $\varepsilon$  è un omomorfismo di insiemi parzialmente ordinati, perché se  $A, B \in L$  e  $A \subseteq B$  allora  $\varepsilon(A) = A \subseteq B = \varepsilon(B)$ . Invece  $\varepsilon$  non è un omomorfismo di reticoli, perché ad esempio  $\varepsilon(\{a\} \vee \{b\}) = \varepsilon(X) = X$  mentre  $\varepsilon(\{a\}) \vee \varepsilon(\{b\}) = \varepsilon(\{a\}) \cup \varepsilon(\{b\}) = \{a\} \cup \{b\} = \{a, b\}$ , e pertanto  $\varepsilon(\{a\} \vee \{b\}) \neq \varepsilon(\{a\}) \vee \varepsilon(\{b\})$ .  $\square$

### Esercizi svolti

**29.1.** Si dimostri che ogni anello booleano con due elementi è un campo isomorfo all'anello delle classi resto  $\mathbb{Z}_2$ . Si dimostri che ogni anello booleano con più di due elementi non è un dominio d'integrità.

*Soluzione.* Se  $R$  è un anello booleano,  $R$  ha caratteristica 2, e quindi il suo sottoanello fondamentale  $P$  è isomorfo a  $\mathbb{Z}_2$ . Ma  $\mathbb{Z}_2 \cong P \subseteq R$ , e pertanto se  $R$  ha due elementi si deve avere  $P = R$ . Quindi  $R \cong \mathbb{Z}_2$  è un campo.

Supponiamo invece che  $R$  sia un anello booleano con più di due elementi. Quindi in  $R$  oltre a  $0_R$  e a  $1_R$  c'è almeno un terzo elemento  $e \in R$ ,  $e \neq 0_R$ ,  $e \neq 1_R$ . Da  $e \neq 1_R$  segue che  $1_R - e \neq 0_R$  (perché se fosse  $1_R - e = 0_R$ , allora  $1_R = e$ , il che non è). Quindi  $e \neq 0_R$ ,  $1_R - e \neq 0_R$  ed  $e(1_R - e) = e - e^2 = e - e = 0_R$ . Quindi  $R$  non è un dominio d'integrità.  $\square$

**29.2.** Si provi che in un anello booleano ogni ideale primo è massimale.

*Soluzione.* Sia  $P$  un ideale primo di un anello booleano  $R$ . Allora  $R/P$  è un dominio d'integrità per la proposizione 28.7, ed è un anello booleano perché per ogni  $x + P \in R/P$  si ha

$$(x + P)^2 = (x + P)(x + P) = x^2 + P = x + P.$$

Quindi  $R/P$  è un anello booleano che è anche un dominio d'integrità. Per quanto visto nella seconda parte dell'esercizio 29.1  $R/P$  non può avere più di due elementi. Ma ogni anello con identità ha almeno due elementi. Quindi  $R/P$  è un anello booleano con esattamente due elementi. Per quanto visto nella prima parte dell'esercizio 29.1  $R/P$  è un campo (isomorfo a  $\mathbb{Z}_2$ ), e quindi  $P$  è un ideale massimale di  $R$  per la proposizione 28.7.  $\square$

### Altri esercizi

**29.3.** Sia  $R^X$  l'anello delle applicazioni di un insieme fissato non vuoto  $X$  in  $R$  (esercizio 26.5). Si determinino gli elementi idempotenti in questo anello.

29.4. Si dimostri che se  $(R, +, \cdot)$  è un anello booleano,  $e \in R$ ,  $e \neq 0$  ed  $S = \{er \mid r \in R\}$ , allora  $S$  è un sottoinsieme di  $R$  chiuso rispetto a entrambe le operazioni  $+$  e  $\cdot$ , e che  $(S, +, \cdot)$ , ossia l'insieme  $S$  dotato delle operazioni indotte da quelle di  $R$ , è un anello booleano.

29.5. (a) Si dimostri che in un anello booleano  $R$  ogni elemento  $x$  diverso da  $0_R$  e da  $1_R$  è un divisore dello zero.

(b) Si determini il gruppo  $U(R)$  degli elementi invertibili di un anello booleano  $R$ .

29.6. Sia  $(R, +, \cdot)$  un anello commutativo con identità ed

$$E_R = \{e \in R \mid e^2 = e\}$$

l'insieme degli elementi idempotenti di  $R$ .

(a) È vero che qualunque sia l'anello commutativo con identità  $R$ , il sottoinsieme  $E_R$  è un sottoanello di  $R$ ?

(b) Si dimostri che  $E_R$  è chiuso per l'operazione  $\oplus$  definita, per ogni  $a, b \in E_R$ , da  $a \oplus b = a + b - ab$  (e quindi  $\oplus$  è un'operazione in  $E_R$ ).

(c) Si dimostri che  $E_R$  è un sottomonoidale del monoidale  $(R, \cdot)$ .

(d) Si dimostri che  $(E_R, \oplus, \cdot)$  è un anello booleano.

29.7. Si consideri  $Z_2[x]$ , anello dei polinomi nell'indeterminata  $x$  a coefficienti nel campo  $Z_2$ . Sia  $I = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid n \in \mathbb{N}, a_i \in Z_2 \text{ per ogni } i = 0, 1, \dots, n, a_0 = a_1 = 0\}$ .

(a) Si dimostri che  $I = \{x^2f \mid f \in Z_2[x]\}$ .

(b) Si dimostri che  $I$  è un ideale di  $Z_2[x]$ .

(c) Si calcoli la caratteristica di  $Z_2[x]/I$ .

(d) Si dica se  $Z_2[x]/I$  è un anello booleano.

29.8. Si consideri l'anello commutativo con identità  $Z_2 \times Z_2$  con le operazioni definite da  $(a, x) + (b, y) = (a + b, x + y)$  e  $(a, x)(b, y) = (ab, xy)$  per ogni  $(a, x), (b, y) \in Z_2 \times Z_2$ .

(a) Si calcoli la caratteristica di  $Z_2 \times Z_2$ .

(b) Si dica se  $Z_2 \times Z_2$  è un anello booleano.

29.9. Sia  $(R^R, \leq)$  il reticolo dell'esempio 3 del capitolo 11 e sia

$$L = \{f \in R^R \mid f(R) \subseteq \{0, 1\}\}.$$

(a) Si dimostri che  $L$  è un sottoreticolo di  $R^R$ .

(b) Si dimostri che il reticolo  $L$  è booleano.

(c) Sia  $(L, \oplus, \otimes)$  l'anello booleano associato al reticolo booleano  $L$ . Siano  $f, g: R \rightarrow R$  definite da

$$f(x) = \begin{cases} 0 & \text{se } x \leq 1 \\ 1 & \text{se } x > 1 \end{cases}, \quad g(x) = \begin{cases} 1 & \text{se } x < 2 \\ 0 & \text{se } x \geq 2 \end{cases}.$$

Si determinino le applicazioni  $f \oplus g$  ed  $f \otimes g$ .

29.10. Si consideri il reticolo di Boole  $(L, |)$ , ove  $L \subseteq \mathbb{N}^*$  denota l'insieme dei divisori positivi di 330.  $L$  è quindi un sottoreticolo del reticolo  $(\mathbb{N}^*, |)$ .

(a) Si dica quali sono il massimo e il minimo di  $L$ .

(b) Si calcoli  $6 \vee 10$  in  $L$  e il complemento di 6 in  $L$ .

(c) Quanti elementi ha  $L$ ?

(d) Si provi che  $L$  è isomorfo a  $(\mathcal{P}(\{1, 2, 3, 4\}), \subseteq)$ .

(e) Sia ora  $(L, \oplus, \otimes)$  l'anello booleano associato al reticolo booleano  $(L, |)$ . Si determinino  $6 \oplus 10$  e  $6 \otimes 10$ .

29.11. Si dia un esempio di un anello booleano avente otto elementi.

29.12. Sia  $R$  un anello booleano con quattro elementi. Siano  $a$  e  $b$  i due elementi di  $R$  diversi da 0 e 1. Si provi che  $a + b = 1$ .

29.13. Sia  $B = \{a, b, c, d\}$  un anello booleano con quattro elementi. Si dimostri che  $a + b + c + d = 0$ .

29.14. (a) Esiste un anello commutativo con 14 elementi?

(b) Esiste un anello booleano con 14 elementi?

29.15. Si dia un esempio, se esiste, di un reticolo booleano avente esattamente 8 elementi.

29.16. Sia  $R$  un anello booleano finito. Si provi che il prodotto di tutti gli elementi non nulli di  $R$  è  $1_R$  se  $R$  ha due elementi, mentre è  $0_R$  se  $R$  ha più di due elementi.

29.17. Sia  $(B, \leq)$  un reticolo booleano avente 8 elementi. Sia 0 il minimo di  $B$  e si consideri il sottoinsieme ordinato  $B \setminus \{0\}$  di  $B$ . Si dimostri che  $B \setminus \{0\}$  ha esattamente tre elementi minimali.

29.18. Si dimostri che se  $R$  è un anello booleano che è un dominio d'integrità, allora  $R$  è isomorfo all'anello  $Z_2$ .

29.19. Sia  $\varphi: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$  l'applicazione definita, per ogni  $X \in \mathcal{P}(\mathbb{N})$ , da  $\varphi(X) = \{n \in \mathbb{N} \mid \text{esiste } x \in X \text{ tale che } x \leq n\}$ .

(a) Si dica se  $\varphi$  è un omomorfismo di reticoli del reticolo  $(\mathcal{P}(\mathbb{N}), \subseteq)$  in sé stesso.

(b) Si dica se  $\varphi$  è un isomorfismo di reticoli del reticolo  $(\mathcal{P}(\mathbb{N}), \subseteq)$  in sé stesso.



- (c) Si dica se  $\varphi$  è un omomorfismo di insiemi parzialmente ordinati.  
 (d) Si dica se  $\varphi$  è un isomorfismo di insiemi parzialmente ordinati.

### Capitolo 30. Algebre di Boole

**TEOREMA 30.1.** Sia  $(B, \leq)$  un reticolo booleano. Nell'insieme  $B$  si definiscano due operazioni binarie  $\vee : B \times B \rightarrow B$ , definita da  $(x, y) \mapsto x \vee y$  per ogni  $x, y \in B$ , e  $\wedge : B \times B \rightarrow B$ , definita da  $(x, y) \mapsto x \wedge y$  per ogni  $x, y \in B$ , e un'operazione unaria  $' : B \rightarrow B$ , definita da  $x \mapsto x'$  per ogni  $x \in B$ . Allora le operazioni  $\vee$ ,  $\wedge$  e  $'$  soddisfano alle seguenti proprietà:

- (a) *commutatività:*  $x \vee y = y \vee x$ ,  $x \wedge y = y \wedge x$  per ogni  $x, y \in B$ ;  
 (b) *associatività:*  $x \vee (y \vee z) = (x \vee y) \vee z$ ,  $x \wedge (y \wedge z) = (x \wedge y) \wedge z$  per ogni  $x, y, z \in B$ ;  
 (c) *proprietà di assorbimento:*  $x \vee (x \wedge y) = x$ ,  $x \wedge (x \vee y) = x$  per ogni  $x, y \in B$ ;  
 (d) *distributività:*  $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ ,  $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$  per ogni  $x, y, z \in B$ .  
 (e) *elementi neutri:* esistono  $0_B, 1_B \in B$  tali che  $x \vee 0_B = x$ ,  $x \wedge 1_B = x$  per ogni  $x \in B$ ;  
 (f) *proprietà del complemento:*  $x \vee x' = 1_B$  e  $x \wedge x' = 0_B$  per ogni  $x \in B$ .

Viceversa sia  $(B, \vee, \wedge, ')$  un insieme  $B$  su cui sono definite due operazioni binarie  $\vee$  e  $\wedge$  e un'operazione unaria  $'$  soddisfacenti le sei proprietà (a), (b), (c), (d), (e), (f) precedenti. Nell'insieme  $B$  si definisca una relazione  $\leq$  ponendo, per ogni  $x, y \in B$ ,  $x \leq y$  se  $x \wedge y = x$ . Allora  $(B, \leq)$  è un reticolo booleano.

Un'algebra di Boole  $(B, \vee, \wedge, ')$  è un insieme  $B$  dotato di due operazioni binarie  $\vee$  e  $\wedge$  e di un'operazione unaria  $'$  per le quali sono soddisfatte le sei proprietà dell'enunciato del teorema 30.1.

**ESEMPIO 1.** Sia  $X$  un insieme. Abbiamo già visto ripetutamente che  $(\mathcal{P}(X), \subseteq)$  è un reticolo booleano. L'algebra di Boole ad esso corrispondente è  $(\mathcal{P}(X), \cup, \cap, ')$ , dove, per ogni  $A \in \mathcal{P}(X)$ , si ha  $A' = X \setminus A$ . Il lettore ricordi che l'anello booleano corrispondente al reticolo booleano  $(\mathcal{P}(X), \subseteq)$  è l'anello  $(\mathcal{P}(X), \Delta, \cap)$ .  $\square$

Se  $B$  è un'algebra di Boole e  $C$  è un sottoinsieme di  $B$ ,  $C$  si dice una *subalgebra di Boole* di  $B$  se  $0_B, 1_B \in C$  e per ogni  $x, y \in B$  si ha  $x \vee y, x \wedge y, x' \in C$ .

**LEMMA 30.2.** Siano  $B, C$  due algebre di Boole e sia  $\varphi : B \rightarrow C$  un omomorfismo di reticoli. Le seguenti affermazioni sono equivalenti:

- (a)  $\varphi(0_B) = 0_C$ ,  $\varphi(1_B) = 1_C$ ;  
 (b)  $\varphi(x') = (\varphi(x))'$  per ogni  $x \in B$ .

*Dimostrazione.* (a)  $\Rightarrow$  (b) Si supponga che valga (a) e si fissi un elemento  $x \in B$ . Per dimostrare che  $\varphi(x') = (\varphi(x))'$ , cioè che  $\varphi(x')$  è il complemento di  $\varphi(x)$ , si deve provare che  $\varphi(x') \wedge \varphi(x) = 0$  e  $\varphi(x') \vee \varphi(x) = 1$ . Per l'ipotesi (a) si ha  $\varphi(x') \wedge \varphi(x) = \varphi(x' \wedge x) = \varphi(0) = 0$  e  $\varphi(x') \vee \varphi(x) = \varphi(x' \vee x) = \varphi(1) = 1$ .  
 (b)  $\Rightarrow$  (a) Si fissi un qualunque elemento  $x_0 \in B$ . Allora  $\varphi(0_B) = \varphi(x'_0 \wedge x_0) = \varphi(x'_0) \wedge \varphi(x_0) = (\varphi(x_0))' \wedge \varphi(x_0) = 0_C$ . Analogamente  $\varphi(1_B) = 1_C$ .  $\square$

Un omomorfismo di reticoli tra due algebre di Boole  $B$  e  $C$  che soddisfa alle condizioni equivalenti del lemma 30.2 si dice un *omomorfismo di algebre di Boole*. Un omomorfismo di algebre di Boole che sia biiettivo si dice un *isomorfismo* (di algebre di Boole). Se esiste un isomorfismo di  $B$  in  $C$  le due algebre  $B$  e  $C$  si dicono *isomorfe*.

**LEMMA 30.3.** Siano  $(B, \vee, \wedge, ')$ ,  $(C, \vee, \wedge, ')$  due algebre di Boole, e siano  $(B, +, \cdot)$ ,  $(C, +, \cdot)$  le corrispondenti strutture di anello booleano su  $B$  e  $C$ . Sia  $\varphi : B \rightarrow C$  un'applicazione. Le seguenti affermazioni sono equivalenti:

- (a)  $\varphi$  è un omomorfismo di algebre di Boole;  
 (b)  $\varphi$  è un omomorfismo di anelli con identità.

*Dimostrazione.* (a)  $\Rightarrow$  (b) Se  $\varphi$  è un omomorfismo di algebre di Boole, per ogni  $a, b \in B$  si ha  $\varphi(a + b) = \varphi((a \wedge b') \vee (a' \wedge b)) = (\varphi(a) \wedge \varphi(b')) \vee (\varphi(a') \wedge \varphi(b)) = \varphi(a) + \varphi(b)$ ,  $\varphi(ab) = \varphi(a \wedge b) = \varphi(a) \wedge \varphi(b) = \varphi(a)\varphi(b)$ , e  $\varphi(1) = 1$ . Quindi  $\varphi$  è un omomorfismo di anelli con identità.

(b)  $\Rightarrow$  (a) Se  $\varphi$  è un omomorfismo di anelli con identità, allora  $\varphi(0) = 0$  e  $\varphi(1) = 1$ . Per dimostrare che  $\varphi$  è un omomorfismo di algebre di Boole è quindi sufficiente dimostrare che è un omomorfismo di reticoli, cioè che per ogni  $a, b \in B$  si ha  $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$  e  $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$ . In base alle formule per  $a \vee b$  e  $a \wedge b$  scritte subito dopo l'enunciato del teorema 29.2 si ottiene che  $\varphi(a \vee b) = \varphi(a + b + ab) = \varphi(a) + \varphi(b) + \varphi(a)\varphi(b) = \varphi(a) \vee \varphi(b)$  e che  $\varphi(a \wedge b) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi(a) \wedge \varphi(b)$ . Questo conclude la dimostrazione.  $\square$

**COROLLARIO 30.4.** Siano  $(B, \vee, \wedge, ')$ ,  $(C, \vee, \wedge, ')$  due algebre di Boole, siano  $(B, +, \cdot)$ ,  $(C, +, \cdot)$  le corrispondenti strutture di anello booleano su  $B$  e  $C$ , e  $(B, \leq)$ ,  $(C, \leq)$  le strutture di reticolo booleano su  $B$  e  $C$ . Sia  $\varphi : B \rightarrow C$  un'applicazione. Le seguenti affermazioni sono equivalenti:

- (a)  $\varphi$  è un isomorfismo di algebre di Boole dell'algebra di Boole  $(B, \vee, \wedge, ')$  in  $(C, \vee, \wedge, ')$ ;

(b)  $\varphi$  è un isomorfismo di anelli con identità di  $(B, +, \cdot)$  in  $(C, +, \cdot)$ ;

(c)  $\varphi$  è un isomorfismo di insiemi parzialmente ordinati di  $(B, \leq)$  in  $(C, \leq)$ .

**COROLLARIO 30.5.** Ogni algebra di Boole è isomorfa a una sottoalgebra dell'algebra di Boole  $(\mathcal{P}(X), \cup, \cap, ')$  per un opportuno insieme non vuoto  $X$ . Ogni algebra di Boole finita è isomorfa all'algebra di Boole  $(\mathcal{P}(X), \cup, \cap, ')$  per un opportuno insieme finito  $X$ .

**COROLLARIO 30.6.** Esiste un'algebra di Boole finita con  $n$  elementi se e solo se  $n = 2^m$  per qualche intero  $m \geq 0$ .

**COROLLARIO 30.7.** Due algebre di Boole finite sono isomorfe se e solo se sono equipotenti.

Fissiamo ora l'insieme  $A = \{\vee, \wedge, ', 0, 1\}$  e definiamo un'applicazione  $\tau: A \rightarrow \mathbb{N}$  ponendo  $\tau(\vee) = \tau(\wedge) = 2$ ,  $\tau(') = 1$ ,  $\tau(0) = \tau(1) = 0$ . Allora  $(A, \tau)$  è un alfabeto valutato (vedi capitolo 20); in questo alfabeto le costanti sono 0 e 1. Fissiamo poi un insieme  $X = \{x_1, x_2, \dots, x_n\}$  di  $n$  elementi (che come nel capitolo 20 chiameremo *variabili*). Si possono quindi considerare le parole generate da  $(A, \tau)$  e  $X$ . Se  $w_1, w_2$  sono parole scriveremo  $(w_1 \vee w_2)$  invece di  $\vee w_1 w_2$ , scriveremo  $(w_1 \wedge w_2)$  invece di  $\wedge w_1 w_2$ , e scriveremo  $(w_1')$  invece di  $'w_1$ . Le parole generate da  $(A, \tau)$  e  $X$  si dicono i *polinomi booleani* nelle variabili  $x_1, x_2, \dots, x_n$ .

**ESEMPIO 2.** Sono polinomi booleani nelle variabili  $x_1, x_2, x_3, x_4, x_5$  i polinomi  $x_1 \vee (x_2')$ ,  $(x_1 \vee x_5) \wedge (x_1 \wedge x_2')$ ,  $(x_1 \wedge x_2) \vee (x_1 \wedge x_3)$ ,  $(x_1 \vee x_4)'$ .  $\square$

Fissato un qualunque polinomio booleano  $E(x_1, x_2, \dots, x_n)$  nelle  $n$  variabili  $x_1, x_2, \dots, x_n$  e una qualunque algebra booleana  $B$ , ad ogni  $n$ -upla  $(b_1, b_2, \dots, b_n)$  di elementi di  $B$  resta associato un elemento  $E(b_1, b_2, \dots, b_n)$  di  $B$  ottenuto sostituendo gli elementi  $b_i \in B$  alle variabili  $x_i$ . Quindi fissato un arbitrario polinomio booleano

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

e un'arbitraria algebra booleana  $B$  resta determinata un'applicazione

$$\underbrace{B \times \dots \times B}_{n \text{ volte}} \rightarrow B, \quad (b_1, b_2, \dots, b_n) \mapsto E(b_1, b_2, \dots, b_n).$$

Due polinomi booleani  $E_1(x_1, x_2, \dots, x_n)$ ,  $E_2(x_1, x_2, \dots, x_n)$  si dicono *equivalenti*, e scriveremo

$$E_1(x_1, x_2, \dots, x_n) \equiv E_2(x_1, x_2, \dots, x_n),$$

se si ha  $E_1(b_1, b_2, \dots, b_n) = E_2(b_1, b_2, \dots, b_n)$  per ogni algebra di Boole  $B$  e ogni  $n$ -upla  $(b_1, b_2, \dots, b_n)$  di elementi di  $B$ . Se  $\mathcal{E}(x_1, x_2, \dots, x_n)$  è l'insieme di tutti i polinomi booleani nelle variabili  $x_1, x_2, \dots, x_n$ , la relazione  $\equiv$  è un'equivalenza nell'insieme  $\mathcal{E}(x_1, x_2, \dots, x_n)$ . Nell'insieme quoziente  $\mathcal{B}(x_1, x_2, \dots, x_n) =$

$\mathcal{E}(x_1, x_2, \dots, x_n) / \equiv$  si definiscono due operazioni binarie  $\vee$  e  $\wedge$  e un'operazione unaria  $'$  ponendo

$$\begin{aligned} [E_1(x_1, x_2, \dots, x_n)] \vee [E_2(x_1, x_2, \dots, x_n)] &= [E_1(x_1, x_2, \dots, x_n) \vee E_2(x_1, x_2, \dots, x_n)], \\ [E_1(x_1, x_2, \dots, x_n)] \wedge [E_2(x_1, x_2, \dots, x_n)] &= [E_1(x_1, x_2, \dots, x_n) \wedge E_2(x_1, x_2, \dots, x_n)], \\ [E_1(x_1, x_2, \dots, x_n)]' &= [E_1(x_1, x_2, \dots, x_n)'] \end{aligned}$$

per ogni  $[E_1(x_1, x_2, \dots, x_n)], [E_2(x_1, x_2, \dots, x_n)] \in \mathcal{B}(x_1, x_2, \dots, x_n)$ .

È possibile dimostrare che  $(\mathcal{B}(x_1, x_2, \dots, x_n), \vee, \wedge, ')$  è un'algebra di Boole.

**TEOREMA 30.8.** Per ogni numero naturale  $n$  le algebre di Boole

$$\mathcal{P}(\mathcal{P}(\{x_1, \dots, x_n\})) \quad \text{e} \quad \mathcal{B}(x_1, x_2, \dots, x_n)$$

sono isomorfe.

Di questo teorema omettiamo la dimostrazione. Diciamo solamente come è definito l'isomorfismo di algebre di Boole

$$\varphi: \mathcal{P}(\mathcal{P}(\{x_1, \dots, x_n\})) \rightarrow \mathcal{B}(x_1, x_2, \dots, x_n).$$

Un arbitrario elemento di  $\mathcal{P}(\mathcal{P}(\{x_1, \dots, x_n\}))$  è della forma

$$\{A_1, A_2, \dots, A_m\}$$

dove  $A_1, A_2, \dots, A_m$  sono sottoinsiemi di  $X = \{x_1, x_2, \dots, x_n\}$ . L'isomorfismo  $\varphi$  è definito ponendo

$$\varphi(\{A_1, A_2, \dots, A_m\}) = \bigvee_{j=1}^m \left( \left( \bigwedge_{x \in A_j} x \right) \wedge \left( \bigwedge_{x \in X \setminus A_j} x' \right) \right).$$

Ne segue che dato un qualunque polinomio booleano  $E(x_1, x_2, \dots, x_n)$  esiste sempre un unico polinomio booleano ad esso equivalente del tipo

$$\bigvee_{j=1}^m \left( \left( \bigwedge_{x \in A_j} x \right) \wedge \left( \bigwedge_{x \in X \setminus A_j} x' \right) \right),$$

cioè ogni polinomio booleano è equivalente ad una disgiunzione di congiunzioni di variabili complementate e variabili non complementate. Un polinomio siffatto si dice in *forma normale disgiuntiva*.

Per trasformare un polinomio booleano nel polinomio in forma normale disgiuntiva ad esso equivalente si può procedere in tre passi: (1) innanzitutto applicando le regole di De Morgan (vedi esercizio 30.1) si fa in modo che la complementazione si applichi solo alle variabili; (2) poi mediante le proprietà

distributive si trasforma il polinomio in una disgiunzione di congiunzioni; le congiunzioni potranno non contenere qualche  $x_i$ , ma per ogni  $i$  conterranno o  $x_i$  o  $x'_i$  oppure nessuno dei due; (3) se infine nelle congiunzioni  $E_j$  così ottenute non appare una qualche variabile  $x_i$ , è sufficiente sostituire il polinomio  $E_j$  con il polinomio booleano ad esso equivalente  $E_j \wedge (x_i \vee x'_i) \equiv (E_j \wedge x_i) \vee (E_j \wedge x'_i)$ , ripetendo questa operazione finché tutte le variabili  $x_i$  appaiono (eventualmente complementate) in ogni congiunzione.

ESEMPIO 3. Si consideri il polinomio booleano

$$(x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \wedge x_3)'$$

nelle variabili  $x_1, x_2, x_3$ . Il primo passo (applicazione delle regole di De Morgan) ci porta alla seguente successione di polinomi booleani tra loro equivalenti:

$$\begin{aligned} (x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \wedge x_3)' &\equiv (x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \vee x'_3)' \\ &\equiv (x_1 \wedge (x_1 \vee x_2)) \vee x_1 \vee x_3. \end{aligned}$$

Distribuendo si ha poi

$$\begin{aligned} (x_1 \wedge (x_1 \vee x_2)) \vee x_1 \vee x_3 &\equiv (x_1 \wedge x_1) \vee (x_1 \wedge x_2) \vee x_1 \vee x_3 \equiv \\ &\equiv x_1 \vee (x_1 \wedge x_2) \vee x_1 \vee x_3 \equiv \\ &\equiv x_1 \vee (x_1 \wedge x_2) \vee x_3. \end{aligned}$$

Infine osservando che

$$\begin{aligned} x_1 &\equiv x_1 \wedge (x_2 \vee x'_2) \equiv (x_1 \wedge x_2) \vee (x_1 \wedge x'_2) \equiv \\ &\equiv (x_1 \wedge x_2 \wedge (x_3 \vee x'_3)) \vee (x_1 \wedge x'_2 \wedge (x_3 \vee x'_3)) \equiv \\ &\equiv (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x'_3) \vee (x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x'_2 \wedge x'_3), \\ x_1 \wedge x_3 &\equiv x_1 \wedge x_3 \wedge (x_2 \vee x'_2) \equiv (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x'_2 \wedge x_3), \end{aligned}$$

e similmente

$$x'_3 \equiv (x_1 \wedge x_2 \wedge x'_3) \vee (x'_1 \wedge x_2 \wedge x'_3) \vee (x_1 \wedge x'_2 \wedge x'_3) \vee (x'_1 \wedge x'_2 \wedge x'_3),$$

si ricava che il polinomio booleano  $(x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \wedge x_3)'$  da cui eravamo partiti è equivalente al polinomio

$$\begin{aligned} (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x'_3) \vee (x_1 \wedge x'_2 \wedge x_3) \vee \\ \vee (x_1 \wedge x'_2 \wedge x'_3) \vee (x'_1 \wedge x_2 \wedge x'_3) \vee (x'_1 \wedge x'_2 \wedge x'_3) \end{aligned}$$

che è in forma normale disgiuntiva. In particolare nell'isomorfismo tra  $\mathcal{B}(x_1, x_2, x_3)$  e  $\mathcal{P}(\mathcal{P}(\{x_1, x_2, x_3\}))$  l'elemento  $[(x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \wedge x_3)']$  di  $\mathcal{B}(x_1, x_2, x_3)$  corrisponde all'elemento

$$\{\{x_1, x_2, x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_1\}, \{x_2\}, \emptyset\}$$

di  $\mathcal{P}(\mathcal{P}(\{x_1, x_2, x_3\}))$ .  $\square$

Si osservi che il teorema 30.8 ha il seguente immediato corollario:

COROLLARIO 30.9. *L'algebra di Boole  $\mathcal{B}(x_1, x_2, \dots, x_n)$  ha  $2^{2^n}$  elementi.*

### Esercizi svolti

30.1. (Formule di De Morgan).

(a) Si dimostri che se  $B$  è un'algebra di Boole e  $a_1, a_2$  sono due suoi elementi allora

$$(a_1 \vee a_2)' = a'_1 \wedge a'_2 \quad \text{e} \quad (a_1 \wedge a_2)' = a'_1 \vee a'_2.$$

(b) Si dimostri che se  $E_1(x_1, x_2, \dots, x_n)$  ed  $E_2(x_1, x_2, \dots, x_n)$  sono due polinomi booleani, allora

$$\begin{aligned} (E_1(x_1, x_2, \dots, x_n) \vee E_2(x_1, x_2, \dots, x_n))' &\equiv \\ &\equiv (E_1(x_1, x_2, \dots, x_n))' \wedge (E_2(x_1, x_2, \dots, x_n))' \end{aligned}$$

$$\begin{aligned} \text{e} \quad (E_1(x_1, x_2, \dots, x_n) \wedge E_2(x_1, x_2, \dots, x_n))' &\equiv \\ &\equiv (E_1(x_1, x_2, \dots, x_n))' \vee (E_2(x_1, x_2, \dots, x_n))'. \end{aligned}$$

*Soluzione.* (a) Per dimostrare che  $(a_1 \vee a_2)' = a'_1 \wedge a'_2$ , cioè che  $a'_1 \wedge a'_2$  è il complemento di  $a_1 \vee a_2$ , è sufficiente dimostrare che

$$(a'_1 \wedge a'_2) \wedge (a_1 \vee a_2) = 0_B \quad \text{e} \quad (a'_1 \wedge a'_2) \vee (a_1 \vee a_2) = 1_B.$$

Un facile calcolo fa vedere che

$$\begin{aligned} (a'_1 \wedge a'_2) \wedge (a_1 \vee a_2) &= ((a'_1 \wedge a'_2) \wedge a_1) \vee ((a'_1 \wedge a'_2) \wedge a_2) = \\ &= ((a'_1 \wedge a_1) \wedge a'_2) \vee (a'_1 \wedge (a'_2 \wedge a_2)) = \\ &= (0_B \wedge a'_2) \vee (a'_1 \wedge 0_B) = 0_B \vee 0_B = 0_B, \end{aligned}$$

e in modo del tutto analogo si verifica che  $(a'_1 \wedge a'_2) \vee (a_1 \vee a_2) = 1_B$ .

(b) Per dimostrare che

$$\begin{aligned} (E_1(x_1, x_2, \dots, x_n) \vee E_2(x_1, x_2, \dots, x_n))' &\equiv \\ &\equiv (E_1(x_1, x_2, \dots, x_n))' \wedge (E_2(x_1, x_2, \dots, x_n))' \end{aligned}$$

si deve far vedere che per ogni algebra booleana  $B$  ed ogni  $n$ -upla  $(b_1, b_2, \dots, b_n)$  di elementi di  $B$  si ha  $(E_1(b_1, b_2, \dots, b_n) \vee E_2(b_1, b_2, \dots, b_n))' \equiv (E_1(b_1, b_2, \dots, b_n))' \wedge (E_2(b_1, b_2, \dots, b_n))'$ . Questo segue immediatamente da quanto dimostrato in (a) prendendo  $a_1 = E_1(b_1, b_2, \dots, b_n)$  e  $a_2 = E_2(b_1, b_2, \dots, b_n)$ . Similmente si dimostra la seconda formula.  $\square$

## Altri esercizi

30.2. Sia  $(L, |)$  il reticolo di Boole dei divisori positivi di 330 visto nell'esercizio 29.18, e sia  $(L, \vee, \wedge, ')$  l'algebra di Boole ad esso associata.

- (a) Si dica come sono definite le tre operazioni  $\vee, \wedge$  e  $'$ .  
 (b) Si dica se  $\{1, 3, 330\}$  è una sottoalgebra di Boole di  $L$ .  
 (c) Si dica se  $\{1, 2, 165, 330\}$  è una sottoalgebra di Boole di  $L$ .  
 (d) Sia  $\varphi: L \rightarrow \{0, 1\}$  definita da

$$\varphi(x) = \begin{cases} 0 & \text{se 2 non divide } x, \\ 1 & \text{se 2 divide } x. \end{cases}$$

Si dica se  $\varphi$  è un omomorfismo di algebre di Boole. Qui si intende naturalmente che  $\{0, 1\}$  è l'algebra di Boole con due elementi, ossia l'algebra di Boole associata al reticolo  $(\{0, 1\}, \leq)$  nel quale  $0 \leq 1$ .

30.3. Sia  $L$  il reticolo booleano dell'esercizio 29.9, e sia  $\varphi: L \rightarrow \{0, 1\}$  definita da  $\varphi(f) = f(\pi)$  per ogni  $f \in L$ . Si dica se  $\varphi$  è un omomorfismo di algebre di Boole.

30.4. Sia  $L$  il reticolo booleano dell'esercizio 29.9.

- (a) Si determinino come sono definite le operazioni  $\vee, \wedge$  e  $'$  nell'algebra di Boole associata.  
 (b) Sia  $\varphi: R \rightarrow R$  una biiezione, e si definisca un'applicazione  $\Phi: L \rightarrow L$  ponendo  $\Phi(f) = f \circ \varphi$  per ogni  $f \in L$ . Si dimostri che  $\Phi$  è un isomorfismo di algebre di Boole.  
 (c) Si costruisca un isomorfismo di algebre di Boole tra

$$L \text{ e } (\mathcal{P}(R), \cup, \cap, ').$$

30.5. Si costruisca, se è possibile, un'algebra di Boole  $B_1$  con un elemento, un'algebra di Boole  $B_2$  con due elementi, un'algebra di Boole  $B_3$  con tre elementi, un'algebra di Boole  $B_4$  con quattro elementi, un'algebra di Boole  $B_5$  con cinque elementi, un'algebra di Boole  $B_6$  con sei elementi.

30.6. Siano  $X = \{1, 2, 3\}$  e  $Y = \{y_1, y_2, y_3\}$  due insiemi con tre elementi. Si definisca un isomorfismo tra le algebre di Boole  $(\mathcal{P}(X), \cup, \cap, ')$  e  $(\mathcal{P}(Y), \cup, \cap, ')$ .

30.7. Un sottoinsieme  $I$  di un'algebra di Boole  $B$  si dice un *ideale* di  $B$  se valgono le seguenti tre proprietà: (a)  $0_B \in I$ ; (b) se  $x, y \in I$  allora  $x \vee y \in I$ ; (c) se  $x \in I$  e  $b \in B$  allora  $x \wedge b \in I$ . Si dimostri che un sottoinsieme  $I$  di un'algebra di Boole  $B$  è un ideale di  $B$  se e solo se valgono le seguenti tre proprietà: (a)  $I \neq \emptyset$ ; (b) se  $x, y \in I$  allora  $x \vee y \in I$ ; (c) se  $x \in I, b \in B$  e  $b \leq x$ , allora  $b \in I$ .

30.8. Sia  $(B, \vee, \wedge, ')$  un'algebra di Boole e sia  $(B, +, \cdot)$  l'anello booleano ad essa corrispondente. Sia  $I$  un sottoinsieme di  $B$ . Si dimostri che le seguenti affermazioni sono equivalenti:

- (a)  $I$  è un ideale dell'algebra di Boole  $B$  (vedi esercizio precedente);  
 (b)  $I$  è un ideale dell'anello  $B$ .

30.9. Un sottoinsieme  $F$  di un'algebra di Boole  $B$  si dice un *filtro* di  $B$  se valgono le seguenti tre proprietà: (a)  $1_B \in F$ ; (b) se  $x, y \in F$  allora  $x \wedge y \in F$ ; (c) se  $x \in F$  e  $b \in B$  allora  $x \vee b \in F$ . Si dimostri che:

- (a) se  $I$  è un ideale di  $B$ , allora  $F_I = \{x' \mid x \in I\}$  è un filtro di  $B$ ;  
 (b) se  $F$  è un filtro di  $B$ , allora  $I_F = \{x' \mid x \in F\}$  è un ideale di  $B$ ;  
 (c) se  $\mathcal{I}(B)$  e  $\mathcal{F}(B)$  sono, rispettivamente, l'insieme di tutti gli ideali e l'insieme di tutti i filtri di  $B$ , le applicazioni  $\Phi: \mathcal{I}(B) \rightarrow \mathcal{F}(B)$ , definita da  $\Phi(I) = F_I$  per ogni  $I \in \mathcal{I}(B)$ , e  $\Psi: \mathcal{F}(B) \rightarrow \mathcal{I}(B)$ , definita da  $\Psi(F) = I_F$  per ogni  $F \in \mathcal{F}(B)$ , sono due biiezioni una l'inversa dell'altra;  
 (d) se  $X$  è un insieme e  $\mathcal{P}_{\text{cof}}(X) = \{Y \mid Y \subseteq X, X \setminus Y \text{ finito}\}$  è l'insieme di tutti i sottoinsiemi cofiniti di  $X$  (cioè dei sottoinsiemi di  $X$  il cui complementare è finito), allora  $\mathcal{P}_{\text{cof}}(X)$  è un filtro dell'algebra di Boole  $(\mathcal{P}(X), \cup, \cap, ')$ ;  
 (e) se  $B$  è un'algebra di Boole e  $A$  è un suo sottoinsieme non vuoto, allora  $F = \{x \mid \text{esistono } n \in \mathbb{N}^* \text{ e } a_1, a_2, \dots, a_n \in A \text{ tali che } x \geq a_1 \wedge a_2 \wedge \dots \wedge a_n\}$  è un filtro di  $B$ .

30.10. I due polinomi booleani

$$(x_1 \vee (x_2 \wedge x_1)) \wedge x_2 \quad \text{e} \quad (x_1 \wedge x_2) \wedge (x_3 \vee x_3')$$

nelle variabili  $x_1, x_2, x_3$  sono equivalenti?

30.11. Si determini un insieme  $A$  tale che le algebre di Boole

$$\mathcal{B}(x_1, x_2, x_3) \quad \text{e} \quad \mathcal{P}(A)$$

siano isomorfe.

30.12. Si trovi il polinomio booleano in forma normale disgiuntiva nelle variabili  $x_1, x_2$  equivalente a ciascuno dei seguenti polinomi booleani:

- (a)  $x_1$ ;  
 (b)  $x_1 \wedge x_2$ ;  
 (c)  $(x_1 \wedge x_2) \vee x_1$ ;  
 (d)  $(x_1 \wedge x_2)' \vee x_1$ .

30.13. Si trovi il polinomio booleano in forma normale disgiuntiva equivalente al polinomio booleano  $((x_1' \vee x_2) \wedge x_3') \vee x_1$  nelle variabili  $x_1, x_2$  e  $x_3$ .

PARTE SESTA  
APPENDICI

## A. Alcuni esercizi più difficili

! 2.24. Si consideri l'applicazione  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definita, per ogni  $n \in \mathbb{N}$ , da

$$\varphi(n) = \begin{cases} 2n & \text{se } n \text{ è pari,} \\ 3n & \text{se } n \text{ è dispari.} \end{cases}$$

- (a) L'applicazione  $\varphi$  è iniettiva?
- (b) L'applicazione  $\varphi$  è suriettiva?

! 2.25. Si consideri l'applicazione  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definita, per ogni  $n \in \mathbb{N}$ , da

$$\varphi(n) = \begin{cases} n/2 & \text{se } n \text{ è pari,} \\ n/3 & \text{se } n \text{ è dispari e } 3 \text{ divide } n, \\ n & \text{se } n \text{ è dispari e } 3 \text{ non divide } n. \end{cases}$$

- (a) L'applicazione  $\varphi$  è iniettiva?
- (b) L'applicazione  $\varphi$  è suriettiva?

! 2.26. Si consideri l'applicazione  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$  definita da

$$\varphi(z) = \min\{z^3 - 64, z^2\}$$

per ogni  $z \in \mathbb{Z}$ .

- (a) L'applicazione  $\varphi$  è iniettiva?
- (b) L'applicazione  $\varphi$  è suriettiva?

! 2.27. Sia  $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$  l'applicazione definita da  $\varphi(x) = x^4$  per ogni  $x \in \mathbb{Z}$ .

- (a) L'applicazione  $\varphi$  è iniettiva? È suriettiva?



- (b) Si determinino due diversi sottoinsiemi  $S, T$  di  $\mathbb{R}$  tali che

$$\varphi^{-1}(S) = \varphi^{-1}(T).$$

- (c) Esiste un'applicazione  $\psi: \mathbb{R} \rightarrow \mathbb{Z}$  tale che  $\varphi(\psi(\alpha)) = \alpha$  per ogni  $\alpha \in \mathbb{R}$ ?

**2.28.** Siano  $A, B$  insiemi ed  $f: A \rightarrow B$  un'applicazione.

- (a) Si dimostri che  $f$  è iniettiva se e solo se  $f(A \setminus X) \subseteq B \setminus f(X)$  per ogni sottoinsieme  $X$  di  $A$ .  
 (b) Si dimostri che  $f$  è suriettiva se e solo se  $f(A \setminus X) \supseteq B \setminus f(X)$  per ogni sottoinsieme  $X$  di  $A$ .

**3.22.** Siano  $\mathbb{N}, \mathbb{R}$  e  $\mathbb{R}^*$  gli insiemi dei numeri naturali, reali e reali non nulli rispettivamente. Si consideri l'applicazione  $\varphi: \mathbb{R} \rightarrow \mathbb{R}^*$  definita da

$$\varphi(x) = \begin{cases} x+1 & \text{se } x \in \mathbb{N}, \\ x & \text{se } x \in \mathbb{R} \setminus \mathbb{N}. \end{cases}$$

- (a) Si dimostri che  $\varphi$  è iniettiva.  
 (b) Si dimostri che  $\varphi$  è suriettiva.  
 (c) Si dica come si definisce l'applicazione inversa  $\varphi^{-1}$  di  $\varphi$ .

**3.23.** Siano  $A, B, C$  insiemi non vuoti ed  $f: A \rightarrow C$  un'applicazione suriettiva. Siano  $B^A$  e  $B^C$  l'insieme di tutte le applicazioni di  $A$  in  $B$  e di  $C$  in  $B$  rispettivamente. Si definisca un'applicazione  $\varphi: B^C \rightarrow B^A$  ponendo  $\varphi(h) = h \circ f$  per ogni  $h \in B^C$ .

- (a) Si dimostri che  $\varphi$  è iniettiva.  
 (b) Si dimostri che

$$\varphi(B^C) = \{g \in B^A \mid \text{per ogni } a, a' \in A, \text{ se } f(a) = f(a') \text{ allora } g(a) = g(a')\}.$$

**7.16.** Siano  $A$  un insieme,  $\sim$  una relazione di equivalenza su  $A$ ,  $A/\sim$  l'insieme quoziente di  $A$  modulo  $\sim$ , e  $\pi: A \rightarrow A/\sim$  la proiezione canonica. Sia  $B$  un sottoinsieme di  $A$  tale che  $[b]_\sim \subseteq B$  per ogni  $b \in B$ . Si dimostri che

$$\pi^{-1}(\pi(B)) = B.$$

**7.17.** Sia  $A$  un insieme non vuoto e sia  $N^A$  l'insieme di tutte le applicazioni di  $A$  nell'insieme  $\mathbb{N}$  dei numeri naturali. In  $N^A$  si definisca una relazione  $\sim$  ponendo, per ogni  $f, g \in N^A$ ,  $f \sim g$  se l'insieme  $\{a \in A \mid f(a) \neq g(a)\}$  è un insieme finito.

- (a) Si dimostri che  $\sim$  è una relazione di equivalenza in  $N^A$ .  
 (b) Si dimostri che la relazione  $\sim$  su  $N^A$  è la relazione banale (cioè  $f \sim g$  per ogni  $f, g \in N^A$ ) se e solo se  $A$  è un insieme finito.

- (c) Per ogni  $n \in \mathbb{N}$  sia  $f_n: A \rightarrow \mathbb{N}$  l'applicazione definita da  $f_n(a) = n$  per ogni  $a \in A$ . Si dimostri che se  $A$  è un insieme infinito, l'applicazione  $\varphi: \mathbb{N} \rightarrow N^A/\sim$  definita da  $\varphi(n) = [f_n]_\sim$  per ogni  $n \in \mathbb{N}$  è iniettiva.

**7.18.** Sia  $B$  un insieme non vuoto e sia  $B^{\mathbb{N}}$  l'insieme di tutte le applicazioni dell'insieme  $\mathbb{N}$  dei numeri naturali in  $B$ . In  $B^{\mathbb{N}}$  si definisca la relazione  $\sim$  ponendo, per ogni  $f, g \in B^{\mathbb{N}}$ ,  $f \sim g$  se esiste  $n \in \mathbb{N}$  tale che  $f(i) = g(i)$  per ogni  $i \geq n$ .

- (a) Si dimostri che  $\sim$  è una relazione di equivalenza in  $B^{\mathbb{N}}$ .  
 (b) Si dimostri che la relazione  $\sim$  su  $B^{\mathbb{N}}$  è la relazione banale (cioè  $f \sim g$  per ogni  $f, g \in B^{\mathbb{N}}$ ) se e solo se  $|B| = 1$ .  
 (c) Per ogni  $b \in B$  sia  $f_b: \mathbb{N} \rightarrow B$  l'applicazione definita da  $f_b(n) = b$  per ogni  $n \in \mathbb{N}$ . Si dimostri che l'applicazione  $\varphi: B \rightarrow B^{\mathbb{N}}/\sim$  definita da  $\varphi(b) = [f_b]_\sim$  per ogni  $b \in B$  è iniettiva.

**7.19.** Sia  $A$  un insieme non vuoto,  $\mathcal{E}$  l'insieme delle equivalenze su  $A$ ,  $\mathcal{P}$  l'insieme delle partizioni di  $A$ . Si definiscano due applicazioni  $f: \mathcal{E} \rightarrow \mathcal{P}$  e  $g: \mathcal{P} \rightarrow \mathcal{E}$  ponendo  $f(\sim) = A/\sim$  per ogni  $\sim \in \mathcal{E}$ , e  $g(\mathcal{F}) = \sim_{\mathcal{F}}$  per ogni  $\mathcal{F} \in \mathcal{P}$ . Si dimostri che  $f$  e  $g$  sono due biezioni, una inversa dell'altra.  
 [Suggerimento: per dimostrare che  $f$  e  $g$  sono due biezioni, una inversa dell'altra, è sufficiente dimostrare che  $g \circ f = \text{id}_{\mathcal{E}}$  e  $f \circ g = \text{id}_{\mathcal{P}}$ .]

**10.12.** Siano  $\mathbb{N}$  l'insieme dei numeri naturali e  $\leq$  l'ordine usuale su  $\mathbb{N}$ . Sia  $\preceq$  l'ordinamento parziale su  $\mathbb{N}$  definito da

$$a \preceq b \text{ se } \begin{cases} a \text{ e } b \text{ sono entrambi pari e } a \leq b, \text{ oppure} \\ a \text{ e } b \text{ sono entrambi dispari e } a \leq b, \text{ oppure} \\ a \text{ è pari e } b \text{ è dispari.} \end{cases}$$

- (a) Si dimostri che l'ordinamento  $\preceq$  su  $\mathbb{N}$  è totale.  
 (b) Si dimostri che l'insieme ordinato  $(\mathbb{N}, \preceq)$  è bene ordinato.  
 (c) In  $(\mathbb{N}, \preceq)$  esiste l'estremo superiore del suo sottoinsieme  $P = \{2n \mid n \in \mathbb{N}\}$ ? Se esiste lo si calcoli.

**10.13.** Siano  $A$  un insieme e  $\varrho$  una relazione riflessiva e transitiva su  $A$ . Si definisca una relazione  $\sigma$  su  $A$  ponendo, per ogni  $a, b \in A$ ,  $a \sigma b$  se  $a \varrho b$  e  $b \varrho a$ .

- (a) Si provi che  $\sigma$  è un'equivalenza su  $A$ .  
 (b) Sull'insieme quoziente  $A/\sigma$  si definisca una relazione  $\tau$  ponendo, per ogni  $[a]_\sigma, [b]_\sigma \in A/\sigma$ ,  $[a]_\sigma \tau [b]_\sigma$  se  $a \varrho b$ . Si provi che la relazione  $\tau$  su  $A/\sigma$  è ben definita.  
 (c) Si provi che  $\tau$  è un ordinamento parziale su  $A/\sigma$ .

**19.13.** Siano  $A$  un insieme e  $\sim$  una relazione di equivalenza su  $A$ . Siano  $(A^A, \circ)$  il monoide di tutte le applicazioni di  $A$  in  $A$  e  $S$  il sottoinsieme di  $A^A$  i cui

elementi sono le applicazioni  $f \in A^A$  tali che per ogni  $x, y \in A$  si ha che  $x \sim y$  implica  $f(x) \sim f(y)$ .

- (a) Si dimostri che  $S$  è un sottomonoido di  $A^A$ .  
 (b) Per ogni  $f \in S$  si definisca un'applicazione  $\tilde{f} : A/\sim \rightarrow A/\sim$  ponendo  $\tilde{f}([a]) = [f(a)]$  per ogni  $a \in A$ . Si dimostri che l'applicazione  $\tilde{f}$  è ben definita.  
 (c) Si definisca ora un'applicazione  $\varphi : S \rightarrow (A/\sim)^{(A/\sim)}$  ponendo  $\varphi(f) = \tilde{f}$  per ogni  $f \in S$ . Si dimostri che  $\varphi$  è un omomorfismo di monoidi. Qui, come al solito, si intende che l'operazione sul monoido  $(A/\sim)^{(A/\sim)}$  è la composizione di applicazioni.

### B. Soluzione di alcuni esercizi

1.4. La (a) è vera, perché se  $x \in \{0\}$ , allora  $x = 0$ , e quindi  $x \in A$ . La (b) è falsa, perché gli elementi di  $A$  sono i tre numeri naturali  $0, 1, 2$ , e l'insieme  $\{0\}$  non è nessuno di questi. La (c) è vera. La (d) è falsa: se  $x \in \{0\}$ , allora  $x = 0$ , mentre  $0 \notin A$ , perché gli elementi di  $A$  sono  $0, 1, 2$ . La (e) è falsa: gli elementi di  $A$  sono  $0, 1, 2$ , e l'insieme  $\{0\}$  non è nessuno di questi. La (f) è falsa: gli elementi di  $A$  sono  $0, 1, 2$ , e  $0$  non è nessuno di questi. La (g) è vera, in quanto  $0 \subseteq A$  per ogni insieme  $A$ .  $\square$

1.14. Dato che  $A \supseteq A \setminus B$ , si ha certamente che  $A \cup B \supseteq (A \setminus B) \cup B$ . Viceversa se  $x \in A \cup B$ , allora  $x \in A$  oppure  $x \in B$ . Se  $x \in B$ , allora  $x \in (A \setminus B) \cup B$ . Se invece  $x \notin B$ , allora deve essere  $x \in A$ . Quindi  $x \in A \setminus B$ , e da questo segue che  $x \in (A \setminus B) \cup B$ . Abbiamo così dimostrato che da  $x \in A \cup B$  segue che  $x \in (A \setminus B) \cup B$ . Quindi  $A \cup B \subseteq (A \setminus B) \cup B$ .  $\square$

1.20. Si osservi che in questo caso si ha  $A_i = \mathbb{N}$  per ogni intero  $i \leq 0$ . Quindi alcuni tra gli insiemi  $A_i$  coincidono tra loro, ossia si ha  $A_i = A_j$  per certi  $i \neq j$ . Questo non è comunque un problema:  $\bigcup_{i \in \mathbb{Z}} A_i$  è l'insieme degli  $x \in \mathbb{N}$  tali che  $x \geq i$  per qualche  $i \in \mathbb{Z}$ . Ovviamente ogni numero naturale  $x$  ha questa proprietà, e quindi  $\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{N}$ . Invece  $\bigcap_{i \in \mathbb{Z}} A_i$  è l'insieme degli  $x \in \mathbb{N}$  tali che  $x \geq i$  per ogni  $i \in \mathbb{Z}$ . Nessun numero naturale  $x$  ha questa proprietà, e quindi  $\bigcap_{i \in \mathbb{Z}} A_i = \emptyset$ .  $\square$

2.5. Sono 24.  $\square$

2.6. Quella in (b) lo è, quelle in (a) e (c) non lo sono.  $\square$

2.7. Quella in (b) lo è, quelle in (a) e (c) non lo sono.  $\square$

2.11. Vi sono ovviamente infinite soluzioni possibili. Eccone una. Si prenda  $A = \{1, 2\}$ ,  $B = \{1\}$ ,  $\varphi : A \rightarrow B$  definita da  $\varphi(x) = 1$  per ogni  $x \in A$ ,  $A' = \{1\}$ . Allora  $\varphi^{-1}(\varphi(A')) = \varphi^{-1}(\varphi(\{1\})) = \varphi^{-1}(\{1\}) = \{1, 2\} = A \supset A'$ .  $\square$

2.13. ( $\subseteq$ ) Sia  $b \in \varphi(\varphi^{-1}(B'))$ . Allora  $b = \varphi(a)$  per qualche  $a \in \varphi^{-1}(B')$ . Da  $a \in \varphi^{-1}(B')$  segue che  $\varphi(a) \in B'$ , e quindi  $b = \varphi(a) \in B'$ . Inoltre dato che  $a \in \varphi^{-1}(B') \subseteq A$ , si ha che  $b = \varphi(a) \in \varphi(A)$ . Pertanto  $b \in B' \cap \varphi(A)$ .

( $\supseteq$ ) Sia  $b \in B' \cap \varphi(A)$ . Allora  $b \in B'$  e  $b \in \varphi(A)$ . Da  $b \in \varphi(A)$  segue che  $b = \varphi(a)$  per qualche  $a \in A$ . Essendo  $\varphi(a) = b \in B'$  si deve avere  $a \in \varphi^{-1}(B')$ . Se ne conclude che  $b = \varphi(a) \in \varphi(\varphi^{-1}(B'))$ .  $\square$

2.18. Innanzi tutto si osservi che  $\pi_A$  è un'applicazione, perché associa ad ogni elemento  $(a, b)$  di  $A \times B$  l'unico elemento  $a$  di  $A$ . Mostriamo che  $\pi_A$  è suriettiva. Fissiamo un elemento  $b \in B$  (questo è possibile perché  $B \neq \emptyset$ ). Allora per ogni  $a \in A$  si ha che  $(a, b) \in A \times B$  e  $\pi_A(a, b) = a$ . Pertanto  $\pi_A$  è suriettiva. La dimostrazione per  $\pi_B$  è analoga (e usa il fatto che  $A \neq \emptyset$ ).  $\square$

2.21. (a) Sia  $b \in f(X) \setminus f(Y)$ . Allora  $b \in f(X)$  e  $b \notin f(Y)$ . Quindi esiste  $x \in X$  tale che  $b = f(x)$ . Si noti che non può essere che  $x \in Y$ , altrimenti  $b = f(x) \in f(Y)$ , contraddizione. Quindi  $x \in X$  e  $x \notin Y$ . Ma allora  $x \in X \setminus Y$  e  $b = f(x) \in f(X \setminus Y)$ .

(b) Supponiamo  $f$  iniettiva. Abbiamo già dimostrato in (a) che  $f(X) \setminus f(Y) \subseteq f(X \setminus Y)$ . Viceversa supponiamo che  $b \in f(X \setminus Y)$ . Allora esiste  $x \in X \setminus Y$  tale che  $b = f(x)$ . In particolare  $x \in X$  e  $b = f(x) \in f(X)$ . Mostriamo che  $f(x) \notin f(Y)$ . Se per assurdo si avesse che  $f(x) \in f(Y)$ , allora  $f(x) = f(y)$  per qualche  $y \in Y$ . Dato che  $f$  è iniettiva ne segue che  $x = y$ . Questa è una contraddizione perché  $y \in Y$  e  $x \in X \setminus Y$ . Abbiamo così dimostrato che  $b \in f(X)$  e  $b = f(x) \notin f(Y)$ . Pertanto  $b \in f(X) \setminus f(Y)$ . Questo conclude la dimostrazione.  $\square$

2.22. (a) Supponiamo  $f$  iniettiva. Siano  $X$  e  $Y$  sottoinsiemi di  $A$  tali che  $X \cap Y = \emptyset$ . Dobbiamo dimostrare che  $f(X) \cap f(Y) = \emptyset$ . Se per assurdo fosse  $f(X) \cap f(Y) \neq \emptyset$ , allora esisterebbe un elemento  $b \in f(X) \cap f(Y)$ . Allora  $b \in f(X)$  e  $b \in f(Y)$ , e quindi esisterebbero un  $x \in X$  tale che  $f(x) = b$  e un  $y \in Y$  tale che  $f(y) = b$ . Da  $X \cap Y = \emptyset$  segue che  $x \neq y$ , mentre  $f(x) = b = f(y)$ . Questo contraddice l'iniettività di  $f$ .

Viceversa supponiamo che per ogni coppia di sottoinsiemi  $X$  e  $Y$  di  $A$  tali che  $X \cap Y = \emptyset$  si abbia  $f(X) \cap f(Y) = \emptyset$ , e mostriamo che  $f$  è iniettiva. Siano  $x, y \in A$ ,  $x \neq y$ . Allora i sottoinsiemi  $X = \{x\}$  e  $Y = \{y\}$  di  $A$  sono disgiunti. Quindi per la nostra ipotesi si ha  $f(X) \cap f(Y) = \emptyset$ . Ma  $f(X) = \{f(x)\}$  e  $f(Y) = \{f(y)\}$ , e quindi  $\{f(x)\} \cap \{f(y)\} = \emptyset$ . Se ne deduce che  $f(x) \neq f(y)$ , e quindi  $f$  è iniettiva.

(b) Supponiamo che  $f$  sia iniettiva e che  $X$  e  $Y$  siano due sottoinsiemi di  $A$ . Dobbiamo dimostrare che  $f(X \setminus Y) = f(X) \setminus f(Y)$ . Proviamolo con la doppia inclusione.

Mostriamo che  $f(X \setminus Y) \subseteq f(X) \setminus f(Y)$ . Sia  $b \in f(X \setminus Y)$ . Allora  $b \in f(X \setminus Y) \subseteq f(X)$ . Se fosse  $b \in f(Y)$ , allora  $b = f(y)$  per qualche  $y \in Y$ . Ma  $b \in f(X \setminus Y)$ , e quindi  $b = f(x)$  per qualche  $x \in X \setminus Y$ . Da  $y \in Y$  e  $x \in X \setminus Y$  segue che  $x \neq y$ , mentre  $f(x) = b = f(y)$ . Questo contraddice l'iniettività di  $f$ . Quindi non può essere che  $b \in f(Y)$ , e deve essere pertanto  $b \notin f(Y)$ . Abbiamo così dimostrato che  $b \in f(X) \setminus f(Y)$ .

Viceversa mostriamo che  $f(X) \setminus f(Y) \subseteq f(X \setminus Y)$ . Sia  $b \in f(X) \setminus f(Y)$ . Allora  $b \in f(X)$  e  $b \notin f(Y)$ . Quindi esiste  $x \in X$  tale che  $b = f(x)$ , e non si può avere che  $x \in Y$ , altrimenti  $b = f(x) \in f(Y)$ , contraddizione. Quindi  $x \in X \setminus Y$ . Ma allora  $x \in X \setminus Y$  e  $b = f(x) \in f(X \setminus Y)$ .

Supponiamo infine che si abbia  $f(X \setminus Y) = f(X) \setminus f(Y)$  per ogni coppia di sottoinsiemi  $X$  e  $Y$  di  $A$  e mostriamo che  $f$  è iniettiva. Siano  $x, y \in A$  tali che  $f(x) = f(y)$ . Allora  $f(\{x\} \setminus \{y\}) = f(\{x\}) \setminus f(\{y\}) = \{f(x)\} \setminus \{f(y)\} = \emptyset$ . Da  $f(\{x\} \setminus \{y\}) = \emptyset$  segue che  $\{x\} \setminus \{y\} = \emptyset$ . Pertanto  $x = y$  ed  $f$  è iniettiva.  $\square$

**3.8.** Calcoliamo l'applicazione composta  $\psi \circ \varphi : \mathbb{R} \rightarrow \mathbb{Z}$ . Per ogni  $x \in \mathbb{R}$  si ha  $\varphi(x) = \frac{1}{1+x^2}$ , e quindi  $\varphi(x) > 0$  per ogni  $x \in \mathbb{R}$ . Pertanto l'applicazione composta  $\psi \circ \varphi : \mathbb{R} \rightarrow \mathbb{Z}$  è definita da  $(\psi \circ \varphi)(x) = 1$  per ogni  $x \in \mathbb{R}$ . L'applicazione  $\varphi$  non è iniettiva perché  $\varphi(1) = \varphi(-1)$ ; l'applicazione  $\psi$  non è iniettiva perché  $\psi(1) = \psi(2) = 1$ ; l'applicazione  $\psi \circ \varphi$  non è suriettiva perché ad esempio  $(\psi \circ \varphi)(0) = (\psi \circ \varphi)(1) = 1$ . L'applicazione  $\varphi$  non è suriettiva perché non esiste nessun  $x \in \mathbb{R}$  tale che  $\varphi(x) = 0$ ; infine l'applicazione  $\psi \circ \varphi$  non è suriettiva perché non esiste nessun  $x \in \mathbb{R}$  tale che  $(\psi \circ \varphi)(x) = 0$ .  $\square$

**3.10.** Si veda l'esempio 3 del capitolo 2.  $\square$

**3.11.** Si veda l'esempio 4 del capitolo 2.  $\square$

**3.13.** Sia  $\varphi : A \rightarrow B$  un'applicazione suriettiva ma non biiettiva. Supponiamo per assurdo che esista un'applicazione  $\psi_1 : B \rightarrow A$  tale che  $\psi_1 \circ \varphi = \text{id}_A$ . Ma allora che  $\psi_1 \circ \varphi = \text{id}_A$  è iniettiva, anche  $\varphi$  è iniettiva per l'esercizio 3.2 (a). Ma allora  $\varphi$  è sia iniettiva che suriettiva, dunque biiettiva, assurdo.

Essendo invece  $\varphi$  suriettiva, per l'esercizio 3.6 esiste un'applicazione  $\psi_2$  tale che  $\varphi \circ \psi_2 = \text{id}_B$ .  $\square$

**3.16.** (b) e (c) Si prenda ad esempio  $A = \{1, 2\}$ ,  $B = \{1, 2, 3\}$ ,  $C = \{2, 3\}$ . Siano  $\varphi : A \rightarrow B$  l'applicazione definita da  $\varphi(1) = 1$  e  $\varphi(2) = 2$ , e  $\psi : B \rightarrow C$  l'applicazione definita da  $\psi(1) = \psi(2) = 2$  e  $\psi(3) = 3$ . Si noti che  $\varphi$  è iniettiva e  $\psi$  è suriettiva. Si ha  $(\psi \circ \varphi)(1) = 2$  e  $(\psi \circ \varphi)(2) = 2$ , e quindi  $\psi \circ \varphi$  non è né iniettiva

né suriettiva. Quindi le applicazioni  $\varphi$  e  $\psi$  forniscono un esempio che risponde sia al quesito (b) che al quesito (c).  $\square$

**3.19.** Si osservi che se  $n \in \mathbb{N}$  è pari, allora  $\varphi(n) = n/2 \geq 0$ , mentre se  $n$  è dispari, allora  $n \geq 1$ , da cui  $n+1 \geq 2$ , e pertanto  $\varphi(n) = -(n+1)/2 \leq -1$ . Quindi la biiezione  $\varphi$  manda i numeri naturali pari nei numeri interi non negativi, e i numeri naturali dispari nei numeri interi negativi. La sua inversa  $\varphi^{-1} : \mathbb{Z} \rightarrow \mathbb{N}$  dovrà quindi mandare i numeri interi non negativi nei numeri naturali pari, e i numeri interi negativi nei numeri naturali dispari. Ora se  $z \in \mathbb{Z}$  è  $\geq 0$  e  $n \in \mathbb{N}$  è pari si avrà  $\varphi(n) = z$  se e solo se  $n/2 = z$ , cioè se e solo se  $n = 2z$ . Se invece  $z \in \mathbb{Z}$  è  $< 0$  e  $n \in \mathbb{N}$  è dispari si avrà  $\varphi(n) = z$  se e solo se  $-(n+1)/2 = z$ , cioè se e solo se  $n = -2z - 1$ . Pertanto l'applicazione inversa  $\varphi^{-1} : \mathbb{Z} \rightarrow \mathbb{N}$  dell'applicazione  $\varphi$  è definita da  $\varphi^{-1}(z) = 2z$  se  $z \in \mathbb{Z}$  è  $\geq 0$ , e  $\varphi^{-1}(z) = -2z - 1$  se  $z \in \mathbb{Z}$  è  $< 0$ .  $\square$

**3.20.** ( $\Rightarrow$ ) Sia  $f \circ f = f$ . Poniamo  $B = f(A)$ ,  $C = A \setminus f(A)$  e mostriamo che  $B$  e  $C$  hanno le proprietà richieste. Chiaramente  $B \cup C = A$  e  $B \cap C = \emptyset$ . Inoltre  $C \subseteq A$ , e quindi  $f(C) \subseteq f(A) = B$ . Infine se  $b \in B$ , allora  $b \in f(A)$ , e quindi  $b = f(a)$  per qualche  $a \in A$ ; ma allora  $f(b) = f(f(a)) = (f \circ f)(a) = f(a) = b$ .

( $\Leftarrow$ ) Supponiamo che esistano  $B, C \subseteq A$  tali che  $B \cup C = A$ ,  $B \cap C = \emptyset$ ,  $f(C) \subseteq B$  e  $f(b) = b$  per ogni  $b \in B$ . Fissato un qualunque elemento  $a \in A$  si ha o che  $a \in B$  oppure che  $a \in C$ .

Se  $a \in B$ , allora  $f(a) = a$ , e quindi  $f(f(a)) = f(a)$ .

Se invece  $a \in C$ , allora  $f(a) \in B$ , e quindi  $f(f(a)) = f(a)$ .

Pertanto in entrambi i casi si ha che  $f(f(a)) = f(a)$ , cioè  $(f \circ f)(a) = f(a)$  per ogni  $a \in A$ . Se ne deduce che  $f \circ f = f$ .  $\square$

**4.10.** I casi in cui almeno uno tra  $a$  e  $b$  è uguale a 0, 1 o -1 sono facili da trattare; ad esempio se  $a = 0$ ,  $p \mid a$ ; se  $b = 0$ ,  $p \mid b$ ; se  $a = 1$ , da  $p \mid ab$  segue  $p \mid b$ ; eccetera. Possiamo dunque supporre  $a$  e  $b$  entrambi diversi da 0, 1 e -1. Dato che  $p \mid ab$ , esiste  $c \in \mathbb{Z}$  tale che  $ab = cp$ . Distinguiamo due casi a seconda che  $c$  sia diverso da 1 e da -1 o che  $c$  sia uguale a 1 oppure a -1. Se  $c$  è diverso da 1 e da -1, applichiamo il teorema fondamentale dell'aritmetica ad  $a, b$  e  $c$ . Siano  $a = p_1 p_2 \cdots p_r$ ,  $b = p'_1 p'_2 \cdots p'_s$ ,  $c = p''_1 p''_2 \cdots p''_t$  fattorizzazioni di  $a, b$  e  $c$  in prodotto di primi. Allora  $p_1 p_2 \cdots p_r p'_1 p'_2 \cdots p'_s = p''_1 p''_2 \cdots p''_t p$  sono due fattorizzazioni di  $ab = cp$  in prodotto di primi. Per il teorema fondamentale dell'aritmetica si ha  $|p| = |p_i|$  oppure  $|p| = |p'_j|$  per qualche  $i$  o qualche  $j$ . Se  $|p| = |p_i|$  si ha  $p \mid a$ , mentre se  $|p| = |p'_j|$  si ha  $p \mid b$ . Il caso in cui  $c$  è uguale a 1 o a -1 è analogo al precedente ed è lasciato al lettore.  $\square$

**4.11.** Supponiamo  $\sqrt{n} \in \mathbb{Q}$  e mostriamo che  $\sqrt{n} \in \mathbb{Z}$ . Se  $n = 0$  si ha certamente che  $\sqrt{n} \in \mathbb{Z}$ , e quindi supporremo sempre che  $n$  sia non nullo. Se  $\sqrt{n} \in \mathbb{Q}$ , si può scrivere  $\sqrt{n}$  come quoziente di due interi positivi, cioè  $\sqrt{n} = \frac{a}{b}$  con  $a$  e  $b$  in-

teri positivi. Possiamo supporre inoltre che questa frazione sia ridotta ai minimi termini, cioè che  $a$  e  $b$  siano primi tra loro. Elevando al quadrato l'uguaglianza  $\sqrt{n} = \frac{a}{b}$  si ottiene che  $n = \frac{a^2}{b^2}$ , da cui  $nb^2 = a^2$ . Ne segue che se  $p$  è un qualunque numero primo che divide  $b$ , allora  $p$  divide  $nb^2 = a^2$ . Quindi  $p$  divide  $a$  (esercizio 4.10). Abbiamo così dimostrato che ogni primo  $p$  che divide  $b$  divide anche  $a$ . Ma  $a$  e  $b$  sono primi tra loro, e quindi non ci sono numeri primi che dividono sia  $a$  che  $b$ . L'unica possibilità è quindi che  $\sqrt{n} = \frac{a}{b} = \frac{a}{1} \in \mathbb{Z}$ .  $\square$

divide  $b$ , cioè si deve avere  $b = 1$ . Si conclude così che  $\sqrt{n} = \frac{a}{b} = \frac{a}{1} \in \mathbb{Z}$ .  $\square$

4.16. Per  $n = 5$  si ha  $n^2 = 25 = 11n - 30 = 25$ . Quindi il caso  $n = 5$  è verificato. Sia  $n \geq 6$ , e supponiamo che il risultato valga per  $n - 1$ , cioè che  $(n - 1)^2 \geq 11(n - 1) - 30$ . Allora  $n^2 - 2n + 1 \geq 11n - 41$ , da cui  $n^2 \geq 2n - 1 + 11n - 41 \geq 12 - 1 + 11n - 41 = 11n - 30$ . Quindi il risultato vale anche per  $n$ .  $\square$

4.24. Supponiamo per assurdo che esistano dei numeri naturali che possono essere scritti in questa forma in due modi essenzialmente distinti. Sia  $n$  il più piccolo di tutti questi numeri. Siano  $h, c_1, c_2, \dots, c_h, l, d_1, d_2, \dots, d_l \in \mathbb{N}$  tali che  $n = c_1 \cdot 1! + c_2 \cdot 2! + \dots + c_h \cdot h! = d_1 \cdot 1! + d_2 \cdot 2! + \dots + d_l \cdot l!$ ,  $n = c_1 \cdot 1! + c_2 \cdot 2! + \dots + c_h \cdot h! = d_1 \cdot 1! + d_2 \cdot 2! + \dots + d_l \cdot l!$ . Si osservi che  $c_i \leq i$  per ogni  $i = 1, 2, \dots, h$  e  $d_j \leq j$  per ogni  $j = 1, 2, \dots, l$ . Si osservi che  $n > 0$ , in quanto l'unico modo di scrivere  $n$  in questa forma è con tutti i  $c_i = 0$ ; inoltre si può evidentemente assumere senza perdita di generalità che  $c_h \neq 0$ , che  $d_l \neq 0$  e che  $h \leq l$ .

Se  $h < l$ , allora  $n = c_1 \cdot 1! + c_2 \cdot 2! + \dots + c_h \cdot h! \leq 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \dots + h \cdot h! = (h + 1)! - 1$  (esercizio 4.4), e  $n = d_1 \cdot 1! + d_2 \cdot 2! + \dots + d_l \cdot l! \geq d_l \cdot l! \geq l! \geq (h + 1)!$  perché  $l \geq h + 1$ . Questa è una contraddizione.

Deve quindi essere  $h = l$ . Ma allora  $n - h! = c_1 \cdot 1! + c_2 \cdot 2! + \dots + c_{h-1} \cdot (h-1)! = d_1 \cdot 1! + d_2 \cdot 2! + \dots + d_{h-1} \cdot (h-1)!$  è un numero naturale minore di  $n$  che può essere scritto nella forma voluta in due modi distinti, e questo contraddice la minimalità della scelta di  $n$ .  $\square$

5.2. Se  $z, z' \in \mathbb{C}$  e  $zz' = 0$ , allora  $|z| \cdot |z'| = |zz'| = |0| = 0$  per la proposizione 5.2. Quindi  $|z|$  e  $|z'|$  sono due numeri reali il cui prodotto è nullo, e quindi uno dei due è nullo. Ne segue che  $z = 0$  oppure  $z' = 0$ .  $\square$

5.8. (a) Da  $z = a + ib$  segue che  $iz = i(a + ib) = -b + ia$ . Quindi  $iz$  è rappresentato dal punto di coordinate  $(-b, a)$ .

(b)  $iz = \left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}\right) e^{i(\cos \varphi + i \sin \varphi)} = e^{i\left(\cos \frac{\pi}{2} + \varphi\right)} = e^{i\left(\frac{\pi}{2} + \varphi\right)}$ .  $\square$

5.18. Per ogni intero  $n \geq 3$  e ogni numero complesso  $z$  si ha  $z^n = -1$  se e solo se  $z^{2n} = 1$  e  $z^n \neq 1$ . Infatti se  $z^n = -1$  si ha certamente  $z^n \neq 1$  e  $z^{2n} = (z^n)^2 = (-1)^2 = 1$ . Se invece  $z^{2n} = 1$  e  $z^n \neq 1$ , allora  $(z^n)^2 = 1$ , e quindi  $z^n$  è una delle

due radici quadrate 1 e  $-1$  di 1. Dato che  $z^n \neq 1$  ne segue che  $z^n = -1$ .

Sappiamo poi che l'equazione  $z^{2n} = 1$  ha esattamente  $2n$  soluzioni distinte in  $\mathbb{C}$  rappresentate nel piano di Argand-Gauss dai vertici del poligono regolare di  $2n$  lati inscritto nella circonferenza di centro l'origine e raggio 1 e con un vertice nel punto 1, mentre l'equazione  $z^n = 1$  ha esattamente  $n$  soluzioni distinte rappresentate nel piano di Argand-Gauss dai vertici del poligono regolare di  $n$  lati inscritto nella circonferenza di centro l'origine e raggio 1 e con un vertice nel punto 1. Togliendo dall'insieme delle soluzioni dell'equazione  $z^{2n} = 1$  le  $n$  soluzioni distinte in  $\mathbb{C}$ , che esse sono rappresentate nel piano di Argand-Gauss dai vertici di un poligono regolare di  $n$  lati inscritto nella circonferenza di centro l'origine e raggio 1, e che questo poligono è simmetrico rispetto all'asse reale. Se  $n$  è dispari,  $z = -1$  è una soluzione dell'equazione  $z^n = 1$ , perché  $(-1)^n = -1$ . Quindi se  $n$  è dispari uno dei vertici del poligono deve essere nel punto  $z = -1$ .  $\square$

$$6.5. AB = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, BA = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}. \square$$

6.12. Si denotino con  $a_{ij}$  e  $b_{ij}$  gli elementi di posto  $(i, j)$  nelle matrici  $A$  e  $B$  rispettivamente. Dimostriamo che  $(AB)^* = B^* A^*$  facendo vedere che l'elemento di posto  $(i, j)$  in  $(AB)^*$  è uguale all'elemento di posto  $(i, j)$  in  $B^* A^*$  per ogni  $i$  e ogni  $j$ . L'elemento di posto  $(i, j)$  in  $(AB)^*$  è uguale all'elemento di posto  $(j, i)$  in  $AB$ , cioè è  $\sum_{k=1}^n a_{jk} b_{ki}$ . L'elemento di posto  $(i, j)$  in  $B^* A^*$  è  $\sum_{k=1}^n b_{ik}^* a_{kj}^*$ , dove  $a_{ij}^*$  e  $b_{ij}^*$  denotano gli elementi di posto  $(i, j)$  nelle matrici  $A^*$  e  $B^*$  rispettivamente. Quindi  $b_{ik}^* = b_{ki}$  e  $a_{kj}^* = a_{jk}$ . Ne segue che  $\sum_{k=1}^n b_{ik}^* a_{kj}^* = \sum_{k=1}^n b_{ki} a_{jk} = \sum_{k=1}^n a_{jk} b_{ki}$ .  $\square$

7.7. Riflessività. Per ogni  $f \in X^X$  si ha che  $f \sim f$ , in quanto l'applicazione identica  $\iota_X : X \rightarrow X$  è una biiezione e si ha  $\iota_X \circ f \circ \iota_X^{-1} = \iota_X \circ f \circ \iota_X = f$ .

Simmetria. Siano  $f, g \in X^X$  tali che  $f \sim g$ . Allora esiste una biiezione  $\sigma : X \rightarrow X$  tale che  $f = \sigma \circ g \circ \sigma^{-1}$ . Considerando l'inversa  $\sigma^{-1} : X \rightarrow X$ , che è una biiezione, si ha che  $g = \iota_X \circ g \circ \iota_X = (\sigma^{-1} \circ \sigma) \circ g \circ (\sigma^{-1} \circ \sigma) = \sigma^{-1} \circ (\sigma \circ g \circ \sigma^{-1}) \circ \sigma = \sigma^{-1} \circ f \circ \sigma$ , e quindi  $g \sim f$ .

Transitività. Siano  $f, g, h \in X^X$  tali che  $f \sim g$  e  $g \sim h$ . Allora esistono due biiezioni  $\sigma : X \rightarrow X$  e  $\tau : X \rightarrow X$  tali che  $f = \sigma \circ g \circ \sigma^{-1}$  e  $g = \tau \circ h \circ \tau^{-1}$ . Ne segue che l'applicazione composta  $\sigma \circ \tau : X \rightarrow X$  è una biiezione e si ha  $f = \sigma \circ g \circ \sigma^{-1} = \sigma \circ \tau \circ h \circ \tau^{-1} \circ \sigma^{-1} = (\sigma \circ \tau) \circ h \circ (\sigma \circ \tau)^{-1}$ . Pertanto  $f \sim h$ .  $\square$

7.11. (a) Sia  $a \in \psi^{-1}(y)$ . Allora  $\psi(a) = y$ , e quindi  $\max\{a, a^{-1}\} = y$ . Ne segue che  $a = y$  oppure  $a^{-1} = y$ . In entrambi i casi  $a \in \{y, y^{-1}\}$ . Quindi  $\psi^{-1}(y) \subseteq \{y, y^{-1}\}$ .

(b) Da (a) segue che  $|\psi^{-1}(y)| \leq |\{y, y^{-1}\}| \leq 2$  se  $y \neq 0$ . Se invece  $y = 0$  si ha  $\psi^{-1}(y) = \emptyset$ , in quanto per ogni  $a \in \mathbb{R}^*$  si ha  $\psi(a) = \max\{a, a^{-1}\} \neq 0$ .

(c) Sia  $y \in \mathbb{R}$ . Supporremo che  $y \neq 0$  in quanto, come abbiamo visto in (b), se  $y = 0$  si ha  $\psi^{-1} = \emptyset$ . Abbiamo dimostrato in (a) che in questo caso  $\psi^{-1}(y) \subseteq \{y, y^{-1}\}$ . Ne segue che:

- (1) se  $\psi(y) = y$  e  $\psi(y^{-1}) = y$ , allora  $\psi^{-1}(y) = \{y, y^{-1}\}$ ;
- (2) se  $\psi(y) = y$  e  $\psi(y^{-1}) \neq y$ , allora  $\psi^{-1}(y) = \{y\}$ ;
- (3) se  $\psi(y) \neq y$  e  $\psi(y^{-1}) = y$ , allora  $\psi^{-1}(y) = \{y^{-1}\}$ ;
- (4) se  $\psi(y) \neq y$  e  $\psi(y^{-1}) \neq y$ , allora  $\psi^{-1}(y) = \emptyset$ .

Studiamo separatamente questi quattro casi.

(1) Se  $\psi(y) = y$  e  $\psi(y^{-1}) = y$ , allora  $\psi^{-1}(y) = \{y, y^{-1}\}$ . Quindi nel caso in cui  $y = y^{-1}$  si avrà che  $\psi^{-1}(y) = \{y\}$  ha cardinalità 1. Nel caso invece in cui  $y \neq y^{-1}$  l'insieme  $\psi^{-1}(y) = \{y, y^{-1}\}$  ha cardinalità 2.

(2) Si ha  $\psi(y) = y$  e  $\psi(y^{-1}) \neq y$  se e solo se  $\max\{y, y^{-1}\} = y$  e  $\max\{y^{-1}, y\} \neq y$ . Questo caso non può dunque accadere mai.

(3) Anche questo caso non può accadere mai, perché si dovrebbe avere contemporaneamente che  $\max\{y, y^{-1}\} \neq y$  e  $\max\{y^{-1}, y\} = y$ .

(4) In questo caso  $\psi^{-1}(y) = \emptyset$  ha cardinalità 0. Se ne ricava pertanto che  $\psi^{-1}(y)$  ha cardinalità 1 se e solo se  $\psi(y) = y$ ,  $\psi(y^{-1}) = y$ , e  $y = y^{-1}$ . Questo accade evidentemente se e solo se  $y = y^{-1}$ , cioè se e solo se  $y$  è soluzione dell'equazione  $y^2 = 1$ , cioè se e solo se  $y = 1$  oppure  $y = -1$ .

Pertanto gli  $y \in \mathbb{R}$  tali che  $|\psi^{-1}(y)| = 1$  sono solo i numeri 1 e -1.

(d) Si ha  $a \sim_{\psi} b$  se e solo se  $\psi(a) = \psi(b)$ , cioè se e solo se

$$\max\{a, a^{-1}\} = \max\{b, b^{-1}\}.$$

Se questo avviene si ha quindi che  $a = b$ , oppure  $a = b^{-1}$ , oppure  $a^{-1} = b$ , oppure  $a^{-1} = b^{-1}$ . In tutti quattro questi casi si ha  $(a - b)(ab - 1) = 0$ .

Viceversa se  $(a - b)(ab - 1) = 0$ , allora  $a = b$  oppure  $a = b^{-1}$ , da cui  $\{a, a^{-1}\} = \{b, b^{-1}\}$ . Pertanto in questo caso  $\psi(a) = \max\{a, a^{-1}\} = \max\{b, b^{-1}\} = \psi(b)$ , e quindi  $a \sim_{\psi} b$ . □

**7.15.** La  $\sim_{\iota_A}$  è la relazione di uguaglianza su  $A$ . L'applicazione  $\tilde{\iota}_A : A/\sim_{\iota_A} \rightarrow A$  è definita da  $\tilde{\iota}_A(\{a\}) = a$  per ogni  $a \in A$ . È una biiezione perché  $\iota_A$  è suriettiva. □

**8.10.** (a) *Riflessività.* Per ogni  $a \in \mathbb{Z}$  si ha  $f(a) \equiv f(a) \pmod{n}$ , e quindi  $a \sim a$ . *Simmetria.* Se  $a, b \in \mathbb{Z}$  e  $a \sim b$ , allora  $f(a) \equiv f(b) \pmod{n}$ , da cui  $f(b) \equiv f(a) \pmod{n}$ , e pertanto  $b \sim a$ .

*Transitività.* Se  $a, b, c \in \mathbb{Z}$ ,  $a \sim b$  e  $b \sim c$ , allora  $f(a) \equiv f(b)$  e  $f(b) \equiv f(c) \pmod{n}$ , da cui  $f(a) \equiv f(c) \pmod{n}$ . Pertanto  $a \sim c$ . Questo dimostra che  $\sim$  è

un'equivalenza.

(b) Sia  $x \in \mathbb{Z}$ . Si ha  $x \in [a]_{\sim}$  se e solo se  $x \sim a$ , cioè se e solo se  $f(x) \equiv f(a) \pmod{n}$ . Questo accade se e solo se  $f(x) \in [f(a)]_{\equiv_n}$ , cioè se e solo se  $x \in f^{-1}([f(a)]_{\equiv_n})$ . □

**8.11.** Siano  $a, b \in \mathbb{Z}$  tali che  $[a]_{\equiv_3} = [b]_{\equiv_3}$ . Allora  $a \equiv b \pmod{3}$ , cioè  $3 \mid (a - b)$ , vale a dire esiste  $c \in \mathbb{Z}$  tale che  $a - b = 3c$ . Ne segue che  $2a - 2b = 6c$ , ossia  $6 \mid (2a - 2b)$ , cioè  $2a \equiv 2b \pmod{6}$ . Ma allora  $[2a]_{\equiv_6} = [2b]_{\equiv_6}$ . Questo dimostra che ponendo  $\psi([a]_{\equiv_3}) = [2a]_{\equiv_6}$  per ogni  $a \in \mathbb{Z}$  si dà una buona definizione di un'applicazione  $\psi : \mathbb{Z}/\equiv_3 \rightarrow \mathbb{Z}/\equiv_6$ .

Mostriamo che  $\psi$  è iniettiva. Siano  $a, b \in \mathbb{Z}$  tali che  $\psi([a]_{\equiv_3}) = \psi([b]_{\equiv_3})$ . Allora  $[2a]_{\equiv_6} = [2b]_{\equiv_6}$ , da cui  $2a \equiv 2b \pmod{6}$ . Ne segue che  $6 \mid (2a - 2b)$ , cioè esiste  $d \in \mathbb{Z}$  tale che  $2a - 2b = 6d$ . Ma allora  $a - b = 3d$ , ossia  $3 \mid (a - b)$ , da cui  $[a]_{\equiv_3} = [b]_{\equiv_3}$ . Questo dimostra che  $\psi$  è iniettiva. □

**8.12.** (a) Si osservi che 1, 2, 3, 4 sono a due a due non congrui tra loro modulo 5, mentre  $-3 \equiv 2$ ,  $-1 \equiv 4$ ,  $14 \equiv 4$ ,  $23 \equiv 3$ ,  $-7 \equiv 3$ ,  $28 \equiv 3 \pmod{5}$ . Pertanto le classi di equivalenza di  $A$  modulo  $\varrho$  sono

$$\begin{aligned} [1]_{\varrho} &= \{1\} \\ [2]_{\varrho} &= \{2, -3\} \\ [3]_{\varrho} &= \{3, 23, -7, 28\} \\ [4]_{\varrho} &= \{4, -1, 14\}. \end{aligned}$$

In particolare  $A/\varrho$  ha quattro elementi, che sono  $\{1\}$ ,  $\{2, -3\}$ ,  $\{3, 23, -7, 28\}$ ,  $\{4, -1, 14\}$ .

(b) Se  $x, y \in A$  e  $[x]_{\varrho} = [y]_{\varrho}$ , allora  $x \varrho y$ , da cui  $x \equiv_5 y$ , e pertanto  $[x]_{\equiv_5} = [y]_{\equiv_5}$ .  
(c) Sì, in quanto  $\varphi([1]_{\varrho}) = [1]_{\equiv_5}$ ,  $\varphi([2]_{\varrho}) = [2]_{\equiv_5}$ ,  $\varphi([3]_{\varrho}) = [3]_{\equiv_5}$ ,  $\varphi([4]_{\varrho}) = [4]_{\equiv_5}$ , e i quattro elementi  $[1]_{\equiv_5}$ ,  $[2]_{\equiv_5}$ ,  $[3]_{\equiv_5}$ ,  $[4]_{\equiv_5}$  di  $\mathbb{Z}/\equiv_5$  sono tutti distinti tra loro.

(d) No, perché non esiste nessun  $C \in A/\varrho$  tale che  $\varphi(C) = [0]_{\equiv_5}$ . □

**9.11.** Ovviamente se  $m > n$  non ci sono applicazioni iniettive di  $A$  in  $B$ . Supponiamo dunque  $m \leq n$ . Siano  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$ , e sia  $f : A \rightarrow B$  un'arbitraria applicazione iniettiva. Allora  $f(a_1)$  può essere uno qualunque degli elementi di  $B$  (e quindi può essere scelto in  $n$  modi),  $f(a_2)$  può essere uno qualunque degli elementi di  $B$  eccetto  $f(a_1)$  (e quindi può essere scelto in  $n - 1$  modi),  $f(a_3)$  può essere uno qualunque degli elementi di  $B$  eccetto  $f(a_1)$  e  $f(a_2)$  (e quindi può essere scelto in  $n - 2$  modi), e così via, fino ad  $f(a_m)$  che può essere uno qualunque degli elementi di  $B$  eccetto  $f(a_1), f(a_2), \dots, f(a_{m-1})$  (e quindi può essere scelto in  $n - m + 1$  modi). In definitiva nel costruire una applicazione iniettiva  $f : A \rightarrow B$  si hanno  $n(n - 1)(n - 2) \dots (n - m + 1) = n!/(n - m)!$  possibilità di scelta, cioè ci sono  $n!/(n - m)!$  modi di costruire un'applicazione



iniettiva di  $A$  in  $B$ . In altre parole ci sono  $n!/(n-m)!$  applicazioni iniettive di  $A$  in  $B$ .  $\square$

9.12. (a) 1; (b) 2; (c) 5.

[Nota per chi già conosce gli sviluppi in serie di potenze: Indichiamo con  $B_n$  (n-esimo numero di Bell) il numero di relazioni di equivalenza su un insieme  $X$  di cardinalità  $n$ . Abbiamo quindi appena calcolato  $B_1, B_2, B_3$  dimostrando che sono uguali a 1, 2 e 5 rispettivamente. Inoltre  $B_0 = 1$  (perché c'è un'unica relazione su  $\emptyset$  e questa è un'equivalenza). È possibile dimostrare, ma non è facile, che ed è necessario introdurre concetti che esulano dalla portata di questo testo, che la serie  $\sum_{k=0}^{+\infty} B_k \frac{x^k}{k!}$  è lo sviluppo in serie di potenze della funzione  $e^{e^x-1}$ .]  $\square$

9.14. (a) Mostriamo che  $\sigma$  è iniettiva dimostrando che se  $S, S' \subseteq A$  e  $S \neq S'$  allora  $\sigma(S) \neq \sigma(S')$ . Se  $S \neq S'$ , allora esiste un  $a \in S$  non appartenente ad  $S'$  oppure un  $a \in S'$  non appartenente ad  $S$ . Se ad esempio  $a \in S$  e  $a \notin S'$ , allora  $\chi_S(a) = 1$  e  $\chi_{S'}(a) = 0$ . Quindi  $\chi_S(a) \neq \chi_{S'}(a)$ , e pertanto le due applicazioni  $\chi_S$  e  $\chi_{S'}$  sono diverse. Da  $\chi_S \neq \chi_{S'}$  si deduce allora che  $\sigma(S) \neq \sigma(S')$ .

Mostriamo che  $\sigma$  è suriettiva. Sia  $f \in \{0, 1\}^A$ , ossia sia  $f: A \rightarrow \{0, 1\}$  un'applicazione. Allora  $f^{-1}(1) \subseteq A$ , e quindi  $f^{-1}(1) \in \mathcal{P}(A)$ . Per far vedere che  $\sigma$  è suriettiva è pertanto sufficiente far vedere che  $\sigma(f^{-1}(1)) = f$ , ossia che le due applicazioni  $\chi_{f^{-1}(1)}$  e  $f$  di  $A$  in  $\{0, 1\}$  coincidono. Osserviamo che per ogni  $a \in A$  si ha:

- (1)  $\chi_{f^{-1}(1)}(a) = 0$  se e solo se  $a \notin f^{-1}(1)$ , cioè se e solo se  $f(a) \neq 1$ , e quindi se e solo se  $f(a) = 0$ ;
- (2)  $\chi_{f^{-1}(1)}(a) = 1$  se e solo se  $a \in f^{-1}(1)$ , cioè se e solo se  $f(a) = 1$ .

Pertanto  $\chi_{f^{-1}(1)}(a) = f(a)$  per ogni  $a \in A$ , vale a dire  $\chi_{f^{-1}(1)} = f$ . Questo prova che  $\sigma$  è suriettiva.

(b) Come si è visto nella soluzione della parte (a), per ogni  $f \in \{0, 1\}^A$  si ha che  $f^{-1}(1) \in \mathcal{P}(A)$  e che  $\sigma(f^{-1}(1)) = f$ . Inoltre  $\sigma$  è biiettiva. Quindi l'applicazione inversa  $\sigma^{-1}: \{0, 1\}^A \rightarrow \mathcal{P}(A)$  è definita da  $\sigma^{-1}(f) = f^{-1}(1)$  per ogni  $f \in \{0, 1\}^A$ .

(c) Dato che  $\sigma: \mathcal{P}(A) \rightarrow \{0, 1\}^A$  è una biiezione, si ha  $|\mathcal{P}(A)| = |\{0, 1\}^A| = 2^{|A|}$ .  $\square$

9.15. Sia  $A$  un insieme con  $n$  elementi. Se  $n = 0$ , allora anche  $k$  deve essere 0, e in questo caso l'unico sottoinsieme di  $A = \emptyset$  avente zero elementi è  $\emptyset$  stesso. In questo caso si ha inoltre  $\binom{0}{0} = 1$ . Quindi nel caso  $n = 0$  l'asserto è vero.

Possiamo quindi supporre  $n \geq 1$  (cioè che l'insieme  $A$  sia non vuoto). Osserviamo intanto che l'asserto è vero se  $k = 0$  o se  $k = n$ . Infatti: per  $k = 0$  c'è un unico sottoinsieme di  $A$  di cardinalità 0 (l'insieme vuoto) e  $\binom{n}{0} = 1$ ; per  $k = n$

c'è un unico sottoinsieme di  $A$  di cardinalità  $n$  (l'insieme  $A$  stesso) e  $\binom{n}{n} = 1$ . Supporremo quindi anche  $1 \leq k \leq n-1$ . Per l'ipotesi induttiva sappiamo poi che un insieme di cardinalità  $n-1$  ha esattamente  $\binom{n-1}{i}$  sottoinsiemi di cardinalità  $i$  per ogni  $0 \leq i \leq n-1$ . Fissiamo un elemento  $a_0$  nell'insieme  $A$ . Un sottoinsieme di  $A$  con  $k$  elementi può non contenere l'elemento  $a_0$  oppure può contenerlo. I sottoinsiemi di  $A$  con  $k$  elementi che non contengono l'elemento  $a_0$  sono esattamente i sottoinsiemi di  $A \setminus \{a_0\}$  con  $k$  elementi; poiché  $|A \setminus \{a_0\}| = n-1$ , esattamente i sottoinsiemi di  $A \setminus \{a_0\}$  con  $k$  elementi,  $\binom{n-1}{k}$ . I sottoinsiemi di  $A$  con tali sottoinsiemi sono, per l'ipotesi induttiva,  $\binom{n-1}{k-1}$ . I sottoinsiemi di  $A$  con  $k$  elementi che contengono  $a_0$  sono esattamente quelli del tipo  $S \cup \{a_0\}$  ove  $S$  è un sottoinsieme con  $k-1$  elementi di  $A \setminus \{a_0\}$ ; quindi tali sottoinsiemi sono, per l'ipotesi induttiva  $\binom{n-1}{k-1}$ . Quindi i sottoinsiemi di  $A$  con  $k$  elementi sono in tutto  $\binom{n-1}{k} + \binom{n-1}{k-1}$ . Dato che abbiamo supposto  $1 \leq k \leq n-1$ , vale la formula dell'esercizio 9.4, cioè  $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ . Questo dimostra che vi sono esattamente  $\binom{n}{k}$  sottoinsiemi di cardinalità  $k$  di  $A$ , come si voleva dimostrare.  $\square$

10.7. (a) Gli insiemi totalmente ordinati  $(\mathbb{N}, \leq)$  e  $(\mathbb{Z}, \leq)$  non sono isomorfi perché, ad esempio,  $\mathbb{N}$  ha minimo mentre  $\mathbb{Z}$  non ce l'ha.

(b)  $A$  ed  $\mathbb{N}$  non sono isomorfi perché  $A$  ha massimo mentre  $\mathbb{N}$  non ce l'ha.  $A$  e  $\mathbb{Z}$  non sono isomorfi perché  $A$  ha minimo mentre  $\mathbb{Z}$  non ce l'ha.

(c) Di esempi se ne possono trovare tanti; ad esempio vanno bene i seguenti sottoinsiemi ordinati di  $\mathbb{R}$ :  $B = \left\{ \frac{1}{z} \mid z \in \mathbb{N}, z \neq 0 \right\}$ ,  $C = A \cup \{0\}$ ,  $D = B \cup \{0\}$ , eccetera.  $\square$

10.9. (a) Sia  $(Z, m)$  un maggiorante di  $\mathcal{G}$  in  $\mathcal{F}$ . Allora  $Z$  è un sottoinsieme di  $A$ , si abbia  $f(a) = g(a)$ . Poniamo  $S = \bigcup_{(X,f) \in \mathcal{G}} X$  e sia  $\varphi: S \rightarrow B$  l'applicazione definita nel testo dell'esercizio. Per dimostrare che l'applicazione  $\varphi$  è ben definita basta osservare che se  $a \in S$ , scegliendo due coppie  $(X, f), (Y, g) \in \mathcal{G}$  tali che  $a \in X$  e  $a \in Y$ , si ha  $f(a) = g(a)$ . Quindi la definizione di  $\varphi(a)$  non dipende dalla scelta della coppia  $(X, f) \in \mathcal{G}$  tale che  $a \in X$ , ma solo dall'elemento  $a$ .

Questo dimostra che l'applicazione  $\varphi$  è ben definita.

Dato che  $S \subseteq A$  e  $\varphi: S \rightarrow B$  è un'applicazione, la coppia  $(S, \varphi)$  è un elemento di  $\mathcal{F}$ . Per dimostrare che  $(S, \varphi)$  è l'estremo superiore di  $\mathcal{G}$  in  $\mathcal{F}$  si deve dimostrare che  $(S, \varphi) \geq (X, f)$  per ogni  $(X, f) \in \mathcal{G}$ , e che se  $(Z, m) \in \mathcal{F}$  e  $(Z, m) \geq (X, f)$  che  $(S, \varphi) \geq (X, f)$  per ogni  $(X, f) \in \mathcal{G}$ , allora  $(Z, m) \geq (S, \varphi)$ . Ora se  $(X, f) \in \mathcal{G}$ , si ha  $S \supseteq X$  e per ogni  $(X, f) \in \mathcal{G}$  allora  $(Z, m) \geq (X, f)$ . Quindi  $(S, \varphi) \geq (X, f)$  per ogni  $(X, f) \in \mathcal{G}$ . Per ogni  $x \in X$  si ha  $\varphi(x) = f(x)$ . Inoltre se  $(Z, m) \in \mathcal{F}$  e  $(Z, m) \geq (X, f)$  per ogni  $(X, f) \in \mathcal{G}$ , allora  $Z \supseteq X$  per qualche  $(X, f) \in \mathcal{G}$  e quindi  $Z \supseteq S$ ; inoltre per ogni  $s \in S$  si ha  $s \in X$  per qualche  $(X, f) \in \mathcal{G}$ , ed essendo  $(Z, m) \geq (X, f)$  si ha  $\varphi(s) = f(s) = m(s)$ . Pertanto  $(X, f) \in \mathcal{G}$ , ed essendo  $(Z, m) \geq (X, f)$  si ha  $\varphi(s) = f(s) = m(s)$ . Pertanto  $(Z, m) \geq (S, \varphi)$ . Questo dimostra che  $(S, \varphi)$  è l'estremo superiore di  $\mathcal{G}$  in  $\mathcal{F}$ .

(c) Abbiamo già dimostrato in (a) che se esiste un maggiorante di  $\mathcal{G}$  in  $\mathcal{F}$ , allora per ogni  $(X, f), (Y, g) \in \mathcal{G}$  ed ogni  $a \in X \cap Y$  si ha  $f(a) = g(a)$ . Viceversa supponiamo che per ogni  $(X, f), (Y, g) \in \mathcal{G}$  ed ogni  $a \in X \cap Y$  si abbia  $f(a) = g(a)$ . Allora per quanto visto in (b) la coppia  $(S, \varphi)$  è l'estremo superiore di  $\mathcal{G}$  in  $\mathcal{F}$ . Quindi a maggior ragione l'elemento  $(S, \varphi) \in \mathcal{F}$  è un maggiorante di  $\mathcal{G}$  in  $\mathcal{F}$ .  $\square$

**11.7.** Per ogni  $x, y \in L$  si ha  $\varphi(x \vee y) = (x \vee y) \vee a = x \vee (y \vee a) = x \vee (a \vee y) = x \vee ((a \vee a) \vee y) = x \vee (a \vee (a \vee y)) = (x \vee a) \vee (y \vee a) = \varphi(x) \vee \varphi(y)$  e  $\varphi(x \wedge y) = (x \wedge y) \vee a = (x \vee a) \wedge (y \vee a) = \varphi(x) \wedge \varphi(y)$ . Quindi  $\varphi$  è un omomorfismo di reticoli.

(a)  $\Rightarrow$  (b) Supponiamo che  $\varphi$  sia un isomorfismo di reticoli, cioè che  $\varphi$  sia biettiva. Allora per ogni  $l \in L$  esiste  $x \in L$  tale che  $\varphi(x) = l$ , e quindi  $a \leq x \vee a = \varphi(x) = l$ . Questo dimostra che  $L$  ha minimo e che  $a$  è tale minimo.

(b)  $\Rightarrow$  (c) Supponiamo che  $a$  sia il minimo di  $L$ . Allora per ogni  $x \in L$  si ha  $\varphi(x) = x \vee a = x$  (perché  $a \leq x$ ). Quindi  $\varphi$  è l'applicazione identica di  $L$  in  $L$ .

(c)  $\Rightarrow$  (a) Ovvio.  $\square$

**11.10.** (a) Per dimostrare che  $A \vee B = A \cup B$  si deve far vedere che  $A \subseteq A \cup B$ , che  $B \subseteq A \cup B$ , e che se  $Z \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ ,  $A \subseteq Z$  e  $B \subseteq Z$ , allora  $A \cup B \subseteq Z$ . Tutte queste affermazioni sono ovvie.

Per la seconda affermazione distinguamo due casi a seconda che l'insieme  $A \cap B$  sia infinito o finito. Supponiamo che  $A \cap B$  sia infinito. Per dimostrare che  $A \wedge B = A \cap B$  si deve far vedere che  $A \cap B \subseteq A$ , che  $A \cap B \subseteq B$ , e che se  $Z \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ ,  $Z \subseteq A$  e  $Z \subseteq B$ , allora  $Z \subseteq A \cap B$ . Tutte queste affermazioni sono ovvie. Supponiamo invece che  $A \cap B$  sia finito. Per dimostrare che  $A \wedge B = \emptyset$  si deve far vedere che  $\emptyset \subseteq A$ , che  $\emptyset \subseteq B$ , e che se  $Z \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ ,  $Z \subseteq A$  e  $Z \subseteq B$ , allora  $Z \subseteq \emptyset$ . Le prime due di queste affermazioni sono ovvie. Per la terza si osservi che se  $Z \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ ,  $Z \subseteq A$  e  $Z \subseteq B$ , allora  $Z \subseteq A \cap B$ ; ma  $Z$  è un insieme vuoto o infinito e  $A \cap B$  è un insieme finito. Ne segue che  $Z$  deve essere l'insieme vuoto. Quindi  $Z \subseteq \emptyset$ , come volevamo dimostrare.

(b) Si ha  $1_L = Z$  perché  $A \subseteq Z$  per ogni  $A \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ , e  $0_L = \emptyset$  perché  $\emptyset \subseteq A$  per ogni  $A \in \mathcal{P}_\infty(Z) \cup \{\emptyset\}$ . Quindi il reticolo  $L$  è limitato.

(c) Sia  $A \in L$  tale che  $Z \setminus A$  sia un insieme finito e non vuoto. Ragioniamo per assurdo e supponiamo che  $A$  abbia un complemento  $B \in L$ . Allora  $A \vee B = 1_L$  e  $A \wedge B = 0_L$ . Per quanto visto in (a) e (b) si deve avere  $A \cup B = Z$ . Distinguiamo i due casi in cui  $A \cap B$  è un insieme finito o un insieme infinito. Se  $A \cap B$  è un insieme finito, allora  $B = [A \cup (Z \setminus A)] \cap B = (A \cap B) \cup [(Z \setminus A) \cap B] \subseteq (A \cap B) \cup (Z \setminus A)$  è un insieme finito perché è un sottoinsieme dell'unione di due insiemi finiti. Dato che  $B \in L$  ne segue che  $B = \emptyset$ . Ma allora da  $A \cup B = Z$  segue che  $A = Z$  e quindi  $Z \setminus A$  è l'insieme vuoto, contraddizione. Nel secondo caso, in cui  $A \cap B$  è un insieme infinito, allora  $A \wedge B = A \cap B \neq \emptyset = 0_L$ , che è pure una contraddizione. Dunque  $A$  non può avere un complemento  $B$  in  $L$ .

(d)  $(2Z_{\geq 0} \wedge 2Z_{\leq 0}) \vee D = \emptyset \vee D = \emptyset \cup D = D$  e  $(2Z_{\geq 0} \vee D) \wedge (2Z_{\leq 0} \vee D) = (2Z_{\geq 0} \vee D) \wedge (2Z_{\leq 0} \vee D)$ . Dato che  $(2Z_{\geq 0} \vee D) \cap (2Z_{\leq 0} \vee D) = D \cup \{0\}$  è un insieme infinito ne segue che  $(2Z_{\geq 0} \vee D) \wedge (2Z_{\leq 0} \vee D) = (2Z_{\geq 0} \vee D) \cap (2Z_{\leq 0} \vee D) = D \cup \{0\}$ .  $\square$

**11.15.** (a) Per dimostrare che  $f(x') = (f(x))'$ , cioè che  $f(x')$  è il complemento di  $f(x)$ , si deve far vedere che  $f(x') \vee f(x) = 1_C$  e  $f(x') \wedge f(x) = 0_C$ . Un facile calcolo mostra che  $f(x') \vee f(x) = f(x' \vee x) = f(1_B) = 1_C$  e che  $f(x') \wedge f(x) = f(x' \wedge x) = f(0_B) = 0_C$ .

(b) Per ogni  $x, y \in K$  si ha  $f(x \vee y) = f(x) \vee f(y) = 0_C \vee 0_C = 0_C$ , e quindi  $x \vee y \in K$ .

(c) Per ogni  $x \in K$  e ogni  $y \in B$  si ha  $f(x \wedge y) = f(x) \wedge f(y) = 0_C \wedge f(y) = 0_C$ , e quindi  $x \wedge y \in K$ .

(d) Siano  $x, x', y, y' \in B$  tali che  $[x]_{\sim_f} = [x']_{\sim_f}$  e  $[y]_{\sim_f} = [y']_{\sim_f}$ . Allora  $x \sim_f x'$  e  $y \sim_f y'$ , cioè  $f(x) = f(x')$  e  $f(y) = f(y')$ . Quindi  $f(x) \leq f(y)$  se e solo se  $f(x') \leq f(y')$ .

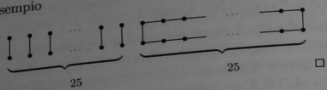
(e) **Riflessività.** Per ogni  $x \in B$  si ha  $f(x) \leq f(x)$ , e quindi  $[x]_{\sim_f} \preceq [x]_{\sim_f}$  per ogni  $[x]_{\sim_f} \in B/\sim_f$ .

**Simmetria.** Due generici elementi di  $B/\sim_f$  sono del tipo  $[x]_{\sim_f}, [y]_{\sim_f}$ , dove  $x$  e  $y$  sono due elementi di  $B$ . Supponiamo che  $[x]_{\sim_f} \preceq [y]_{\sim_f}$  e  $[y]_{\sim_f} \preceq [x]_{\sim_f}$ . Allora  $f(x) \leq f(y)$  e  $f(y) \leq f(x)$ , da cui  $f(x) = f(y)$ . Pertanto  $x \sim_f y$ , e quindi  $[x]_{\sim_f} = [y]_{\sim_f}$ .

**Transitività.** Tre generici elementi di  $B/\sim_f$  sono del tipo  $[x]_{\sim_f}, [y]_{\sim_f}, [z]_{\sim_f}$ , dove  $x, y, z$  sono elementi di  $B$ . Supponiamo che  $[x]_{\sim_f} \preceq [y]_{\sim_f}$  e  $[y]_{\sim_f} \preceq [z]_{\sim_f}$ . Allora  $f(x) \leq f(y)$  e  $f(y) \leq f(z)$ , da cui  $f(x) \leq f(z)$ , e quindi  $[x]_{\sim_f} \preceq [z]_{\sim_f}$ .  $\square$

**12.4.** No, in un grafo con 100 vertici si deve avere  $d(v) < 100$  per ogni vertice  $v$ , e quindi non può essere  $d(v_{100}) = 100$ .  $\square$

12.5. Sì, ad esempio



12.6. No. I numeri naturali dispari  $i \leq 98$  sono  $98/2 = 49$ , che è dispari, mentre ogni grafo deve avere un numero pari di vertici dispari.  $\square$

12.7. Un grafo non orientato regolare con 5 vertici deve avere grado  $d < 5$ . Inoltre deve avere  $\frac{1}{2}dn = \frac{5}{2}d$  lati, e quindi  $d$  deve essere un numero pari. Ne segue che  $d = 0, 2$  o  $4$ .

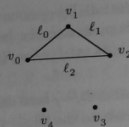
Per  $d = 4$  il grafo deve essere il grafo completo con 5 vertici, cioè



Per  $d = 0$  il grafo deve essere

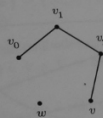


Per  $d = 2$  il grafo  $G$  deve essere un grafo regolare di grado 2 con 5 vertici e 5 lati. Fissiamo un vertice qualunque e chiamiamolo  $v_1$ . Dato che  $G$  è un grafo regolare di grado 2,  $v_1$  appartiene ad esattamente due lati; chiamiamoli  $\ell_0$  e  $\ell_1$ . Siano  $v_0$  e  $v_2$  i vertici diversi da  $v_1$  di  $\ell_0$  e  $\ell_1$  rispettivamente. Quindi  $\ell_0 = \{v_0, v_1\}$  e  $\ell_1 = \{v_1, v_2\}$ . Anche  $v_2$  ha grado 2, e quindi  $v_2$  appartiene ad un altro lato  $\ell_2 = \{v_2, v\}$ . Allora  $v \neq v_0$  e  $v \neq v_1$ . Se fosse  $v = v_0$ , il grafo  $G$  avrebbe come sottografo il grafo



Ma in questo sottografo  $v_0, v_1$  e  $v_2$  hanno già grado 2, e quindi entrambi i restanti due lati di  $G$  dovrebbero avere  $v_3$  e  $v_4$  come estremi, e questo è assurdo. Quindi  $v \neq v_0$ .

Ne segue che il grafo  $G$  ha come sottografo il grafo



Dato che  $w, v_0$  e  $v$  devono avere tutti grado 2, si conclude che i due lati rimanenti devono essere  $\{w, v_0\}$  e  $\{w, v\}$ . Quindi il grafo regolare è

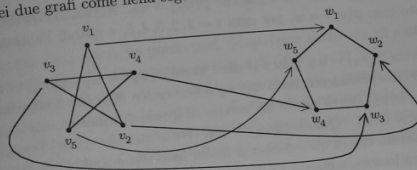


Abbiamo così dimostrato che a meno di isomorfismi ci sono esattamente tre grafi regolari con 5 vertici, aventi grado 0, 2 e 4 rispettivamente.  $\square$

12.8. (a) Etichettiamo gli insiemi

$$V = \{v_1, v_2, v_3, v_4, v_5\} \quad \text{e} \quad W = \{w_1, w_2, w_3, w_4, w_5\}$$

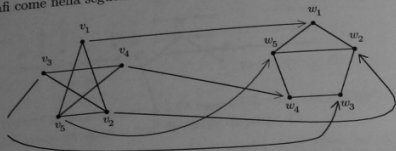
dei vertici dei due grafi come nella seguente figura.



L'applicazione  $\varphi : V \rightarrow W$  definita da  $\varphi(v_i) = w_i$  per ogni  $i = 1, 2, 3, 4, 5$  è un isomorfismo di grafi in quanto si tratta di una biiezione e due vertici  $v_i \in V$  qualunque sono adiacenti se e solo se le loro immagini  $\varphi(v_i) \in W$  sono adiacenti.

(b) Siano  $V = \{v_1, v_2, v_3, v_4, v_5\}$  e  $W = \{w_1, w_2, w_3, w_4, w_5\}$  gli insiemi dei vertici

dei due grafi come nella seguente figura.



L'applicazione  $\varphi: V \rightarrow W$  definita da  $\varphi(v_i) = w_i$  per ogni  $i = 1, 2, 3, 4, 5$  è un isomorfismo di grafi in quanto è una biiezione e due vertici arbitrari  $v_i \in V$  sono adiacenti se e solo se le loro immagini  $\varphi(v_i) \in W$  sono adiacenti.

(c) Sia  $W = \{w_1, w_2, w_3, w_4, w_5\}$  l'insieme dei vertici del grafo come nella figura precedente e sia  $\varphi$  un automorfismo del grafo. Allora  $\varphi: W \rightarrow W$  è una biiezione che "conserva i gradi", cioè si ha che  $d(w_i) = d(\varphi(w_i))$  per ogni  $i$  (si veda la soluzione dell'esercizio 12.3). Dato che  $d(w_1) = 2$ ,  $d(w_2) = 3$ ,  $d(w_3) = 2$ ,  $d(w_4) = 2$ ,  $d(w_5) = 3$ , si dovrà avere pertanto  $\varphi(\{w_2, w_5\}) \subseteq \{w_2, w_5\}$  e  $\varphi(\{w_1, w_3, w_4\}) \subseteq \{w_1, w_3, w_4\}$ . Inoltre  $w_1$  è l'unico vertice di grado 2 adiacente a due vertici entrambi di grado 2. Quindi  $\varphi(w_1) = w_1$  e  $\varphi(\{w_3, w_4\}) \subseteq \{w_3, w_4\}$ .

Distinguiamo ora due casi a seconda che  $\varphi(w_3) = w_3$  o che  $\varphi(w_3) = w_4$ .

Se  $\varphi(w_3) = w_3$ , allora si deve avere  $\varphi(w_4) = w_4$  e  $\varphi(w_1) = w_1$ . Inoltre, dato che  $w_2$  è un vertice di grado 3 adiacente sia a  $w_1$  che a  $w_3$ ,  $\varphi(w_2)$  dovrà essere un vertice di grado 3 adiacente sia a  $\varphi(w_1) = w_1$  che a  $\varphi(w_3) = w_3$ . Quindi si deve avere  $\varphi(w_2) = w_2$ . Ne segue che  $\varphi(w_5) = w_5$ . Abbiamo così dimostrato che in questo caso  $\varphi(w_i) = w_i$  per ogni  $i = 1, 2, 3, 4, 5$ , e quindi l'automorfismo  $\varphi$  è l'identità.

Se invece  $\varphi(w_3) = w_4$ , allora si deve avere  $\varphi(w_4) = w_3$  e  $\varphi(w_1) = w_1$ . Inoltre, come nel caso precedente, dato che  $w_2$  è un vertice di grado 3 adiacente sia a  $w_1$  che a  $w_3$ ,  $\varphi(w_2)$  dovrà essere un vertice di grado 3 adiacente sia a  $\varphi(w_1) = w_1$  che a  $\varphi(w_3) = w_4$ . Quindi  $\varphi(w_2) = w_5$ . Ne segue che  $\varphi(w_5) = w_2$ . Abbiamo così dimostrato che in questo caso  $\varphi$  lascia fisso  $w_1$ , scambia tra loro  $w_2$  e  $w_5$ , e scambia tra loro  $w_3$  e  $w_4$ .

Pertanto il grafo in questione ha esattamente due automorfismi, l'identità e l'automorfismo  $\varphi$  appena descritto.  $\square$

**12.9.** Siano  $G = (V, L)$  e  $G' = (V', L')$  due grafi orientati. Un isomorfismo (di grafi orientati) di  $G$  in  $G'$  è una biiezione  $\varphi: V \rightarrow V'$  tale che per ogni  $v, w \in V$  si ha  $(v, w) \in L$  se e solo se  $(\varphi(v), \varphi(w)) \in L'$ .  $\square$

© 88-08-10250-5

**12.10.** (a) Se  $\rho$  è la relazione di uguaglianza  $=$ , il suo grafo è  $G_\rho = G_\theta = (V, \rho)$  dove  $\rho = \{(a, b) \mid a, b \in V, a \rho b\} = \{(a, b) \mid a, b \in V, a = b\} = \{(a, a) \mid a \in V\} = D_V$ . Quindi  $G_\rho = (V, D_V)$ .

(b) Si deve dimostrare che se  $\rho$  è un'equivalenza su  $V$ , allora  $\rho = (\pi \times \pi)^{-1}(D_{V/\rho})$ , cioè che per ogni coppia  $(v, v') \in V \times V$  si ha  $(v, v') \in \rho$  se e solo se  $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\rho})$ .

Si ha  $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\rho})$  se e solo se  $(\pi(v), \pi(v')) \in D_{V/\rho}$ , cioè se e solo se  $(\pi(v), \pi(v')) \in D_{V/\rho}$ , ossia se e solo se  $\pi(v) = \pi(v')$ . Ma  $\pi(v) = [v]_\rho$  e  $\pi(v') = [v']_\rho$ . Quindi  $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\rho})$  se e solo se  $[v]_\rho = [v']_\rho$ , e questo accade se e solo se  $v \rho v'$ , cioè se e solo se  $(v, v') \in \rho$ .  $\square$

**13.5.** (a) Per dimostrare che  $G'$  è connesso si deve far vedere che per ogni coppia di vertici distinti  $v, w \in V \cup \{v_0\}$  esiste un cammino da  $v$  a  $w$  in  $G'$ . Distinguiamo il caso in cui né  $v$  né  $w$  sono uguali a  $v_0$  da quello in cui uno tra  $v$  e  $w$  è uguale a  $v_0$ . Nel primo caso entrambi i vertici  $v$  e  $w$  appartengono a  $V$ , e dato che  $G$  è connesso esiste un cammino in  $G$  da  $v$  a  $w$ ; quindi a maggior ragione esiste un cammino in  $G'$  da  $v$  a  $w$ . Nel secondo caso, cioè se uno dei due vertici  $v$  o  $w$  appartiene a  $V$  e l'altro è  $v_0$ , si ragiona invece nel modo seguente. Per simmetria possiamo supporre che sia  $w$  il vertice che appartiene a  $V$  e  $v$  il vertice uguale a  $v_0$ . Dato che il grafo  $G$  non ha circuiti euleriani, non tutti i vertici di  $G$  hanno grado pari. Sia  $v_1 \in V$  un vertice di grado dispari in  $G$ . Dato che  $G$  è connesso esiste un cammino in  $G$  da  $w$  a  $v_1$ , e  $\{v_1, v_0\} \in L'$  è un lato di  $G'$  da  $v_1$  a  $v_0$ . Ne segue che esiste un cammino in  $G'$  da  $w$  a  $v_0 = v$ .

(b) Contiamo i lati a cui  $v_0$  appartiene. Per come è stato definito  $G'$  i lati a cui  $v_0$  appartiene sono tanti quanti i vertici di grado dispari in  $G$ . Per il corollario 12.2  $G$  ha un numero pari di vertici dispari. Quindi  $v_0$  appartiene a un numero pari di lati.

(c) Abbiamo già visto che  $v_0$  ha grado pari. Mostriamo anche che gli altri vertici  $v$  di  $G'$  hanno grado pari. Ogni altro vertice  $v$  di  $G'$  sta in  $V$ . I lati di  $G'$  a cui  $v$  appartiene sono tutti i lati di  $G$  a cui  $v$  appartiene più eventualmente il lato  $\{v, v_0\}$  se  $v$  è un vertice di grado dispari in  $G$ . Quindi il grado di  $v$  in  $G'$  è uguale al grado di  $v$  in  $G$  se tale grado è pari, mentre è uguale a uno più il grado di  $v$  in  $G$  se tale grado è dispari. Quindi in entrambi i casi il grado di  $v$  in  $G'$  è pari.

Abbiamo così dimostrato che tutti i vertici di  $G'$  sono pari. Mostriamo ora che  $G'$  non ha vertici isolati. Se per assurdo  $v_0$  fosse un vertice isolato, allora  $|L'| = 0$ , e quindi  $G$  non avrebbe vertici di grado dispari. In questo caso  $G$  sarebbe un grafo finito connesso con tutti i vertici pari, e quindi avrebbe un circuito euleriano, contrariamente all'ipotesi. Se invece ci fosse in  $G'$  un vertice isolato  $v \in V$ , allora  $v$  sarebbe un vertice isolato di  $G$ . Ma  $G$  è connesso, e quindi  $G$  dovrebbe avere un unico vertice, il vertice  $v$ . Anche questo è contrario all'ipotesi, perché  $|V| > 1$ .

Pertanto  $G'$  è un grafo connesso, con tutti i vertici pari e privo di vertici isolati. Dal teorema di Eulero segue (c).

(d) Sia  $G$  un grafo finito connesso. Distinguiamo tre casi a seconda che (1)  $G$  ha un circuito euleriano, (2)  $G$  ha un solo vertice, (3)  $G$  ha più di un vertice e non ha un circuito euleriano. Nel caso (1) non c'è nulla da dimostrare, perché  $G$  non ha un circuito euleriano. Nel caso (2)  $G$  è sottografo del grafo completo  $K_3$  con tre vertici, che ha un circuito euleriano. Nel caso (3) si può invece applicare la costruzione del grafo  $G'$  vista nelle parti (a), (b) e (c) di questo esercizio.  $\square$

13.9. Siano  $1 \leq m \leq n$  numeri naturali.

(a)  $K_{m,n}$  ha un circuito euleriano se e solo se  $m$  ed  $n$  sono entrambi pari.

(b)  $K_{m,n}$  ha un cammino euleriano se e solo se  $m$  ed  $n$  sono entrambi pari, oppure  $m = 1$  e  $n = 2$ , oppure  $m = 2$  ed  $n \geq 2$  è un numero naturale arbitrario.  $\square$

14.4. (a)  $n(m-1) + m(n-1)$ .

(b)  $(n-1)(m-1) + 1$ .

(c)  $G$  ha un cammino euleriano se e solo se  $n = 1$  oppure  $m = 1$  oppure  $n + m \leq 5$ . Infatti supponiamo che  $G$  abbia un cammino euleriano, che  $n > 1$  e che  $m > 1$ . Allora  $G$  ha al più due vertici dispari. Ora  $G$  ha tutti i vertici "interi" di grado 4, e i  $2(n+m) - 4$  sul bordo sono 4 di grado 2 e i rimanenti  $2(n+m) - 8$  di grado 3. Quindi se  $G$  ha un cammino euleriano si deve avere  $2(n+m) - 8 \leq 2$ , ossia  $n + m \leq 5$ .

Viceversa è chiaro che se  $n = 1$  oppure  $m = 1$   $G$  ha un cammino euleriano. Supponiamo dunque  $n > 1$ ,  $m > 1$  e  $n + m \leq 5$ . Allora la coppia  $(n, m)$  sarà o  $(2, 2)$  o  $(2, 3)$  o  $(3, 2)$ . È chiaro in tutti e tre i casi  $G$  avrà un cammino euleriano.  $\square$

14.6.



(a)

(b) Lo stesso di (a), in quanto ogni grafo finito con 8 lati è piano per l'esercizio 14.5.  $\square$

15.3. Sono tutte vere.  $\square$

15.10. Il concetto di "più semplice" non è univocamente definito, e quindi le soluzioni possibili sono diverse. Eccone una:

(a)  $A \wedge B$ ; (b)  $A$ ; (c)  $\neg(A \vee B)$ ; (d)  $B$ .  $\square$

16.4. (d) è falsa.

(e) è vera: basta prendere per  $y$  il numero reale  $-x$ .  $\square$

16.5. Le formule in (a) e (c) sono chiuse, quella in (b) non lo è.  $\square$

16.6. Dato che  $\exists x p(x)$  è una proposizione vera, le proposizioni  $\neg \exists x p(x)$  e  $\forall x \neg p(x)$  sono false. Ma allora  $(\forall x \neg p(x)) \rightarrow (\forall x p(x))$  è vera in quanto il suo antecedente è falso.  $\square$

16.7. Ci sono varie soluzioni possibili. Una di queste è

$$\forall x (\neg p(x) \rightarrow \exists y q(x, y)). \quad \square$$

16.8. Una soluzione possibile è

$$(\forall x \forall y (\exists z (p(x, z) \wedge p(y, z))) \rightarrow q(x, y)) \wedge \neg (\forall y \exists x p(x, y)). \quad \square$$

17.6. (a) Si deve dimostrare che  $(f * g) * h = f * (g * h)$  per ogni  $f, g, h \in S^X$ . Per dimostrare che le due applicazioni  $(f * g) * h$  e  $f * (g * h)$  di  $X$  in  $S$  coincidono si deve far vedere che  $((f * g) * h)(x) = (f * (g * h))(x)$  per ogni  $x \in X$ . Questo è immediato, in quanto per ogni  $x \in S$  si ha  $((f * g) * h)(x) = (f * g)(x) \cdot h(x) = (f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x)) = f(x) \cdot (g * h)(x) = (f * (g * h))(x)$ .

(b) Supponiamo che  $S$  sia un semigruppato commutativo. Per dimostrare che anche  $S^X$  è un semigruppato commutativo si deve dimostrare che  $f * g = g * f$  per ogni  $f, g \in S^X$ . Per ogni  $x \in X$  si ha  $(f * g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g * f)(x)$ . Quindi le due applicazioni  $f * g$  e  $g * f$  di  $X$  in  $S$  coincidono.  $\square$

17.8. (a) Per ogni  $(a, b), (a', b'), (a'', b'') \in R \times R$  si ha  $((a, b) * (a', b')) * (a'', b'') = (aa', ab' + b) * (a'', b'') = (aa'a'', aa'b'' + ab' + b) = (aa'a'', aa'b'' + b' + b) = (aa'a'', aa'b'' + ab' + b) = (a, b) * ((a', b') * (a'', b'')) = (a, b) * (a'a'', a'b'' + b'') = (aa'a'', a(a'b'' + b'') + b) = (aa'a'', aa'b'' + ab' + b)$ . Quindi  $((a, b) * (a', b')) * (a'', b'') = (a, b) * ((a', b') * (a'', b''))$ .

(b) No, ad esempio  $(2, 0) * (2, 1) = (4, 2)$  e  $(2, 1) * (2, 0) = (4, 1)$ . Quindi  $(2, 0) * (2, 1) \neq (2, 1) * (2, 0)$ .

(c) Il sottoinsieme  $\{1\} \times R$  di  $R \times R$  è un sottosemigruppato di  $(R \times R, *)$ , in quanto per ogni  $b, b' \in R$  si ha  $(1, b) * (1, b') = (1, b + b') \in \{1\} \times R$ . Analogamente  $R \times \{0\}$  è un sottosemigruppato di  $(R \times R, *)$ , in quanto per ogni  $a, a' \in R$  si ha  $(a, 0) * (a', 0) = (aa', 0 + 0) = (aa', 0) \in R \times \{0\}$ .

(d) Sia  $b \in R$ . Dimostriamo per induzione che per ogni intero positivo  $n$  si ha  $(1, b)^n = (1, nb)$ . Per  $n = 1$  si ha  $(1, b)^1 = (1, b) = (1, 1 \cdot b)$ . Supponiamo che l'uguaglianza sia vera per  $n - 1$ , cioè che  $(1, b)^{n-1} = (1, (n-1)b)$ . Allora il principio di induzione si conclude che l'uguaglianza è vera per ogni intero positivo  $n$ .



Sia ora invece  $a \in \mathbb{R}$ . Dimostriamo che per ogni intero positivo  $n$  si ha  $(a, 0)^n = (a^n, 0)$ . Per  $n = 1$  si ha  $(a, 0)^1 = (a, 0) = (a^1, 0)$ . Supponiamo che l'uguaglianza sia vera per  $n - 1$ , cioè che  $(a, 0)^{n-1} = (a^{n-1}, 0)$ . Allora  $(a, 0)^n = (a, 0)^{n-1} * (a, 0) = (a^{n-1}, 0) * (a, 0) = (a^{n-1}a, 0 + 0) = (a^n, 0)$ . Per il principio di induzione si conclude.  $\square$

**17.12.** Sia  $(S, +)$  un semigruppato. Se  $a \in S$  ed  $m, n$  sono interi positivi, allora  $na + ma = (n + m)a$  e  $m(na) = (mn)a$ . Se  $a, b \in S$ ,  $a + b = b + a$  ed  $n$  è un intero positivo, allora  $n(a + b) = na + nb$ .  $\square$

**18.4.** Cerchiamo le identità sinistre. Un elemento  $e \in A$  è un'identità sinistra se e solo se  $e * a = a$  per ogni  $a \in A$ , cioè se  $e = a$  per ogni  $a \in A$ . Quindi  $A$  ha un'identità sinistra se e solo se  $A$  ha un unico elemento, e in tal caso quell'unico elemento è un'identità (sinistra).

Cerchiamo le identità destre. Un elemento  $e \in A$  è un'identità destra se e solo se  $a * e = a$  per ogni  $a \in A$ . Dato che questo accade qualunque sia  $e \in A$ , se ne conclude che tutti gli elementi di  $A$  sono identità sinistre.

In particolare  $A$  è un monoide se e solo se  $A$  ha un'identità sinistra e destra, se e solo se  $|A| = 1$ .  $\square$

**18.9.** (a) Si osservi che l'identità del monoide  $M$  è  $(0, 0)$  e l'identità del monoide  $(\mathbb{N}, \cdot)$  è  $1$ . Si ha  $f(0, 0) = a^0 b^0 = 1$ . Inoltre per ogni  $(x, y), (x', y') \in M$  si ha  $f((x, y) + (x', y')) = f(x + x', y + y') = a^{x+x'} b^{y+y'} = a^x a^{x'} b^y b^{y'} = a^x b^y a^{x'} b^{y'} = f(x, y) f(x', y')$ , dove abbiamo denotato con  $+$  anche l'operazione sul monoide  $M$ .

(b)  $f^{-1}(1) = \{(x, y) \in M \mid f(x, y) = 1\} = \{(x, y) \mid x, y \in \mathbb{N}, a^x b^y = 1\} = \{(x, y) \mid x, y \in \mathbb{N}, a^x (a^2)^y = 1\} = \{(x, y) \mid x, y \in \mathbb{N}, a^{x+2y} = 1\} = \{(x, y) \mid x, y \in \mathbb{N}, x + 2y = 0\} = \{(0, 0)\}$ .

(c) Si ha  $f(2, 0) = a^2 b^0 = a^2$ ,  $f(0, 1) = a^0 b^1 = a^2$  e  $(2, 0) \neq (0, 1)$ .

(d) Siano  $(x, y), (x', y') \in M$  tali che  $f(x, y) = f(x', y')$ . Allora  $a^x b^y = a^{x'} b^{y'}$ . Per il teorema fondamentale dell'aritmetica si ha quindi che  $x = x'$  e  $y = y'$ . Pertanto  $(x, y) = (x', y')$ .  $\square$

**18.10.** (a) Si ha

$$\begin{aligned} S &= \{(-1, 0)\} = \\ &= \{1_{\mathbb{R}}, x_1 x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{-1, 0\}\} = \\ &= \{1, (-1)^a 0^b \mid a, b \in \mathbb{N}\} = \{1, (-1)^a, 0 \mid a \in \mathbb{N}\} = \{1, -1, 0\}. \end{aligned}$$

In particolare  $S$  ha 3 elementi.

(b) *Unicità.* Se  $\varphi$  è un endomorfismo del monoide  $(\mathbb{R}, \cdot)$  tale che  $\varphi(0) = 0$  e  $\varphi(\alpha) = -1$  per ogni numero reale negativo  $\alpha$ , allora per ogni reale positivo  $\beta$  si

deve avere

$$\varphi(\beta) = \varphi((-\sqrt{\beta})(-\sqrt{\beta})) = \varphi(-\sqrt{\beta})\varphi(-\sqrt{\beta}) = (-1)(-1) = 1,$$

in quanto  $-\sqrt{\beta}$  è un numero reale negativo. Quindi l'endomorfismo  $\varphi$  deve essere definito da

$$\varphi(x) = \begin{cases} 1 & \text{se } x > 0, \\ 0 & \text{se } x = 0, \\ -1 & \text{se } x < 0. \end{cases}$$

Questo dimostra che l'endomorfismo con le proprietà richieste, se esiste, è unico.

*Esistenza.* Mostriamo che l'applicazione  $\varphi$  definita nel paragrafo precedente è un endomorfismo di  $(\mathbb{R}, \cdot)$ . Dato che  $\varphi(1) = 1$ , è sufficiente dimostrare che  $\varphi(xy) = \varphi(x)\varphi(y)$  per ogni  $x, y \in \mathbb{R}$ . Distinguiamo i quattro casi  $xy = 0$ ,  $x$  e  $y$  entrambi positivi,  $x$  e  $y$  entrambi negativi,  $x$  e  $y$  uno positivo e l'altro negativo. Se  $xy = 0$ , allora uno tra  $x$  e  $y$  è nullo, e quindi uno tra  $\varphi(x)$  e  $\varphi(y)$  è nullo; ne segue che  $\varphi(xy)$  e  $\varphi(x)\varphi(y)$  sono uguali perché sono entrambi nulli. Se  $x$  e  $y$  sono entrambi positivi, allora  $xy$  è positivo, e quindi  $\varphi(x) = \varphi(y) = \varphi(xy) = 1$ ; pertanto  $\varphi(xy) = \varphi(x)\varphi(y)$  anche in questo secondo caso. Se  $x$  e  $y$  sono entrambi negativi, allora  $xy$  è positivo, e quindi  $\varphi(x) = \varphi(y) = -1$  e  $\varphi(xy) = 1$ ; pertanto anche in questo terzo caso  $\varphi(xy) = \varphi(x)\varphi(y)$ . Infine se  $x$  e  $y$  sono uno positivo e l'altro negativo, allora  $xy$  è negativo,  $\varphi(xy) = -1$ , e tra  $\varphi(x)$  e  $\varphi(y)$  uno è  $1$  e l'altro è  $-1$ . Quindi in questo quarto caso  $\varphi(xy)$  e  $\varphi(x)\varphi(y)$  sono uguali perché sono entrambi uguali a  $-1$ . Questo dimostra che  $\varphi$  è un endomorfismo di monoide.  $\square$

(c) Si ha  $\varphi(\mathbb{R}) = \{1, 0, -1\} = S$ .  $\square$

**18.11.** (a) Siano  $a, b \in M$ . Se  $a = b = 0$ , allora  $a + b = 0 \in M$ . Altrimenti o  $a \geq 2$  oppure  $b \geq 2$ , nel qual caso  $a + b$  è un numero naturale  $\geq 2$  e quindi  $a + b \in M$ .

(b) Ragioniamo per assurdo e supponiamo che il monoide  $M$  sia chiuso. Se  $a \in M$  è un generatore di  $M$ , allora  $M = \{na \mid n \in \mathbb{N}\}$ . Dato che  $2 \in M$ , deve essere  $2 = an$  per qualche  $n \in \mathbb{N}$ . Dato che  $1 \notin M$  si avrà quindi  $a = 2$ . Pertanto si deve avere  $M = \{2n \mid n \in \mathbb{N}\}$ , il che è assurdo perché  $3 \in M$ .  $\square$

**19.5.** (a) *Riflessività.* Per ogni  $x \in M$  si ha  $x^1 = x^1$ , e quindi  $x \sim x$ . *Transitività.* Siano  $x, y, z \in M$  tali che  $x \sim y$  e  $y \sim z$ . Allora esistono  $n, m \in \mathbb{N}^*$  tali che  $x^n = y^n e y^m = z^m$ . Ne segue che  $nm \in \mathbb{N}^*$  e  $x^{nm} = (x^n)^m = (y^m)^n = y^{nm} = (y^m)^n = (z^m)^n = z^{nm}$ . Quindi  $y \sim z$ .

(b) Siano  $x, y, z, t$  elementi del monoide commutativo  $M$  tali che  $x \sim y$  e  $z \sim t$ . Allora esistono  $n, m \in \mathbb{N}^*$  tali che  $x^n = y^n$  e  $z^m = t^m$ . Ma allora  $(xz)^{nm} = x^{nm} z^{nm} = (x^n)^m (z^m)^n = (y^n)^m (t^m)^n = y^{nm} t^{nm} = (yt)^{nm}$ . Quindi  $xz \sim yt$ .

(c) Siano  $x \in M$  ed  $n \in \mathbb{N}^*$  tali che  $x^n \sim 1_M$ . Allora esiste  $m \in \mathbb{N}^*$  tale che  $(x^n)^m = (1_M)^m$ , da cui  $x^{nm} = (x^n)^m = (1_M)^m = 1_M = (1_M)^{nm}$ . Pertanto  $x \sim 1_M$ .  $\square$

19.8. (a) *Riflessività*. Per ogni  $a \in Z$  si ha  $2^0 a = 2^0 a$ , e quindi  $a \sim a$ .

*Transitività*. Siano  $a, b, c \in Z$  tali che  $a \sim b$  e  $b \sim c$ . Allora esistono  $n, m, p, q \in \mathbb{N}$  tali che  $2^n a = 2^m b$  e  $2^p b = 2^q c$ . Ne segue che  $2^{n+p} a = 2^p 2^n a = 2^p 2^m b = 2^{m+q} c = 2^{m+q} c$ . Quindi  $a \sim c$ .

(b) Siano  $a, b, c, d \in Z$  tali che  $a \sim b$  e  $c \sim d$ . Allora esistono  $n, m, p, q \in \mathbb{N}$  tali che  $2^n a = 2^m b$  e  $2^p c = 2^q d$ . Moltiplicando membro a membro si ottiene che  $2^{n+p} ac = 2^{m+q} bd$ . Quindi  $ac \sim bd$ .

(c) Basta osservare che  $1 \in D \cup 0$ , che il prodotto di due numeri dispari è un numero dispari, e che il prodotto di un qualunque numero intero per zero fa zero.

(d) *Iniettività*. Siano  $a, b \in D \cup 0$  tali che  $\phi(a) = \phi(b)$ . Allora  $[a]_{\sim} = [b]_{\sim}$ , da cui  $a \sim b$ , e quindi esistono  $n, m \in \mathbb{N}$  tali che  $2^n a = 2^m b$ . Se uno tra  $a$  e  $b$  è zero, anche l'altro deve essere zero, e quindi in questo caso  $a = b$ . Altrimenti contando il numero di fattori uguali a 2 in una fattorizzazione di  $2^n a = 2^m b$  come prodotto di primi, si ricava che  $n = m$  dal teorema fondamentale dell'aritmetica. Ne segue che  $a = b$ , come desiderato.

*Suriettività*. Sia  $X \in Z/\sim$ . Allora esiste  $x \in Z$  tale che  $X = [x]_{\sim}$ . Se  $x = 0$ , allora  $\phi(0) = [0]_{\sim} = X$ . Altrimenti si scriva  $x$  nella forma  $x = 2^n a$  con  $n \in \mathbb{N}$  e  $a \in Z$  dispari. Si ha  $2^0 a = 2^n a$ , e quindi  $x \sim a$ , da cui  $[x]_{\sim} = [a]_{\sim}$ . Ma allora  $a \in D$  è un elemento tale che  $\phi(a) = [a]_{\sim} = [x]_{\sim} = X$ .  $\phi$  è un omomorfismo di monoidi. Si ha  $\phi(1) = [1]_{\sim} = 1_{Z/\sim}$  e  $\phi(ab) = [ab]_{\sim} = [a]_{\sim} [b]_{\sim} = \phi(a)\phi(b)$  per ogni  $a, b \in D \cup 0$ .  $\square$

19.9. (a) Si consideri l'applicazione  $\varphi: S \rightarrow f(S)$  definita da  $\varphi(x) = f(x)$  per ogni  $x \in S$  ( $\varphi$  è l'applicazione ottenuta da  $f$  restringendo il codominio a  $f(S)$ ). Si osservi che  $f(S)$  è un sottosemigruppato di  $S'$  (esercizio 19.6 (a)), che  $\varphi$  è un omomorfismo del semigruppato  $S$  nel semigruppato  $f(S)$ , e che l'applicazione  $\varphi$  è ovviamente suriettiva. Per il teorema fondamentale di omomorfismo per i semigruppato esiste un'unica applicazione  $\tilde{\varphi}: S/\sim_{\varphi} \rightarrow f(S)$  che rende commutativo il diagramma

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & f(S) \\ \pi \searrow & & \nearrow \tilde{\varphi} \\ & S/\sim_{\varphi} & \end{array}$$

e inoltre  $\tilde{\varphi}$  è un isomorfismo di semigruppato perché  $\varphi$  è suriettiva. Quindi  $S/\sim_{\varphi}$  ed  $f(S)$  sono semigruppato isomorfi. Ma le relazioni  $\sim_f$  e  $\sim_{\varphi}$  su  $S$  coincidono, in quanto per ogni  $x, y \in S$  si ha  $x \sim_f y$  se e solo se  $f(x) = f(y)$ , cioè se e solo se

$\varphi(x) = \varphi(y)$ , vale a dire se e solo se  $x \sim_{\varphi} y$ . Quindi i semigruppato  $S/\sim_f$  ed  $f(S)$  sono isomorfi.

La dimostrazione della parte (b) è analoga a quella della parte (a).  $\square$

20.5. *Iniettività*. Siano  $h, h' \in \text{Hom}(W, M)$  tali che  $\Phi(h) = \Phi(h')$ . Allora  $h \circ \varphi = h' \circ \varphi$ . Per la proprietà universale dei monoidi liberi (teorema 20.1), in corrispondenza all'applicazione  $f = h \circ \varphi = h' \circ \varphi: A \rightarrow M$  esiste un unico omomorfismo di monoidi  $\hat{f}: W \rightarrow M$  tale che  $\hat{f} \circ \varphi = f$ . Dato che  $h, h'$  sono entrambi due omomorfismi di  $W$  in  $M$  tali che  $h \circ \varphi = h' \circ \varphi = f$ , ne segue che  $\hat{f} = h = h'$ .

*Suriettività*. Sia  $f$  un qualunque elemento di  $M^A$ , cioè un'applicazione  $f: A \rightarrow W$ . Per la proprietà universale dei monoidi liberi, esiste un omomorfismo di monoidi  $\hat{f}: W \rightarrow M$  tale che  $\hat{f} \circ \varphi = f$ . Allora  $\hat{f} \in \text{Hom}(W, M)$  e  $\Phi(\hat{f}) = \hat{f} \circ \varphi = f$ .  $\square$

21.7. Se  $mZ \supseteq nZ$ , allora  $n = n \cdot 1 \in nZ \subseteq mZ$ , e quindi esiste  $t \in Z$  tale che  $n = mt$ . Ne segue che  $m \mid n$ .

Viceversa se  $m \mid n$ , cioè se esiste  $t \in Z$  tale che  $n = mt$ , verifichiamo che vale l'inclusione  $mZ \supseteq nZ$ : se  $x \in nZ$ , allora  $x = nz$  per qualche  $z \in Z$ , e quindi  $x = nz = m(tz) \in mZ$ .  $\square$

21.8. (a) Intanto  $G[n] \neq \emptyset$  perché essendo  $n \cdot 0_G = 0_G$  si ha  $0_G \in G[n]$ . Inoltre se  $g, g' \in G[n]$ , allora  $g, g' \in G$  e  $ng = ng' = 0_G$ , da cui  $n(g - g') = ng - ng' = 0_G - 0_G = 0_G$ . Quindi  $g - g' \in G[n]$ . Questo dimostra che  $G[n]$  è un sottogruppo di  $G$ .

(b) Poniamo  $S = \{g + h \mid g \in G[m], h \in G[n]\}$ . Dimostriamo che  $S \subseteq G[mn]$ . Se  $x \in S$ , allora  $x = g + h$  per qualche  $g \in G[m]$  e qualche  $h \in G[n]$ , da cui  $g, h \in G$ ,  $mg = 0_G$  e  $nh = 0_G$ . Ma allora  $mnx = mn(g + h) = mng + mn h = n(mg) + m(nh) = n \cdot 0_G + m \cdot 0_G = 0_G$ . Pertanto  $x \in G[mn]$ .

Dimostriamo che viceversa  $G[mn] \subseteq S$ . Sia  $x \in G[mn]$ . Dato che  $m$  ed  $n$  sono primi tra loro, per il corollario 4.2 esistono  $\alpha, \beta \in Z$  tali che  $\alpha n + \beta m = 1$ . Allora  $x = (\alpha n + \beta m)x = \alpha nx + \beta mx$ . Ma essendo  $x \in G[mn]$  si ha  $mnx = 0_G$  e quindi  $nx \in G[m]$  e  $mx \in G[n]$ . Pertanto  $x = \alpha(nx) + \beta(mx) \in G[m] + G[n]$ .

Dimostriamo che  $G[m] \cap G[n] = \{0_G\}$ . Dato che  $0_G \in G[m] \cap G[n]$  si ha certamente che  $G[m] \cap G[n] \supseteq \{0_G\}$ . Viceversa se  $x \in G[m] \cap G[n]$ , allora  $mx = 0_G$  e  $nx = 0_G$ . Se  $\alpha$  e  $\beta$  sono interi tali che  $\alpha n + \beta m = 1$  (esistono per il corollario 4.2), allora  $x = \alpha nx + \beta mx = 0_G$ . Questo dimostra che  $G[m] \cap G[n] = \{0_G\}$ .  $\square$

21.9. (b) Se  $e \in G$  è idempotente, allora moltiplicando a sinistra per  $e^{-1}$  l'uguaglianza  $e^2 = e$  si ottiene che  $e^{-1}e^2 = e^{-1}e$ , da cui  $e = 1_G$ .

(c) Mostriamo che  $eMe = \{eme \mid m \in M\}$  è un sottosemigruppato di  $M$ . Se  $x, y \in eMe$ , allora  $x = eme$  e  $y = em'e$  per opportuni  $m, m' \in M$ , e quindi

$xy = emecm'e$ . Dato che  $meem' \in M$ , se ne deduce che  $xy \in eMe$ .

Mostriamo che  $eMe$  è un monoide. Abbiamo già dimostrato che  $eMe$  è un semigrupp. Resta da dimostrare che possiede un'identità. Il suo elemento  $e$  lo è, infatti  $e^2 = e$  è un'identità di  $eMe$ , in quanto per ogni  $x \in eMe$  esiste  $m \in M$  tale che  $x = eme$ , e pertanto  $xe = emee = eme = x$  e analogamente  $ex = eeme = eme = x$ .  $\square$

**21.12.** (a) Il gruppo  $(C^*, \cdot)$  non ha la proprietà: ad esempio l'elemento  $i \in C^*$  è tale che  $i^4 = 1$ , mentre  $i \neq 1$ . Invece il gruppo  $(C, +)$  ha la proprietà: se  $x \in C$ ,  $n$  è un intero positivo e  $nx = 0$ , allora  $x = 0$ .

(b) Sia  $x \in G$ ,  $x \neq 1_G$ , e supponiamo che  $n$  ed  $m$  siano interi positivi tali che  $x^n = x^m$ . Per simmetria si può supporre che  $n \geq m$ . Allora  $x^{n-m} = x^n x^{-m} = x^n = x^m$ . Per simmetria si può supporre che  $n > m$  allora  $x \in G$ ,  $x \neq 1_G$ , ed  $n - m$  sarebbe un numero intero positivo tale che  $x^{n-m} = 1_G$ . Per ipotesi  $G$  non possiede elementi  $x \neq 1_G$  tali che  $x^{n-m} = 1_G$ . Quindi deve essere  $n = m$ .

possiede elementi  $x \neq 1_G$  tali che  $x^{n-m} = 1_G$ . Quindi deve essere  $n = m$ .

(c) **Riflessività.** Per ogni  $x \in G$  si ha  $x = x^1$ . Quindi  $x \leq x$ .  
**Antisimmetria.** Siano  $x, y \in G$  tali che  $x \leq y$  e  $y \leq x$ . Allora esistono numeri naturali  $n, m$  tali che  $x = y^n$  e  $y = x^m$ . Ma allora  $x^1 = x = y^n = (x^m)^n = x^{mn}$ , naturali  $n, m$  tali che  $x = y^n$  e  $y = x^m$ . Ma allora  $x^1 = x = y^n = (x^m)^n = x^{mn}$ , e quindi per quanto visto in (b) deve essere  $x = 1_G$  oppure  $mn = 1$ . Se  $x = 1_G$ , allora anche  $y = x^m = 1_G$ , e quindi  $x = y$ . Se invece  $mn = 1$ , allora  $m = n = 1$ , e quindi anche in questo caso  $x = y$ .

**Transitività.** Siano  $x, y, z \in G$  tali che  $x \leq y$  e  $y \leq z$ . Allora esistono numeri naturali  $n, m$  tali che  $x = y^n$  e  $y = z^m$ . Ma allora  $x = y^n = (z^m)^n = z^{mn}$ , e quindi  $x \leq z$ .

(d) Supponiamo che  $G \neq \{1_G\}$ . Allora esiste un elemento  $x \in G$ ,  $x \neq 1_G$ . Consideriamo gli elementi  $x^2$  e  $x^3$ . Non può essere che  $x^2 \leq x^3$ , altrimenti esisterebbe un numero naturale  $n$  tale che  $x^2 = (x^3)^n$ , e quindi  $x^2 = x^{3n}$ , da cui, per quanto visto nella parte (b), si dovrebbe avere che  $2 = 3n$ , il che non può essere. Analogamente non si può avere che  $x^3 \leq x^2$ , altrimenti si avrebbe che  $3 = 2n$ . Per un opportuno numero naturale  $n$ , e anche questo è assurdo. Abbiamo così dimostrato che non si può avere né che  $x^2 \leq x^3$ , né che  $x^3 \leq x^2$ . Quindi l'ordine  $\leq$  sull'insieme  $G$  non è totale.

Se viceversa supponiamo che  $G = \{1_G\}$ , allora  $G$ , insieme parzialmente ordinato con un solo elemento, è certamente un insieme totalmente ordinato.  $\square$

**22.4.** (a) La relazione  $\rho$  è definita, per ogni  $a, b \in \mathbb{Z}$ , da  $a \rho b$  se  $a = b$  oppure  $a = -b$ , e quindi  $a \rho b$  se e solo se  $|a| = |b|$ . È immediato verificare che questa è un'equivalenza. La relazione  $\sigma$  è definita, per ogni  $a, b \in \mathbb{Z}$ , da  $a \sigma b$  se  $a = b$  oppure  $2a = b$ . Quindi si ha ad esempio  $1 \sigma 2$ , ma non si ha  $2 \sigma 1$ . Pertanto la relazione  $\sigma$  non è simmetrica, e quindi, in particolare, non è un'equivalenza. La relazione  $\tau$  è definita, per ogni  $a, b \in \mathbb{Z}$ , da  $a \tau b$  se  $a = b$  oppure  $ab = 5$ . Quindi

due elementi stanno nella relazione  $\tau$  se e solo se sono uguali oppure appartengono entrambi a  $\{1, 5\}$  oppure appartengono entrambi a  $\{-1, -5\}$ . Ne segue quindi che  $\tau$  è la relazione  $\sim_{\mathcal{F}}$  associata alla partizione

$$\mathcal{F} = \{\{1, 5\}, \{-1, -5\}, \{z \mid z \in \mathbb{Z} \setminus \{1, 5, -1, -5\}\}\}.$$

In particolare  $\tau$  è una relazione di equivalenza.

(b) In (a) abbiamo visto che  $\rho$  e  $\tau$  sono equivalenze, mentre  $\sigma$  non lo è. Per la proposizione 22.1 le relazioni di equivalenza su  $\mathbb{Z}$  compatibili con l'addizione sono tutte e sole le congruenze modulo un numero naturale. Dato che né  $\rho$  né  $\tau$  sono congruenze, ne segue che nessuna delle equivalenze trovate in (a) è compatibile con l'addizione tra numeri naturali.

(c) L'equivalenza  $\rho$  è compatibile con la moltiplicazione tra numeri naturali, in quanto se  $a, b, c, d \in \mathbb{Z}$  sono numeri interi,  $|a| = |b|$  e  $|c| = |d|$ , allora  $|ac| = |a||c| = |b||d| = |bd|$ . Per quanto riguarda invece l'equivalenza  $\tau$ , si vede subito che essa non è compatibile con la moltiplicazione tra numeri interi, in quanto ad esempio  $2 \tau 2$ ,  $1 \tau 5$ , mentre non si ha  $(2 \cdot 1) \tau (2 \cdot 5)$ .  $\square$

**22.5.** (a) **Riflessività.** Per ogni  $a \in \mathbb{Z}$  si ha  $(aa - 3)(a - a) = 0$ , e quindi  $a \rho a$ .

**Simmetria.** Se  $a \rho b$ , allora  $(ab - 3)(a - b) = 0$ , e quindi  $(ba - 3)(b - a) = 0$ , vale a dire  $b \rho a$ .

**Transitività.** Siano  $a, b, c \in \mathbb{Z}$  tali che  $a \rho b$  e  $b \rho c$ . Allora  $(ab - 3)(a - b) = 0$  e  $(bc - 3)(b - c) = 0$ . Se  $a = b$  o  $b = c$ , allora  $a \rho c$ . Se invece  $a \neq b$  e  $b \neq c$ , allora  $ab - 3 = 0$  e  $bc - 3 = 0$ , da cui  $b \neq 0$ ,  $a = 3/b$  e  $c = b/3$ . Ne segue che  $a = c$ , da cui  $(ac - 3)(a - c) = 0$ . Quindi  $a \rho c$ .

(b) Sia  $a \in \mathbb{Z}$ . Allora

$$[a]_{\rho} = \{x \mid x \in \mathbb{Z}, x \rho a\} = \{x \mid x \in \mathbb{Z}, (xa - 3)(x - a) = 0\} = \{x \mid x \in \mathbb{Z}, xa = 3 \text{ oppure } x = a\}.$$

Quindi se  $a$  è uguale a 1 o 3 si ha che  $[a]_{\rho} = \{1, 3\}$  ha due elementi, se  $a$  è uguale a  $-1$  o  $-3$  si ha che  $[a]_{\rho} = \{-1, -3\}$  ha ancora due elementi, mentre se  $a$  è diverso da 1, 3,  $-1, -3$  allora  $[a]_{\rho} = \{a\}$  ha un solo elemento.

(c) No, perché la relazione  $\rho$  non coincide con nessuna congruenza modulo un numero naturale.  $\square$

**22.6.** C'è solo la congruenza modulo 1, cioè la relazione banale  $\omega$ .  $\square$

**22.7.** Sono quattro: le congruenze modulo 2, 3, 6, e relazione banale  $\omega$ .  $\square$

**22.8.** Sono tre:  $\sim_{0,1}$  (cioè la relazione banale  $\omega$ ),  $\sim_{1,1}$  e  $\sim_{2,1}$ .  $\square$

**22.9.** Sono dodici:  $\sim_{0,1}$  (cioè la relazione banale  $\omega$ ),  $\sim_{1,1}$ ,  $\sim_{2,1}$ ,  $\sim_{0,2}$ ,  $\sim_{1,2}$ ,  $\sim_{2,2}$ ,  $\sim_{0,3}$ ,  $\sim_{1,3}$ ,  $\sim_{2,3}$ ,  $\sim_{0,6}$ ,  $\sim_{1,6}$ ,  $\sim_{2,6}$ .  $\square$

**22.10.** (a) Dimostriamo che  $\varphi$  è ben definita. Siano  $x, x' \in \mathbb{Z}$  tali che  $[x]_{\equiv_n} = [x']_{\equiv_n}$ . Allora  $x \equiv x' \pmod{n}$ , cioè  $x - x' = nt$  per qualche  $t \in \mathbb{Z}$ . Ma allora  $qx - qx' = qnt$ , ed essendo  $m = nq$  se ne ricava che  $qx - qx' = mt$ . Quindi  $m \mid (qx - qx')$ , ossia  $qx \equiv qx' \pmod{m}$ . Pertanto  $[qx]_{\equiv_m} = [qx']_{\equiv_m}$ . Questo prova che ponendo  $\varphi([x]_{\equiv_n}) = [qx]_{\equiv_m}$  per ogni  $[x]_{\equiv_n} \in \mathbb{Z}/\equiv_n$  si dà una buona definizione di un'applicazione  $\varphi: \mathbb{Z}/\equiv_n \rightarrow \mathbb{Z}/\equiv_m$ . Inoltre  $\varphi$  è un omomorfismo di gruppi additivi, perché se  $x, y \in \mathbb{Z}$  si ha  $\varphi([x]_{\equiv_n} + [y]_{\equiv_n}) = \varphi([x+y]_{\equiv_n}) = [q(x+y)]_{\equiv_m} = [qx+qy]_{\equiv_m} = [qx]_{\equiv_m} + [qy]_{\equiv_m} = \varphi([x]_{\equiv_n}) + \varphi([y]_{\equiv_n})$ .

(b) Mostriamo che l'omomorfismo  $\varphi$  è iniettivo. Se  $x, y \in \mathbb{Z}$  sono tali che  $\varphi([x]_{\equiv_n}) = \varphi([y]_{\equiv_n})$ , allora  $[qx]_{\equiv_m} = [qy]_{\equiv_m}$ , da cui  $qx \equiv qy \pmod{m}$ . Ma allora  $m \mid (qx - qy)$ , e quindi esiste  $t \in \mathbb{Z}$  tale che  $qx - qy = mt$ . Essendo  $m = nq$  se ne ricava che  $x - y = nt$ . Pertanto  $x \equiv y \pmod{n}$ , da cui  $[x]_{\equiv_n} = [y]_{\equiv_n}$ . Questo dimostra che  $\varphi$  è iniettivo.

(c) Siano  $m$  un intero positivo ed  $n$  un divisore positivo di  $m$ . Abbiamo visto in (a) e (b) che c'è un omomorfismo iniettivo di gruppi additivi  $\varphi: \mathbb{Z}/\equiv_n \rightarrow \mathbb{Z}/\equiv_m$ . Quindi  $\varphi(\mathbb{Z}/\equiv_n)$  è un sottogruppo di  $\mathbb{Z}/\equiv_m$  isomorfo a  $\mathbb{Z}/\equiv_n$ .  $\square$

**22.12.** Abbiamo già osservato prima dell'enunciato della proposizione 22.4 che  $[1]_{\sim_{k,n}}$  è un generatore del monoide ciclico  $(\mathbb{N}/\sim_{k,n}, +)$ . Dimostriamo che è l'unico generatore di  $(\mathbb{N}/\sim_{k,n}, +)$ . Sia  $t \in \mathbb{N}$  un numero naturale tale che  $[t]_{\sim_{k,n}}$  sia un generatore di  $(\mathbb{N}/\sim_{k,n}, +)$ . Allora  $\mathbb{N}/\sim_{k,n} = \{m[t]_{\sim_{k,n}} \mid m \in \mathbb{N}\}$  e quindi in particolare deve esistere un  $m \in \mathbb{N}$  tale che  $[1]_{\sim_{k,n}} = [mt]_{\sim_{k,n}}$ . Ne segue che  $1 \sim_{k,n} mt$ . Dato che  $k > 1$  ne segue che  $1 = mt$ . Ma  $m$  e  $t$  sono numeri naturali, e quindi  $m = t = 1$ . Abbiamo così dimostrato che  $[1]_{\sim_{k,n}}$  è l'unico generatore di  $(\mathbb{N}/\sim_{k,n}, +)$  per ogni  $k > 1$  e ogni  $n \geq 1$ .  $\square$

**22.14.** Si ha  $[Y] = \{Y^n \mid n \in \mathbb{N}\}$ . Ora  $Y^n = 1_{\mathcal{P}(X)} = X$  se  $n = 0$  e  $Y^n = Y \cap Y \cap \dots \cap Y$  se  $n > 0$ . Quindi  $[Y] = \{X, Y\}$  ha due elementi se  $Y \neq X$ .

ha un solo elemento se  $Y = X$ . Inoltre se  $Y \neq X$  si ha che  $\min\{p \in \mathbb{N} \mid \text{esiste } q \in \mathbb{N}, q \neq p, \text{ tale che } Y^p = Y^q\} = 1$ . Quindi in questo caso  $[Y]$  è isomorfo a  $\mathbb{N}/\sim_{1,1}$ . Se invece  $Y = X$ , allora  $\min\{p \in \mathbb{N} \mid \text{esiste } q \in \mathbb{N}, q \neq p, \text{ tale che } Y^p = Y^q\} = 0$ , e quindi  $[Y]$  è isomorfo a  $\mathbb{N}/\sim_{0,1}$ .  $\square$

**22.15.** È isomorfo a  $\mathbb{N}/\sim_{0,4}$ .  $\square$

**22.16.** È isomorfo a  $\mathbb{N}$ .  $\square$

**22.18.** (c) Si ha  $(i\sqrt{2})^0 = 1$ ,  $(i\sqrt{2})^1 = i\sqrt{2}$ ,  $(i\sqrt{2})^2 = -2$ , eccetera. Si noti però che  $(i\sqrt{2})^0 = 1 \neq i\sqrt{2}$ , in quanto  $\frac{1}{i\sqrt{2}} = \frac{-i\sqrt{2}}{2} \notin \mathbb{R}$ , mentre  $(i\sqrt{2})^0 = 1 \sim (i\sqrt{2})^2 = -2$ , in quanto  $\frac{1}{-2} \in \mathbb{R}$ . Quindi  $[i\sqrt{2}]_{\sim} = [(i\sqrt{2})^0]_{\sim} = [1]_{\sim} \neq [i\sqrt{2}]_{\sim} = [(i\sqrt{2})^1]_{\sim} = [i\sqrt{2}]_{\sim}$ , mentre  $[i\sqrt{2}]_{\sim}^0 = [1]_{\sim}$  è uguale a  $[-2]_{\sim} = [(i\sqrt{2})^2]_{\sim} =$

$[i\sqrt{2}]_{\sim}^2$ . Da  $[i\sqrt{2}]_{\sim}^0 = [i\sqrt{2}]_{\sim}^2 = [1]_{\sim}$  segue che  $[i\sqrt{2}]_{\sim}^n = [1]_{\sim}$  per ogni  $n \geq 0$  pari, mentre  $[i\sqrt{2}]_{\sim}^n = [i\sqrt{2}]_{\sim}$  per ogni  $n$  dispari. In particolare il sottomonoido ciclico  $[i\sqrt{2}]_{\sim}$  di  $(C^*/\sim, \cdot)$  generato da  $[i\sqrt{2}]_{\sim}$  ha due elementi.

(d) È isomorfo a  $\mathbb{N}/\sim_{0,2}$ .  $\square$

**23.4.** (a) Sono ventiquattro:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

eccetera.

(b) Dato che  $S_4$  è un gruppo, il suo elemento  $f$  ha un inverso  $f^{-1}$ . Quindi se  $f \circ g = f$ , allora  $f^{-1} \circ f \circ g = f^{-1} \circ f$ , e quindi  $g = \text{id}$ . Pertanto l'unico elemento  $g$  di  $S_4$  tale che  $f \circ g = f$  è l'identità.  $\square$

**23.11.** (a) *Iniettività.* Se  $z, z' \in E$  e  $\varphi(z) = \varphi(z')$ , allora  $iz = iz'$ , da cui, moltiplicando per  $-i$ ,  $z = z'$ .

*Suriettività.* Se  $w \in E$ , allora  $-iw \in E$  (perché  $-iw \in \mathbb{C}$  e  $(-iw)^8 = (-i)^8 w^8 = 1$ ), e  $\varphi(-iw) = i(-iw) = w$ .

(b) Si osservi che

$$\begin{aligned} \varphi(z_h) &= iz_h = (\cos(\pi/2) + i\sin(\pi/2))(\cos(\pi h/4) + i\sin(\pi h/4)) = \\ &= \cos(\pi(2+h)/4) + i\sin(\pi(2+h)/4), \end{aligned}$$

e quindi  $\varphi(z_h) = z_{2+h}$  per ogni  $h = 1, 2, \dots, 6$ ,  $\varphi(z_7) = z_1$ ,  $\varphi(z_8) = z_2$ . Pertanto  $f(h) = \psi^{-1} \circ \varphi \circ \psi(h) = \psi^{-1} \varphi(z_h) = \psi^{-1}(z_{2+h}) = 2+h$  per ogni  $h = 1, 2, \dots, 6$ ,  $f(7) = 1$ ,  $f(8) = 2$ . Nella notazione con cui si denotano le permutazioni si ha quindi

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix}.$$

Ne segue che come prodotto di cicli disgiunti si ha  $f = (1\ 3\ 5\ 7) \circ (2\ 4\ 6\ 8)$ . Pertanto  $\lambda(f) = 4 + 4 - 2 = 6$ ,  $\text{sgn}(f) = (-1)^6 = 1$ , e quindi  $f$  è di classe pari.  $\square$

**23.12.** (a) Se  $d = 2$ , allora  $f$  è una trasposizione, e quindi è evidente che  $f^2$  debba essere l'identità del gruppo  $S_n$ .

(b) Se  $d$  è dispari e  $f = (a_1\ a_2\ a_3\ \dots\ a_d)$ , allora

$$f^2 = (a_1\ a_3\ a_5\ \dots\ a_{d-2}\ a_d\ a_2\ a_4\ a_6\ \dots\ a_{d-3}\ a_{d-1})$$

è un ciclo di lunghezza  $d$ .









**27.11.** Dato che  $R$  è un campo,  $R$  ha i soli due ideali  $\{0\}$  e  $R$  (questo si può dedurre ad esempio dal fatto che ogni ideale  $\neq \{0\}$  di  $R$  contiene un elemento invertibile, e quindi coincide con  $R$  per quanto visto nell'esercizio 27.6). Per il teorema 27.1 ci sono esattamente due equivalenze su  $R$  compatibili con l'addizione e la moltiplicazione. La prima è  $\sim_{\{0\}}$ , definita, per ogni  $a, b \in R$ , da  $a \sim_{\{0\}} b$  se e solo se  $a = b$ ; quindi  $\sim_{\{0\}}$  è l'uguaglianza. La seconda è  $a \sim_{\{0\}} b$  se e solo se  $a - b \in \{0\}$ , cioè se e solo se  $a = b$ ; quindi  $\sim_{\{0\}}$  è l'uguaglianza. La seconda è  $a \sim_R b$ , definita, per ogni  $a, b \in R$ , da  $a \sim_R b$  se  $a - b \in R$ . Quindi  $a \sim_R b$  per ogni  $a, b \in R$ , vale a dire  $\sim_R$  è l'equivalenza banale  $\omega$  su  $R$ . Abbiamo così dimostrato che le uniche due relazioni di equivalenza su  $R$  compatibili sia con l'addizione che con la moltiplicazione sono l'uguaglianza e la relazione banale  $\omega$ .  $\square$

**28.4.** (a)  $R$  ha  $4 \cdot 4 \cdot 4 = 64$  elementi.

(b)  $E(\bar{1}, \bar{0}, \bar{0})$ .

(c) Se  $(\bar{0}, \bar{a}, \bar{b})$  è un qualunque elemento di  $R$  si ha  $(\bar{0}, \bar{a}, \bar{b})(\bar{0}, \bar{0}, \bar{1}) = (\bar{0}, \bar{0}, \bar{0})$ .

(d) Abbiamo già osservato in (a) che  $1_R = (\bar{1}, \bar{0}, \bar{0})$ . Quindi per ogni intero  $n > 0$  si ha  $\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} = (\bar{n}, \bar{0}, \bar{0})$ , e pertanto  $\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} = 0_R$  se e solo se  $\bar{n} = \bar{0}$ , cioè se e solo se  $n \equiv 0 \pmod{4}$ . Dato che il più piccolo intero  $n > 0$  tale che  $n \equiv 0 \pmod{4}$  è 4, se ne deduce che  $\text{char } R = 4$ .  $\square$

**28.5.** (a) Sia  $R = \mathbb{Z}_n^X$ . Si vede facilmente che l'identità di  $R$  è l'applicazione  $i: X \rightarrow \mathbb{Z}_n$  definita da  $i(x) = \bar{1}$  per ogni  $x \in X$ . Fissato un qualunque elemento  $z \in \mathbb{Z}$  definiamo un'applicazione  $f_z: X \rightarrow \mathbb{Z}_n$  ponendo  $f_z(x) = \bar{z}$  per ogni  $x \in X$ . Allora  $z \cdot i = f_z$  per ogni  $z \in \mathbb{Z}$ , in quanto se  $x \in X$  si ha

$$\begin{aligned} (z \cdot i)(x) &= \underbrace{(i + \dots + i)(x)}_{z \text{ volte}} = \underbrace{i(x) + \dots + i(x)}_{z \text{ volte}} = \\ &= \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{z \text{ volte}} = \bar{z} = f_z(x) \end{aligned}$$

quando  $z > 0$ ,

$$\begin{aligned} (z \cdot i)(x) &= \underbrace{((-i) + (-i) + \dots + (-i))(x)}_{-z \text{ volte}} = \\ &= \underbrace{(-i)(x) + (-i)(x) + \dots + (-i)(x)}_{-z \text{ volte}} = \\ &= \underbrace{(-\bar{1}) + (-\bar{1}) + \dots + (-\bar{1})}_{-z \text{ volte}} = z \cdot \bar{1} = \bar{z} = f_z(x) \end{aligned}$$

quando  $z < 0$ , e

$$(z \cdot i)(x) = 0_R(x) = \bar{0} = \bar{z} = f_z(x)$$

quando  $z = 0$ . Quindi il sottoanello fondamentale di  $R$  è  $P_R = \{z \cdot i \mid z \in \mathbb{Z}\} = \{f_z \mid z \in \mathbb{Z}\}$ .

(b) Per ogni  $z \in \mathbb{Z}$ ,  $z > 0$ , si ha  $z \cdot i = 0_R$  se e solo se  $f_z = 0_R$ , cioè se e solo se  $f_z(x) = \bar{0}$  per ogni  $x \in X$ . Quindi  $z \cdot i = 0_R$  se e solo se  $\bar{z} = \bar{0}$ , cioè se e solo se  $z \equiv 0 \pmod{n}$ . Il più piccolo intero  $z > 0$  tale che  $z \equiv 0 \pmod{n}$  è  $n$ . Quindi  $\text{char } \mathbb{Z}_n^X = n$ .

(c) Supponiamo che  $R = \mathbb{Z}_n^X$  sia un campo. Allora  $n = \text{char } \mathbb{Z}_n^X$  deve essere un numero primo. Se per assurdo  $X$  avesse cardinalità  $> 1$ ,  $X$  avrebbe almeno due elementi distinti  $x_1$  e  $x_2$ . Siano  $f, g: X \rightarrow \mathbb{Z}_n$  definite per ogni  $x \in X$  da

$$f(x) = \begin{cases} \bar{0} & \text{se } x = x_1, \\ \bar{1} & \text{se } x \neq x_1, \end{cases} \quad g(x) = \begin{cases} \bar{1} & \text{se } x = x_1, \\ \bar{0} & \text{se } x \neq x_1. \end{cases}$$

Allora  $(fg)(x) = f(x)g(x) = \bar{0} = 0_R(x)$  per ogni  $x \in X$ . Quindi  $f \neq 0_R$ ,  $g \neq 0_R$ , ma  $fg = 0_R$ . Pertanto  $R = \mathbb{Z}_n^X$  non sarebbe un dominio d'integrità, assurdo.

Viceversa supponiamo che  $X$  abbia cardinalità 1 e che  $n$  sia un numero primo. Allora  $|\mathbb{Z}_n^X| = n^1 = n$ . Ne segue che  $P_R \subseteq \mathbb{Z}_n^X$  e  $n = |P_R| \leq |\mathbb{Z}_n^X| = n$ . Quindi  $\mathbb{Z}_n^X$  coincide con il suo sottoanello fondamentale  $P_R$ . Inoltre  $P_R \simeq \mathbb{Z}_n$  perché  $\text{char } \mathbb{Z}_n^X = n$ . Pertanto  $\mathbb{Z}_n^X \simeq \mathbb{Z}_n$  è un campo perché  $n$  è primo.  $\square$

**28.7.** Se  $R$  ha caratteristica 2, si ha  $1_R + 1_R = 0_R$ , e quindi per ogni  $a \in R$  si ha  $a + a = 1_R \cdot a + 1_R \cdot a = (1_R + 1_R) \cdot a = 0_R \cdot a = 0_R$ . Pertanto  $a = -a$ .  $\square$

**28.10.** (a) Dimostriamo che se  $\text{char } R = n \neq 0$ , allora anche  $\text{char } S \neq 0$  (dimostrazione indiretta). Se  $\text{char } R = n \neq 0$ , allora  $\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} = 0_R$ . Ne segue che

$$\begin{aligned} \underbrace{1_S + 1_S + \dots + 1_S}_{n \text{ volte}} &= \underbrace{f(1_R) + f(1_R) + \dots + f(1_R)}_{n \text{ volte}} = \\ &= \underbrace{f(1_R + 1_R + \dots + 1_R)}_{n \text{ volte}} = f(0_R) = 0_S. \end{aligned}$$

Quindi  $\text{char } S \neq 0$ .

(b) Siano  $P_R = \{z \cdot 1_R \mid z \in \mathbb{Z}\}$  e  $P_S = \{z \cdot 1_S \mid z \in \mathbb{Z}\}$ . Allora

$$f(P_R) = \{f(z \cdot 1_R) \mid z \in \mathbb{Z}\} = \{z \cdot f(1_R) \mid z \in \mathbb{Z}\} = \{z \cdot 1_S \mid z \in \mathbb{Z}\} = P_S.$$

(c) Supponiamo  $\text{char } R = n > 0$  e  $\text{char } S = m$ . Abbiamo già visto in (a) che  $m \neq 0$  e che  $n \cdot 1_S = \underbrace{1_S + 1_S + \dots + 1_S}_{n \text{ volte}} = 0_S$ . Dividiamo  $n$  per  $m$ . Allora

$$n = qm + r \text{ con } q, r \in \mathbb{Z}, \text{ e } 0 \leq r < m, \text{ e quindi } 0_S = n \cdot 1_S = (qm + r) \cdot 1_S = (qm) \cdot 1_S + r \cdot 1_S = q(m \cdot 1_S) + r \cdot 1_S = q \cdot 0_S + r \cdot 1_S = r \cdot 1_S \text{ perché } \text{char } S = m.$$

$m$ . Se fosse  $r > 0$ , allora  $\underbrace{1_S + 1_S + \dots + 1_S}_{r \text{ volte}} = 0_S$ , e questo è assurdo perché  $\text{char } S = m > r$ . Quindi si deve avere  $r = 0$  ed  $n = qm$ .  $\square$

**28.11.** Denotiamo con  $0$  e  $1$  i numeri razionali  $0$  e  $1$ , che sono gli elementi neutri per l'addizione e la moltiplicazione nell'anello  $(\mathbb{Q}, +, \cdot)$ , e con  $0_R$  e  $1_R$  gli elementi neutri per l'addizione e la moltiplicazione nell'anello  $(\mathbb{Q}, +, *)$ . Dato che le addizioni nei due anelli coincidono, si ha  $0 = 0_R$ .

(a) Si ha  $1_R * q = q$  per ogni  $q \in \mathbb{Q}$  se e solo se  $\frac{5}{3} 1_R q = q$  per ogni  $q \in \mathbb{Q}$ , cioè se e solo se  $1_R = \frac{3}{5}$ . Quindi  $1_R = \frac{3}{5}$ .

(b) Per ogni  $n \in \mathbb{Z}$ ,  $n > 0$ , si ha

$$\underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ volte}} = \underbrace{\frac{3}{5} + \frac{3}{5} + \dots + \frac{3}{5}}_{n \text{ volte}} = \frac{3n}{5},$$

e questo è sempre diverso da  $0 = 0_R$ . Quindi la caratteristica dell'anello  $(\mathbb{Q}, +, *)$  è  $0$ .

(c) Il sottoanello fondamentale di  $R$  è

$$P_R = \{z \cdot 1_R \mid z \in \mathbb{Z}\} = \left\{z \cdot \frac{3}{5} \mid z \in \mathbb{Z}\right\} = \left\{\frac{3z}{5} \mid z \in \mathbb{Z}\right\}.$$

(d) Si consideri l'applicazione  $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$  definita da  $\varphi(x) = \frac{5}{3}x$  per ogni  $x \in \mathbb{Q}$ . L'applicazione  $\varphi$  è chiaramente una biiezione. Inoltre si ha

$$\begin{aligned}\varphi(x+y) &= \frac{5}{3}(x+y) = \frac{5}{3}x + \frac{5}{3}y = \varphi(x) + \varphi(y), \\ \varphi(xy) &= \varphi\left(\frac{5}{3}xy\right) = \frac{5}{3}\left(\frac{5}{3}xy\right) = \left(\frac{5}{3}x\right)\left(\frac{5}{3}y\right) = \varphi(x)\varphi(y)\end{aligned}$$

per ogni  $x, y \in \mathbb{Q}$ , e

$$\varphi(1_R) = \varphi\left(\frac{3}{5}\right) = \frac{5}{3} \cdot \frac{3}{5} = 1.$$

Quindi  $\varphi$  è un isomorfismo dell'anello  $(\mathbb{Q}, +, *)$  nel campo  $(\mathbb{Q}, +, \cdot)$ .  $\square$

**28.12.** (a) Si ha  $0_A = (0, \bar{0})$  e  $1_A = (1, \bar{1})$ . I due elementi  $(0, \bar{1})$  e  $(1, \bar{0})$  di  $A$  non sono nulli, ma il loro prodotto è nullo. Quindi  $A$  non è un dominio d'integrità.

(b) Si consideri la proiezione canonica sul primo fattore  $\pi_R: R \times Z_8 \rightarrow R$  definita da  $\pi_R(a, \bar{b}) = a$  per ogni  $a \in R$ ,  $\bar{b} \in Z_8$ . Allora  $\pi_R$  è un omomorfismo suriettivo d'anelli, come è immediato verificare, e il suo nucleo è

$$\begin{aligned}\ker \pi_R &= \{(a, \bar{b}) \mid a \in R, \bar{b} \in Z_8, \pi_R(a, \bar{b}) = 0\} = \\ &= \{(a, \bar{b}) \mid a \in R, \bar{b} \in Z_8, a = 0\} = \{(0, \bar{b}) \mid \bar{b} \in Z_8\} = \{0\} \times Z_8.\end{aligned}$$

Applicando il teorema fondamentale di omomorfismo per gli anelli all'omomorfismo  $\pi_R: R \times Z_8 \rightarrow R$  si deduce che esiste un isomorfismo d'anelli  $\bar{\pi}_R: R \times Z_8 / \ker \pi_R \rightarrow R$ . Quindi

$$R \times Z_8 / \{0\} \times Z_8 = R \times Z_8 / \ker \pi_R \simeq R$$

è un campo. Pertanto  $\{0\} \times Z_8$  è un ideale massimale di  $R \times Z_8$ .

(c) Si consideri l'elemento  $(0, \bar{4})$  di  $A$ . Si ha  $(0, \bar{4}) \notin R \times \{0\}$  mentre  $(0, \bar{4})(0, \bar{4}) = (0, \bar{16}) = (0, \bar{0}) \in R \times \{0\}$ . Quindi  $R \times \{0\}$  non è un ideale primo di  $A$ .

(d) Per ogni  $n \in \mathbb{Z}$ ,  $n > 0$ , si ha

$$\underbrace{1_A + 1_A + \dots + 1_A}_{n \text{ volte}} = \underbrace{(1, \bar{1}) + (1, \bar{1}) + \dots + (1, \bar{1})}_{n \text{ volte}} = (n, \bar{n}),$$

e questo è sempre diverso da  $(0, \bar{0}) = 0_A$ . Quindi  $\text{char } A = 0$ .  $\square$

**28.13.** (a) Chiaramente  $1 = 1 + 0 \in A + M$ .

Se  $a + m, a' + m' \in A + M$  con  $a, a' \in A$  e  $m, m' \in M$ , allora  $(a + m) - (a' + m') = (a - a') + (m - m') \in A + M$  e  $(a + m)(a' + m') = aa' + (am' + a'm + mm') \in A + M$  perché  $am' + a'm + mm' \in M$ . Questo dimostra che  $A + M$  è un sottoanello dell'anello con identità  $R$ .

(b) Si osservi intanto che  $M$  è un ideale di  $A + M$ , perché è un ideale di  $R$  contenuto in  $A + M$ . Inoltre l'ideale  $M$  di  $A + M$  è proprio, perché se per assurdo fosse  $A + M = M$ , allora  $A \subseteq M$ , da cui  $1 \in M$ . Ma allora  $M = R$  (esercizio 27.6), e questa è una contraddizione perché l'ideale massimale  $M$  di  $R$  deve essere proprio. Infine dato che  $M$  è un ideale massimale di  $R$ ,  $M$  è a maggior ragione un ideale primo di  $R$ . Quindi se  $x, y \in A + M$  e  $xy \in M$ , allora  $x, y \in R$  e  $xy \in M$ , e da questo segue che  $0$  o  $y$  devono appartenere ad  $M$ . Pertanto  $M$  è un ideale primo di  $A + M$ .  $\square$

**29.3.** Sono le applicazioni  $f: X \rightarrow R$  tali che  $f(X) \subseteq \{0, 1\}$ .  $\square$

**29.6.** (a) No, ad esempio se  $R$  è l'anello  $\mathbb{Z}$  degli interi,  $E_{\mathbb{Z}} = \{0, 1\}$  è un sottoinsieme di  $\mathbb{Z}$  che non è chiuso per l'addizione.

(b) Si deve dimostrare che per ogni  $a, b \in E_R$ , l'elemento  $a \oplus b = a + b - ab$  di  $R$  appartiene a  $E_R$ , cioè che se  $a$  e  $b$  sono idempotenti anche  $a + b - ab$  è idempotente. Un semplice calcolo mostra che  $(a + b - ab)^2 = a^2 + b^2 + a^2b^2 + 2ab - 2a^2b - 2ab^2 = a + b + ab + 2ab - 2ab - 2ab = a + b - ab$ .

(c) Se  $a, b \in E_R$ , allora  $(ab)^2 = a^2b^2 = ab$ , e quindi  $ab \in E_R$ . Inoltre  $1_R \in E_R$ , perché  $1_R$  è idempotente.

(d) Si è già dimostrato in (b) che  $E_R$  è chiuso per l'addizione  $\oplus$ . Mostriamo che  $(E_R, \oplus)$  è un gruppo abeliano. Per ogni  $a, b, c \in E_R$  si ha  $a \oplus (b \oplus c) = a \oplus (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - bc - ab - ac + abc$

e  $(a \oplus b) \oplus c = (a + b - ab) \oplus c = a + b - ab + c - (a + b - ab)c = a + b - ab + c - ac - bc + abc$ . Quindi  $\oplus$  è associativa. L'operazione  $\oplus$  è anche commutativa in quanto  $a \oplus b = a + b - ab = b + a - ba = b \oplus a$ . Per quanto riguarda lo zero si ha che  $0_R \in E_R$  e  $0_R \oplus a = 0_R + a - 0_R a = a$ . Inoltre in  $E_R$  ogni elemento è l'opposto di sé stesso, in quanto per ogni  $a \in E_R$  si ha  $a \oplus a = a + a - a^2 = a$ . Quindi  $(E_R, \oplus)$  è un gruppo abeliano.

Abbiamo già dimostrato in (c) che  $E_R$  è un sottomonoido di  $(R, \cdot)$ . Quindi  $(E_R, \cdot)$  è un monoido commutativo con identità  $1_R \neq 0_R$ .

Per quanto riguarda la distributività si ha, per ogni  $a, b, c \in R$ ,  $a(b \oplus c) = a(b + c - bc) = ab + ac - abc = ab + ac - (ab)(ac) = ab \oplus ac$ . Infine ogni elemento di  $E_R$  è idempotente come elemento dell'anello  $R$ , e quindi è idempotente anche come elemento dell'anello  $E_R$ .  $\square$

**29.7.** (a) " $\subseteq$ " Sia  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  un elemento di  $I$ , dove  $n \in \mathbb{N}$ ,  $a_i \in \mathbb{Z}_2$  per ogni  $i = 0, 1, \dots, n$  e  $a_0 = a_1 = 0$ . Allora

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n = a_2x^2 + a_3x^3 + \dots + a_nx^n = x^2(a_2 + a_3x + \dots + a_nx^{n-2}) = x^2f$$

dove  $f = a_2 + a_3x + \dots + a_nx^{n-2} \in \mathbb{Z}_2[x]$ .

" $\supseteq$ " Sia  $f \in \mathbb{Z}_2[x]$ . Allora  $f = b_0 + b_1x + \dots + b_nx^n$  per qualche  $n \in \mathbb{N}$  e qualche  $b_0, b_1, \dots, b_n \in \mathbb{Z}_2$ . Pertanto  $x^2f = b_0x^2 + b_1x^3 + \dots + b_nx^{n+2} = 0 + 0$ .

(b) Se  $g, g' \in I$ , allora  $g = x^2f$ ,  $g' = x^2f'$  per certi  $f, f' \in \mathbb{Z}_2[x]$ , e quindi  $g - g' = x^2f - x^2f' = x^2(f - f') \in I$ . Se  $g \in I$  e  $h \in \mathbb{Z}_2[x]$ , allora  $g = x^2f$  per qualche  $f \in \mathbb{Z}_2[x]$ , e pertanto  $gh = (x^2f)h = x^2(fh) \in I$ . Infine  $0 = x^2 \cdot 0 \in I$ .

(c) L'identità dell'anello  $\mathbb{Z}_2[x]/I$  è  $\bar{1} + I$ . Dato che  $(\bar{1} + I) + (\bar{1} + I) = \bar{2} + I = \bar{0} + I = 0_{\mathbb{Z}_2[x]/I}$ , ne segue che la caratteristica dell'anello  $\mathbb{Z}_2[x]/I$  è 2.

(d) Consideriamo l'elemento  $x + I$  dell'anello  $\mathbb{Z}_2[x]/I$ . È non nullo perché  $x \notin I$  (lo zero di  $\mathbb{Z}_2[x]/I$  è  $0 + I = I$ , e si ha  $f + I = I$  se e solo se  $f \in I$ ). Invece  $(x + I)^2 = x^2 + I = I$  (perché  $x^2 \in I$ ). Quindi l'elemento  $x + I$  di  $\mathbb{Z}_2[x]/I$  non è idempotente. In particolare l'anello  $\mathbb{Z}_2[x]/I$  non è booleano.  $\square$

**29.10.** (a) Il massimo è 330 (perché  $a \mid 330$  per ogni  $a \in L$ ) e il minimo è 1 (perché  $1 \mid a$  per ogni  $a \in L$ ).

(b) I maggioranti di  $\{6, 10\}$  in  $L$ , cioè gli elementi di  $L$  divisibili per 6 e per 10 sono 30 e 330. Il minimo di  $\{30, 330\}$  è 30 (perché  $30 \mid 330$ ). Quindi  $6 \vee 10 = 30$ . Il complemento di 6 in  $L$  è 55 (perché  $6 \vee 55 = 330$  e  $6 \wedge 55 = 1$ ).

(c) 16.

(d) Due reticoli booleani finiti sono isomorfi se e solo se sono equipotenti.

(e)  $6 \oplus 10 = (6 \wedge 10') \vee (6' \wedge 10) = (6 \wedge 33) \vee (55 \wedge 10) = 3 \vee 5 = 15$ ;

$6 \otimes 10 = 6 \wedge 10 = 2$ .  $\square$

**29.11.** Ogni anello booleano  $S$  con un numero finito di elementi è isomorfo a  $(\mathcal{P}(X), \Delta, \cap)$  per un opportuno insieme finito  $X$ . Affinché  $\mathcal{P}(X)$  abbia otto elementi,  $X$  deve avere 3 elementi (perché  $8 = 2^3$ ). Quindi  $(\mathcal{P}(X), \Delta, \cap)$ , ove  $X$  è un qualunque insieme con tre elementi, è un anello booleano  $S$  avente otto elementi.  $\square$

**29.12.** Dato che  $R = \{0_R, 1_R, a, b\}$  ha quattro elementi,  $R$  è isomorfo all'anello  $(\mathcal{P}(X), \Delta, \cap)$ , dove  $X$  è un insieme tale che  $|R| = |\mathcal{P}(X)|$ , cioè un insieme di cardinalità 2. Poniamo  $X = \{x, y\}$ . Allora se  $\varphi: R \rightarrow \mathcal{P}(X)$  è un isomorfismo d'anelli, si dovrà avere che  $\varphi(0_R) = 0_{\mathcal{P}(X)} = \emptyset$  e che  $\varphi(1_R) = 1_{\mathcal{P}(X)} = X$ . Quindi  $\varphi(\{a, b\}) = \{\{x\}, \{y\}\}$  (in altre parole i due elementi  $a$  e  $b$  di  $R$  diversi da 0 e 1 devono avere come immagini i due elementi  $\{x\}$  e  $\{y\}$  di  $\mathcal{P}(X)$  diversi da  $\emptyset$  e  $X$ ). Ma allora  $\varphi(a + b) = \varphi(a) \Delta \varphi(b) = \{x\} \Delta \{y\} = (\{x\} \setminus \{y\}) \cup (\{y\} \setminus \{x\}) = \{x, y\} = X = 1_{\mathcal{P}(X)} = \varphi(1_R)$ . Dato che  $\varphi$  è iniettiva si avrà pertanto  $a + b = 1_R$ .  $\square$

**29.18.** Si è visto nell'esercizio 29.1 che un anello booleano con più di due elementi non è un dominio d'integrità. Quindi se  $R$  è un anello booleano che è un dominio d'integrità, si deve avere  $|R| \leq 2$ . Ma abbiamo visto nel lemma 29.1 che  $R$  ha caratteristica 2, e ogni anello di caratteristica 2 ha un sottoanello  $P$  (il suo sottoanello fondamentale) isomorfo a  $\mathbb{Z}_2$ . Quindi  $P$  ha due elementi. Da  $2 = |P| \leq |R| \leq 2$  si deduce che  $|P| = |R| = 2$  e che  $R = P \cong \mathbb{Z}_2$ .  $\square$

**29.19.** (a) Non lo è.

(b) Non lo è.

(c) Lo è.

(d) Non lo è.  $\square$

**30.2.** (a) Per ogni  $a, b \in L$ ,  $a \vee b$  è il mcm di  $a$  e  $b$ ,  $a \wedge b$  è il MCD di  $a$  e  $b$ , e  $a' = \frac{330}{a}$ .

(b) Non lo è.

(c) Lo è.

(d) Lo è.  $\square$

**30.4.** (a) Per ogni  $f, g \in L$  si ha  $(f \vee g)(x) = \max\{f(x), g(x)\}$ ,  $(f \wedge g)(x) = \min\{f(x), g(x)\}$ ,  $f'(x) = 1 - f(x)$  per ogni  $x \in R$ .

(c) L'isomorfismo è  $\varphi: L \rightarrow \mathcal{P}(R)$  definito da  $\varphi(f) = f^{-1}(1)$  per ogni  $f \in L$ .  $\square$

**30.6.** Un isomorfismo è  $\varphi: \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$  definito da  $\varphi(I) = \{y_i \mid i \in I\}$  per ogni  $I \in \mathcal{P}(X)$ .  $\square$



**30.11.** Le algebre di Boole finite  $\mathcal{B}(x_1, x_2, x_3)$  e  $\mathcal{P}(A)$  sono isomorfe se e solo se sono equipotenti. Dato che  $\mathcal{B}(x_1, x_2, x_3)$  ha  $2^3 = 2^8$  elementi (corollario 30.9) e  $\mathcal{P}(A)$  ha  $2^{|A|}$  elementi, ne segue che  $\mathcal{B}(x_1, x_2, x_3)$  e  $\mathcal{P}(A)$  sono isomorfe se e solo se  $A$  è un qualunque insieme di cardinalità 8.  $\square$

### Soluzione di alcuni esercizi dell'Appendice A

**2.24.** (a) Si osservi che  $\varphi(n) = 2n$  è pari se  $n$  è pari, e  $\varphi(n) = 3n$  è dispari se  $n$  è dispari. Quindi se  $\varphi(n) = \varphi(m)$ , ne segue che  $n$  ed  $m$  sono entrambi pari o entrambi dispari.

Mostriamo che  $\varphi$  è iniettiva. Se  $n, m \in \mathbb{N}$  e  $\varphi(n) = \varphi(m)$  allora, come abbiamo appena osservato,  $n$  ed  $m$  sono entrambi pari o entrambi dispari. Se  $n$  ed  $m$  sono entrambi pari, allora da  $\varphi(n) = \varphi(m)$  segue che  $2n = 2m$ , e quindi  $n = m$ . Se invece  $n$  ed  $m$  sono entrambi dispari, allora da  $\varphi(n) = \varphi(m)$  segue che  $3n = 3m$ , e quindi  $n = m$ . Questo dimostra che in tutti i casi si ha  $n = m$ , e quindi  $\varphi$  è iniettiva.

(b) L'applicazione  $\varphi$  non è suriettiva. Infatti non esiste, ad esempio, nessun  $n \in \mathbb{N}$  tale che  $\varphi(n) = 1$ . Infatti se per assurdo esistesse un tale  $n$ , allora si avrebbe o che  $n$  è pari e  $2n = 1$ , e questo è assurdo, oppure che  $n$  è dispari e  $3n = 1$ , e anche questo è assurdo. Quindi in entrambi i casi si giunge a un assurdo.  $\square$

**2.25.** È suriettiva, ma non iniettiva.  $\square$

**2.26.** (a) Si osservi che se  $z \in \mathbb{Z}$  e  $z \leq 4$  allora  $z^3 - 64 \leq 0 \leq z^2$ , mentre se  $z \geq 5$  allora  $z^3 - 64 \geq z^2$ . Quindi l'applicazione  $\varphi$  è definita da

$$\varphi(z) = \begin{cases} z^3 - 64 & \text{se } z \leq 4, \\ z^2 & \text{se } z \geq 5. \end{cases}$$

In particolare  $\varphi$  è strettamente crescente, cioè se  $z, z' \in \mathbb{Z}$  e  $z < z'$ , allora  $\varphi(z) < \varphi(z')$ . Quindi  $\varphi$  è iniettiva.

(b) No, ad esempio non esistono  $z \in \mathbb{Z}$  tali che  $\varphi(z) = 2$ . Infatti se un tale  $z$  esistesse, si avrebbe che  $\min\{z^3 - 64, z^2\} = 2$ , e quindi o  $z^3 - 64 = 2$  oppure  $z^2 = 2$ . Nel primo caso si avrebbe che 66 è il cubo di un intero, nel secondo si avrebbe che 2 è il quadrato di un intero. Quindi si giunge in entrambi i casi a un assurdo.  $\square$

**2.28.** (a) Supponiamo che  $f$  sia iniettiva, e fissiamo un sottoinsieme  $X$  di  $A$ . Sia  $y = f(A \setminus X)$ . Allora  $y \in f(A) \subseteq B$ . Se si avesse che  $y \in f(X)$ , allora esisterebbero  $a \in A \setminus X$  e  $x \in X$  tali che  $y = f(a)$  e  $y = f(x)$ . Essendo  $f$  iniettiva si deve avere pertanto che  $a = x$ , e questo non è possibile perché  $a \notin X$  mentre  $x \in X$ . Quindi si ha  $y \in B$  e  $y \notin f(X)$ , ossia  $y \in B \setminus f(X)$ .

Viceversa supponiamo che  $f(A \setminus X) \subseteq B \setminus f(X)$  per ogni  $X \subseteq A$  e mostriamo che  $f$  è iniettiva. Siano  $a, a' \in A$  tali che  $f(a) = f(a')$ . Dato che  $f(A \setminus \{a\}) \subseteq B \setminus f(\{a\}) = B \setminus \{f(a)\}$  e che  $f(a') = f(a) \notin B \setminus \{f(a)\}$ , si deve avere che  $f(a') \notin f(A \setminus \{a\})$ . Ma allora a maggior ragione  $a' \notin A \setminus \{a\}$ . Quindi  $a' \in \{a\}$  e  $a = a'$ .

(b) Supponiamo che  $f$  sia suriettiva. Sia  $X$  un sottoinsieme di  $A$  e mostriamo che  $B \setminus f(X) \subseteq f(A \setminus X)$ . Se per assurdo esistesse un elemento  $b \in B \setminus f(X)$  tale che  $b \notin f(A \setminus X)$ , allora  $b \in B$ ,  $b \notin f(X)$  e  $b \notin f(A \setminus X)$ . Quindi  $b \notin f(X) \cup f(A \setminus X) = f(X \cup (A \setminus X)) = f(A) = B$ , e questa è una contraddizione.

Viceversa supponiamo che  $f(A \setminus X) \supseteq B \setminus f(X)$  per ogni  $X \subseteq A$ . Per  $X = A$  si ha  $f(A \setminus A) \supseteq B \setminus f(A)$ , cioè  $f(\emptyset) \supseteq B \setminus f(A)$ . Ma  $f(\emptyset) = \emptyset$ , e quindi si deve avere  $B \setminus f(A) = \emptyset$ . Dato che  $f(A) \subseteq B$  ne segue che  $f(A) = B$ , e quindi  $f$  è suriettiva.  $\square$

**3.23.** (a) Siano  $h, h' \in B^C$  tali che  $\varphi(h) = \varphi(h')$ . Allora  $h \circ f = h' \circ f$ . Si deve mostrare che  $h = h'$ , cioè che per ogni  $c \in C$  si ha  $h(c) = h'(c)$ . Dato  $c \in C$ , esiste  $a \in A$  tale che  $f(a) = c$  perché  $f$  è suriettiva. Ma allora  $h(c) = h(f(a)) = (h \circ f)(a) = (h' \circ f)(a) = h'(f(a)) = h'(c)$ , come desiderato.

(b) " $\subseteq$ " Sia  $g \in \varphi(B^C)$ . Allora  $g \in B^A$  ed esiste  $h \in B^C$  tale che  $\varphi(h) = g$ . Se  $a, a' \in A$  e  $f(a) = f(a')$ , allora  $g(a) = (\varphi(h))(a) = (h \circ f)(a) = h(f(a)) = h(f(a')) = (h \circ f)(a') = (\varphi(h))(a') = g(a')$ .

" $\supseteq$ " Sia  $g \in B^A$  un'applicazione con la proprietà che per ogni  $a, a' \in A$ , se  $f(a) = f(a')$  allora  $g(a) = g(a')$ . Definiamo un'applicazione  $h: C \rightarrow B$  nel modo seguente: per ogni  $c \in C$  esiste  $a \in A$  tale che  $f(a) = c$ , perché  $f$  è suriettiva; si ponga  $h(c) = g(a)$ . Mostriamo che in questo modo si è data una buona definizione di un'applicazione  $h: C \rightarrow B$ , cioè che per ogni  $c \in C$  l'elemento  $g(a)$  di  $B$  non dipende dalla scelta di  $a$ . Se infatti  $a' \in A$  è un altro elemento tale che  $f(a') = c$ , dipende dalla scelta di  $a$ . Se infatti  $a' \in A$  è un altro elemento tale che  $f(a') = c$ , allora  $f(a) = f(a')$ , e quindi, per la proprietà che si è richiesta a  $g$ ,  $g(a) = g(a')$ . Quindi l'applicazione  $h: C \rightarrow B$  è ben definita. Mostriamo che  $h \circ f = g$ . Se  $a \in A$ , allora, per come è definita  $h$ , si ha  $h(f(a)) = g(a)$ . Quindi  $(h \circ f)(a) = g(a)$  per ogni  $a \in A$ , ossia  $h \circ f = g$ . Ma allora  $g = h \circ f = \varphi(h) \in \varphi(B^C)$ .  $\square$

**7.16.** Sia  $b \in B$ . Allora  $\pi(b) \in \pi(B)$ , e quindi  $b \in \{x \in A \mid \pi(x) \in \pi(B)\} = \pi^{-1}(\pi(B))$ . Questo dimostra che  $B \subseteq \pi^{-1}(\pi(B))$ .

Viceversa sia  $a \in \pi^{-1}(\pi(B))$ . Allora  $\pi(a) \in \pi(B)$ , vale a dire  $\pi(a) = \pi(b)$  per qualche  $b \in B$ . Ma allora  $[a]_{\sim} = [b]_{\sim}$ , e quindi  $a \in [a]_{\sim} = [b]_{\sim} \subseteq B$ . Quindi  $\pi^{-1}(\pi(B)) \subseteq B$ .  $\square$

**7.17.** (a) *Riflessività.* Sia  $f \in \mathbb{N}^A$ . Allora  $\{a \in A \mid f(a) \neq f(a)\}$  è vuoto, e quindi finito. Pertanto  $f \sim f$ .

*Simmetria.* Siano  $f, g \in \mathbb{N}^A$  tali che  $f \sim g$ . Allora  $\{a \in A \mid g(a) \neq f(a)\} = \{a \in A \mid f(a) \neq g(a)\}$ , e quindi è un insieme finito. Pertanto  $g \sim f$ .

**Transitività.** Siano  $f, g, h \in N^A$  tali che  $f \sim g$  e  $g \sim h$ . Allora  $\{a \in A \mid f(a) \neq g(a)\}$  e  $\{a \in A \mid g(a) \neq h(a)\}$  sono insiemi finiti. Mostriamo che  $\{a \in A \mid f(a) \neq h(a)\} \subseteq \{a \in A \mid f(a) \neq g(a)\} \cup \{a \in A \mid g(a) \neq h(a)\}$ , dal che seguirà che  $\{a \in A \mid f(a) \neq h(a)\}$  è un insieme finito.

Supponiamo per assurdo che esista un elemento  $b \in A$  tale che  $f(b) \neq h(b)$  ma  $b \notin \{a \in A \mid f(a) \neq g(a)\} \cup \{a \in A \mid g(a) \neq h(a)\}$ . Allora  $f(b) = g(b)$  e  $g(b) = h(b)$ , da cui  $f(b) = h(b)$  e  $f(b) \neq h(b)$ , assurdo. Quindi  $\{a \in A \mid f(a) \neq h(a)\}$  è un insieme finito, cioè  $f \sim h$ .

(b) Sia  $\sim$  la relazione banale su  $N^A$ . Allora per ogni  $f, g \in N^A$ ,  $\{a \in A \mid f(a) \neq g(a)\}$  è un insieme finito. Siano in particolare  $f, g: A \rightarrow N$  le applicazioni definite da  $f(a) = 0$  per ogni  $a \in A$  e  $g(a) = 1$  per ogni  $a \in A$ . Allora  $\{a \in A \mid f(a) \neq g(a)\} = A$  è un insieme finito.

Viceversa supponiamo che  $A$  sia un insieme finito. Allora per ogni  $f, g \in N^A$  si ha che  $\{a \in A \mid f(a) \neq g(a)\} \subseteq A$  è un insieme finito. Ma allora  $f \sim g$  per ogni  $f, g \in N^A$ , cioè  $\sim$  è la relazione banale su  $N^A$ .

(c) Siano  $n, m \in N$  tali che  $\varphi(n) = \varphi(m)$ . Dobbiamo dimostrare che  $n = m$ . Se  $\varphi(n) = \varphi(m)$ , allora  $[f_n]_{\sim} = [f_m]_{\sim}$ , da cui  $f_n \sim f_m$ , e quindi  $\{a \in A \mid f_n(a) \neq f_m(a)\}$  è un insieme finito. Ma  $\{a \in A \mid f_n(a) \neq f_m(a)\} = A$  se  $n \neq m$  (perché  $f_n(a) = n$  e  $f_m(a) = m$  per ogni  $a \in A$ ), e  $\{a \in A \mid f_n(a) \neq f_m(a)\}$  è un insieme finito se  $n = m$  (perché in questo caso  $f_n(a) = n = m = f_m(a)$  per ogni  $a \in A$ ). Dato che  $A$  è un insieme infinito e  $\{a \in A \mid f_n(a) \neq f_m(a)\}$  è un insieme finito, si dovrà avere  $\{a \in A \mid f_n(a) \neq f_m(a)\} = \emptyset$ , cioè che  $n = m$ .  $\square$

**7.18. (a) Transitività.** Siano  $f, g, h \in B^N$  tali che  $f \sim g$  e  $g \sim h$ . Allora esistono  $n, m \in N$  tali che  $f(i) = g(i)$  per ogni  $i \geq n$  e  $g(i) = h(i)$  per ogni  $i \geq m$ . Sia  $p$  il maggiore tra  $n$  ed  $m$ . Allora  $f(i) = g(i)$  e  $g(i) = h(i)$  per ogni  $i \geq p$ , e quindi  $f(i) = h(i)$  per ogni  $i \geq p$ . Pertanto  $f \sim h$ .

(b) Supponiamo che  $\sim$  sia la relazione banale su  $B^N$ . Mostriamo che l'insieme non vuoto  $B$  ha esattamente un elemento. Se per assurdo  $B$  avesse più di un elemento, esisterebbero in  $B$  due elementi distinti  $a$  e  $b$ . Siano  $f_a, f_b: N \rightarrow B$  le applicazioni definite da  $f_a(n) = a$  per ogni  $n \in N$  e  $f_b(n) = b$  per ogni  $n \in N$ . Dato che  $\sim$  è la relazione banale su  $B^N$ , si deve avere  $f_a \sim f_b$ . Quindi esiste  $n \in N$  tale che  $f_a(i) = f_b(i)$  per ogni  $i \geq n$ . In particolare  $f_a(n) = f_b(n)$ , cioè  $a = b$ . Questo contraddice il fatto che gli elementi  $a$  e  $b$  erano distinti.

Viceversa supponiamo che  $|B| = 1$ . Allora c'è un'unica applicazione  $f: N \rightarrow B$ , cioè  $|B^N| = 1$ . Dato che sull'insieme  $B^N$  di cardinalità 1 c'è un'unica equivalenza, ne segue che le due equivalenze, la  $\sim$  e la relazione banale, devono coincidere.

(c) Siano  $a, b \in B$  tali che  $\varphi(a) = \varphi(b)$ . Allora  $[f_a]_{\sim} = [f_b]_{\sim}$ , e quindi  $f_a \sim f_b$ . Ne segue che esiste  $n \in N$  tale che  $f_a(i) = f_b(i)$  per ogni  $i \geq n$ . In particolare

$f_a(n) = f_b(n)$ , cioè  $a = b$ . Questo dimostra che l'applicazione  $\varphi$  è iniettiva.  $\square$

**7.19.** Per dimostrare che  $f$  e  $g$  sono due biezioni, una inversa dell'altra, è sufficiente dimostrare che  $g \circ f = \text{id}$  e  $f \circ g = \text{id}$ .

Dimostriamo che  $g \circ f = \text{id}$ . Si osservi intanto che le due applicazioni  $g \circ f$  e  $\text{id}$  hanno entrambe dominio e codominio uguali a  $E$ . Quindi per dimostrare che le due applicazioni coincidono si deve dimostrare che  $g \circ f(\sim) = \text{id}(\sim)$  per ogni  $\sim \in \mathcal{E}$ . Ora

$$g \circ f(\sim) = g(f(\sim)) = g(A/\sim) = A/\sim$$

e  $\text{id}(\sim) = \sim$ . Pertanto dobbiamo dimostrare che  $A/\sim = \sim$ , cioè che le due equivalenze  $A/\sim$  e  $\sim$  su  $A$  coincidono. A questo scopo si deve verificare che per ogni  $a, b \in A$  si ha  $a \sim A/\sim b$  se e solo se  $a \sim b$ . Per come è definita  $A/\sim$  si ha che  $a \sim A/\sim b$  se e solo se esiste  $X \in A/\sim$  tale che  $a \in X$  e  $b \in X$ . Ma  $A/\sim = \{[c]_{\sim} \mid c \in A\}$ , e quindi  $a \sim A/\sim b$  se e solo se esiste  $c \in A$  tale che  $a \in [c]_{\sim}$  e  $b \in [c]_{\sim}$ . Ora se esiste un  $c \in A$  tale che  $a \in [c]_{\sim}$  e  $b \in [c]_{\sim}$ , allora  $a \sim c$  e  $b \sim c$ , da cui  $c \sim b$  (per la simmetria), e quindi  $a \sim b$  (per la transitività). Se invece  $a \not\sim b$ , allora  $c = b$  è un elemento di  $A$  tale che  $a \in [b]_{\sim}$  e  $b \in [b]_{\sim}$ . Abbiamo così dimostrato che per ogni  $a, b \in A$  si ha  $a \sim A/\sim b$  se e solo se  $a \sim b$ , e quindi le due equivalenze  $A/\sim$  e  $\sim$  sono uguali.

Dimostriamo ora che  $f \circ g = \text{id}$ . Osserviamo intanto che le due applicazioni  $f \circ g$  e  $\text{id}$  hanno entrambe dominio e codominio uguali a  $P$ . Quindi per dimostrare che le due applicazioni sono uguali si deve far vedere che  $f \circ g(\mathcal{F}) = \text{id}(\mathcal{F})$  per ogni  $\mathcal{F} \in P$ . Ora  $f \circ g(\mathcal{F}) = f(g(\mathcal{F})) = f(\sim_{\mathcal{F}}) = A/\sim_{\mathcal{F}}$  e  $\text{id}(\mathcal{F}) = \mathcal{F}$ . Quindi ci resta solo da verificare che  $A/\sim_{\mathcal{F}} = \mathcal{F}$ . Dimostriamolo mediante la doppia inclusione.

Se  $X \in A/\sim_{\mathcal{F}}$ , allora  $X = [a]_{\sim_{\mathcal{F}}}$  per qualche  $a \in A$ . Dato che  $\mathcal{F}$  è una partizione di  $A$ , esiste un unico  $Y \in \mathcal{F}$  tale che  $a \in Y$ . Mostriamo che  $X = Y$ . Se  $t \in X = [a]_{\sim_{\mathcal{F}}}$ , allora  $t \sim_{\mathcal{F}} a$ , e quindi esiste un elemento di  $\mathcal{F}$  che contiene sia  $t$  che  $a$ . Ma, come abbiamo già osservato,  $\mathcal{F}$  è una partizione di  $A$  e quindi ogni elemento di  $A$  è contenuto in un unico elemento di  $\mathcal{F}$ . Inoltre  $a$  è contenuto nell'elemento  $Y$  di  $\mathcal{F}$ . Se ne deduce che  $t \in Y$ . Quindi  $X \subseteq Y$ . Viceversa sia  $u \in Y$ . Dato che sappiamo che anche  $a \in X$ , si ricava che  $u \sim_{\mathcal{F}} a$ , e  $u \in [a]_{\sim_{\mathcal{F}}} = X$ . Questo dimostra che  $Y \subseteq X$ , e pertanto  $X = Y$ . Ma allora  $X = Y \in \mathcal{F}$ , e  $A/\sim_{\mathcal{F}} \subseteq \mathcal{F}$ .

Viceversa sia  $Y \in \mathcal{F}$ . Dato che  $\mathcal{F}$  è una partizione,  $Y$  è non vuoto, e quindi esiste  $a \in Y$ . Mostriamo che  $Y = [a]_{\sim_{\mathcal{F}}}$ . Se  $y \in Y$ , allora i due elementi  $y$  e  $a$  stanno entrambi in  $Y \in \mathcal{F}$ , e quindi  $y \sim_{\mathcal{F}} a$ , da cui  $y \in [a]_{\sim_{\mathcal{F}}}$ ; quindi  $Y \subseteq [a]_{\sim_{\mathcal{F}}}$ . Per l'altra inclusione: se  $z \in [a]_{\sim_{\mathcal{F}}}$ , allora  $z \sim_{\mathcal{F}} a$ , vale a dire  $z$  ed  $a$  appartengono allo stesso elemento di  $\mathcal{F}$ . Dato che sappiamo che  $\mathcal{F}$  è una partizione di  $A$  (e quindi che ogni elemento di  $A$  è contenuto in un unico elemento di  $\mathcal{F}$ ) e sappiamo che  $a$  è contenuto nell'elemento  $Y$  della partizione  $\mathcal{F}$ , se ne deduce che  $z \in Y$ .

Quindi  $Y = [a]_{\sim_{\mathcal{F}}}$ . Pertanto  $Y = [a]_{\sim_{\mathcal{F}}} \in \{[x]_{\sim_{\mathcal{F}}} \mid x \in A\} = A/\sim_{\mathcal{F}}$ . Abbiamo così verificato che  $A/\sim_{\mathcal{F}} = \mathcal{F}$ .  $\square$

**10.13.** (b) Si deve far vedere che se  $[a]_{\sigma} = [a']_{\sigma}$  e  $[b]_{\sigma} = [b']_{\sigma}$ , ove  $a, a', b, b' \in A$ , allora  $[a]_{\sigma} \tau [b]_{\sigma}$  se e solo se  $[a']_{\sigma} \tau [b']_{\sigma}$ . Ricordando che due elementi sono equivalenti se e solo se le loro classi di equivalenza coincidono, e tenendo presente come è definita  $\tau$ , quello che si deve dimostrare è che se  $a \sigma a'$  e  $b \sigma b'$ , ove  $a, a', b, b' \in A$ , allora  $a \rho b$  se e solo se  $a' \rho b'$ . Per come è definita la relazione  $\sigma$ , dobbiamo mostrare pertanto che da  $a \rho a', a' \rho a, b \rho b', b' \rho b$  e  $a \rho b$  segue  $a' \rho b'$ , e che da  $a \rho a', a' \rho a, b \rho b', b' \rho b$  e  $a' \rho b'$  segue  $a \rho b$ . Queste implicazioni sono ovvie perché  $\rho$  è transitiva.

(c) *Riflessività.* Per ogni  $a \in A$  si ha  $a \rho a$  perché  $\rho$  è riflessiva. Quindi per ogni  $[a]_{\sigma} \in A/\sigma$  si ha  $[a]_{\sigma} \tau [a]_{\sigma}$ .

*Simmetria.* Siano  $a, b \in A$  tali che  $[a]_{\sigma} \tau [b]_{\sigma}$  e  $[b]_{\sigma} \tau [a]_{\sigma}$ . Allora  $a \rho b$  e  $b \rho a$ , da cui  $a \sigma b$ , e pertanto  $[a]_{\sigma} = [b]_{\sigma}$ .

*Transitività.* Siano  $a, b, c \in A$  tali che  $[a]_{\sigma} \tau [b]_{\sigma}$  e  $[b]_{\sigma} \tau [c]_{\sigma}$ . Allora  $a \rho b$  e  $b \rho c$ , da cui  $a \rho c$  perché  $\rho$  è transitiva. Quindi  $[a]_{\sigma} \tau [c]_{\sigma}$ .  $\square$

**19.13.** (a) Siano  $f, g \in S$ . Allora per ogni  $x, y \in A$  si ha che  $x \sim y$  implica  $g(x) \sim g(y)$  (perché  $g \in S$ ) e questo implica  $f(g(x)) \sim f(g(y))$  (perché  $f \in S$ ), cioè  $(f \circ g)(x) \sim (f \circ g)(y)$ . Quindi  $f \circ g \in S$ . Inoltre  $1_{A^A} = 1_A \in S$  perché ovviamente  $x \sim y$  implica  $1_A(x) \sim 1_A(y)$ .

(b) Si deve dimostrare che se  $a, b \in A$  e  $[a] = [b]$ , allora  $[f(a)] = [f(b)]$ . Ora se  $a, b \in A$  e  $[a] = [b]$ , allora  $a \sim b$ , da cui  $f(a) \sim f(b)$  perché  $f \in S$ . Ne segue che  $[f(a)] = [f(b)]$ . Questo dimostra che  $\tilde{f}$  è ben definita.

(c) Si deve dimostrare che  $\varphi(f) \circ \varphi(g) = \varphi(f \circ g)$  per ogni  $f, g \in S$  e che  $\varphi(1_S) = 1_{A/\sim}$ . L'uguaglianza  $\varphi(f) \circ \varphi(g) = \varphi(f \circ g)$  equivale a  $\tilde{f} \circ \tilde{g} = \tilde{f \circ g}$ .

Si deve quindi dimostrare che  $(\tilde{f} \circ \tilde{g})([a]) = \tilde{f \circ g}([a])$  per ogni  $a \in A$ . Ma  $(\tilde{f} \circ \tilde{g})([a]) = \tilde{f}(\tilde{g}([a])) = \tilde{f}([g(a)]) = [f(g(a))] = [(f \circ g)(a)] = \tilde{f \circ g}([a])$ . Inoltre  $\varphi(1_S) = \varphi(1_A) = 1_A$  è uguale a  $1_{A/\sim}$  perché per ogni  $a \in A$  si ha  $\tilde{1}_A([a]) = [1_A(a)] = [a] = 1_{A/\sim}([a])$ .  $\square$

## Indice Analitico

Addizione, 124, 191  
 albero, 99  
 — con radice, 101  
 — di supporto, 101  
 — ordinato con radice, 102  
 alfabeto valutato, 145  
 algebra di Boole, 222  
 algebre di Boole isomorfe, 223  
 anelli isomorfi, 201  
 anello, 191  
 — booleano, 215  
 — commutativo, 192  
 — degli endomorfismi, 195  
 — degli interi di Gauss, 206  
 — dei polinomi, 200  
 — delle parti, 215  
 — di Boole, 215  
 — intero, 194  
 — quoziente, 201  
 anomalia, 34  
 antiimmagine, 11  
 applicazione, 10  
 — canonica, 48, 144, 149  
 — composta, 16  
 — identica, 12  
 — inversa, 17  
 argomento, 34  
 arietà, 105, 123  
 associatività, 3, 124  
 automorfismo, 79, 84, 132, 154, 201

Banale, 152  
 biezione, 11  
 buona definizione, 57

Cammino, 86  
 — euleriano, 91  
 — euleriano orientato, 92

— hamiltoniano, 91  
 — hamiltoniano orientato, 92  
 — nullo, 86  
 — orientato, 87  
 campo, 195  
 campo d'azione di un quantificatore, 119  
 coppia, 46, 86  
 caratteristica, 209  
 cardinalità, 59  
 catena, 94  
 cicli disgiunti, 167  
 ciclo, 166  
 circuito, 86  
 — euleriano, 91  
 — euleriano orientato, 92  
 — orientato, 87  
 classe, 1  
 — di equivalenza, 48  
 — di una permutazione, 170  
 — laterale, 173  
 codominio, 11  
 coefficiente binomiale, 62  
 — direttivo, 203  
 coefficienti di un polinomio, 199, 203  
 colonna, 37  
 complemento, 79  
 complesso coniugato, 33, 36  
 componente connessa, 87  
 composizione di relazioni, 157  
 concatenazione, 143  
 congiunzione, 111  
 congruenza, 54  
 connettivo logico, 112  
 contraddizione, 114  
 controimmagine, 11  
 coppie ordinate, 9  
 corpo, 195  
 corrispondenza, 10

— biunivoca, 9, 11  
costante, 145

Diagonale, 90  
— principale, 39  
diametro, 93  
differenza, 3  
— simmetrica, 3  
digrafo, 85  
dimostrazione per assurdo, 115  
— diretta, 115  
— indiretta, 115  
— per contrapposizione, 115  
disgiunzione, 111  
distanza, 93  
divisore, 23  
— dello zero, 194  
dominio, 11, 194  
— di integrità, 194  
— di una funzione proposizionale, 117  
doppia implicazione, 111  
— inclusione, 3

Elemento di un insieme, 1  
— idempotente, 156, 215  
— invertibile, 150, 195  
— massimale, 69  
— minimale, 69  
— neutro, 129  
endomorfismo, 132, 154, 201  
enunciato duale, 77  
equivalenza, 47  
— associata a una applicazione, 48  
estremo inferiore, 70  
— superiore, 70

Faccia, 106  
falso, 111  
famiglia, 1, 5  
fattoriale, 28  
filtro, 229  
foglia, 101  
foresta, 99  
forma normale disgiuntiva, 225  
— proposizionale, 113  
— trigonometrica, 34  
formula, 118  
— chiusa, 120  
Formula di Eulero, 106  
funzione, 10  
— caratteristica, 65  
— proposizionale, 117

Generatore, 131  
giustapposizione, 143  
grado, 85, 203  
— complessivo, 88  
— di entrata, 87  
— di uscita, 88  
grafi isomorfi, 84  
grafo, 84  
— bipartito, 93  
— bipartito completo, 93  
— completo, 87, 92  
— connesso, 86  
— diretto, 85  
— doppiamente connesso, 98  
— finito, 85, 91  
— nullo, 106  
— orientato, 45, 85  
— orientato di una funzione, 108  
— piano, 106  
— regolare, 85  
— sconnesso, 86  
gruppi isomorfi, 154  
gruppo, 151  
— abeliano, 151  
— banale, 155  
— ciclico, 183  
— commutativo, 151  
— degli elementi invertibili, 195  
— delle permutazioni, 165  
— delle radici  $n$ -esime dell'unità, 153  
— identico, 155  
— quoziente, 175  
— simmetrico, 165

Ideale, 199, 228  
— improprio, 200  
— massimale, 210  
— nullo, 200  
— primo, 210  
identità, 129, 192  
immagine, 11  
— inversa, 11  
immersione, 16  
implicazione, 111  
— materiale, 111  
inclusione, 16  
indeterminata, 199  
indice, 4, 5, 174  
iniettiva, 11  
insieme, 1  
— bene ordinato, 71  
— della parti, 3  
— finito, 59

— infinito, 59  
— numerabile, 59  
— parzialmente ordinato, 67  
— quoziente, 48  
— totalmente ordinato, 68  
— vuoto, 1  
insiemi disgiunti, 3  
— equipotenti, 59  
intersezione, 3  
inversa di una matrice, 44  
inverso, 150  
isomorfismo, 68, 78, 84, 88, 132, 154, 201, 218, 223, 248

Lati incidenti, 84  
lato, 84-86  
— orientato, 46, 85  
legge di composizione, 123  
livello, 101  
lunghezza, 166  
— di un cammino, 86  
— di una catena, 94  
— di una parola, 143

Maggiorante, 70  
massimo, 69  
— comun divisore, 23  
matrice, 37  
—  $(0, 1)$ , 157  
— di adiacenza, 94  
— di una corrispondenza, 42  
— quadrata, 39  
— simmetrica, 42  
— trasposta, 41  
minimo, 69  
— comune multiplo, 24  
minorante, 70  
modulo, 23, 26, 34  
molteplicità, 88  
moltiplicazione, 124, 191  
monoide, 129  
— ciclico, 131  
— delle parole, 144  
— libero, 144  
— quoziente, 137  
monoidi isomorfi, 132  
multigrafo, 85, 86  
— orientato, 85  
— semplice, 86  
multiplo, 23, 125

Negazione, 111  
notazione a infisso, 105

— additiva, 124  
— moltiplicativa, 124  
— polacca, 105  
nucleo, 180, 202  
numeri complessi, 31  
— di Bell, 242  
— interi, 1  
— naturali, 1  
— primi, 23  
— primi tra loro, 24  
— razionali, 1  
— reali, 1  
—  $n$ -uple, 10

Occorrenza libera, 119  
— di una variabile, 119  
— vincolata, 119  
omomorfismo d'anelli, 201  
— di algebre di Boole, 223  
— di gruppi, 153  
— di insiemi ordinati, 68  
— di monoidi, 132  
— di reticoli, 78, 218  
— di semigrupp, 132  
opposto, 150  
operazione, 105, 123, 146  
—  $n$ -aria, 123  
— binaria, 123, 146  
— unaria, 146  
ordinamento indotto, 69  
— parziale, 66  
— totale, 68  
— usuale, 67  
ordine, 39, 151  
— parziale, 66  
— parziale inverso, 69

Parola, 143  
— vuota, 143  
partizione, 48  
permutazione, 165  
piano di Argand-Gauss, 34  
polinomi booleani equivalenti, 224  
polinomio, 199  
— booleano, 224  
posto di un elemento in una matrice, 38  
potenza, 125, 130, 151  
prodotto, 124, 191  
— cartesiano, 9, 10  
— diretto, 134  
— righe per colonne, 38  
— scalare, 39  
proiezione canonica, 15, 48, 176, 202

proposizione, 111  
 proprietà antisimmetrica, 66  
 — distributiva, 3  
 — riflessiva, 46  
 — simmetrica, 46  
 — transitiva, 46  
 — di cancellazione, 197  
 punto di taglio, 95

Quantificatore esistenziale, 118  
 — universale, 118  
 quot, 23

Radice, 101  
 relazione, 45  
 — banale, 52  
 — di uguaglianza, 47  
 resto, 23  
 restrizione, 143  
 reticoli isomorfi, 79  
 reticolo, 75  
 — complementato, 79  
 — di Boole, 79  
 — distributivo, 78  
 — limitato, 79  
 riga, 37

Segnatura, 170  
 semigrupp isomorfi, 132  
 semigrupp, 124  
 — commutativo, 124  
 — libero, 149  
 — quoziente, 137  
 semiordinamento, 66  
 simbolo di Kronecker, 41  
 somma, 124, 191  
 sottoalgebra di Boole, 222  
 sottoanello, 193  
 — fondamentale, 209  
 sottografo, 85  
 sottogruppo, 152  
 — alterno, 181  
 — ciclico, 183  
 — identico, 152  
 — improprio, 152  
 — normale, 174  
 sottoinsieme, 2  
 — additivamente chiuso, 156  
 — chiuso per un'operazione, 125  
 — cofinito, 82  
 — ordinato, 69  
 — proprio, 2  
 sottomonoide, 131

sottoreticolo, 78  
 sottosemigrupp, 125  
 suriettiva, 11

Tautologia, 114  
 tavola di verità, 112  
 trasposizioni, 169  
 triangolo di Pascal, 63  
 — di Tartaglia, 63

Unione, 3  
 unità, 150, 195

Valore, 11  
 — assoluto, 23, 26  
 — di verità, 111  
 valutazione, 145  
 variabile, 117, 145, 224  
 — proposizionale, 113  
 vero, 111  
 vertice, 45, 84-86  
 — dispari, 85  
 — isolato, 85  
 — pari, 85  
 vertici adiacenti, 84

Zero, 129, 192

N. INV. 813/CIS  
 512 FACCA  
 Oleghe