

Alberto Facchini

ALGEBRA E MATEMATICA DISCRETA

*per studenti di informatica, ingegneria, fisica e matematica
con numerosi esempi ed esercizi svolti*

HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNAE,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Quis & totius operis de Arithmetica, quod
OPVS PÆFECTVM
in scriptis, est in ordine Decimus.



H[oc] Alio in hoc libro, studior[um] Lector Regulis Algebraicis [Itali, de la Cof
fessione] modis administrandis ac demonstracionibus ab Auctore ita
locomptata, ut pro paucis antea usq[ue] tridu[i]am lepidissima exserbitur. Ne
cepsit, ubi innumeris alteri, aut dico undevium etiam, ubi duo dicitur,
etiam undeviis finitimi modis administrantur. Namque invenimus



DECIBEL



ZANICHELLI

Decibel editrice di Giorgio Villella,
via del Santo 30, 35123 Padova,
telefono 0498 756 956, fax 0498 762 305
decibelz@tin.it

Realizzare un libro è un'operazione complessa, che richiede numerosi controlli: sul testo, sulle immagini e sulle relazioni che si stabiliscono tra essi. L'esperienza suggerisce che è praticamente impossibile pubblicare un libro privo di errori. Saremo quindi grati ai lettori che vorranno segnalarli alla Decibel agli indirizzi indicati sopra. Nel sito web

<http://space.tin.it/scienza/gvillell/decibel.html>
sarà periodicamente aggiornata l'errata corrigé di questo volume e saranno fornite eventuali aggiunte al testo e nuovi problemi.

Distribuzione esclusiva e catalogo

Zanichelli editore, via Irnerio 34, 40126 Bologna,
telefono 051 293 111, telex 521587 Zaned I,
fax 051 249 782-293 224,
<http://www.zanichelli.it>

Per legge, i diritti di traduzione, di memorizzazione elettronica, di riproduzione e di adattamento totale e parziale, con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche) sono riservati per tutti i paesi. Tuttavia l'Editore potrà concedere a pagamento l'autorizzazione a riprodurre, mediante fotocopie, una porzione non superiore ad un decimo del presente volume. Le richieste di riproduzione vanno inoltrate all'Associazione Italiana per i Diritti di Riproduzione delle Opere dell'Ingegno (AIDRO), via delle Erbe 2, 20121 Milano, telefono e fax 02 809 506; e-mail aidro@iol.it

Realizzazione editoriale: KWL giankw1@tin.it

Prima edizione settembre 2000

Ristampa: questa è la prima stampa della prima edizione

9 8 7 6 5 2005 2006 2007 2008 2009

*

Alberto Facchini

ALGEBRA E MATEMATICA DISCRETA

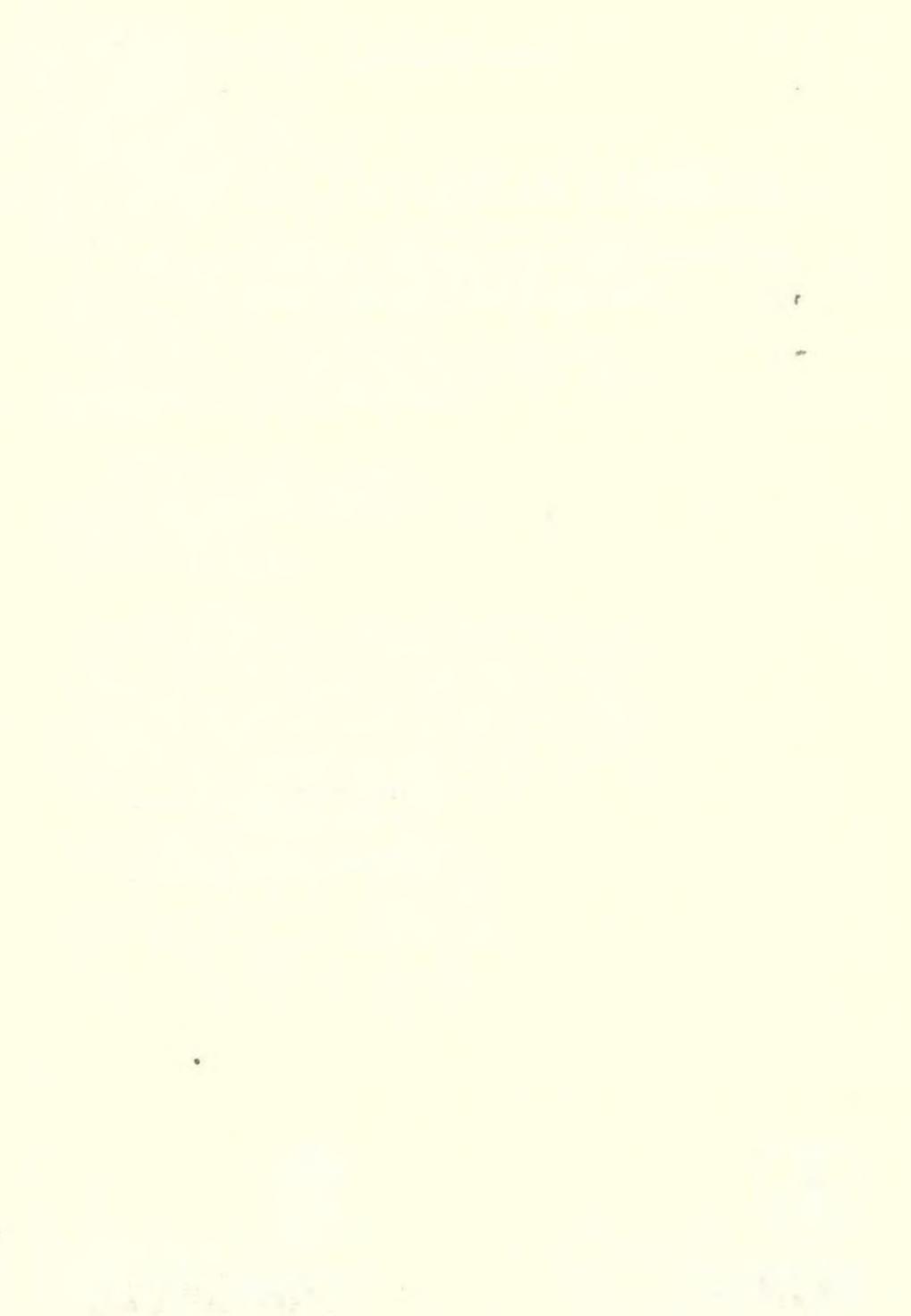
*per studenti di informatica, ingegneria, fisica e matematica
con numerosi esempi ed esercizi svolti*



DECIBEL



ZANICHELLI



INDICE

Prefazione	1
Capitolo 1. Insiemi	
§1 Insiemi	3
§2 Corrispondenze e applicazioni	11
§3 Applicazioni composte	20
§4 Numeri naturali e numeri interi	28
Appendice 4.1. Il sistema posizionale in base b	38
§5 Numeri complessi	43
§6 Matrici	51
Capitolo 2. Insiemi e relazioni	
§7 Equivalenze e partizioni	59
§8 L'insieme delle classi resto	67
§9 Cardinalità di insiemi, tecniche di enumerazione	71
Appendice 9.1. Complementi sugli insiemi numerabili	85
§10 Ordinamenti	87
§11 Reticoli, reticoli booleani	96
§12 Grafi	108
§13 Cammini e circuiti euleriani	117
§14 Alberi e grafi piani	125
Appendice 14.1. I solidi platonici	132
Appendice 14.2. Grafi e colorazioni	133
Appendice 14.3. Alberi con radici, notazione polacca	135
Capitolo 3. Insiemi dotati di un'operazione	
§15 Semigruppi	141
§16 Monoidi	147
§17 Quozienti	156

§18 Il monoide delle parole	162
Appendice 18.1. Alfabeti valutati	165
§19 Gruppi	166
§20 Equivalenze compatibili con l'addizione in \mathbb{N} e in \mathbb{Z}	174
§21 Permutazioni	181
§22 Sottogruppi normali e classi laterali	191
§23 Omomorfismi di gruppi	198
 Capitolo 4. Insiemi dotati di più operazioni	
§24 Anelli	209
§25 Ideali	216
§26 Polinomi	224
§27 L'anello delle classi resto e la caratteristica di un anello	227
§28 Domini euclidei e teorema di Ruffini	239
§29 Serie di potenze, relazioni di ricorrenza e funzioni generatrici	245
§30 Anelli booleani	265
Appendice 30.1. Dimostrazione del teorema 30.7	270
§31 Algebre di Boole	272
 Capitolo 5. Qualche nozione di logica matematica	
§32 Logica proposizionale	283
§33 Logica predicativa	291
 Capitolo 6. Algebra lineare	
§34 Spazi vettoriali	299
§35 Spazio quoziante e applicazioni lineari	307
§36 Dipendenza lineare e basi di uno spazio vettoriale	312
§37 Somma di spazi vettoriali	321
§38 Estensione per linearità	326
§39 Matrice associata a un'applicazione lineare	332
§40 Cambi di base	348
§41 Sistemi di equazioni lineari	352
§42 Determinante	359
§43 Altre proprietà del determinante	370
§44 Autovalori, autovettori	377
 Capitolo 7. Estensioni di campi	
§45 Estensioni di campi	387
§46 Campi algebricamente chiusi e campi finiti	394
 Capitolo 8. Ancora esercizi. Soluzioni	
§47 Alcuni esercizi più difficili	399
§48 Soluzione di alcuni esercizi	403
Indice analitico	449

PREFAZIONE

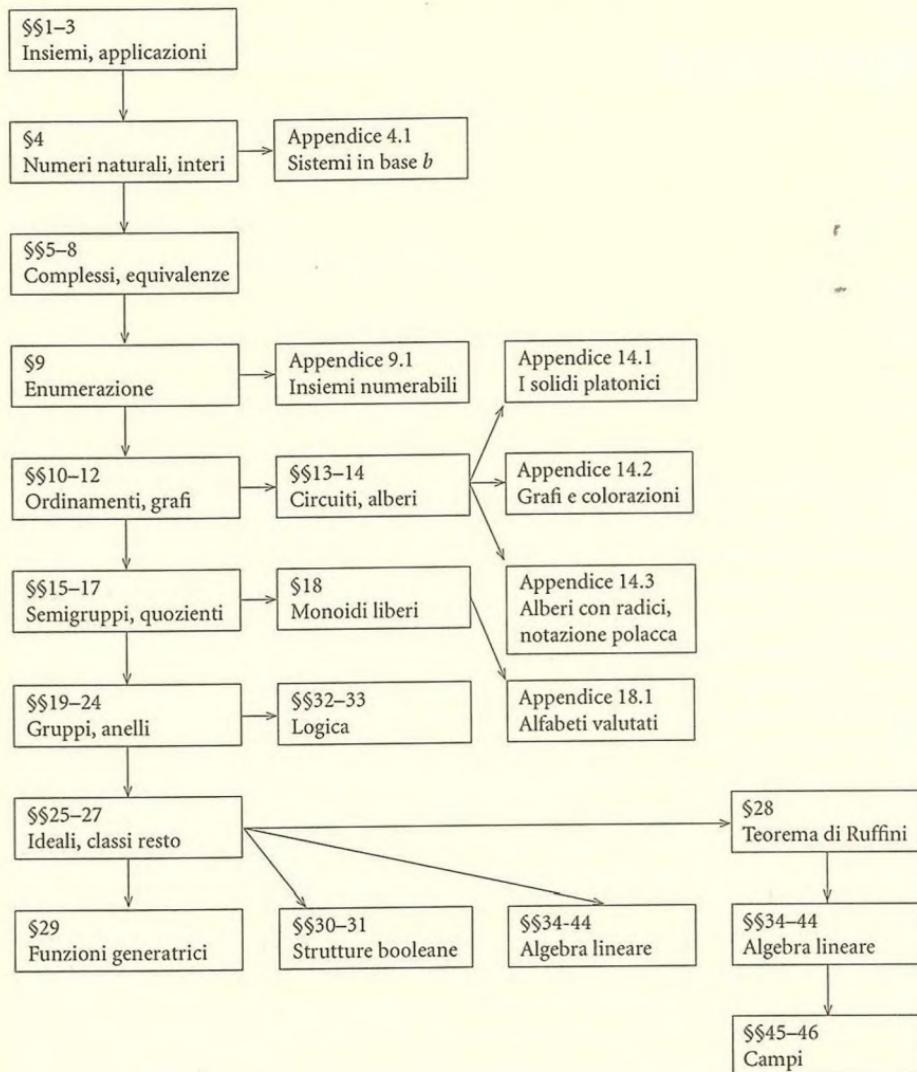
Non ci si spaventi a vedere la mole di questo libro. Due terzi delle pagine sono riservate ad esempi, a esercizi svolti e ad altri esercizi graduali. Ho preferito cioè cercare di essere chiaro invece di cercare di essere conciso.

Sono stati i notevoli cambiamenti in atto nei curricula universitari in Italia a spingermi a rivedere i contenuti dei miei due precedenti testi *Algebra × informatica* e *Sussidiario di algebra e matematica discreta*. Aumentando i contenuti di matematica discreta e combinatoria e aggiungendo una parte di algebra lineare, ho arricchito il testo rispetto ai due precedenti. Il docente potrà così scegliere tra vari percorsi didattici, alcuni suggeriti nella pagina seguente, al fine di organizzare il proprio corso nel modo più consono possibile. Si tratta quindi di un volume duttile, adatto a tutti gli studenti ai quali sia necessaria una buona preparazione di algebra, matematica discreta e/o algebra lineare, ossia pensato per gli studenti di informatica, di ingegneria, di fisica o di matematica. Lo scopo è quello di fornire parte del linguaggio algebrico di base e familiarità con alcune tra le più comuni tecniche matematiche.

Come dicevo sopra, di molti esercizi viene data una soluzione, che per alcuni segue immediatamente il testo dell'esercizio stesso, mentre per altri è riportata in fondo al libro (§48). L'idea è ovviamente quella di cercare di fare in modo che lo studente provi davvero a risolvere l'esercizio per conto proprio prima di andare a guardare la soluzione in fondo al volume. Gli esercizi del §47 sono invece un po' più difficili, rivolti agli studenti già maturi, e si dovrà cercare di risolverli verso la fine del corso, anche quelli riguardanti solo le nozioni apprese nelle prime pagine del testo.

Desidero ringraziare la dr Giovanna D'Agostino che ha scritto con me la parte di logica matematica (§§32 e 33).

Interdipendenza delle sezioni



Capitolo 1

INSIEMI

§1. Insiemi

Spesso conviene considerare alcuni o molti oggetti come un unico oggetto; si ha così la nozione di *insieme* di oggetti. Non daremo una definizione rigorosa del concetto di insieme, supporremo la nozione di insieme intuitivamente nota; diciamo semplicemente che un insieme è una collezione di oggetti (o di elementi).

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 \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*.¹

¹I numeri reali verranno studiati in modo particolare nel corso di analisi matematica. Sono numeri reali tutti i numeri razionali, $\sqrt{2}$, $\log \sqrt[3]{5}$, π , ecc. Ogni numero reale è esprimibile in notazione decimale (cioè in base 10, ma lo si può scrivere anche in qualunque altra base $b \geq 2$, come vedremo nell'appendice 4.1), 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 , cioè che x appartiene ad A . La sua negazione è $x \notin A$ (che si legge x non è un elemento di A , o anche x non appartiene ad A). Così $3 \in \mathbb{N}$ e $\frac{1}{2} \notin \mathbb{Z}$.

Se A e B sono insiemi, diremo che A è sottoinsieme di B (o che A è contenuto in 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) $\mathbb{A} \subseteq \mathbb{A}$ per ogni insieme A (A è detto il sottoinsieme proprio di A); (2) $\mathbb{N}^* \subseteq \mathbb{N}$; (3) $\mathbb{N} \subseteq \mathbb{Z}$; (4) $\mathbb{Q} \subseteq \mathbb{R}$.

Se A e B sono insiemi, scriveremo $A = B$ (uguaglianza tra insiemi) 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 $A \subseteq B$ e $A \neq B$, e in questo caso diremo che A è un sottoinsieme proprio di B (o che A è propriamente contenuto in 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.

L'insieme vuoto \emptyset è l'insieme privo di elementi. Questo significa che $x \notin \emptyset$ per ogni oggetto x . Si ha $\emptyset \subseteq A$ per ogni insieme A .

Come si denota un insieme

Abbiamo visto che ad alcuni insiemi vengono riservati simboli particolari: è questo il caso di $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \emptyset$. Più generalmente gli insiemi vengono denotati in due modi.

Il 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 $\{0, 1, 2, 3, 4\}$, e l'insieme i cui elementi sono le soluzioni dell'equazione $x^2 - 1$ può essere denotato con $\{1, -1\}$. Altri esempi sono $\{1, 2, 3, 4, 5\}$, $\{a, b, c, z\}$ e $\{1, 5, 28, \pi, a\}$. A volte è sufficiente iniziare l'elenco, purché sia chiaro cosa si intenda; così abbiamo $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$, $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$.

Il secondo modo per denotare un insieme consiste nel far uso di una proprietà soddisfatta da tutti e soli gli elementi di quell'insieme. Denoteremo allora l'insieme nella forma $\{x \mid \dots\}$ ove al posto dei punti scriveremo la proprietà. Ad esempio l'insieme $\{0, 1, 2, 3, 4\}$ può anche essere denotato con

$$\{x \mid x \in \mathbb{N} \text{ e } x < 5\}$$

(che si legge "l'insieme degli x tali che $x \in \mathbb{N}$ e $x < 5$ "), e 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.

Ecco altri esempi:

(a) $\{x \mid x \in \mathbb{Z}, 2 < x < 5\} = \{3, 4\}$;

- (b) $\{x \mid x \in \mathbb{N}, x \text{ è un numero primo}, 3 \leq x \leq 15\} = \{3, 5, 7, 11, 13\}$;
 (c) $\{x \mid x = 2y \text{ per qualche } y \in \mathbb{Z}\}$ è l'insieme dei numeri pari;
 (d) $\{x \mid x \in \mathbb{Q}, x^2 - 4 = 0\} = \{2, -2\}$.

Si osservi che negli esempi (a), (b), (d) si hanno delle ugualanze tra insiemi; gli insiemi sono uguali perché hanno gli stessi elementi. Per lo stesso motivo gli insiemi $\{a, b\}$, $\{b, a\}$, $\{a, a, b\}$, $\{a, a, b, a, b, b\}$ sono tutti uguali tra loro perché hanno gli stessi elementi, che sono le due lettere a e b .

Si faccia attenzione a non confondere x (l'oggetto x) con $\{x\}$ (l'insieme che contiene il solo oggetto 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

Siano A e B insiemi. L'insieme $A \cup B$ (*unione* di A e di B) è l'insieme di tutti gli elementi che appartengono ad A o a B (o a entrambi):

$$A \cup B = \{x \mid x \in A \text{ oppure } x \in B\}.$$

L'insieme $A \cap B$ (*intersezione* di A e di B) è l'insieme di tutti gli elementi che appartengono sia ad A che a B :

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}.$$

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

L'insieme $A \setminus B$ (*differenza* di A e di B , o *complementare* di B in A) è l'insieme di tutti gli elementi che appartengono ad A e non appartengono a B :

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}.$$

L'insieme $A \Delta B$ (*differenza simmetrica* di A e B) è l'insieme di tutti gli elementi che appartengono ad A o a B ma non a entrambi:

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

Se si hanno tre insiemi A, B, C è evidente che $A \cup (B \cup C) = (A \cup B) \cup C$. Possiamo quindi tralasciare le parentesi e scrivere $A \cup B \cup C$. Similmente se si hanno n insiemi A_1, A_2, \dots, A_n è facile intuire il significato di $A_1 \cup A_2 \cup \dots \cup A_n$.

Analogamente si hanno $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cap B \cap C$, $A_1 \cap A_2 \cap \dots \cap A_n$, ecc.

Se A è un insieme, l'*insieme delle 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 . In simboli

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

1.1 ESEMPIO. Se $A = \{1, 2, 3\}$, allora

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}. \quad \square$$

1.2 ESEMPIO. Se $A = \{\emptyset, \{\emptyset\}\}$, allora

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

1.3 ESEMPIO (PROPRIETÀ DISTRIBUTIVE). Dimostriamo che se A, B, C sono insiemi, allora

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

Proviamo 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 far vedere che ciascuno di due insiemi è sottoinsieme dell'altro, è il metodo usuale con cui si dimostra che due insiemi coincidono, cioè sono uguali.

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 $x \in B \cup C$. Distinguiamo due casi a seconda che $x \in B$ o $x \notin B$. Se $x \in B$ allora, dato che $x \in A$, si ha che $x \in A \cap B$. Quindi, a maggior ragione, si ha che $x \in (A \cap B) \cup (A \cap C)$ in questo caso. Se invece $x \notin B$, allora da $x \in B \cup C$ segue che $x \in C$. Ma allora $x \in A \cap C$, e pertanto $x \in (A \cap B) \cup (A \cap C)$. Abbiamo così dimostrato che $x \in (A \cap B) \cup (A \cap C)$ in entrambi i casi. Si è quindi verificato che $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Dimostriamo ora che $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Se $x \in (A \cap B) \cup (A \cap C)$, 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 nell'altro caso: 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 secondo 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 ora 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 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, degli 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

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

Si usa una notazione simile anche per denotare i prodotti. In questo caso scriveremo \prod , cioè una pi greca maiuscola, invece di \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

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

(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 $A_1 \cap A_2 \cap \dots \cap A_n$.

1.4 ESEMPIO. Se $A_1 = \{1, 2, 3\}$, $A_2 = \{2, 3, 4\}$, $A_3 = \{3, 4, 5\}$, ..., $A_{10} = \{10, 11, 12\}$, allora $\bigcup_{i=1}^{10} A_i = \{1, 2, 3, \dots, 12\}$, $\bigcap_{i=1}^3 A_i = \{3\}$, $\bigcap_{i=1}^{10} A_i = \emptyset$. \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* (cioè un insieme) 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

$$\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{Z} \quad \text{e} \quad \bigcap_{i \in \mathbb{Z}} A_i = \emptyset.$$

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

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

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 $\bigcup_{i \in \mathbb{Z}} A_i = \mathbb{Q}$. 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 $\bigcap_{i \in \mathbb{N}} A_i = \mathbb{Q} \setminus \mathbb{N}$.

Il caso generale è il seguente. Sia $\mathcal{F} = \{A_i \mid i \in I\}$ una *famiglia* (cioè un insieme) di insiemi A_i , ove l'*indice* i , ossia il "parametro" i , appartiene all'insieme I . Allora

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ per qualche } i \in I\} \quad \text{e} \quad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ per ogni } i \in I\}.$$

Esercizi svolti

1.1. Si dimostri che se B è un insieme e $A \subseteq B$, 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 dedurne una contraddizione. Ad esempio 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 $B \subseteq (B \setminus A) \cup A$ fissiamo $b \in B$. Allora si possono avere i due casi $b \in A$ oppure $b \notin A$. Se $b \in A$, allora $b \in (B \setminus A) \cup A$. 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 pertanto $b \in (B \setminus A) \cup A$, e questo prova che $B \subseteq (B \setminus A) \cup A$. \square

1.2. Si dimostri che se A, B, C sono insiemi, $A \cap B = \emptyset$ 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 $a \in A$. Allora $a \in A \cup B$, cioè $a \in C$. Mostriamo che $a \notin B$. Se per assurdo fosse $a \in B$, allora $a \in A \cap B$, e questa è una contraddizione 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 $c \notin B$, cioè $c \in A \cup B$ e $c \notin B$. Ma allora si deve avere che $c \in A$. 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 a maggior ragione 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) $\{\emptyset\} \subseteq A$;
- (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 $A \Delta B$?

1.12. Gli insiemi $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$ sono disgiunti?

Negli esercizi 1.13–1.22 A, B, C sono insiemi; si provi che:

1.13. Se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$.

1.14. Se $A \subseteq B$, allora $B \setminus (B \setminus A) = A$.

1.15. $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ e $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$.

1.16. $A \cup A = A$ e $A \cap A = A$.

1.17. $A \cup \emptyset = A$ e $A \cap \emptyset = \emptyset$.

1.18. $A \cap B = B \cap A$ e $A \cup B = B \cup A$.

1.19. $A \cap (A \cup B) = A$ e $A \cup (A \cap B) = A$.

1.20. $A \cup B = (A \setminus B) \cup B$.

1.21. Se $A = \emptyset$; allora $B = (A \setminus B) \cup (B \setminus A)$.

1.22. Se $B = (A \setminus B) \cup (B \setminus A)$, allora $A = \emptyset$.

1.23. Si determini $\mathcal{P}(A)$, ove:

- (a) $A = \{2, 4, 8\}$;
- (b) $A = \{0, 1, 2, 3\}$;
- (c) $A = \{\{\emptyset\}, 2\}$;
- (d) $A = \{a, 1, \{\{\emptyset\}\}\}$;
- (e) $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

1.24. Siano A, B, C insiemi. Si provi che:

- (a) $A \Delta B = B \Delta A$;
- (b) se X, Y, Z sono insiemi, allora

- (i) $(X \cup Y) \setminus Z = (X \setminus Z) \cup (Y \setminus Z)$;
- (ii) $X \setminus (Y \setminus Z) = (X \setminus Y) \cup (X \cap Z)$;
- (iii) $(X \setminus Y) \setminus Z = X \setminus (Y \cup Z)$;

- (c) facendo uso delle uguaglianze dimostrate in (b) provare che l'operazione Δ è associativa:
 $(A \Delta B) \Delta C = A \Delta (B \Delta C)$;
- (d) se X, Y, Z sono insiemi, allora $X \cap (Y \setminus Z) = (X \cap Y) \setminus (X \cap Z)$;
- (e) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

1.25. 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) $(-1)^1 + (-1)^2 + (-1)^3 + (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7$.

1.26. Si calcoli $\sum_{n=1}^5 (-1)^n n$.

1.27. Si calcoli $\prod_{k=1}^5 k$.

1.28. Per ogni $n \in \mathbb{N}$ sia $A_n = \{x \mid x \in \mathbb{N}, 0 \leq x \leq n\}$.

Si calcolino $\bigcup_{n=0}^5 A_n$, $\bigcap_{n=0}^5 A_n$, $\bigcup_{n \in \mathbb{N}} A_n$, $\bigcap_{n \in \mathbb{N}} A_n$.

1.29. 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 $\bigcap_{i \in \mathbb{Z}} A_i$.

1.30. Dimostrare che se A è un insieme, allora

$$\bigcup_{X \subseteq A} X = A \quad \text{e} \quad \bigcap_{X \subseteq A} X = \emptyset.$$

§2. Corrispondenze e 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 π . È noto al lettore come sia possibile definire un *sistema di coordinate* in un piano π dopo aver fissato due rette ortogonali nel piano (gli *assi*), un orientamento su ciascuna di esse, e un'unità di misura. Si ottiene così che ad ogni punto P del piano π 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 π avente (a, b) come coordinate. In questo caso si ha cioè una corrispondenza biunivoca tra l'insieme dei punti del piano π 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.

Dati due elementi a e b è possibile formare la *coppia ordinata* (a, b) , avente *primo elemento* (o *prima coordinata*) a e *secondo elemento* (o *seconda coordinata*) b . Due coppie ordinate $(a, b), (a', b')$ sono uguali se e solo se $a = a'$ e $b = b'$. Si presta attenzione al fatto che la coppia ordinata (a, b) non è l'insieme $\{a, b\}$. Ad esempio consideriamo gli elementi 1 e 2 di \mathbb{N} . Allora $(1, 2) \neq (2, 1)$, mentre $\{1, 2\} = \{2, 1\}$. Inoltre $(1, 1)$ è una coppia, mentre $\{1, 1\} = \{1\}$ è un insieme con un solo elemento.

Se A e B sono insiemi, il *prodotto cartesiano* $A \times B$ di A per B è l'insieme delle coppie ordinate (a, b) , ove $a \in A$ e $b \in B$:

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

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

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

Più in generale, se A_1, A_2, \dots, A_n sono insiemi, il loro prodotto cartesiano

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

è l'insieme delle n -uple ordinate (a_1, a_2, \dots, a_n) ove $a_i \in A_i$ per ogni $i = 1, 2, \dots, n$. Nel caso particolare in cui gli n insiemi A_1, A_2, \dots, A_n coincidono tutti con uno stesso insieme A si scrive A^n in luogo di $\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}}$. Ad esempio $\mathbb{R}^2 = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\}$.

Corrispondenze e applicazioni

Capita spesso in matematica di dover far corrispondere ad elementi di un insieme A elementi di un insieme B . Ad esempio agli elementi x di \mathbb{R} possiamo far corrispondere gli elementi y di \mathbb{R} con x minore o uguale a y . In questo caso $A = B = \mathbb{R}$. Per fare un secondo esempio, possiamo far corrispondere ad un elemento x di \mathbb{Z} l'elemento y di \mathbb{Z} se x è il quadrato di y . In questo caso $A = B = \mathbb{Z}$.

Si noti come sia possibile disegnare il grafico di queste corrispondenze, cioè il luogo geometrico dei punti (x, y) tali che x corrisponde a y (o, più precisamente, il luogo geometrico dei punti del piano cartesiano le cui coordinate (x, y) sono tali che x corrisponde a y). I grafici dei nostri due esempi sono disegnati in figura 2.1.

Come terzo esempio fissiamo un piano π e una circonferenza in questo piano. Se A è l'insieme dei punti del piano π e B è l'insieme delle rette di π , 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 .

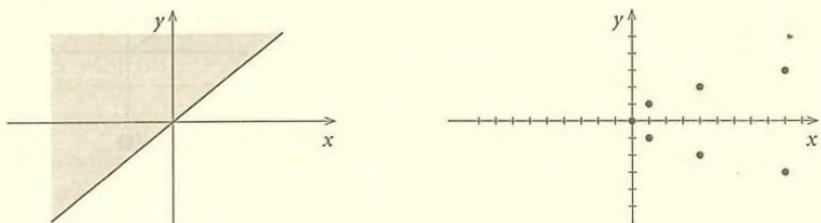
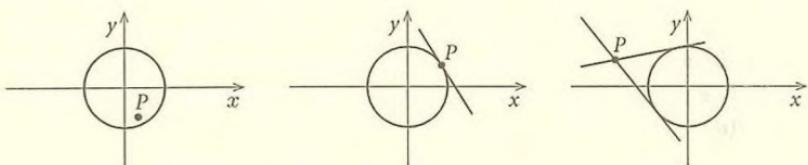


FIGURA 2.1.

FIGURA 2.2. Un punto P e le rette corrispondenti a P .

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:

2.1 DEFINIZIONE. Una *corrispondenza* ϱ 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 ϱ . \square

In questo modo abbiamo formalizzato la nozione intuitiva di corrispondenza identificando una corrispondenza di A in B con il suo grafico (che è un sottoinsieme di $A \times B$). Quindi, nel primo esempio che abbiamo dato, la corrispondenza di \mathbb{R} in \mathbb{R} che fa corrispondere agli $x \in \mathbb{R}$ gli $y \in \mathbb{R}$ con x minore o uguale a y è il sottoinsieme

$$\varrho = \{(x, y) \mid x, y \in \mathbb{R}, x \leq y\}$$

di \mathbb{R}^2 . La corrispondenza di \mathbb{Z} in \mathbb{Z} del secondo esempio è il sottoinsieme $\varrho = \{(x, y) \mid x, y \in \mathbb{Z}, x = y^2\}$ di \mathbb{Z}^2 . Nel terzo esempio che abbiamo dato, la corrispondenza che a un punto del piano fa corrispondere le tangenti alla circonferenza per quel punto è il sottoinsieme

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

Si noti che questa è una corrispondenza di A in B perché è un sottoinsieme di $A \times B$.

2.2 ESEMPIO. Sia X un insieme. Allora “appartiene a” è una corrispondenza ϱ di X in $\mathcal{P}(X)$:

$$\varrho = \{(x, Y) \mid x \in X, Y \in \mathcal{P}(X) \text{ e } x \in Y\} \subseteq X \times \mathcal{P}(X).$$

Si ha che x corrisponde a Y se e solo se $x \in Y$. \square

2.3 ESEMPIO. La corrispondenza di \mathbb{Q} in \mathbb{Q} “è il doppio di” è

$$\varrho = \{(x, y) \mid x, y \in \mathbb{Q}, x = 2y\}.$$

In questo esempio 0 corrisponde a 0, 1 corrisponde a $1/2$, ecc. \square

Siano A e B insiemi. Un'applicazione (o funzione o mappa) di A in B è una corrispondenza φ 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 φ 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 $(a, b) \in \varphi$.

2.4 ESEMPI. Ecco cinque esempi di applicazioni:

(1) La corrispondenza φ_1 di \mathbb{Z} in \mathbb{Z} che ad ogni elemento $x \in \mathbb{Z}$ fa corrispondere $2x \in \mathbb{Z}$ è un'applicazione $\varphi_1: \mathbb{Z} \rightarrow \mathbb{Z}$. Per questa applicazione si ha $\varphi_1(x) = 2x$ per ogni $x \in \mathbb{Z}$, o, con notazione equivalente, $\varphi_1: x \mapsto 2x$.

Se vogliamo descrivere rigorosamente tale applicazione φ_1 come corrispondenza di \mathbb{Z} in \mathbb{Z} , cioè come sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$, dobbiamo dire che

$$\varphi_1 = \{(x, 2x) \mid x \in \mathbb{Z}\}.$$

Come abbiamo già fatto osservare nel caso più generale delle corrispondenze, anche per le applicazioni tale descrizione rigorosa non fa altro che “confondere”, cioè identificare, l'applicazione e il suo grafico.

(2) Un altro esempio di applicazione $\varphi_2: \mathbb{N} \rightarrow \mathbb{Z}$ si ha ponendo

$$\varphi_2(n) = -n$$

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}). In questo caso si ha $\varphi_2 = \{(n, -n) \mid n \in \mathbb{N}\}$.

(3) $\varphi_3: \mathbb{Z} \rightarrow \mathbb{N}$ definita da $\varphi_3(x) = x^2$ per ogni $x \in \mathbb{Z}$. In questo caso si ha $\varphi_3 = \{(x, x^2) \mid x \in \mathbb{Z}\}$.

(4) $\varphi_4: \mathbb{N} \rightarrow \mathbb{N}$ definita da $\varphi_4(x) = 2x$ per ogni $x \in \mathbb{N}$. Si ha $\varphi_4 = \{(x, 2x) \mid x \in \mathbb{N}\}$. Si noti che $\varphi_4 \neq \varphi_1$.

(5) $\varphi_5: \mathbb{Q} \rightarrow \mathbb{Q}$ definita ponendo $\varphi_5(x) = 1/(1+x^2)$ per ogni $x \in \mathbb{Q}$. Si ha $\varphi_5 = \{(x, y) \mid x, y \in \mathbb{Q}, (1+x^2)y = 1\}$.

(6) I grafici di figura 2.3 rappresentano sottoinsiemi di \mathbb{R}^2 che non sono applicazioni di \mathbb{R} in \mathbb{R} . Si spieghi perché. \square

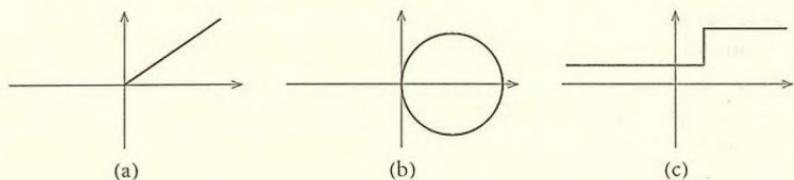


FIGURA 2.3.

Se $\varphi: A \rightarrow B$ è un'applicazione, l'insieme A si dice il *dominio* di φ , e l'insieme B si dice il *codominio* di φ . In pratica per descrivere un'applicazione φ è sufficiente darne il dominio A , il codominio B , e specificare per ogni elemento $x \in A$ l'elemento $\varphi(x) \in B$. In tal caso si dirà che l'applicazione $\varphi: A \rightarrow B$ è definita dalla posizione $x \mapsto \varphi(x)$. Così, negli esempi precedenti, $\varphi_1: \mathbb{Z} \rightarrow \mathbb{Z}$ è definita dalla posizione $x \mapsto 2x$, $\varphi_2: \mathbb{N} \rightarrow \mathbb{Z}$ è definita dalla posizione $n \mapsto -n$, $\varphi_3: \mathbb{Z} \rightarrow \mathbb{N}$ è definita da $x \mapsto x^2$, $\varphi_4: \mathbb{N} \rightarrow \mathbb{N}$ da $x \mapsto 2x$, e $\varphi_5: \mathbb{Q} \rightarrow \mathbb{Q}$ da $x \mapsto 1/(1+x^2)$.

Sia $\varphi: A \rightarrow B$ un'applicazione. Se $a \in A$, $\varphi(a)$ si chiama l'*immagine* di a secondo φ (o il *valore* di φ in a); se $A' \subseteq A$, $\varphi(A') = \{\varphi(x) \mid x \in A'\}$ è l'*immagine* di A' (secondo φ). L'insieme $\varphi(A)$, ossia l'immagine di tutto il dominio, è detto anche l'*immagine dell'applicazione* φ . Se $B' \subseteq B$, l'insieme

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

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

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

Si osservi che l'antiimmagine $\varphi^{-1}(b)$ di un *elemento* b del codominio è un *sottoinsieme* del dominio.

2.5 ESEMPIO. Siano $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5$ le applicazioni dell'esempio 2.4. Allora $\varphi_1(2) = 4$, cioè l'immagine di 2 è 4. L'immagine di φ_2 è l'insieme dei numeri interi minori o uguali a zero, $\varphi_3(\{-1, 0, 1, 2\}) = \{0, 1, 4\}$, $\varphi_4^{-1}(\{1, 2, 3, 4, 5\}) = \{1, 2\}$, $\varphi_4^{-1}(6) = \{3\}$, $\varphi_4^{-1}(7) = \emptyset$. Infine $\varphi_5(\{1, 2, 3\}) = \{1/2, 1/5, 1/10\}$ e $\varphi_5(\{1, -1\}) = \{1/2\}$. \square

2.6 ESEMPIO. Sia $A = \{1, 2, 3\}$, $B = \{1, 4, 5, 6\}$. Allora ponendo $\varphi_6(1) = 1$, $\varphi_6(2) = 4$, $\varphi_6(3) = 1$ si definisce un'applicazione $\varphi_6: A \rightarrow B$. In questo caso l'immagine di 2 è 4, l'immagine di $\{1, 2\} \subseteq A$ è $\varphi_6(\{1, 2\}) = \{1, 4\}$, l'immagine dell'applicazione φ_6 è $\{1, 4\}$, l'antiimmagine di $\{1, 5\}$ è $\varphi_6^{-1}(\{1, 5\}) = \{1, 3\}$, l'antiimmagine di $\{5, 6\}$ è $\varphi_6^{-1}(\{5, 6\}) = \emptyset$, le antiimmagini degli elementi 1, 4 e 5 di B sono rispettivamente $\varphi_6^{-1}(1) = \{1, 3\}$, $\varphi_6^{-1}(4) = \{2\}$ e $\varphi_6^{-1}(5) = \emptyset$. \square

Sia $\varphi: A \rightarrow B$ un'applicazione. Allora φ si dice:

- ▷ *iniettiva* se, per ogni $a, a' \in A$, $\varphi(a) = \varphi(a')$ implica $a = a'$. Quindi φ è iniettiva se e solo se elementi distinti del dominio hanno immagini distinte, o equivalentemente, se e solo se l'antiimmagine di ogni elemento del codominio contiene al più un elemento del dominio;
- ▷ *suriettiva* se $\varphi(A) = B$. Quindi φ è suriettiva se e solo se per ogni $b \in B$ esiste $a \in A$ tale che $\varphi(a) = b$;
- ▷ *biiettiva* se è iniettiva e suriettiva.

Le applicazioni biiettive si chiamano anche *biiezioni* (o *corrispondenze biuniwoche*). Se esiste una biiezione $\varphi: A \rightarrow B$ si dice che A e B sono *in corrispondenza biunivoca*. Con riferimento agli esempi precedenti, l'applicazione φ_1 è iniettiva, perché per ogni $a, a' \in \mathbb{Z}$, da $\varphi_1(a) = \varphi_1(a')$, cioè $2a = 2a'$, segue che $a = a'$. Non è però suriettiva, perché non esiste nessun $a \in \mathbb{Z}$ tale che $\varphi_1(a)$ sia uguale all'elemento 1 del codominio \mathbb{Z} di φ_1 . Quindi φ_1 non è una biiezione. L'applicazione φ_2 è iniettiva, perché per ogni $a, a' \in \mathbb{N}$, $\varphi_2(a) = \varphi_2(a')$, cioè $-a = -a'$, implica $a = a'$. Non è suriettiva, perché non esiste nessun $a \in \mathbb{N}$ tale che $\varphi_2(a)$ sia uguale all'elemento 1 del codominio \mathbb{Z} di φ_2 . Quindi nemmeno φ_2 non è una biiezione. L'applicazione φ_3 non è iniettiva perché $\varphi_3(1) = \varphi_3(-1) = 1$ e non è suriettiva perché 2 non è il quadrato di nessun numero intero. L'applicazione φ_4 è iniettiva, perché se $a, a' \in \mathbb{N}$ e $\varphi_4(a) = \varphi_4(a')$, allora $2a = 2a'$, da cui $a = a'$; non è suriettiva perché 3 non è il doppio di nessun numero naturale. L'applicazione φ_5 non è iniettiva perché $\varphi_5(1) = \varphi_5(-1) = 1/2$; non è nemmeno suriettiva perché $1/(1+x^2)$ è sempre un numero positivo, e quindi i numeri razionali negativi appartengono al codominio ma non appartengono all'immagine di φ_5 . Infine $\varphi_6: A \rightarrow B$ non è iniettiva perché $\varphi_6(1) = \varphi_6(3)$. Non è nemmeno suriettiva perché non esiste nessun $a \in A$ tale che $\varphi_6(a) = 5$.

2.7 ESEMPIO. 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 φ non è iniettiva perché $\varphi(0) = \varphi(1)$, mentre φ è suriettiva perché per ogni $x \in \mathbb{N}$ si ha $\varphi(x+1) = x$. \square

2.8 ESEMPIO. Sia $\psi: \mathbb{N} \rightarrow \mathbb{N}$ l'applicazione definita da $\psi(x) = x + 1$ per ogni $x \in \mathbb{N}$. L'applicazione ψ è iniettiva, perché se $x, x' \in \mathbb{N}$ e $\psi(x) = \psi(x')$, allora $x + 1 = x' + 1$, e quindi $x = x'$. L'applicazione ψ non è suriettiva perché non esiste nessun $x \in \mathbb{N}$ tale che $\psi(x) = 0$. \square

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

2.10 ESEMPIO. Sia $\sigma: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definita da $(x, y) \mapsto x + y$. Allora σ non è iniettiva perché $\sigma((0, 0)) = \sigma((1, -1)) = 0$, mentre σ è suriettiva, perché per ogni z appartenente al codominio \mathbb{Z} di σ si ha che $\sigma((z, 0)) = z$. \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 (o l'*identità* di A). È immediato verificare che ι_A è una biiezione di A in A .

Due applicazioni $\varphi: A \rightarrow B$ e $\varphi': A' \rightarrow B'$ si considerano uguali se e solo se $A = A'$, $B = B'$, e $\varphi(x) = \varphi'(x)$ per ogni $x \in A = A'$. Quindi ad esempio le applicazioni $\varphi_3: \mathbb{Z} \rightarrow \mathbb{N}$, $\varphi_3(x) = x^2$ per ogni $x \in \mathbb{Z}$, $\varphi'_3: \mathbb{N} \rightarrow \mathbb{N}$, $\varphi'_3(x) = x^2$ per ogni $x \in \mathbb{N}$, e $\varphi''_3: \mathbb{Z} \rightarrow \mathbb{Q}$, $\varphi''_3(x) = x^2$ per ogni $x \in \mathbb{Z}$, sono tutte distinte tra loro. Invece sono uguali le applicazioni $\psi: \mathbb{Z} \rightarrow \mathbb{Z}$, $\psi(x) = \sqrt{x^2}$ per ogni $x \in \mathbb{Z}$, e $\psi': \mathbb{Z} \rightarrow \mathbb{Z}$, $\psi'(x) = \sqrt[4]{x^4}$ per ogni $x \in \mathbb{Z}$.

Si noti che anche le applicazioni $\psi: \mathbb{N} \rightarrow \mathbb{N}$ dell'esempio 2.8 e $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ dell'esempio 2.9 sono distinte fra loro, in quanto hanno domini e codomini differenti. Quindi $\psi \neq \varphi$ anche se entrambe mandano x in $x + 1$. Tra l'altro ψ non è suriettiva mentre φ lo è.

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 χ 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 1.14) $Y = Y'$. Quindi χ è iniettiva.

Mostriamo che χ 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 χ è anche suriettiva, e pertanto χ 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 φ è una biiezione.

Soluzione. Mostriamo che φ 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 $\varphi(n) = \varphi(n')$, allora 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 φ è iniettiva.

Mostriamo che φ 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 φ è anche suriettiva. \square

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

- (a) se $A', A'' \subseteq A$, allora $\varphi(A' \cup A'') = \varphi(A') \cup \varphi(A'')$;
- (b) se $A', A'' \subseteq A$, allora $\varphi(A' \cap A'') \subseteq \varphi(A') \cap \varphi(A'')$;
- (c) se $B', B'' \subseteq B$, allora $\varphi^{-1}(B' \cup B'') = \varphi^{-1}(B') \cup \varphi^{-1}(B'')$;
- (d) se $B', B'' \subseteq B$, allora $\varphi^{-1}(B' \cap B'') = \varphi^{-1}(B') \cap \varphi^{-1}(B'')$;
- (e) se $B' \subseteq B$, allora $\varphi^{-1}(B' \setminus B') = A \setminus \varphi^{-1}(B')$;
- (f) se $A' \subseteq A$, allora $A' \subseteq \varphi^{-1}(\varphi(A'))$;
- (g) 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 far vedere 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} :

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

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

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

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 e $A \neq B$, allora ovviamente $A \times B \neq B \times A$. Si provi che l'applicazione $\sigma: A \times B \rightarrow B \times A$, $\sigma((a, b)) = (b, a)$ per ogni $(a, b) \in A \times B$, è una biiezione.

2.19. 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 π_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.]

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

- Si provi che l'applicazione ε è iniettiva.
- Si provi che l'applicazione ε è biiettiva se e solo se $A = B$.

[L'applicazione ε è detta l'*applicazione di inclusione* o l'*immersione* di A in B .]

2.21. Si provi che se $\varphi: A \rightarrow B$ è un'applicazione e $\varphi(A)$ è la sua immagine, allora $\psi: A \rightarrow \varphi(A)$ definita da $\psi(a) = \varphi(a)$ per ogni $a \in A$ è un'applicazione suriettiva.

2.22. Si dia un esempio di un'applicazione $\mathbb{N} \rightarrow \mathbb{N}$ che sia iniettiva ma non suriettiva. Si dia un esempio di un'applicazione $\mathbb{N} \rightarrow \mathbb{N}$ che sia suriettiva ma non iniettiva.

2.23. Si provi che se $\varphi: A \rightarrow B$ è un'applicazione, $A' \subseteq A$, $B' \subseteq B$ e $\varphi(A') \subseteq B'$, allora $\varphi': A' \rightarrow B'$ definita dalla posizione $\varphi'(x) = \varphi(x)$ per ogni $x \in A'$ è un'applicazione.

2.24. Sia $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ l'applicazione definita dalla posizione $\varphi(n) = 0$ per ogni $n \in \mathbb{N}$. Si provi che gli insiemi $\varphi(\mathbb{N} \setminus \{0\})$ e $\mathbb{N} \setminus \varphi(\{0\})$ sono disgiunti.

2.25. Si dia un esempio di due insiemi A e B , di due sottoinsiemi $A', A'' \subseteq A$ e di un'applicazione $\varphi: A \rightarrow B$ tali che $\varphi(A' \cap A'') \subset \varphi(A') \cap \varphi(A'')$.

2.26. 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 $h^{-1}(B' \times C') = f^{-1}(B') \cap g^{-1}(C')$.

2.27. 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 ?

§3. Applicazioni composte

Siano A, B, C insiemi e $\varphi: A \rightarrow B$, $\psi: B \rightarrow C$ applicazioni. L'*applicazione composta* (o *applicazione prodotto*) di φ per ψ , denotata $\psi \circ \varphi$, o semplicemente $\psi\varphi$, è l'applicazione $\psi \circ \varphi: A \rightarrow C$ definita ponendo $(\psi \circ \varphi)(a) = \psi(\varphi(a))$ per ogni $a \in A$.

Ad esempio, date $\varphi_1: \mathbb{Z} \rightarrow \mathbb{N}$, $\varphi_1(x) = x^2$ per ogni $x \in \mathbb{Z}$, e $\varphi_2: \mathbb{N} \rightarrow \mathbb{N}$, $\varphi_2(x) = 2x$ per ogni $x \in \mathbb{N}$, allora $\varphi_2 \circ \varphi_1: \mathbb{Z} \rightarrow \mathbb{N}$ è definita da $(\varphi_2 \circ \varphi_1)(x) = 2x^2$ per ogni $x \in \mathbb{Z}$, perché $(\varphi_2 \circ \varphi_1)(x) = \varphi_2(\varphi_1(x)) = \varphi_2(x^2) = 2x^2$.

Se $\sigma: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ è definita da $\sigma(x, y) = x + y$, allora $\varphi_1 \circ \sigma: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{N}$ è definita da $(\varphi_1 \circ \sigma)(x, y) = (x + y)^2$ per ogni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, perché $(\varphi_1 \circ \sigma)(x, y) = \varphi_1(\sigma(x, y)) =$

$$\varphi_1(x+y) = (x+y)^2.$$

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 $z \in \mathbb{Z}$.

3.1 PROPOSIZIONE. Siano $\varphi: A \rightarrow B$ e $\psi: B \rightarrow C$ applicazioni. Allora:

- (a) se φ e ψ sono iniettive, allora $\psi \circ \varphi$ è iniettiva;
- (b) se φ e ψ sono suriettive, allora $\psi \circ \varphi$ è suriettiva;
- (c) se φ e ψ sono biiettive, allora $\psi \circ \varphi$ è biiettiva.

Dimostrazione. (a) Siano φ e ψ iniettive. Se $a, a' \in A$ e $(\psi \circ \varphi)(a) = (\psi \circ \varphi)(a')$, allora $\psi(\varphi(a)) = \psi(\varphi(a'))$, da cui $\varphi(a) = \varphi(a')$ perché ψ è iniettiva, e quindi $a = a'$ perché φ è iniettiva. Pertanto $\psi \circ \varphi$ è iniettiva.

(b) Siano φ e ψ suriettive. Fissiamo $c \in C$. Dato che ψ è suriettiva, esiste $b \in B$ tale che $\psi(b) = c$. Dato che φ è suriettiva, esiste $a \in A$ tale che $\varphi(a) = b$. Ma allora $(\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(b) = c$, e quindi $\psi \circ \varphi$ è suriettiva.

(c) Ovvio per (a) e (b). \square

3.2 PROPOSIZIONE. Siano $\varphi: A \rightarrow B$ e $\psi: B \rightarrow C$ applicazioni.

- (a) Se $\psi \circ \varphi$ è iniettiva, allora φ è iniettiva.
- (b) Se $\psi \circ \varphi$ è suriettiva, allora ψ è suriettiva.

Dimostrazione. (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 φ è iniettiva.

(b) Dobbiamo dimostrare che per ogni $c \in C$ esiste $b \in B$ tale che $\psi(b) = c$. Fissiamo quindi un elemento $c \in C$. Poiché $\psi \circ \varphi$ 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 ψ è suriettiva. \square

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 φ e ψ 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 $(\psi \circ \varphi)(n) = \psi(n) = n^2$ 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 ψ 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 φ e ψ 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 φ non è suriettiva, perché ad esempio non esiste nessun $n \in \mathbb{N}$ per il quale $\varphi(n) = 1$.

Si noti che la composizione di applicazioni è *associativa*, cioè se $\varphi: A \rightarrow B$, $\psi: B \rightarrow C$ e $\omega: C \rightarrow D$ sono applicazioni, allora $\omega \circ (\psi \circ \varphi) = (\omega \circ \psi) \circ \varphi$. Infatti per $a \in A$ si ha

$$[\omega \circ (\psi \circ \varphi)](a) = \omega[(\psi \circ \varphi)(a)] = \omega[\psi(\varphi(a))] = (\omega \circ \psi)(\varphi(a)) = [(\omega \circ \psi) \circ \varphi](a),$$

vale a dire $\omega \circ (\psi \circ \varphi) = (\omega \circ \psi) \circ \varphi$. Dato che le applicazioni $\omega \circ (\psi \circ \varphi)$ e $(\omega \circ \psi) \circ \varphi$ coincidono, possiamo non scrivere le parentesi e usare la notazione $\omega \circ \psi \circ \varphi$ (o più brevemente $\omega \psi \varphi$).

Si faccia attenzione al fatto che se $\varphi: A \rightarrow B$ e $\psi: C \rightarrow D$ sono applicazioni, l'applicazione composta $\psi \circ \varphi$ è definita se e solo se $B = C$. Ad esempio se $\varphi_1: \mathbb{N} \rightarrow \mathbb{Z}$ e $\psi_1: \mathbb{Z} \rightarrow \mathbb{Z}$, allora $\psi_1 \circ \varphi_1$ è definita, mentre la scrittura $\varphi_1 \circ \psi_1$ non ha significato. Inoltre anche se $A = B = C = D$, si ha che $\varphi \circ \psi$ e $\psi \circ \varphi$ sono entrambe definite, però si può avere $\varphi \circ \psi \neq \psi \circ \varphi$, cioè la *composizione di applicazioni non è commutativa*. Ad esempio siano $\varphi_2: \mathbb{N} \rightarrow \mathbb{N}$ definita da $\varphi_2(x) = x + 1$ per ogni $x \in \mathbb{N}$ e $\psi_2: \mathbb{N} \rightarrow \mathbb{N}$ definita da $\psi_2(x) = x^2$ per ogni $x \in \mathbb{N}$. Il lettore calcoli $\psi_2 \circ \varphi_2$ e $\varphi_2 \circ \psi_2$, e dimostri che $\psi_2 \circ \varphi_2 \neq \varphi_2 \circ \psi_2$.

3.3 PROPOSIZIONE. *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 $\psi_1 = \psi_2$.*

Dimostrazione. $\psi_1 = \psi_1 \circ \iota_B = \psi_1 \circ (\varphi \circ \psi_2) = (\psi_1 \circ \varphi) \circ \psi_2 = \iota_A \circ \psi_2 = \psi_2$. \square

3.4 PROPOSIZIONE. *Sia $\varphi: A \rightarrow B$ un'applicazione. Le seguenti affermazioni sono equivalenti:*

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

Dimostrazione. (a) \Rightarrow (b). Sia $\psi: B \rightarrow A$ un'applicazione tale che $\psi \circ \varphi = \iota_A$ e $\varphi \circ \psi = \iota_B$. Per la proposizione 3.2, e dal fatto che ι_A è iniettiva, segue che φ è iniettiva. Similmente per la stessa proposizione e per la suriettività di ι_B segue che φ è suriettiva. Quindi φ è biiettiva.

(b) \Rightarrow (a). Supponiamo che φ sia biiettiva. Sia $b \in B$. Dato che φ è suriettiva, esiste $a \in A$ tale che $\varphi(a) = b$. Dato che φ è iniettiva tale elemento a è unico. Quindi per ogni $b \in B$ esiste un unico $a \in A$ tale che $\varphi(a) = b$. Questo significa che la posizione che ad ogni $b \in B$ associa l'unico elemento $a \in A$ tale che $\varphi(a) = b$ definisce un'applicazione $\psi: B \rightarrow A$. Per ogni $a \in A$ e ogni $b \in B$ si ha $\psi(b) = a$ se e solo se $\varphi(a) = b$. In particolare se ne deduce

che $\psi(\varphi(a)) = a$ per ogni $a \in A$, e quindi $\psi \circ \varphi = \iota_A$, e che $\varphi(\psi(b)) = b$ per ogni $b \in B$, vale a dire $\varphi \circ \psi = \iota_B$. \square

Ricapitoliamo quanto visto nella dimostrazione di $(b) \Rightarrow (a)$. Data un'applicazione biiettiva $\varphi: A \rightarrow B$, 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 φ^{-1} ed è detta l'*applicazione inversa* di φ . Pertanto, per ogni applicazione biiettiva $\varphi: A \rightarrow B$ 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 φ 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.

3.5 ESEMPIO. 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 φ è una biiezione. L'applicazione φ 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 φ 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 φ è una biiezione. Cerchiamone l'applicazione inversa. L'espressione $\varphi(a) = b$ che definisce l'applicazione φ è in questo caso l'espressione $a^2 = b$ (qui $a, b \in \mathbb{R}^+$). Ricavando a 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 φ . \square

3.6 ESEMPIO. 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

Si osservi la differenza tra l'applicazione dell'esempio 3.5 e quella dell'esempio 3.6. Entrambe mandano a in a^2 . Ma mentre la $\varphi: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ dell'esempio 3.5 è una biiezione e quindi possiede un'applicazione inversa, la $\varphi: \mathbb{R} \rightarrow \mathbb{R}$ dell'esempio 3.6 non è una biiezione e quindi non possiede un'inversa.

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 $\varphi \circ \psi = \iota_B$; dimostrato questo si ha necessariamente che φ è una biiezione e che $\varphi^{-1} = \psi$.

3.7 ESEMPIO. Facciamo vedere che l'applicazione $\omega: \mathbb{Q} \rightarrow \mathbb{Q}$ definita da $\omega(x) = 3x + 4$ per ogni $x \in \mathbb{Q}$ è biiettiva e che la sua applicazione inversa è $\omega^{-1}: \mathbb{Q} \rightarrow \mathbb{Q}$, $\omega^{-1}(y) = (y - 4)/3$ per ogni $y \in \mathbb{Q}$.

Sia $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$ l'applicazione definita da $\varphi(y) = (y - 4)/3$ per ogni $y \in \mathbb{Q}$. Per dimostrare che ω è biiettiva e che φ è la sua inversa è sufficiente verificare che $\varphi \circ \omega = \iota_{\mathbb{Q}}$ e $\omega \circ \varphi = \iota_{\mathbb{Q}}$. Per ogni $x \in \mathbb{Q}$ si ha $(\varphi \circ \omega)(x) = \varphi(\omega(x)) = \varphi(3x + 4) = ((3x + 4) - 4)/3 = x$.

$x = \iota_{\mathbb{Q}}(x)$, e quindi $\varphi \circ \omega = \iota_{\mathbb{Q}}$. E per ogni $y \in \mathbb{Q}$ si ha $(\omega \circ \varphi)(y) = \omega(\varphi(y)) = \omega((y-4)/3) = 3((y-4)/3) + 4 = y = \iota_{\mathbb{Q}}(y)$, e quindi si ha anche che $\omega \circ \varphi = \iota_{\mathbb{Q}}$. \square

3.8 ESEMPIO. 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

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

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

3.9 ESEMPIO. Sia $\mathbb{Q}^* = \{x \mid x \in \mathbb{Q}, x \neq 0\}$ l'insieme dei numeri razionali non nulli. Consideriamo l'applicazione $\varphi: \mathbb{Q}^* \rightarrow \mathbb{Q}^*$ definita da $\varphi(x) = 1/x$ per ogni $x \in \mathbb{Q}^*$. Allora $\varphi \circ \varphi = \iota_{\mathbb{Q}^*}$, perché $\varphi \circ \varphi$ e $\iota_{\mathbb{Q}^*}$ hanno entrambe dominio e codominio \mathbb{Q}^* e inoltre $(\varphi \circ \varphi)(x) = \varphi(1/x) = 1/(1/x) = x = \iota_{\mathbb{Q}^*}(x)$ per ogni $x \in \mathbb{Q}^*$. Da $\varphi \circ \varphi = \iota_{\mathbb{Q}^*}$ e dalla proposizione 3.4 otteniamo immediatamente che φ è biiettiva e che $\varphi = \varphi^{-1}$, cioè che φ coincide con la propria inversa. \square

3.10 ESEMPIO. 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

3.11 ESEMPIO. 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 χ è una biezione e che $\chi^{-1} = \chi$. \square

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

Dimostrazione. Per mostrare che $(\varphi_1^{-1})^{-1} = \varphi_1$, cioè che φ_1 è l'inversa di φ_1^{-1} , si deve far vedere che moltiplicando φ_1^{-1} a destra e a sinistra per φ_1 si ottengono le applicazioni identiche, cioè che $\varphi_1^{-1} \circ \varphi_1 = \iota_A$ e $\varphi_1 \circ \varphi_1^{-1} = \iota_B$. Questa è la definizione di φ_1^{-1} .

Similmente per mostrare che $(\varphi_2 \circ \varphi_1)^{-1} = \varphi_1^{-1} \circ \varphi_2^{-1}$, cioè che $\varphi_1^{-1} \circ \varphi_2^{-1}$ è l'inversa di $\varphi_2 \circ \varphi_1$, si deve far vedere che moltiplicando $\varphi_2 \circ \varphi_1$ a destra e a sinistra per $\varphi_1^{-1} \circ \varphi_2^{-1}$ si ottengono le applicazioni identiche. Infatti

$$(\varphi_2 \circ \varphi_1) \circ (\varphi_1^{-1} \circ \varphi_2^{-1}) = \varphi_2 \circ (\varphi_1 \circ \varphi_1^{-1}) \circ \varphi_2^{-1} = \varphi_2 \circ \iota_B \circ \varphi_2^{-1} = \varphi_2 \circ \varphi_2^{-1} = \iota_C.$$

Similmente $(\varphi_1^{-1} \circ \varphi_2^{-1}) \circ (\varphi_2 \circ \varphi_1) = \iota_A$. \square

Attenzione: data un'applicazione $\varphi: A \rightarrow B$ abbiamo impiegato il simbolo φ^{-1} in due situazioni distinte con due significati distinti. Se φ è una biiezione, abbiamo denotato con $\varphi^{-1}: B \rightarrow A$ l'applicazione inversa (che esiste solo quando φ è una biiezione). Se φ 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.

Esercizi svolti

3.1. Sia $\varphi: A \rightarrow B$ un'applicazione. Si provi che se $\iota_A: A \rightarrow A$ e $\iota_B: B \rightarrow B$ denotano le applicazioni identiche di A e di 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 φ coincidono. Osserviamo intanto che queste tre applicazioni 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 $(\varphi \circ \iota_A)(a) = \varphi(a) = (\iota_B \circ \varphi)(a)$ per ogni $a \in A$. Si conclude che $\varphi \circ \iota_A = \iota_B \circ \varphi = \varphi$. \square

3.2. 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 $x = \sqrt[3]{y+1}$. Ponendo $\psi(y) = \sqrt[3]{y+1}$ per ogni $y \in \mathbb{R}$ si definisce quindi un'applicazione $\psi: \mathbb{R} \rightarrow \mathbb{R}$ che è l'applicazione inversa di φ . \square

3.3. 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) φ è iniettiva.

Soluzione. (a) \Rightarrow (b) Segue dalla proposizione 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 φ 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 ψ , 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 φ è $\varphi(a)$). Quindi $(\psi \circ \varphi)(a) = \iota_A(a)$ per ogni $a \in A$, ossia $\psi \circ \varphi = \iota_A$. \square

3.4. 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) φ è suriettiva.

Soluzione. (a) \Rightarrow (b) Segue dalla proposizione 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

3.5. Si considerino le applicazioni $\varphi: \mathbb{N} \rightarrow \mathbb{N}^*$ definita da $\varphi(x) = x + 1$ per ogni $x \in \mathbb{N}$, 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 φ , ψ e $\psi \circ \varphi$ quali sono iniettive? suriettive? biiettive?

3.6. Si considerino le applicazioni

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

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 φ , ψ e $\psi \circ \varphi$ quali sono iniettive? suriettive? biiettive?

3.7. 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 π_1 , ε 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.]

3.8. 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 $\varphi \circ \psi_2 = \iota_B$.

3.9. 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 $\varphi \circ \psi_2 = \iota_B$.

3.10. Siano φ e ψ le applicazioni definite negli esempi 2.7 e 2.8 rispettivamente. Si dimostri che:

- $\varphi \circ \psi = \iota_{\mathbb{N}}$, $\psi \circ \varphi \neq \iota_{\mathbb{N}}$;
- non esistono applicazioni $\psi_1: \mathbb{N} \rightarrow \mathbb{N}$ tali che $\psi_1 \circ \varphi = \iota_{\mathbb{N}}$;
- non esistono applicazioni $\psi_2: \mathbb{N} \rightarrow \mathbb{N}$ tali che $\psi \circ \psi_2 = \iota_{\mathbb{N}}$.

3.11. Si consideri l'applicazione $\psi: \mathbb{N} \rightarrow \mathbb{N}$ definita da $\psi(n) = n + 1$ per ogni $n \in \mathbb{N}$. Si è già visto nell'esempio 2.8 che tale applicazione è iniettiva e non suriettiva. Si determinino tutte le applicazioni $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ tali che $\varphi \circ \psi = \iota_{\mathbb{N}}$.

3.12. Si consideri l'applicazione $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ definita da $\varphi(n) = n - 1$ se $n > 0$, e $\varphi(0) = 0$. Si è già visto nell'esempio 2.7 che l'applicazione φ è suriettiva e non iniettiva. Si determinino tutte le applicazioni $\psi: \mathbb{N} \rightarrow \mathbb{N}$ tali che $\varphi \circ \psi = \iota_{\mathbb{N}}$.

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

- Si provi che se $\psi \circ \varphi$ è biiettiva, allora φ è iniettiva e ψ è suriettiva.
- Si trovi un esempio in cui φ è iniettiva, ψ è suriettiva, ma $\psi \circ \varphi$ non è iniettiva.
- Si trovi un esempio in cui φ è iniettiva, ψ è suriettiva, ma $\psi \circ \varphi$ non è suriettiva.

3.14. 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 φ , ψ , $\varphi \circ \psi$ e $\psi \circ \varphi$ sono biiettive e si calcolino le loro inverse.

3.15. Si verifichi che le applicazioni che seguono sono biiettive e si calcolino le loro inverse:

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

3.16. Calcolare, se esistono, le applicazioni inverse delle seguenti applicazioni:

- l'applicazione $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ definita da $\varphi(x) = x + 28$ per ogni $x \in \mathbb{Z}$;
- l'applicazione $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ definita da $\varphi(x) = -x + 28$ per ogni $x \in \mathbb{Z}$;
- l'applicazione φ_4 dell'esempio 2.4;
- l'applicazione σ dell'esercizio 2.18.

3.17. Si provi che se $\varphi: A \rightarrow B$ è suriettiva, $\psi_1, \psi_2: B \rightarrow C$ sono applicazioni e $\psi_1 \circ \varphi = \psi_2 \circ \varphi$, allora $\psi_1 = \psi_2$.

3.18. Si provi che se $\psi_1, \psi_2: A \rightarrow B$ sono applicazioni, $\varphi: B \rightarrow C$ è un'applicazione iniettiva e $\varphi \circ \psi_1 = \varphi \circ \psi_2$, allora $\psi_1 = \psi_2$.

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

3.20. 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 $g(B) = h(A)$.

§4. Numeri naturali e numeri interi

In questa sezione verranno ricordate alcune nozioni di aritmetica. Si tratterà in genere di aspetti meno noti di proprietà dei numeri naturali o interi già studiate in parte alle scuole inferiori.

Divisione tra numeri interi

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.)

Divisori e multipli

Siano $a, b \in \mathbb{Z}$. Si dice che b divide a (o che b è un *divisore di* a , o che a è un *multiplo di* b) se esiste $c \in \mathbb{Z}$ tale che $a = bc$. Per indicare che b divide a scriveremo $b | a$. Ad esempio, se $a, a', b \in \mathbb{Z}$, $b | a$ e $b | a'$, allora $b | (a - a')$.

Numeri primi

Un numero $p \in \mathbb{Z}$ si dice *primo* se $p \neq 1, p \neq -1$ e i suoi divisori sono solo $1, -1, p, -p$. Si noti che 0 non è un numero primo perché in base alla nostra definizione $n | 0$ per ogni $n \in \mathbb{Z}$ (infatti $0 = n \cdot 0$). Quindi $0, 1$ e -1 non sono numeri primi, mentre $2, -2, 3, -3, 5$ e -5 lo sono.

Vale il

4.1 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 con $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ numeri primi, allora $r = s$ e si possono riordinare i fattori in modo che

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

4.2 TEOREMA. Esistono infiniti numeri primi.

Dimostrazione (Euclide). Supponiamo per assurdo che esistano solo un numero finito di numeri primi. Siano quindi p_1, p_2, \dots, p_n tutti i numeri primi. Consideriamo il numero $a = p_1 p_2 \cdots p_n + 1$. Per il teorema fondamentale dell'aritmetica a è un prodotto di primi. In particolare esiste un numero primo q che divide a . Ma q è uno tra p_1, p_2, \dots, p_n , perché questi erano tutti i numeri primi. Quindi q divide anche $p_1 p_2 \cdots p_n$, e pertanto q divide $a - p_1 p_2 \cdots p_n = 1$. Ma solo 1 e -1 dividono 1, e quindi $q = 1$ oppure $q = -1$, e questo è assurdo perché 1 e -1 non sono primi. Questa contraddizione dimostra che esistono infiniti numeri primi. \square

Massimo comun divisore, minimo comune multiplo

Siano a, b due numeri interi. Un numero intero d si dice un *massimo comun divisore* (MCD) di a e b se valgono le seguenti proprietà:

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

Se $a = b = 0$, l'unico MCD di a e b è 0. Supporremo d'ora in poi che a e b non siano entrambi nulli.

4.3 TEOREMA. Siano a, b 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 $d = \alpha a + \beta b$.

Dimostrazione. Consideriamo l'insieme

$$S = \{xa + yb \mid x \in \mathbb{Z}, y \in \mathbb{Z}, xa + yb > 0\}.$$

Allora $S \subseteq \mathbb{N}^*$ ed $S \neq \emptyset$. Sia d il più piccolo degli elementi di S . Dato che $d \in S$ si ha $d > 0$ e $d = \alpha a + \beta b$ per opportuni $\alpha, \beta \in \mathbb{Z}$. Per concludere la dimostrazione è quindi sufficiente far vedere che d è un MCD di a e b . Mostriamo che $d | a$.

Dividiamo a per d : si ha $a = dq + r$ e $0 \leq r < |d| = d$ per opportuni $q, r \in \mathbb{Z}$. Se per assurdo fosse $r \neq 0$, allora $r > 0$ e $r = a - dq = a - (\alpha a + \beta b)q = (1 - \alpha q)a + (-\beta q)b$, e quindi si avrebbe $r \in S$ ed $r < d$, e questo contraddirrebbe il fatto che d era stato scelto come il più piccolo elemento di S . Quindi $r = 0$, e pertanto $a = dq$, ossia $d | a$. Similmente $d | b$.

Per dimostrare che d è un MCD di a e b resta da dimostrare che se $c \in \mathbb{Z}$, $c | a$ e $c | b$, allora $c | d$. Ora se $c | a$ e $c | b$, si ha $a = a'c$, $b = b'c$ con $a', b' \in \mathbb{Z}$, e quindi $d = \alpha a + \beta b = (\alpha a' + \beta b')c$, cioè $c | d$. Questo conclude la dimostrazione. \square

Si noti che se d è un MCD di a e b , allora $d \neq 0$, perché a e b non sono entrambi nulli. (Infatti se 0 fosse un MCD di a e b , allora $0 | a$ e $0 | b$, da cui $a = 0 \cdot a'$ e $b = 0 \cdot b'$ per opportuni $a', b' \in \mathbb{Z}$. Ma allora $a = 0$ e $b = 0$ sarebbero entrambi nulli).

4.4 PROPOSIZIONE. Se a, b sono numeri interi non entrambi nulli, ci sono esattamente due loro MCD, uno l'opposto dell'altro.

Dimostrazione. Siano d_1 e d_2 due MCD di a e b . Allora per la (a) della definizione di MCD si ha che $d_1 \mid a$ e $d_1 \mid b$. Dato che d_2 è MCD di a e b , per la (b) della definizione ne segue che $d_1 \mid d_2$. Analogamente $d_2 \mid d_1$. Quindi $d_2 = xd_1$ e $d_1 = yd_2$ per opportuni $x, y \in \mathbb{Z}$. In particolare $d_2 = xd_1 = xyd_2$, ed essendo $d_2 \neq 0$ se ne deduce $xy = 1$, e quindi $x = 1$ oppure $x = -1$. Pertanto $d_2 = d_1$, oppure $d_2 = -d_1$. \square

Dalla proposizione 4.4 segue che se a e b sono numeri interi non entrambi nulli, allora a e b hanno un unico MCD positivo, che verrà da noi indicato con (a, b) . L'altro MCD di a e b è pertanto $-(a, b)$.

Due numeri interi a, b si dicono *primi tra loro* (o *relativamente primi*) se $(a, b) = 1$, cioè se 1 è un loro MCD.

4.5 COROLLARIO. Siano $a, b \in \mathbb{Z}$. Le seguenti affermazioni sono equivalenti:

- (a) a e b sono primi tra loro;
- (b) esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$.

Dimostrazione. (a) \Rightarrow (b). Se a e b sono primi tra loro, cioè se $(a, b) = 1$, allora per il teorema 4.3 esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$.

(b) \Rightarrow (a). Supponiamo che esistano $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta b = 1$. Mostriamo che 1 è un MCD di a e b . Ovviamente $1 \mid a$ e $1 \mid b$. Supponiamo che $c \in \mathbb{Z}$, $c \mid a$ e $c \mid b$. Allora $a = a'c$ e $b = b'c$ con $a', b' \in \mathbb{Z}$, e quindi $1 = \alpha a + \beta b = (\alpha a' + \beta b')c$, ossia $c \mid 1$. Quindi 1 è un MCD di a e b . \square

Se a, b sono due numeri interi, 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 $[a, b]$.

Per calcolare l'MCD esiste il metodo seguente, detto *algoritmo di Euclide*.

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

$$\begin{aligned} r_{-1} &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ r_2 &= r_3 q_4 + r_4 \\ r_3 &= r_4 q_5 + r_5 \\ &\dots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \end{aligned}$$

$$\begin{aligned}r_{n-2} &= r_{n-1}q_n + r_n \\r_{n-1} &= r_nq_{n+1}\end{aligned}$$

ove i q_i e gli r_i sono i quoti e i resti delle $n+1$ 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 un MCD di a e b .

Dimostrazione. La successione termina perché per la prima divisione $0 \leq r_1 < |b|$, per la seconda $0 \leq r_2 < r_1$, per la terza $0 \leq r_3 < r_2, \dots$. In definitiva si ha la successione strettamente decrescente $|b| > r_1 > r_2 > r_3 > \dots$ in \mathbb{N} , che quindi deve terminare dopo un numero finito di passi. Questo prova (a). Inoltre $r_n \mid r_{n-1}$, e quindi per la penultima riga $r_n \mid r_{n-2}$. “Risalendo” la successione di divisioni, si ottiene successivamente $r_n \mid r_{n-3}, \dots, r_n \mid r_3, r_n \mid r_2, r_n \mid r_1, r_n \mid r_0 = b, r_n \mid r_{-1} = a$. Quindi r_n divide a e b . Se poi $c \in \mathbb{Z}$, $c \mid a$ e $c \mid b$, cioè $c \mid r_{-1}$ e $c \mid r_0$, allora per la prima divisione della successione $c \mid r_1$, per la seconda $c \mid r_2, \dots$ “Scendendo” la successione di divisioni si ha successivamente $c \mid r_3, \dots, c \mid r_{n-1}, c \mid r_n$. Questo prova che $c \mid r_n$. Quindi r_n è un MCD di a e b . \square

4.7 ESEMPIO. Calcoliamo il MCD positivo di 1956 e 1992 facendo uso dell’algoritmo di Euclide.

Si ha

$$\begin{aligned}1956 &= 0 \cdot 1992 + 1956; \\1992 &= 1956 \cdot 1 + 36; \\1956 &= 36 \cdot 54 + 12; \\36 &= 12 \cdot 3.\end{aligned}$$

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

4.8 ESEMPIO. Determinare il MCD positivo di 987 654 321 e 98 765 432.

Si ha

$$\begin{aligned}987\,654\,321 &= 98\,765\,432 \cdot 10 + 1; \\98\,765\,432 &= 1 \cdot 98\,765\,432.\end{aligned}$$

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

Principio di induzione

Di fondamentale importanza per la matematica sono le *dimostrazioni per induzione*. Le dimostrazioni per induzione si applicano per verificare che una certa asserzione P , cioè una certa proprietà P , vale per tutti i numeri naturali $n \in \mathbb{N}$. Per verificare che P vale per tutti i numeri naturali è sufficiente dimostrare che:

- (a) la proprietà P vale per il numero $n = 0$;
- (b) per ogni $n \in \mathbb{N}$, $n > 0$, se la proprietà P vale per il numero $n - 1$, allora P vale anche per il numero n .

4.9 ESEMPIO. Vogliamo verificare che la somma $1 + q + q^2 + \cdots + q^n$ delle potenze da 0 a n di un numero reale $q \neq 1$ è $(1 - q^{n+1})/(1 - q)$. In questo caso la proprietà P è

$$1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q} \quad \text{per ogni numero reale } q \neq 1.$$

Dobbiamo verificare:

- (a) che la proprietà P vale per $n = 0$; questo è vero perché $1 = (1 - q^{0+1})/(1 - q)$;
- (b) supposto ora che $1 + q + q^2 + \cdots + q^{n-1} = (1 - q^n)/(1 - q)$ dobbiamo verificare che $1 + q + q^2 + \cdots + q^n = (1 - q^{n+1})/(1 - q)$. Anche questo è vero perché

$$1 + q + q^2 + \cdots + q^n = (1 + q + q^2 + \cdots + q^{n-1}) + q^n = \frac{1 - q^n}{1 - q} + q^n$$

(per l'*ipotesi induttiva*), e questo è uguale a

$$\frac{1 - q^n + (1 - q)q^n}{1 - q} = \frac{1 - q^{n+1}}{1 - q}.$$

Quindi l'uguaglianza è stata dimostrata per ogni numero naturale n . \square

Il metodo sopra esposto è utile nel verificare asserzioni riguardanti i numeri naturali, cioè i numeri interi $n \geq 0$, e si generalizza facilmente alla verifica di proprietà dei numeri interi n maggiori o uguali ad un numero intero fissato n_0 :

4.10 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 $n \geq n_0$.

A volte può essere utile applicare il principio di induzione in una forma un po' diversa. Sarebbe possibile dimostrare infatti che il principio di induzione nella forma appena enunciata è equivalente al principio di induzione enunciato nella forma seguente:

4.11 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.

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

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

Dobbiamo dimostrare che l'uguaglianza $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ 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 $1 \cdot (1 + 1)/2$ nel membro a destra. Quindi il caso $n = 1$ è verificato. Supponiamo ora che l'uguaglianza sia vera per $n - 1$, cioè che $1 + 2 + 3 + \cdots + (n - 1) = (n - 1)n/2$. Allora

$$\begin{aligned} 1 + 2 + 3 + \cdots + n &= [1 + 2 + 3 + \cdots + (n - 1)] + n \\ &= \frac{(n - 1)n}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n^2 + n}{2} = \frac{n(n + 1)}{2}, \end{aligned}$$

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

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

Dobbiamo dimostrare che l'uguaglianza $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$ 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 $1 + 3 + 5 + 7 + \cdots + (2n - 3) = (n - 1)^2$. Allora $1 + 3 + 5 + 7 + \cdots + (2n - 1) = [1 + 3 + 5 + 7 + \cdots + (2n - 3)] + (2n - 1) = (n - 1)^2 + (2n - 1) = n^2$, 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

4.14 ESEMPIO. Dimostriamo per induzione che per ogni intero $n \geq 2$ si ha

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \cdots \left(1 - \frac{1}{n}\right) = \frac{1}{n}.$$

Per $n = 2$ si ha ovviamente $1 - (1/2) = 1/2$. Supponiamo ora che $(1 - 1/2)(1 - 1/3) \cdots (1 - 1/(n - 1)) = 1/(n - 1)$ e proviamo che $(1 - 1/2)(1 - 1/3) \cdots (1 - 1/n) = 1/n$. Per fare questo è sufficiente osservare che $(1 - 1/2)(1 - 1/3) \cdots (1 - 1/(n - 1))(1 - 1/n)$ è uguale per l'ipotesi induttiva a

$$\frac{1}{n - 1} \left(1 - \frac{1}{n}\right) = \frac{1}{n - 1} \frac{n - 1}{n} = \frac{1}{n}. \quad \square$$

4.15 ESEMPIO. 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 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 $a | c$ e $b | c$ si ha $m | c$. Inoltre $a | m'$ e $b | m'$. Quindi $m | m'$. Analogamente $m' | m$. 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 $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, eccetera.

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

$3! + \dots + c_\ell \cdot \ell! + c_h \cdot h!$, 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 $0 | a$ se e solo se $a = 0$.

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

4.9. Sia $a \in \mathbb{Z}$. Si dimostri che $a | 1$ 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 $p | ab$, allora $p | a$ oppure $p | b$. [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. Si dimostri che se $a \in \mathbb{Z}$, allora 0 è l'unico mcm di a e 0 .

4.13. Si è già visto nelle scuole inferiori che se a, b sono due numeri interi entrambi non nulli, scritto $a = \pm p_1^{n_1} \cdots p_t^{n_t}$, $b = \pm p_1^{m_1} \cdots p_t^{m_t}$, ove p_1, \dots, p_t sono primi positivi distinti ed $n_1, \dots, n_t, m_1, \dots, m_t$ sono numeri interi ≥ 0 , allora $(a, b) = p_1^{\ell_1} \cdots p_t^{\ell_t}$ e $[a, b] = p_1^{f_1} \cdots p_t^{f_t}$, ove, per ogni $i = 1, \dots, t$, ℓ_i è il minimo tra n_i ed m_i ed f_i è il massimo tra n_i ed m_i . Usando questo fatto si provi che $(a, b)[a, b] = |ab|$.

4.14. 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.

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

Si dimostrino le uguaglianze degli esercizi 4.16–4.19 per induzione su n :

4.16. La somma $1^2 + 2^2 + 3^2 + \dots + n^2$ dei quadrati dei primi n numeri interi positivi è uguale a $n(n+1)(2n+1)/6$.

4.17. $1^3 + 2^3 + 3^3 + \dots + n^3 = (n(n+1)/2)^2$.

4.18. $1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \dots + 1/(n(n+1)) = n/(n+1)$.

4.19. Se $x, y \in \mathbb{R}$, allora $x + (x+y) + (x+2y) + \dots + (x+ny) = (n+1)(2x+ny)/2$ per ogni $n \in \mathbb{N}^*$.

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

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

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

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

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

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

4.24. Dimostrare che per ogni intero positivo n si ha

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

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

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

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

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

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

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

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

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

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

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

²Quasi tutte le formule che si incontrano in questa sezione sono note da moltissimo tempo. Ad esempio la formula di questo esercizio si trova nel *Talckys* di Ibn Albanna del tredicesimo secolo.

Appendice 4.1. Il sistema posizionale in base b

Sia $b \geq 2$ un numero naturale. Ad ogni numero naturale $< b$ si associa un simbolo, detto *cifra*. Ad esempio, nel sistema posizionale decimale, cioè in base $b = 10$, che è quello che usiamo più di frequente, ai primi dieci numeri naturali si associano le cifre 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Useremo queste b cifre per denotare i numeri naturali $< b$. Dato ora un qualunque numero naturale $n > 0$, possiamo rappresentare in base b il numero n in modo unico nella forma $c_N c_{N-1} \dots c_1 c_0$, dove $c_N, c_{N-1}, \dots, c_1, c_0$ sono le cifre associate ai numeri naturali $a_N, a_{N-1}, \dots, a_1, a_0 < b$ tali che $n = \sum_{i=0}^N a_i b^i$ e $a_N \neq 0$.

Scriveremo $\alpha = c_N c_{N-1} \dots c_1 c_0$ per dire che α si scrive $c_N c_{N-1} \dots c_1 c_0$ in base b , anche se in realtà α e la sua rappresentazione in base b sono due cose totalmente diverse: α è un elemento di \mathbb{N} , mentre $c_N c_{N-1} \dots c_1 c_0$ è una sequenza di simboli (le b cifre).

Si noti che i numeri naturali $a_N, a_{N-1}, \dots, a_1, a_0 < b$ tali che $n = \sum_{i=0}^N a_i b^i$ e $a_N \neq 0$ sono univocamente determinati, in quanto a_0 è il resto della divisione di n per b , e se q_0 è il quoto di questa divisione ($n = bq_0 + a_0$, $a_0 < b$), allora a_1 è il resto della divisione di q_0 per b , eccetera. I numeri $a_0, a_1, \dots, a_{N-1}, a_N$ sono quindi univocamente determinati in quanto sono i resti nella seguente successione di divisioni:

$$\begin{aligned}
 n &= bq_0 + a_0 \\
 q_0 &= bq_1 + a_1 \\
 q_1 &= bq_2 + a_2 \\
 &\vdots \\
 q_{N-2} &= bq_{N-1} + a_{N-1} \\
 q_{N-1} &= bq_N + a_N
 \end{aligned}
 \tag{4.1}$$

dove la successione termina non appena si trova un quoto $q_N = 0$. Si osservi che la successione termina sempre in un numero finito di passi, in quanto, dato che $b \geq 2$, si ha $n > q_0 > q_1 > q_2 > \dots$.

4.16 ESEMPIO. Se n è il numero che in base 10 si scrive 1243, come si scrive n in base 6? (Qui, come si fa di consueto, supporremo che le cifre scelte per indicare i primi 6 numeri naturali in base 6 siano 0, 1, 2, 3, 4, 5.)

La successione di divisioni (4.1) è in questo caso la seguente

$$\begin{aligned}
 1234 &= 6 \cdot 205 + 4 \\
 205 &= 6 \cdot 34 + 1 \\
 34 &= 6 \cdot 5 + 4 \\
 5 &= 6 \cdot 0 + 5.
 \end{aligned}$$

I resti sono 4, 1, 4, 5. Quindi n in base 6 si scrive 5414. \square

In modo del tutto analogo si procede per rappresentare in base b un qualunque numero reale $\alpha \geq 0$. Osserviamo innanzi tutto che ogni numero reale $\alpha \geq 0$ si può scrivere in

modo unico nella forma $\alpha = [\alpha] + \text{frac}(\alpha)$, dove $[\alpha]$ è un numero naturale e $\text{frac}(\alpha)$ è un numero reale con $0 \leq \text{frac}(\alpha) < 1$. Il numero naturale $[\alpha]$ si dice la *parte intera* di α , mentre $\text{frac}(\alpha)$ è detto impropriamente la *parte frazionaria* di α . Se α è un numero reale ≥ 0 , sappiamo già rappresentare la sua parte intera $[\alpha]$ nella forma $c_N c_{N-1} \dots c_1 c_0$. Anche per rappresentare il numero reale $\text{frac}(\alpha)$ faremo uso di divisioni successive, ma usando questa volta una divisione particolare, differente dalla divisione vista a pagina 28. Se $\alpha \geq 0$ e $\beta > 0$ sono due numeri reali, esiste un'unica coppia $(q, \varrho) \in \mathbb{N} \times \mathbb{R}$ tale che

$$\alpha = \beta q + \varrho \quad \text{e} \quad 0 \leq \varrho < \beta.$$

(Basta prendere come q la parte intera di α/β e come ϱ il numero reale $\beta \text{frac}(\alpha/\beta)$.) Chiamiamo q e ϱ rispettivamente il *quofo* e il *resto* della divisione di α per β . Per ogni $i \geq 1$ siano ora a_{-i} i numeri naturali $< b$ ottenuti come quoti nella successione infinita di divisioni:

$$(4.2) \quad \begin{aligned} \text{frac}(\alpha) &= a_{-1} b^{-1} + \varrho_1 \\ \varrho_1 &= a_{-2} b^{-2} + \varrho_2 \\ \varrho_2 &= a_{-3} b^{-3} + \varrho_3 \\ \varrho_3 &= a_{-4} b^{-4} + \varrho_4 \\ &\vdots \end{aligned}$$

Eliminando $\varrho_1, \varrho_2, \dots, \varrho_{n-1}$ nelle prime n di queste uguaglianze si vede che

$$\text{frac}(\alpha) = \sum_{i=1}^n a_{-i} b^{-i} + \varrho_n$$

per ogni $n \geq 1$. Dato che ϱ_n è il resto di una divisione per b^{-n} , deve quindi essere

$$(4.3) \quad 0 \leq \text{frac}(\alpha) - \sum_{i=1}^n a_{-i} b^{-i} = \varrho_n < b^{-n}.$$

Mostriamo che $a_{-n} < b$ per ogni $n \geq 1$. Per $n = 1$ si ha che il quofo a_{-1} della divisione di $\text{frac}(\alpha)$ per b^{-1} è la parte intera di $\text{frac}(\alpha)/b^{-1} = \text{frac}(\alpha)b < b$, e quindi $0 \leq a_{-1} < b$. Per $n > 1$ dalla (4.3) si ha che $0 \leq \varrho_{n-1} < b^{-(n-1)}$. Quindi il quofo a_{-n} della divisione di ϱ_{n-1} per b^{-n} è la parte intera di $\varrho_{n-1}/b^{-n} = \varrho_{n-1} b^n < b$, e pertanto $a_{-n} < b$.

La (4.3) ci dice, come si vedrà nel corso di analisi matematica, che $\text{frac}(\alpha)$ è la somma della serie

$$\text{frac}(\alpha) = \sum_{i=1}^{+\infty} a_{-i} b^{-i}.$$

Se c_{-i} è la cifra associata ad a_{-i} per ogni $i \geq 1$, rappresenteremo α nella forma

$$\alpha = c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots$$

con infinite cifre dopo la virgola, eventualmente tutte denotanti il numero zero da un certo punto in poi.

Si osservi che i numeri naturali $a_{-i} < b$ non possono essere del tutto arbitrari. Se ad esempio si avesse $a_{-i} = b - 1$ per ogni $i \geq 1$, allora si avrebbe che $\text{frac}(\alpha) = \sum_{i=1}^{+\infty} a_{-i} b^{-i} = \sum_{i=1}^{+\infty} (b - 1) b^{-i}$, e, come si vedrà nel corso di analisi matematica, $\sum_{i=1}^{+\infty} (b - 1) b^{-i} = 1$. Questo è assurdo, perché non si può avere $\text{frac}(\alpha) = 1$ per nessun numero reale α .³ Con qualche conoscenza di analisi matematica in più non sarebbe difficile vedere che questa è essenzialmente l'unica eccezione. Si trova pertanto che ogni numero reale $\alpha \geq 0$ si scrive in modo unico nella forma $c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots$ dove non esiste $p \in \mathbb{N}$ tale che $c_{-p}, c_{-(p+1)}, c_{-(p+2)}, \dots$ denotino tutti il numero $b - 1$. Si ha pertanto una corrispondenza biunivoca tra l'insieme degli allineamenti di cifre $c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots$ di questo tipo e l'insieme \mathbb{R} dei numeri reali.

Fissiamo un numero intero $b \geq 2$. Diciamo che la rappresentazione

$$c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots$$

in base b di un numero reale $\alpha \geq 0$ è *periodica* se esistono due interi $p \geq 1$ e $q \geq 0$ tali che $c_{-i} = c_{-(i+p)}$ per ogni $i > q$, ossia se la rappresentazione è del tipo

$$\begin{aligned} &c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots c_{-q} c_{-(q+1)} c_{-(q+2)} \dots \\ &\quad c_{-(q+p)} c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)} c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)} \dots \end{aligned}$$

Per comodità di notazione scriveremo di solito una tale rappresentazione nella forma

$$\alpha = c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots c_{-q} \overline{c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)}},$$

e diremo che $c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)}$ è il *periodo* e $c_{-1} c_{-2} c_{-3} \dots c_{-q}$ è l'*antiperiodo*.

4.17 PROPOSIZIONE. *La rappresentazione di un numero $\alpha \geq 0$ è periodica se e solo se $\alpha \in \mathbb{Q}$.*

Dimostrazione. Supponiamo che la rappresentazione del numero $\alpha \geq 0$ sia periodica:

$$\alpha = c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots c_{-q} \overline{c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)}}.$$

Allora

$$^* b^q \alpha = c_N c_{N-1} \dots c_1 c_0 c_{-1} c_{-2} c_{-3} \dots c_{-q} \overline{c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)}}$$

e

$$\begin{aligned} b^{p+q} \alpha &= c_N c_{N-1} \dots c_1 c_0 c_{-1} c_{-2} c_{-3} \dots c_{-(q-1)} c_{-q} c_{-(q+1)} \dots \\ &\quad c_{-(q+p)}, \overline{c_{-(q+1)} c_{-(q+2)} \dots c_{-(q+p)}}. \end{aligned}$$

³Per convincersi ulteriormente di questo fatto, si osservi che tra due numeri reali distinti è sempre possibile trovare almeno un ulteriore numero reale intermedio. Che numero reale si riuscirebbe a scrivere tra i numeri reali 0,99999... e 1, se fossero distinti?

Sottraendo membro a membro si trova che $b^{p+q}\alpha - b^q\alpha$ è il numero naturale $m = c_N c_{N-1} \dots c_{-(q+p)} - c_N c_{N-1} \dots c_{-q}$. Quindi $\alpha = m/(b^{p+q} - b^q) \in \mathbb{Q}$.

Viceversa supponiamo che $\alpha \in \mathbb{Q}$, cioè che $\alpha = m/n$ per opportuni interi $m \geq 0, n > 0$. Dividendo m per n si trovano due numeri naturali q_0, r tali che $m = nq_0 + r$ e $r < n$. Allora $\alpha = \frac{m}{n} = q_0 + \frac{r}{n}$, e quindi $[\alpha] = q_0$ e $\text{frac}(\alpha) = \frac{r}{n}$. Chiaramente la rappresentazione di α è periodica se e solo se la rappresentazione di $\text{frac}(\alpha)$ è periodica, e quindi dimostreremo che la rappresentazione di $\frac{r}{n} = \text{frac}(\alpha)$ è periodica. Per determinare le cifre c_{-i} di $\text{frac}(\alpha)$ eseguiamo le divisioni della successione (4.2), ossia troviamo i numeri naturali $a_{-i} < b$ e i numeri reali ϱ_i tali che

$$(4.4) \quad \begin{aligned} \frac{r}{n} &= a_{-1}b^{-1} + \varrho_1 & 0 \leq \varrho_1 < b^{-1} \\ \varrho_1 &= a_{-2}b^{-2} + \varrho_2 & 0 \leq \varrho_2 < b^{-2} \\ \varrho_2 &= a_{-3}b^{-3} + \varrho_3 & 0 \leq \varrho_3 < b^{-3} \\ \varrho_3 &= a_{-4}b^{-4} + \varrho_4 & 0 \leq \varrho_4 < b^{-4} \\ &\vdots & \end{aligned}$$

Poniamo $\varrho_0 = \frac{r}{n}$. Per ogni $i \geq 1$ la i -esima riga di (4.4) dice quindi che $\varrho_{i-1} = a_{-i}b^{-i} + \varrho_i$ e $0 \leq \varrho_i < b^{-i}$. Moltiplicando per nb^i si trova che

$$(4.5) \quad \varrho_{i-1}nb^i = a_{-i}n + \varrho_i nb^i \quad \text{e} \quad 0 \leq \varrho_i nb^i < n$$

per ogni $i \geq 1$.

Mostriamo per induzione che per ogni $i \geq 1$ si ha che $\varrho_{i-1}nb^{i-1}$ è un numero intero e che a_{-i} e $\varrho_i nb^i$ sono rispettivamente il quoto e il resto della divisione del numero intero $(\varrho_{i-1}nb^{i-1})b$ per n . Per $i = 1$ si ha che $\varrho_0n = \frac{r}{n}n = r$ è un numero intero. Inoltre le (4.5) diventano $\varrho_0nb = a_{-1}n + \varrho_1nb$ e $0 \leq \varrho_1nb < n$. Quindi a_{-1} e ϱ_1nb sono proprio il quoto e il resto della divisione del numero intero $(\varrho_0n)b = rb$ per n . Questo conclude la dimostrazione per il caso $i = 1$. Supponiamo ora $i > 1$ e di sapere già che il numero $\varrho_{i-2}nb^{i-2}$ è intero e che $a_{-(i-1)}$ e $\varrho_{i-1}nb^{i-1}$ sono rispettivamente il quoto e il resto della divisione del numero intero $(\varrho_{i-2}nb^{i-2})b$ per n . In particolare il numero $\varrho_{i-1}nb^{i-1}$ è intero, perché resto della divisione tra due interi. Quindi anche $\varrho_{i-1}nb^i$ è intero. La (4.5) ci dice ora che a_{-i} e $\varrho_i nb^i$ sono il quoto e il resto della divisione del numero intero $(\varrho_{i-1}nb^{i-1})b$ per n . Questo conclude l'induzione. Ora sappiamo che per ogni $i \geq 1$ i numeri $\varrho_i nb^i$ sono interi e che $0 \leq \varrho_i nb^i < n$. Dato che ci sono solo un numero finito di interi tra 0 ed n , almeno due di questi $\varrho_i nb^i$ devono coincidere, e quindi devono esistere due interi $p \geq 1$ e $q \geq 0$ tali che $\varrho_q nb^q = \varrho_{q+p} nb^{q+p}$.

Mostriamo per induzione che $\varrho_i nb^i = \varrho_{i+p} nb^{i+p}$ per ogni $i \geq q$. Sappiamo già che questo è vero per $i = q$. Supponiamo che sia vero per $i - 1$, cioè che $\varrho_{i-1}nb^{i-1} = \varrho_{i-1+p} nb^{i-1+p}$. Allora, dato che $\varrho_i nb^i$ è il resto della divisione del numero intero $(\varrho_{i-1}nb^{i-1})b$ per n , e $\varrho_{i+p} nb^{i+p}$ è il resto della divisione dello stesso numero $(\varrho_{i-1+p} nb^{i-1+p})b$ per n , dovremo avere necessariamente che i resti coincidono, ossia che $\varrho_i nb^i = \varrho_{i+p} nb^{i+p}$. Abbiamo così dimostrato che $\varrho_i nb^i = \varrho_{i+p} nb^{i+p}$ per ogni $i \geq q$.

Quindi le divisioni (4.5) si ripetono ciclicamente con periodo p per $i > q$. In particolare i quoti a_{-i} devono ripetersi ciclicamente con periodo p per $i > q$, ossia $a_{-i} = a_{-(i+p)}$ per ogni $i > q$. Questo mostra che la rappresentazione di α in base b è periodica. \square

Dalla proposizione 4.17 si vede quindi in particolare che il fatto che un certo numero abbia una rappresentazione periodica in una certa base b non dipende dalla base b fissata, ma solo da α , ossia che se un certo α ha una rappresentazione periodica in una certa base b , allora la rappresentazione di α in una qualunque altra base $b' \neq b$, $b' \geq 2$, sarà sempre periodica.

Si noti infine un'altra conseguenza della proposizione 4.17. Dato un numero reale α arbitrario, non è affatto detto che la sua parte frazionaria $\text{frac}(\alpha)$ sia un numero razionale, cioè una frazione di due numeri interi. Questo è il motivo per cui a pagina 39 abbiamo detto che il termine *parte frazionaria* era improprio: $\text{frac}(\alpha)$ si dice parte frazionaria, ma non è detto che sia una frazione!

Altri esercizi

- 4.31. Si scriva in base 12 il numero che in base 10 si scrive 1234. (Come cifre prendere i simboli 0, 1, 2, ..., 9, A, B.)
- 4.32. Scrivere il numero 5 in base 2.
- 4.33. Scrivere il numero 124 in base 2.
- 4.34. Scrivere in notazione binaria, cioè in base 2, i numeri che in notazione decimale, cioè in base 10, si scrivono 9, 15, 21, 32, 37, 68, 100.
- 4.35. Scrivere in notazione decimale i numeri che in notazione binaria si scrivono 101, 110, 1110, 11011, 101001, 111101.
- 4.36. Sia $b \geq 2$ un numero naturale. Come si scrive b in base b ?
- 4.37. Se α in base b si scrive $0.\overline{1}$, come si scrive α come frazione m/n con m, n interi?
- 4.38. Si scriva in notazione decimale $1/7$.
- 4.39. La dimostrazione della proposizione 4.17 fa vedere come si può scrivere un numero razionale nella forma di frazione m/n a partire dalla sua rappresentazione decimale. Si scriva nella forma m/n il numero $1,\overline{234}$.
- 4.40. Il numero $\alpha = 0,10110111011110111110\dots$ è razionale?
- 4.41. Quante cifre sono necessarie per scrivere in base b i numeri $< n$?
- 4.42. Sia $2 \leq b \leq 10$. In base b usiamo come cifre i simboli 0, 1, 2, ... fino alla cifra usata in base 10 per denotare il numero $b - 1$. In quale base b si ha che
 - (a) $61 + 6 = 100$?
 - (b) $61 - 1 = 60$?

(c) $14 + 14 = 33?$

§5. Numeri complessi

Sia \mathbb{R} l'insieme dei numeri reali e $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ il prodotto cartesiano di \mathbb{R} per \mathbb{R} . Gli elementi di \mathbb{C} , ossia le coppie ordinate (a, b) con a e b reali, sono detti *numeri complessi*. Se $z = (a, b)$ e $z' = (a', b')$ sono due numeri complessi, definiamo la loro somma $z + z'$ e il loro prodotto zz' mediante le formule

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

In questo modo $z + z'$ e zz' sono ancora due numeri complessi. Il lemma seguente mostra che con queste definizioni di somma e prodotto valgono le usuali proprietà del calcolo letterale, quali l'associatività, la commutatività, la distributività, ecc.

5.1 LEMMA. *Per ogni $z = (a, b), z' = (a', b'), z'' = (a'', b'') \in \mathbb{C} = \mathbb{R} \times \mathbb{R}$ 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

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

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

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

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

- (d) $zz' = (a,b)(a',b') = (aa' - bb', ab' + ba') = (a'a - b'b, a'b + b'a) = z'z$.
 (e) Si ha

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

(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

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

Conformemente all'uso, indicheremo il numero complesso $(a,0)$ con il simbolo a . In questo modo i numeri complessi del tipo $(a,0)$, ossia le coppie di numeri reali (a,b) con $b = 0$, vengono identificati con il corrispondente numero reale a . Si noti che questa identificazione "conserva" la somma e il prodotto, in quanto se $z = (a,0)$ e $z' = (a',0)$, allora in base alle definizioni precedenti $z + z' = (a + a', 0)$ e $zz' = (aa', 0)$. Quindi per quanto riguarda l'addizione e la moltiplicazione un numero complesso del tipo $(a,0)$ si può trattare come il corrispondente numero reale a .

Indicheremo inoltre con il simbolo i il numero complesso $(0,1)$. Tale numero è detto *unità immaginaria*, e si ha $i^2 = i \cdot i = (0,1)(0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -1$. Quindi in base all'identificazione appena vista $i^2 = -1$, ossia i è una radice quadrata di -1 .

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

Si ha

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

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

5.3 ESEMPIO. 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 5.3 il numero complesso (a, b) è uguale ad $a + ib$, e pertanto i numeri complessi sono tutti e soli del tipo $a + ib$, con $a, b \in \mathbb{R}$, cioè

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

Naturalmente se $a, a', b, b' \in \mathbb{R}$, si ha che i numeri complessi $a + ib$ e $a' + ib'$ sono uguali se e solo se $(a, b) = (a', b')$, e quindi se e solo se $a = a'$ e $b = b'$.

Denotare i numeri complessi nella forma $a + ib$ è particolarmente conveniente. Infatti per sommare o moltiplicare due numeri $a + ib$ e $a' + ib'$ è possibile operare applicando le usuali regole del calcolo letterale (quelle del lemma 5.1) con l'avvertenza di porre -1 al posto di i^2 .

5.4 ESEMPIO. Si ha

$$(a + ib)(a' + ib') = aa' + aib' + iba' + i^2bb' = (aa' - bb') + i(ab' + ba').$$

Si noti che questa uguaglianza equivale all'uguaglianza

$$(a, b)(a', b') = (aa' - bb', ab' + ba')$$

che è proprio la definizione di prodotto di due numeri complessi. \square

5.5 ESEMPIO. Si ha

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

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

$$(1 + i3)(-4 + i\sqrt{2}) = -4 + i\sqrt{2} - i12 + i^23\sqrt{2} = (-4 - 3\sqrt{2}) + i(\sqrt{2} - 12);$$

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

Si osservi come si è 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:

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

Se $z = a + ib \in \mathbb{C}$ ($a, b \in \mathbb{R}$), diremo che a è la *parte reale* di z e che ib è la *parte immaginaria* di z .

Fissiamo ora un sistema di coordinate cartesiane ortogonali x, y su un piano (che chiameremo *piano di Argand-Gauss*). Ogni numero complesso $a + ib$ può essere rappresentato geometricamente dal punto del piano di coordinate (a, b) . Si ha così una corrispondenza biunivoca tra l'insieme \mathbb{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 quindi rappresentati come i punti del piano di Argand-Gauss.

Si noti che i numeri reali $a = a + i0$ corrispondono ai punti di coordinate $(a, 0)$ e che questi punti sono esattamente i punti dell'asse x . L'asse x viene detto pertanto l'*asse reale*. L'asse y si dice invece l'*asse immaginario*. La distanza del punto di coordinate (a, b) dall'origine, cioè il numero reale non negativo $\varrho = \sqrt{a^2 + b^2}$, è detto il *modulo* (o il *valore assoluto*) del numero complesso $z = a + ib$, ed è denotato con $|z|$:

$$|z| = \sqrt{a^2 + b^2}.$$

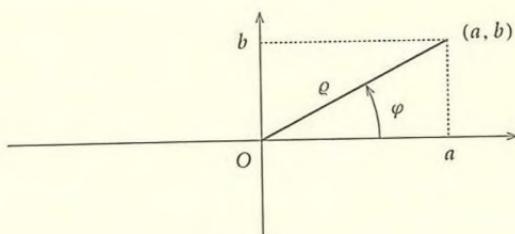


FIGURA 5.1.

Un punto P di coordinate (a, b) può essere anche individuato mediante le misure della distanza $\varrho = \sqrt{a^2 + b^2}$ e dell'angolo orientato φ formato dal semiasse positivo delle x e dalla semiretta di origine O e passante per P .

Il numero reale φ è detto *argomento* (o *anomalia*) di $z = a + ib$; naturalmente se φ è un argomento di $z = a + ib$ anche $\varphi + 2h\pi$ è un argomento di z per ogni $h \in \mathbb{Z}$. Inoltre φ non è determinato se $P = O$, cioè se $z = 0$. Quindi un numero complesso diverso da zero determina univocamente il proprio modulo, ma determina il proprio argomento solo a meno di multipli interi di 2π .

Per la definizione di seno e coseno si ha

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

e quindi

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

È così possibile scrivere un numero complesso $z = a + ib$ nella *forma trigonometrica* $\varrho(\cos \varphi + i \sin \varphi)$, ove ϱ è un numero reale non negativo (il modulo di z) e φ è un numero reale (l'argomento di z). Naturalmente due numeri non nulli $\varrho(\cos \varphi + i \sin \varphi)$ e $\varrho'(\cos \varphi' + i \sin \varphi')$ scritti in forma trigonometrica sono uguali se e solo se i loro moduli ϱ e ϱ' coincidono e i loro argomenti φ e φ' differiscono per un multiplo intero di 2π .

La scrittura in forma trigonometrica è particolarmente conveniente nell'eseguire la moltiplicazione tra due numeri complessi: se $z = \varrho(\cos \varphi + i \sin \varphi)$ e $z' = \varrho'(\cos \varphi' + i \sin \varphi')$, con $\varrho, \varrho', \varphi, \varphi' \in \mathbb{R}$, $\varrho \geq 0$ e $\varrho' \geq 0$, allora

$$\begin{aligned} zz' &= [\varrho(\cos \varphi + i \sin \varphi)][\varrho'(\cos \varphi' + i \sin \varphi')] \\ &= \varrho\varrho'[(\cos \varphi \cos \varphi' - \sin \varphi \sin \varphi') + i(\cos \varphi \sin \varphi' + \sin \varphi \cos \varphi')] \\ &= (\varrho\varrho')[\cos(\varphi + \varphi') + i \sin(\varphi + \varphi')]. \end{aligned}$$

Abbiamo così dimostrato che:

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

Da questa proposizione si deduce il corollario seguente:

5.7 COROLLARIO (FORMULA DI DE MOIVRE). *Se $z = \varrho(\cos \varphi + i \sin \varphi)$ è un numero complesso scritto in forma trigonometrica e $n \in \mathbb{N}$, allora*

$$z^n = \varrho^n(\cos n\varphi + i \sin n\varphi).$$

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

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

e quindi in questo caso l'uguaglianza è vera. Supponiamo poi che l'uguaglianza sia vera per $n - 1$, cioè che $z^{n-1} = \varrho^{n-1}(\cos(n-1)\varphi + i \sin(n-1)\varphi)$, vale a dire che il modulo di z^{n-1} sia ϱ^{n-1} e che il suo argomento sia $(n-1)\varphi$. Allora per la proposizione 5.6

$z^n = z^{n-1}z$ ha come modulo $\varrho^{n-1}\varrho = \varrho^n$ e come argomento $(n-1)\varphi + \varphi = n\varphi$. Quindi

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

Applichiamo la formula di De Moivre al calcolo delle soluzioni $z \in \mathbb{C}$ dell'equazione $x^n - 1 = 0$, ove $n \geq 1$ è un intero. Le soluzioni di tale equazione, ossia i numeri complessi z tali che $z^n = 1$, sono dette le *radici n-esime dell'unità*. Per calcolare i numeri complessi z tali che $z^n = 1$ scriviamo z in forma trigonometrica,

$$z = \varrho(\cos \varphi + i \sin \varphi),$$

ove ϱ è il modulo di z ($\varrho \in \mathbb{R}, \varrho \geq 0$) e φ è l'argomento di z ($\varphi \in \mathbb{R}$). L'uguaglianza $z^n = 1$ equivale per la formula di De Moivre all'uguaglianza $\varrho^n(\cos n\varphi + i \sin n\varphi) = 1$. Ma il numero 1 ha modulo 1 e argomento 0, e quindi i due numeri complessi $\varrho^n(\cos n\varphi + i \sin n\varphi)$ e $1 = 1 \cdot (\cos 0 + i \sin 0)$ coincidono se e solo se $\varrho^n = 1$ ed $n\varphi = 0$ differiscono per un multiplo intero di 2π , ossia se e solo se $\varrho = 1$ (si ricordi che ϱ è un numero reale ≥ 0) ed $n\varphi$ è un multiplo intero di 2π (cioè $\varphi = 2h\pi/n$ per qualche $h \in \mathbb{Z}$). Abbiamo così dimostrato il seguente:

5.8 COROLLARIO. *Sia $n \geq 1$ un numero intero. Le radici n-esime dell'unità, ossia i numeri complessi z tali che $z^n = 1$, sono tutti e soli i numeri complessi*

$$z_h = \cos(2h\pi/n) + i \sin(2h\pi/n), \quad h \in \mathbb{Z}.$$

Riportiamo nel piano di Argand-Gauss i punti corrispondenti ai numeri complessi $z_h = \cos(2h\pi/n) + i \sin(2h\pi/n)$ nel caso in cui $n = 6$. Dato che $|z_h| = 1$ per ogni h , tutti i punti si trovano sulla circonferenza di centro l'origine e raggio 1. I punti che si ottengono, partendo da $z_0 = 1$, sono rappresentati nella figura 5.2.

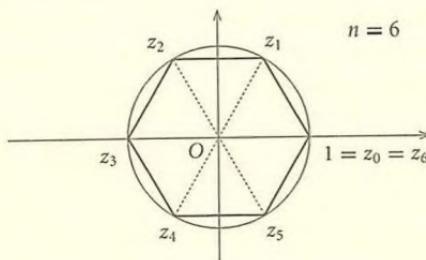


FIGURA 5.2.

Arrivati a z_6 si ha $z_6 = z_0, z_7 = z_1, z_8 = z_2, \dots$. Il procedimento descritto nel caso $n = 6$ si applica ad ogni $n \geq 1$. Infatti 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:

5.9 PROPOSIZIONE. *Sia $n \geq 1$ un numero intero fissato. In \mathbb{C} vi sono esattamente n radici n -esime distinte dell'unità. Esse 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 , α , dove α 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 $\pi/2$ 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 $3\pi/2$ 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 $-\pi/4$ 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 α è un numero reale negativo, il modulo di α è $-\alpha$ e il suo argomento è π . 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 α 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 $|z - 1| < 1$.

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 $a, b, \varrho, \varphi \in \mathbb{R}$ e $\varrho \geq 0$.

- 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 ?
- Dato un numero complesso $z = \varrho(\cos \varphi + i \sin \varphi)$ in forma trigonometrica, si scriva in forma trigonometrica il numero iz .

5.9. Verificare che se $\varrho, \varphi \in \mathbb{R}$ e $\varrho \geq 0$, allora il modulo del numero complesso $\varrho(\cos \varphi + i \sin \varphi)$ è ϱ .

5.10. Se $z = a + ib$ è un numero complesso ($a, b \in \mathbb{R}$), il numero complesso $\bar{z} = a - ib$ si dice il *coniugato* di z . Si provi che:

- $z\bar{z} = |z|^2$;
- $\bar{\bar{z}} = z$;
- $z + \bar{z}$ è un numero reale uguale al doppio della parte reale di z ;
- per ogni $z, z' \in \mathbb{C}$ si ha $\overline{z+z'} = \bar{z} + \bar{z}'$ e $\overline{zz'} = \bar{z}\bar{z}'$.

5.11. Come si scrive in forma trigonometrica il coniugato del numero complesso $\varrho(\cos \varphi + i \sin \varphi)$?

5.12. Se $z = \varrho(\cos \varphi + i \sin \varphi) \neq 0$ è un numero complesso in forma trigonometrica, come si scrive in forma trigonometrica il suo inverso $1/z$?

5.13. Siano $z = \varrho(\cos \varphi + i \sin \varphi)$ e $z' = \varrho'(\cos \varphi' + i \sin \varphi') \neq 0$ due numeri complessi scritti in forma trigonometrica. Si scriva, sempre in forma trigonometrica, il numero z/z' .

5.14. Calcolare e riportare nel piano di Argand-Gauss le radici quarte dell'unità. Calcolare e riportare nel piano di Argand-Gauss le radici ottave dell'unità.

5.15. Si calcolino le soluzioni dell'equazione $x^{12} - 1 = 0$ in \mathbb{C} .

5.16. Si calcolino le soluzioni dell'equazione $x^4 + i = 0$ in \mathbb{C} .

5.17. Si calcolino le soluzioni dell'equazione $x^3 - 2i = 0$ in \mathbb{C} .

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

5.19. (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.

§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 $m \times n$

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

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 m di righe e lo stesso numero n 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 .

6.1 ESEMPIO. Siano

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

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 λ 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)* λA 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

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

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 λ, μ 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 λ 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 δ_{ij} ponendo $\delta_{ij} = 1$ se $i = j$, e $\delta_{ij} = 0$ se $i \neq j$ (il simbolo δ_{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:

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

Se A è una matrice $m \times n$ si ha $I_{m \times m}A = AI_{n \times n} = A$ (esercizio 6.9).

Per ogni intero positivo p e ogni matrice quadrata A poniamo

$$A^p = \underbrace{AA \cdots A}_{p \text{ volte}},$$

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

6.2 ESEMPIO. 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

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

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 .

6.3 ESEMPIO. 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 ϱ 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 ϱ .

Soluzione. La soluzione è evidentemente

$$A_\varrho = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad \square$$

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

Altri esercizi

6.3. Si eseguano le operazioni indicate:

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

*

6.4. Si eseguano le operazioni indicate:

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

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:

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

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

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

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

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

6.7. Se $A = B = \{1, 2, 3, 4\}$ si scrivano le matrici delle corrispondenze $\sigma_1 = \{(x, x+1) \mid x \in \{1, 2, 3\}\}$ e $\sigma_2 = \{(x, x) \mid x \in A\}$ di A in B (vedi esercizio 6.1).

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

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

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

6.10. Due matrici A e B quadrate di ordine n si dicono *una l'inversa dell'altra* se $AB = I_{n \times n}$. (Dimostreremo nel corollario 39.7 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.

6.11. 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 $A^4 = -I$.

6.12. 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 $n \geq 2$.

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

6.14. Sia $M_2(\mathbb{R})$ l'insieme delle matrici quadrate di ordine 2. 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 φ 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

$$\varphi((a + ib)(a' + ib')) = \varphi(a + ib)\varphi(a' + ib').$$

Capitolo 2

INSIEMI E RELAZIONI

§7. Equivalenze e partizioni

Come abbiamo visto nel §2, una *corrispondenza* dell'insieme A nell'insieme B è un qualsiasi 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 ϱ è una relazione su A , ossia $\varrho \subseteq A \times A$, e $a, a' \in A$, invece di scrivere $(a, a') \in \varrho$ scriveremo $a \varrho a'$ e diremo che a è *nella relazione ϱ con a'* . Se $(a, a') \notin \varrho$ scriveremo invece $a \not\varrho a'$.

7.1 ESEMPIO. 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 δ 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 δ non descrivendola come sottoinsieme di $\mathbb{N} \times \mathbb{N}$, ma dicendo "sull'insieme $A = \mathbb{N}$ consideriamo la relazione δ definita ponendo, per ogni $x, y \in \mathbb{N}$, $x \delta y$ se $x = 2y$ ". \square

7.2 ESEMPIO. Sull'insieme \mathbb{C} consideriamo la relazione μ 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 μ in modo più formale come sottoinsieme di $\mathbb{C} \times \mathbb{C}$ si ha quindi che

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

7.3 ESEMPIO. Nell'insieme \mathbb{N} si consideri la relazione \leq :

$$\leq = \{(n, m) \mid n, m \in \mathbb{N} \text{ ed esiste } t \in \mathbb{N} \text{ tale che } n + t = m\}.$$

Invece di $(n, m) \in \leq$ si scrive $n \leq m$ (n è nella relazione \leq con m). \square

7.4 ESEMPIO. Se X è un insieme, “essere sottoinsieme di” è una relazione in $\mathcal{P}(X)$:

$$\subseteq = \{(Y, Z) \mid Y, Z \in \mathcal{P}(X), Y \text{ è sottoinsieme di } Z\}. \quad \square$$

7.5 ESEMPIO. Siano π un piano e A l'insieme dei punti di π . La relazione

$$\varrho = \{(P, Q) \mid P, Q \in A \text{ e la distanza tra } P \text{ e } Q \text{ è } 1\}$$

è una relazione su A . \square

Data una relazione ϱ 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 come *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 .

7.6 ESEMPIO. Sia A l'insieme delle 8 radici ottave dell'unità. Definiamo una relazione ϱ su A ponendo, per ogni $a, b \in A$, $a \varrho b$ se $a^2 = b$. Allora A può essere rappresentato mediante il grafo orientato della figura 7.1.

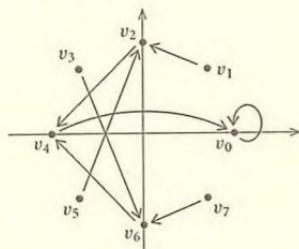


FIGURA 7.1.

Qui gli elementi di A , che sono numeri complessi, sono stati rappresentati nel piano di Argand-Gauss come abbiamo imparato a fare nel §5. Ma questo non era strettamente necessario. Ad esempio la relazione ϱ su A avrebbe potuto essere rappresentata come nella figura 7.2.

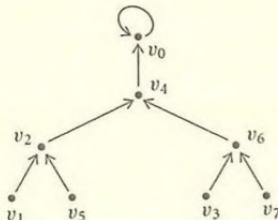


FIGURA 7.2.

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*. \square

Una relazione ϱ 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 $a \varrho c$.

Una relazione ϱ sull'insieme A che sia riflessiva, simmetrica e transitiva si dice una *relazione di equivalenza* (o, semplicemente, un'*equivalenza*). Le equivalenze vengono indicate in genere con simboli come $\sim, \equiv, \approx, \simeq, \cong$, eccetera.

7.7 ESEMPIO. Fissiamo un sistema di coordinate cartesiane ortogonali su un piano π e denotiamo con A l'insieme dei punti di π . 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 . \square

7.8 ESEMPIO. Nell'esempio 7.1 era stata definita una relazione δ sull'insieme \mathbb{N} ponendo, per ogni $x, y \in \mathbb{N}$, $x \delta y$ se $x = 2y$. La relazione δ 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 $x = 2z$). \square

7.9 ESEMPIO. Nell'esempio 7.2 abbiamo incontrato la relazione μ su \mathbb{C} definita ponendo, per ogni $z, z' \in \mathbb{C}$, $z \mu z'$ se $|z| = |z'|$. Allora

- ▷ la relazione μ è riflessiva, perché per ogni $z \in \mathbb{C}$ si ha $|z| = |z|$, cioè $z \mu z$;
- ▷ la relazione μ 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 μ 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 μ è una relazione di equivalenza sull'insieme \mathbb{C} . \square

7.10 ESEMPIO. 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 . \square

7.11 ESEMPIO. 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 . Per ogni $a \in A$ definiamo

$$[a]_\sim = \{x \mid x \in A, x \sim a\},$$

detta la *classe di equivalenza* di a modulo \sim . (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 quoziante 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 π si dice l'*applicazione canonica* (o la *proiezione canonica*) di A su A/\sim .

7.12 ESEMPIO. Nell'esempio 7.2 abbiamo definito una relazione μ 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 μ è una relazione di equivalenza su \mathbb{C} (esempio 7.9). 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 \mathbb{C}_α l'insieme di tutti i numeri complessi di modulo α , cioè dei numeri complessi che nel piano di Argand-Gauss stanno sulla circonferenza di centro l'origine e raggio α , si ha $[z]_\mu = \mathbb{C}_\alpha$, dove $\alpha = |z|$. Inoltre l'insieme quoziante \mathbb{C}/μ è $\{\mathbb{C}_\alpha \mid \alpha \in \mathbb{R}, \alpha \geq 0\}$ e la proiezione canonica $\pi: \mathbb{C} \rightarrow \mathbb{C}/\mu$ è definita da $\pi(z) = \mathbb{C}_{|z|}$ 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

7.13 ESEMPIO. Nell'esempio 7.10 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 quoziante $A/= = \{\{a\} \mid a \in A\}$ e la proiezione canonica $\pi: A \rightarrow A/=$ è definita da $\pi(a) = \{a\}$ per ogni $a \in A$. \square

7.14 ESEMPIO. Dimostriamo per esercizio 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 $[a]_\sim \cap [b]_\sim = \emptyset$.

(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 $[a]_\sim = [b]_\sim$, allora $[a]_\sim \cap [b]_\sim = [a]_\sim \neq \emptyset$.

Per dimostrare l'implicazione inversa, supponiamo che $[a]_\sim \cap [b]_\sim \neq \emptyset$. Ne segue che esiste un elemento $c \in [a]_\sim \cap [b]_\sim$. 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

Sia 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:

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

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

Si osservi intanto che gli elementi \mathbb{C}_α 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

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

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

7.16 ESEMPIO. 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

7.17 ESEMPIO. 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 $a = y/x^2$. 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

7.18 TEOREMA. Sia A un insieme.

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

Dimostrazione. (a) Sia \sim un'equivalenza su A . Dobbiamo dimostrare che A/\sim è una partizione di A . Certamente gli elementi $[a]_{\sim}$ di A/\sim sono sottoinsiemi di A . Dobbiamo far vedere che sono soddisfatte le tre condizioni (a), (b) e (c) della definizione di partizione. Dato che $a \sim a$ per ogni $a \in A$ (proprietà riflessiva), si ha che $a \in [a]_{\sim}$, e quindi ogni elemento $[a]_{\sim}$ di A/\sim è non vuoto. Quindi la (a) della definizione di partizione è soddisfatta. Mostriamo la (b). Dato che $[a]_{\sim} \subseteq A$ per ogni $a \in A$, si ha $\bigcup_{X \in \mathcal{F}} X \subseteq A$. Viceversa, se $x \in A$, si ha $x \in [x]_{\sim}$, e quindi $x \in \bigcup_{a \in A} [a]_{\sim}$. La (c) è stata dimostrata nell'esempio 7.14(b).

(b) Dobbiamo provare che $\sim_{\mathcal{F}}$ è riflessiva, simmetrica e transitiva. Riflessività: Sia $a \in A$. Allora per la condizione (b) nella definizione di partizione si ha che esiste $X \in \mathcal{F}$ tale che $a \in X$. Pertanto $a \in X$ e $a \in X$, cioè $a \sim_{\mathcal{F}} a$. Simmetria: Siano $a, b \in A$ e supponiamo che $a \sim_{\mathcal{F}} b$. Allora $a \in X$ e $b \in X$ per qualche $X \in \mathcal{F}$. Ne segue che $b \sim_{\mathcal{F}} a$. Transitività: Siano $a, b, c \in A$ e sia $a \sim_{\mathcal{F}} b$ e $b \sim_{\mathcal{F}} c$. Allora esiste $X \in \mathcal{F}$ tale che $a \in X$ e $b \in X$, ed esiste $Y \in \mathcal{F}$ tale che $b \in Y$ e $c \in Y$. Ma allora $b \in X \cap Y$. Per la condizione (c) nella definizione di partizione deve quindi essere $X = Y$. Pertanto $c \in X$, e quindi $a \sim_{\mathcal{F}} c$. \square

Nel teorema 7.18 si associa ad ogni equivalenza una partizione, e ad ogni partizione un'equivalenza. È possibile dimostrare (esercizio 7.26 nel §47, la cui soluzione appare nel §48) 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 a e b stanno nello stesso elemento della partizione.

Esercizi svolti

- 7.1. Sia $f: A \rightarrow B$ un'applicazione e \sim_f la relazione di equivalenza su A associata ad f (esempio 7.11). 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'iniettività di f , $a = a'$. Viceversa se $a = a'$, allora $f(a) = f(a')$, 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

7.2. 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

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

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

e si consideri la partizione

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

di \mathbb{C} (vedi esempio 7.15). 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 $a \in \mathbb{C}_\alpha$ e $b \in \mathbb{C}_\alpha$, 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 $|a| = |b|$. Quindi $\sim_{\mathcal{F}}$ è definita, per ogni $a, b \in \mathbb{C}$, da $a \sim_{\mathcal{F}} b$ se e solo se $|a| = |b|$. \square

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

- (a) Come è definita l'equivalenza \sim_f su \mathbb{R} associata ad f ?
- (b) Se $a \in \mathbb{R}$, cos'è la classe di equivalenza $[a]_{\sim_f}$?

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

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

Altri esercizi

7.5. Sia \sim la relazione su \mathbb{R} definita ponendo, per ogni $x, y \in \mathbb{R}$, $x \sim y$ se $x - y \in \mathbb{Z}$. Si provi che \sim è un'equivalenza su \mathbb{R} .

7.6. Come nell'esercizio precedente sostituendo \mathbb{N} a \mathbb{Z} . Si provi che \sim non è un'equivalenza su \mathbb{R} .

7.7. La relazione ϱ su \mathbb{Z} definita da $x \varrho y$ se $xy(x+y) = 0$, $x, y \in \mathbb{Z}$, è un'equivalenza su \mathbb{Z} ?

7.8. Siano A un insieme e ω la relazione su A definita da $a \omega b$ per ogni $a, b \in A$. Si dimostri che ω è un'equivalenza su A . Cos'è A/ω ? [Si noti che si ha $\omega = A \times A$. L'equivalenza ω è detta l'equivalenza *banale* su A : tutti gli elementi di A sono tra loro equivalenti.]

7.9. Sia A un insieme non vuoto. Si dimostri che la relazione ω dell'esercizio 7.8 e la relazione di uguaglianza $=$ dell'esempio 7.10 coincidono se e solo se A ha esattamente un elemento.

7.10. Siano X un insieme, X^X l'insieme di tutte le applicazioni di X in X , e \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 .

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

7.12. Siano A un insieme, \sim una relazione di equivalenza su A , e A/\sim l'insieme quoziante. Si dimostri che la proiezione canonica $\pi: A \rightarrow A/\sim$ è suriettiva.

7.13. Siano A un insieme e $\iota_A: A \rightarrow A$ l'applicazione identica di A . Qual è la relazione di equivalenza \sim_{ι_A} associata a ι_A ?

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

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

7.15. Sia ϱ una relazione qualsiasi su un insieme A . Se $x, y \in A$ poniamo $x \varrho^* y$ se esistono $n \geq 1$ e $x_0, x_1, \dots, x_n \in A$ tali che $x = x_0$, $x_0 \varrho x_1$, $x_1 \varrho x_2$, \dots , $x_{n-1} \varrho x_n$, $x_n = y$. Si provi che ϱ^* è una relazione transitiva su A . (La relazione ϱ^* si chiama la *chiusura transitiva* di ϱ .)

7.16. Se ϱ è una relazione su un insieme A , definiamo la *relazione inversa* ϱ^{-1} su A ponendo $x \varrho^{-1} y$ se $y \varrho x$, ove $x, y \in A$. Si provi che

- (a) ϱ è riflessiva se e solo se ϱ^{-1} è riflessiva;
- (b) ϱ è transitiva se e solo se ϱ^{-1} è transitiva;
- (c) ϱ è simmetrica se e solo se $\varrho = \varrho^{-1}$.

7.17. Se ϱ, ϱ' sono relazioni su un insieme A , definiamo la *relazione composta* $\varrho \circ \varrho'$ ponendo $x(\varrho \circ \varrho')y$ se esiste $z \in A$ tale che $x \varrho z$ e $z \varrho' y$. Si provi che

- (a) se ϱ e ϱ' sono riflessive, allora $\varrho \circ \varrho'$ è riflessiva;
- (b) ϱ è transitiva se e solo se $\varrho \circ \varrho \subseteq \varrho$.

7.18. 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_φ è l'insieme di tutti i numeri complessi non nulli aventi argomento φ , allora $\mathcal{F} = \{X_\varphi \mid \varphi \in \mathbb{R}\}$ è una partizione di $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

7.19. Sia $\mathcal{F} = \{\{n, -n\} \mid n \in \mathbb{N}\}$. Si provi che \mathcal{F} è una partizione di \mathbb{Z} . Qual è la relazione di equivalenza $\sim_{\mathcal{F}}$?

7.20. 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 .

7.21. 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 .

§8. L'insieme delle classi resto

In tutto questo §8 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 $a - b$, cioè se a e b differiscono per un multiplo intero di n .

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

8.2 ESEMPIO. 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 ω (esercizio 7.8). \square

8.3 ESEMPIO. 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 8.2), 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 §8). 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

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

L'insieme \mathbb{Z}/\equiv_n è detto l'*insieme delle classi resto degli interi modulo n*.

8.4 LEMMA. 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 dimostriamo 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 non divide nessun numero strettamente compreso tra 0 e n). In altre parole $j \not\equiv_n i$, 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 quindi \mathbb{Z}/\equiv_n ha esattamente n elementi. \square

8.5 ESEMPIO. 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. 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 disposti attorno ad un tavolo da gioco: 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 $n - 1$ che va al giocatore [$n - 1$]. Completato così il primo giro continuiamo a distribuire i numeri interi: quindi il numero n va la 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 [$n - 3$], ..., il numero $-(n - 1)$ al giocatore [1], il numero $-n$ al giocatore [0], e così via di seguito.

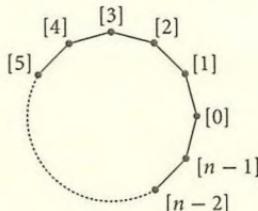


FIGURA 8.1.

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 vengono ripartiti nell'insieme quoziante $\mathbb{Z}/\equiv_n = \{[0], [1], [2], \dots, [n - 1]\}$, 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. 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

8.2. 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 $n \mid (a - b)$ ed $n \mid (c - d)$. 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

8.3. Si dia un esempio di quattro numeri $n, x, y, z \in \mathbb{Z}$ tali che $xz \equiv yz \pmod{n}$, $z \neq 0$ 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

8.4. 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 φ 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 $a - b = tkm$, 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 φ 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 φ è suriettiva. \square

Altri esercizi

8.5. Qual è la classe di equivalenza di 24 nella relazione di congruenza modulo 9 in \mathbb{Z} ? Cioè, cos'è $[24]_{\equiv_9}$?

8.6. 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 $a \equiv b \pmod{[m, n]}$.

8.7. 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 4.5.]

8.8. 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.

8.9. (a) Quanti elementi ha \mathbb{Z}/\equiv_0 ? Quali sono?
 (b) Quanti elementi ha \mathbb{Z}/\equiv_1 ? Quali sono?

8.10. 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 $r(x) =$ "resto della divisione di x 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 8.1.]

8.11. 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 $a, b \in \mathbb{Z}$,

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

- (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 $a \in \mathbb{Z}$.

8.12. 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 ψ è iniettiva.

8.13. Sia $A = \{1, 2, 3, 4, -3, -1, 14, 23, -7, 28\}$. Sia ϱ 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/ϱ ? 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 φ 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 φ è iniettiva?
- (d) L'applicazione φ è suriettiva?

8.14. 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.

§9. Cardinalità di insiemi, tecniche di enumerazione

Si dice che due insiemi A e B sono *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 detto 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 è un insieme finito e $B \subseteq A$, allora B è un insieme finito e $|B| \leq |A|$. Chiaramente se A è un insieme finito, ogni applicazione iniettiva $f: A \rightarrow A$ è anche suriettiva, e dunque biiettiva; similmente, ogni applicazione suriettiva $g: A \rightarrow A$ è anche iniettiva, e dunque biiettiva. Come si è visto negli esempi 2.7 e 2.8 questo non accade per \mathbb{N} : ci sono applicazioni suriettive $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ che non sono iniettive, e applicazioni iniettive $\psi: \mathbb{N} \rightarrow \mathbb{N}$ che non sono suriettive.

È chiaro che

9.1 PROPOSIZIONE. *Se A e B sono insiemi finiti disgiunti, si ha*

$$|A \cup B| = |A| + |B|.$$

Da questo segue, più in generale, che

9.2 COROLLARIO. *Se A e B sono insiemi finiti, allora*

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

Dimostrazione. 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

9.3 COROLLARIO. *Se A_1, A_2, \dots, A_n sono insiemi finiti e $A_i \cap A_j = \emptyset$ per ogni $i \neq j$, allora*

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

Dimostrazione. Induzione su n . 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 $(\bigcup_{i=1}^{n-1} A_i) \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n) = \emptyset$. Quindi $\left| \bigcup_{i=1}^n A_i \right| = \left| (\bigcup_{i=1}^{n-1} A_i) \cup A_n \right| = \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n|$. 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 $\left| \bigcup_{i=1}^n A_i \right| = (\sum_{i=1}^{n-1} |A_i|) + |A_n| = \sum_{i=1}^n |A_i|$. Questo prova l'identità anche per le unioni di n insiemi a due a due disgiunti. \square

9.4 COROLLARIO. *Se A e B sono insiemi finiti, allora $|A \times B| = |A| \cdot |B|$.*

Dimostrazione. Dato che $A \times B = \bigcup_{a \in A} \{a\} \times B$, l'insieme $A \times B$ è unione di $|A|$ insiemi a due a due disgiunti $\{a\} \times B$ ($a \in A$), dove ogni $\{a\} \times B$ è ovviamente equipotente a B . Quindi $A \times B$ è unione di $|A|$ insiemi a due a due disgiunti ciascuno di cardinalità $|B|$. Si conclude per il corollario 9.3. \square

In particolare $|A^n| = |A|^n$ per ogni insieme finito A .

Il corollario 9.4 ha un'interessante interpretazione riguardante il numero di modi in cui si possono costruire delle coppie. Supponiamo di voler contare in quanti modi si può costruire una coppia (a, b) con a appartenente ad un insieme finito A e b appartenente ad un insieme finito B . Se A ha n elementi e B ha m elementi, allora nel costruire la coppia (a, b) posso scegliere a in n modi e posso scegliere b in m modi. Il corollario 9.4 ci dice che la coppia (a, b) può essere costruita in nm modi.

9.5 ESEMPIO. Supponiamo di voler etichettare degli oggetti con delle etichette su cui appaiono due simboli. Il primo simbolo è una delle 26 lettere dell'alfabeto latino e il secondo è una delle dieci cifre 0, 1, 2, ..., 9. Quanti oggetti posso etichettare al più in questo modo?

In ogni etichetta la prima lettera può essere scelta in 26 modi e la seconda cifra può essere scelta in 10 modi. Quindi posso costruire $26 \cdot 10 = 260$ etichette di questo tipo, e pertanto in questo modo posso etichettare al più 260 oggetti. \square

I risultati visti fino ad ora in questo §9 erano tutti ovvi da un punto di vista intuitivo. I risultati che seguono lo saranno un po' meno. Daremo varie dimostrazioni per ciascuna delle due prossime proposizioni. Questo perché da un lato le proposizioni sono importanti, dall'altro perché le loro dimostrazioni sono particolarmente istruttive.

9.6 PROPOSIZIONE. Se A e B sono insiemi finiti e B^A è l'insieme di tutte le applicazioni di A in B , allora $|B^A| = |B|^{|A|}$.

Prima dimostrazione. Siano $|A| = n$, $|B| = m$. Poniamo $A = \{a_1, a_2, \dots, a_n\}$, $B = \{b_1, b_2, \dots, b_m\}$. Se $f: A \rightarrow B$ è un'applicazione, allora $f(a_1)$ può essere un qualunque elemento di B ; ho quindi m modi in cui posso scegliere $f(a_1)$. Anche $f(a_2)$ può essere un qualunque elemento di B , e quindi può essere scelto in m modi. Similmente per $f(a_3), \dots, f(a_n)$. In totale ho $\underbrace{m \cdot m \cdot \dots \cdot m}_{n \text{ volte}} = m^n$ modi in cui posso scegliere $f(a_1), f(a_2), \dots, f(a_n)$. \square

Seconda dimostrazione (essenzialmente equivalente alla precedente). Se A ha n elementi a_1, a_2, \dots, a_n , l'applicazione $\varphi: B^A \rightarrow \underbrace{B \times \dots \times B}_{n \text{ volte}}$, definita da $\varphi(f) = (f(a_1), \dots, f(a_n))$ per ogni $f \in B^A$, è una biiezione. Quindi $|B^A| = |B^n| = |B|^n = |B|^{|A|}$. \square

9.7 PROPOSIZIONE. Se A è un insieme finito e $\mathcal{P}(A)$ è l'insieme delle parti di A , allora $|\mathcal{P}(A)| = 2^{|A|}$.

Prima dimostrazione. Sia $n = |A|$. La dimostrazione è per induzione su n . 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

Seconda dimostrazione. Per ogni sottoinsieme S di 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 χ_S si chiama la *funzione caratteristica* del sottoinsieme S di A .) Definiamo 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 $S \in \mathcal{P}(A)$.

Dimostriamo che σ è una biiezione. Per far vedere che σ è iniettiva proviamo 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 χ_S e $\chi_{S'}$ sono diverse, vale a dire $\sigma(S) \neq \sigma(S')$.

Mostriamo che σ 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 σ 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 dimostra che σ è suriettiva.

Dato che $\sigma: \mathcal{P}(A) \rightarrow \{0, 1\}^A$ è una biiezione, si ha $|\mathcal{P}(A)| = |\{0, 1\}^A| = |\{0, 1\}|^{|A|} = 2^{|A|}$. \square

Terza dimostrazione. Supponiamo che $A = \{a_1, a_2, \dots, a_n\}$ abbia n elementi. Contiamo in quanti modi possiamo costruire un sottoinsieme B di A . L'elemento a_1 può appartenere o non appartenere a B . Abbiamo quindi due possibilità di scelta per quanto riguarda l'elemento a_1 . Analogamente l'elemento a_2 può appartenere o non appartenere a B . Abbiamo quindi due possibilità di scelta per quanto riguarda l'elemento a_2 . E così via per gli elementi a_3, \dots, a_n . In totale ci sono $\underbrace{2 \cdot 2 \cdot \dots \cdot 2}_{n \text{ volte}} = 2^n$ modi in cui possiamo costruire un sottoinsieme B di A , vale a dire $|\mathcal{P}(A)| = 2^n$. \square

Ricordiamo che per ogni intero $n \geq 0$ il numero $n!$ (*n fattoriale*) è definito da $0! = 1$ e $n! = (n-1)!n = 1 \cdot 2 \cdot 3 \cdots n$ per ogni $n \geq 1$.

9.8 PROPOSIZIONE. *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 $n!/(n-m)! = (n-m+1) \cdot (n-m+2)(n-m+3) \cdots (n-1)n$ se $m \leq n$.*

Dimostrazione. Ovviamente se $m > n$ non ci sono applicazioni iniettive di A in B . Supponiamo dunque $m \leq n$. Dobbiamo contare in quanti modi si può costruire un'applicazione iniettiva $f: A \rightarrow B$. Siano $A = \{a_1, \dots, a_m\}$ e $B = \{b_1, \dots, b_n\}$, 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 ci sono $n(n-1)(n-2)\cdots(n-m+1) = n!/(n-m)!$ 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

Se A è un insieme finito, le biiezioni $A \rightarrow A$ si chiamano anche le *permutazioni* di A . Se A è finito di cardinalità n , ogni applicazione iniettiva $A \rightarrow A$ è una biiezione, e per la proposizione 9.8 ci sono $n!/1! = n!$ applicazioni iniettive $A \rightarrow A$. Abbiamo così dimostrato che

9.9 COROLLARIO. Le permutazioni di un insieme di cardinalità n sono $n!$.

Sia ora $n \geq 1$ un numero intero fissato. Vogliamo studiare le permutazioni dell'insieme $X_n = \{1, 2, 3, \dots, n\}$, ossia le biiezioni $X_n \rightarrow X_n$. Sia S_n l'insieme delle permutazioni di X_n .

Un'applicazione $f \in S_n$ viene spesso denotata

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

9.10 ESEMPIO. 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}. \quad \square$$

In questa notazione:

(1) 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 $1 \ 2 \ 3 \ \dots \ n$.

9.11 ESEMPIO. 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 ricava $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$. \square

9.12 ESEMPIO. 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 $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$. \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.

Se scriviamo le $n!$ permutazioni di X_n , vedremo che nella seconda riga avremo scritto gli n numeri da 1 ad n in tutti gli ordini possibili esattamente una volta. Se ne deduce che n oggetti distinti possono essere allineati in $n!$ modi. Estendendo la nostra terminologia, chiameremo *permutazione* di n oggetti distinti un qualunque allineamento degli oggetti. Tali allineamenti si ottengono infatti l'uno dall'altro permutando, cioè "mescolando", gli n oggetti.

9.13 ESEMPIO. Quante parole si possono scrivere usando esattamente una volta le lettere della parola "aiuole"?

Devo contare in quanti modi posso allineare le 6 lettere a,i,u,o,l,e, ossia quante sono le permutazioni di un insieme di 6 lettere. Dato che $6! = 720$, si trova che si possono scrivere 720 parole. \square

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

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

Per ogni intero k con $1 \leq k \leq n-1$ si ha

$$(9.1) \quad \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Infatti

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

L'uguaglianza (9.1) ha un'interessante interpretazione geometrica. Scriviamo i coefficienti binomiali disponendoli in un triangolo illimitato (detto *triangolo di Tartaglia* o *triangolo di Pascal*) nel modo seguente:

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

Dato che

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

per ogni n , il primo e l'ultimo coefficiente binomiale in 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'uguaglianza (9.1)

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

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:

		1						
			1	1				
			1	2	1			
			1	3	3	1		
			1	4	6	4	1	
			1	5	10	10	5	1
	

9.14 PROPOSIZIONE (FORMULA DEL BINOMIO). *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 $n \geq 1$.

La dimostrazione di questa proposizione viene lasciata per esercizio al lettore (si faccia uso dell'induzione e dell'uguaglianza (9.1)).

Il nome di *coefficienti binomiali* deriva dalla formula del binomio: i coefficienti binomiali

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

scritti nella $(n+1)$ -esima riga del triangolo di Tartaglia, 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.

9.15 PROPOSIZIONE. *Siano $n \geq k$ numeri naturali. Un insieme di cardinalità n ha esattamente $\binom{n}{k}$ sottoinsiemi di cardinalità k .*

Dimostrazione. Induzione su n . 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 in questo caso 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 $1 \leq k \leq n - 1$. Per l'ipotesi induttiva sappiamo 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 $A \setminus \{a_0\}$ aventi k elementi; poiché $|A \setminus \{a_0\}| = n - 1$, tali sottoinsiemi sono, per l'ipotesi induttiva, $\binom{n-1}{k}$. 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 avente $k - 1$ 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 (9.1), 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

Supponiamo di avere n oggetti e di sceglierne r senza tener conto dell'ordine. Si dice in questo caso di aver preso una *combinazione* di r degli n oggetti. In altri termini una combinazione di r oggetti non è altro che un sottoinsieme di cardinalità r dell'insieme di partenza che aveva cardinalità n .

9.16 ESEMPIO. Supponiamo che una commissione di 10 persone voglia formare una sottocommissione di 3 persone. In quanti modi può essere fatta questa sottocommissione?

La risposta è: tanti quanti sono i sottoinsiemi di cardinalità 3 di un insieme di 10 elementi, cioè tanti quante sono le combinazioni di 3 tra 10 oggetti, ossia $\binom{10}{3} = 120$. \square

La disciplina della matematica che comprende tra l'altro le tecniche di enumerazione degli oggetti, tecniche di cui abbiamo iniziato lo studio in questo §9, prende il nome proprio dalle combinazioni, e si chiama Combinatoria (o Analisi combinatoria).

Passiamo ad un altro argomento, cioè allo studio degli insiemi infiniti. Ora non è più possibile contare il numero degli elementi, ma il concetto di equipotenza di insiemi resta valido.

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 si dice *numerabile* se è equipotente all'insieme \mathbb{N} dei numeri naturali.¹ Scriveremo in tal caso $|A| = \aleph_0$ (alef zero; alef è la prima lettera dell'alfabeto ebraico). 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. Come vedremo nella proposizione 9.19 ogni sottoinsieme di un insieme numerabile è finito o numerabile.

¹ Si faccia attenzione che in altri testi un insieme è detto *numerabile* se è finito o equipotente ad \mathbb{N} .

9.17 PROPOSIZIONE.

L'insieme \mathbb{Q} dei numeri razionali è numerabile.

Dimostrazione. Si consideri la seguente tabella:

1/1									
1/2	2/1								
1/3	2/2	3/1							
1/4	2/3	3/2	4/1						
1/5	2/4	3/3	4/2	5/1					
1/6	2/5	3/4	4/3	5/2	6/1				
1/7	2/6	3/5	4/4	5/3	6/2	7/1			
:									
1/n	2/(n-1)	3/(n-2)	4/(n-3)	n/1	
:									

La tabella ha infinite righe, ma in ogni riga vi sono solo un numero finito di numeri razionali: nella n -esima riga vi sono tutte le frazioni di due interi positivi in cui la somma del numeratore e del denominatore è $n+1$. Chiaramente tutti i numeri razionali positivi compaiono almeno una volta nella tabella. A questo punto cancelliamo tutte le frazioni che non siano ridotte ai minimi termini. Cancelliamo quindi $2/2, 2/4, 3/3, 4/2, 2/6$, ecc. Ora nella nostra tabella (infinita) compaiono esattamente una volta tutti i numeri razionali positivi. Sia $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$. Definiamo $\psi: \mathbb{N}^* \rightarrow \mathbb{Q}^+$ ponendo $\psi(n) =$ "l' n -esimo numero razionale (non cancellato) che compare nella tabella". Ad esempio $\psi(1) = 1/1, \psi(2) = 1/2, \psi(3) = 2/1, \psi(4) = 1/3, \psi(5) = 3/1$, ecc. Chiaramente ψ è una biiezione. Definiamo quindi $\chi: \mathbb{Z} \rightarrow \mathbb{Q}$ ponendo

$$\chi(z) = \begin{cases} \psi(z) & \text{se } z > 0 \\ 0 & \text{se } z = 0 \\ -\psi(-z) & \text{se } z < 0. \end{cases}$$

Anche χ è una biiezione, e componendo con la biiezione $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$ dell'esercizio 2.2 si ottiene una biiezione $\chi \circ \varphi: \mathbb{N} \rightarrow \mathbb{Q}$. Quindi \mathbb{Q} è numerabile. \square

9.18 PROPOSIZIONE.

L'insieme \mathbb{R} dei numeri reali non è numerabile.

Dimostrazione. Abbiamo visto nell'appendice 4.1 che ogni numero reale si scrive nel sistema decimale in modo unico nella forma $c_N c_{N-1} \dots c_1 c_0, c_{-1} c_{-2} c_{-3} \dots$, dove $c_i \in \{0, 1, 2, \dots, 9\}$ per ogni i e non esiste $p \in \mathbb{N}$ tale che $c_{-p} = c_{-(p+1)} = c_{-(p+2)} = \dots = 9$. Supponiamo per assurdo che \mathbb{R} sia numerabile, cioè che esista una biiezione $\varphi: \mathbb{N} \rightarrow \mathbb{R}$. Per ogni $i = 0, 1, 2, \dots$ poniamo $b_{-i} = 0$ se la cifra di posto $-i$ nella notazione decimale del numero $\varphi(i)$ è $\neq 0$, mentre poniamo $b_{-i} = 1$ se la cifra di posto $-i$ nella notazione decimale del numero $\varphi(i)$ è $= 0$. Consideriamo ora il numero reale $\alpha = b_0, b_{-1} b_{-2} b_{-3} \dots b_{-n} \dots$. Allora α è diverso da $\varphi(n)$ per ogni $n \in \mathbb{N}$, perché sono diverse le loro cifre di posto $-n$ in notazione decimale. Quindi $\alpha \notin \varphi(\mathbb{N})$ e φ non è suriettiva. \square

Esercizi svolti

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 (non necessariamente distinti). 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 . Si noti che

- (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 $a \in A$ (φ_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

$$\varphi_n: A^n \longrightarrow W_n$$

data da

$$\varphi_n(a_1, a_2, \dots, a_n) = a_1 a_2 \dots a_n$$

per ogni $(a_1, a_2, \dots, a_n) \in A^n$.

Denotiamo con W_A l'insieme $\bigcup_{n \in \mathbb{N}} W_n$ di tutte le parole nell'alfabeto A .

Ad esempio, se A è l'insieme delle cifre 0, 1, 2, ..., 9, ogni numero naturale viene rappresentato in base 10 con una parola di lunghezza > 0 .

9.1. L'insieme $A = \{a, b, c, \dots, x, y, z\}$ delle lettere dell'alfabeto latino ha 26 elementi.

- (a) Quante parole di lunghezza 3 nell'alfabeto A si possono scrivere in modo che nessuna lettera appaia nella parola più di una volta?
- (b) Quante parole di lunghezza 4 si possono scrivere?
- (c) Quante parole di tre lettere si possono scrivere di modo che l'ultima lettera sia x o y e inoltre una delle lettere sia z ?

Soluzione. (a) La prima lettera può essere una qualunque delle lettere di A . Ho quindi 26 scelte. La seconda lettera può essere una qualunque delle lettere di A eccetto la prima. Ho quindi 25 scelte. La terza lettera può essere una qualunque delle lettere di A eccetto le prime due. Ho quindi 24 scelte. La risposta è pertanto $26 \cdot 25 \cdot 24 = 15.600$. Si osservi come la soluzione di questo esercizio sia simile alla dimostrazione della proposizione 9.8. Il motivo è che c'è una corrispondenza biunivoca tra l'insieme delle parole di lunghezza 3 nell'alfabeto A in cui nessuna lettera appare più di una volta e l'insieme delle applicazioni iniettive dell'insieme $\{1, 2, 3\}$ nell'insieme A . Tale corrispondenza associa alla parola $a_1 a_2 a_3 \in W_3$, con $a_1, a_2, a_3 \in A$, l'applicazione $\{1, 2, 3\} \rightarrow A$ che manda 1 in a_1 , 2 in a_2 e 3 in a_3 .

- (b) $|W_4| = |A^4| = 26^4 = 456\,976$.
- (c) Le parole di tre lettere nelle quali l'ultima lettera è x e la prima lettera è z sono 26. Le parole di tre lettere nelle quali l'ultima lettera è x , la seconda lettera è z e la prima lettera non è z sono 25. Le parole di tre lettere nelle quali l'ultima lettera è y e la prima lettera è z sono 26. Le parole di tre lettere nelle quali l'ultima lettera è y , la seconda lettera è z e la prima lettera non è z sono 25. La risposta è pertanto $26 + 25 + 26 + 25 = 102$. \square

Consideriamo ora le *permutazioni con ripetizioni*. Supponiamo di voler contare quante parole si riescono a scrivere con le lettere della parola "rosso". Si possono scrivere le parole "oossr", "osso", "rsoso", eccetera. Le cinque lettere r, o, s, s, o, possono essere permutate in $5!$ modi, però se nella parola "rosso" permuto la seconda lettera "o" con la quinta lettera "o" il risultato non cambia: trovo sempre la parola "rosso". Perciò i $5!$ modi non forniscono sempre delle parole distinte tra loro. Chiamiamo *permutazioni con ripetizioni* di r oggetti a_1, a_2, \dots, a_r , di cui il primo preso n_1 volte, il secondo preso n_2 volte, ..., l' r -esimo preso n_r volte, una qualunque $(n_1 + n_2 + \dots + n_r)$ -upla in cui a_1 appare n_1 volte, a_2 appare n_2 volte, ..., e a_r appare n_r volte. Equivalentemente, si tratta di una parola di lunghezza $n_1 + n_2 + \dots + n_r$ nell'alfabeto $A = \{a_1, a_2, \dots, a_n\}$ in cui lettera a_i appare n_i volte per ogni $i = 1, 2, \dots, r$.

9.2. Si dimostri che il numero di permutazioni con ripetizioni di r oggetti a_1, a_2, \dots, a_r , di cui il primo preso n_1 volte, il secondo preso n_2 volte, ..., l' r -esimo preso n_r volte è

$$\frac{(n_1 + n_2 + \dots + n_r)!}{n_1! n_2! \dots n_r!}.$$

Soluzione. Sia $n = n_1 + n_2 + \dots + n_r$. Consideriamo le n coppie distinte $(a_1, 1), (a_1, 2), \dots, (a_1, n_1), (a_2, 1), \dots, (a_2, n_2), \dots, (a_r, n_r)$. Queste n coppie distinte possono essere allineate in tanti modi quante sono le permutazioni di n oggetti, ossia in $n!$ modi. Quindi se All è l'insieme degli allineamenti delle coppie (a_i, j) , All è un insieme di cardinalità $n!$. Sia W l'insieme di tutte le parole di lunghezza n nell'alfabeto $A = \{a_1, a_2, \dots, a_n\}$ in cui lettera a_i appare n_i volte per ogni $i = 1, 2, \dots, r$. L'esercizio chiede di dimostrare che la cardinalità $|W|$ di W è $(n_1 + n_2 + \dots + n_r)!$

$\frac{n_1! n_2! \dots n_r!}{n_1! n_2! \dots n_r!}$. C'è una applicazione suriettiva $\pi: \text{All} \rightarrow W$ che manda ordinatamente un allineamento di coppie (a_i, j) nel corrispondente allineamento delle lettere a_i . Fissiamo una qualunque parola $w \in W$ e calcoliamo quanti degli $n!$ allineamenti delle n coppie (a_i, j) vengono mandati in w mediante π , ossia calcoliamo la cardinalità $|\pi^{-1}(w)|$ di $\pi^{-1}(w)$. Vediamo in quanti modi si può costruire un elemento di $\pi^{-1}(w)$. In w compaiono n_1 lettere uguali ad a_1 . La prima occorrenza della lettera a_1 in w può provenire da una qualunque delle n_1 coppie $(a_1, 1), (a_1, 2), \dots, (a_1, n_1)$. Ho quindi n_1 scelte. La seconda occorrenza della lettera a_1 in w può provare da una qualunque delle n_1 coppie $(a_1, 1), (a_1, 2), \dots, (a_1, n_1)$ eccetto quella da cui proveniva la prima occorrenza. Ho quindi $n_1 - 1$ scelte... La n_1 -esima occorrenza della lettera a_1 in w deve provenire dall'unica delle n_1 coppie $(a_1, 1), (a_1, 2), \dots, (a_1, n_1)$ rimasta. Ho quindi un'unica scelta. La prima occorrenza della lettera a_2 in w può provenire da una qualunque delle n_2 coppie $(a_2, 1), (a_2, 2), \dots, (a_2, n_2)$. Ho quindi n_2 scelte... Procedendo in questo modo si vede che gli allineamenti delle n coppie (a_i, j) che vengono mandati in w mediante π possono essere costruiti in $n_1! n_2! \dots n_r!$ modi. Quindi $|\pi^{-1}(w)| = n_1! n_2! \dots n_r!$ per ogni $w \in W$. Dato che $\pi: \text{All} \rightarrow W$ è un'applicazione suriettiva, $|\text{All}| = n!$ e $|\pi^{-1}(w)| = n_1! n_2! \dots n_r!$ per ogni $w \in W$, ne segue che $|W| = \frac{(n_1 + n_2 + \dots + n_r)!}{n_1! n_2! \dots n_r!}$. \square

Altri esercizi

9.3. Siano A, B sottoinsiemi di un insieme C . Si dimostri che $|C \setminus (A \cup B)| = |C| - |A| - |B| + |A \cap B|$.

9.4. Quando elenchiamo le 26 lettere dell'alfabeto latino siamo soliti dirle nel cosiddetto *ordine alfabetico*, ossia nell'ordine a, b, c, d, \dots , che è il modo convenzionale in cui si ordinano le lettere. In quanti modi si possono ordinare in realtà le 26 lettere dell'alfabeto?

9.5. Si calcoli

- (a) $\binom{10}{8}$;
- (b) $\binom{n+1}{n-2}$.

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

9.7. 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?

9.8. Le targhe automobilistiche di un certo stato sono costituite da due lettere seguite da tre cifre e poi ancora da due lettere. Visto che vi sono 26 lettere e 10 cifre, quante targhe differenti ci possono essere al massimo in quello stato?

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

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

9.10. Sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ la fattorizzazione in prodotto di primi di un numero naturale $n \geq 2$, con p_1, p_2, \dots, p_t primi positivi distinti.

- (a) Si dimostri che i divisori interi di n sono $2(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)$.
- (b) Si dimostri che se n è un quadrato, allora ci sono un numero dispari di numeri naturali che dividono n .
- (c) Si dimostri che se n non è un quadrato, allora ci sono un numero pari di numeri naturali che dividono n .

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

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

- (a) X ha un solo elemento?
- (b) X ha due elementi?
- (c) X ha tre elementi?

9.13. Nella seconda dimostrazione della proposizione 9.7 avevamo considerato la biiezione $\sigma: \mathcal{P}(A) \rightarrow \{0, 1\}^A$ dall'insieme delle parti di A nell'insieme di tutte le applicazioni di A in $\{0, 1\}$ definita ponendo $\sigma(S) = \chi_S$ per ogni $S \in \mathcal{P}(A)$. Qui χ_S denota la funzione caratteristica del sottoinsieme S di A . Come è definita l'applicazione inversa $\sigma^{-1}: \{0, 1\}^A \rightarrow \mathcal{P}(A)$? Cioè, se $f \in \{0, 1\}^A$, cos'è $\sigma^{-1}(f)$?

9.14. 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.]

9.15. Si dimostri che $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$ per ogni $n \geq 0$. [Suggerimento: Usare la formula del binomio. Oppure calcolare in due modi diversi quanti sono i sottoinsiemi di un insieme di cardinalità n .]

9.16. Si dimostri che $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0$ per ogni $n \geq 1$. [Suggerimento: usare la formula del binomio.]

9.17. Sviluppare $(1+x)^5$ facendo uso del triangolo di Tartaglia e della formula del binomio.

9.18. Nel gioco del Lotto si devono indovinare dei numeri scelti tra 1 e 90. In questo esercizio considereremo quindi solo i numeri interi positivi ≤ 90 . Supponiamo di giocare al Lotto in base b . Si tratta quindi di indovinare dei numeri interi positivi, che scriviamo in base b , minori o uguali a $(b-1)b$ (per $b=10$ questo è proprio 90). Se scriviamo i nostri numeri in base b usando le cifre $0, 1, 2, \dots, c_{b-1}$ i numeri che consideriamo si scrivono quindi tutti con una o due cifre, e giocando al Lotto in base b consideriamo solo i numeri interi positivi minori o uguali a $(b-1)b$. Vediamo un po' della terminologia che riguarda il Lotto (anche se questa terminologia ha ben poco di matematico).

- Si chiama *cadenza* un insieme di numeri aventi in comune la cifra finale. Ad esempio la cadenza di 2 è formata dai nove numeri 2, 12, 22, 32, 42, 52, 62, 72, 82. Quindi in una cadenza vi sono nove numeri. Nel Lotto in base b quanti numeri vi sono in una cadenza?
- Si chiama *decina* un insieme di numeri aventi in comune la prima cifra. Ad esempio 20, 21, 22, 23, 24, 25, 26, 27, 28, 29 è una decina. Se si pensa un attimo ci si accorge che per evitare l'eccezione legata al fatto che i numeri tra 1 e 9 hanno una sola cifra e che 90 è l'unico numero avente 9 come prima cifra, ci si rende conto che anche 1, 2, 3, 4, 5, 6, 7, 8, 9, 90 deve essere considerata una decina, che chiameremo *decina eccezionale*. Quindi in una decina vi sono dieci numeri. Nel Lotto in base b quanti numeri vi sono in una decina? Qual è la decina eccezionale?
- Si chiamano *gemelli* gli otto numeri con le due cifre uguali, ossia 11, 22, 33, 44, 55, 66, 77, 88. Nel Lotto in base b quanti numeri gemelli vi sono?
- Si chiama *vertibile* un insieme di due numeri della forma $\{c_1c_2, c_2c_1\}$ con $c_1, c_2 \in \{1, 2, \dots, 8\}$ e $c_1 \neq c_2$. Ad esempio sono vertibili {16, 61}, {67, 76}, {13, 31}, eccetera. I vertibili sono tanti quanti i sottoinsiemi $\{c_1, c_2\}$ di cardinalità due dell'insieme $\{1, 2, 3, \dots, 8\}$ di cardinalità otto, e quindi sono in tutto $\binom{8}{2} = 28$. Nel Lotto in base b quanti vertibili vi sono?
- Si chiamano *numeretti* i nove numeri di una sola cifra, ossia 1, 2, 3, 4, 5, 6, 7, 8, 9. Nel Lotto in base b quanti numeretti vi sono?
- Si chiama *figura* un insieme di dieci numeri tra di loro congrui modulo 9. Ad esempio 3, 12, 21, 30, 39, 48, 57, 66, 75, 84 è una figura. Nel Lotto in base b chiamiamo *figura* un insieme di numeri tra di loro congrui modulo $b-1$. Quanti numeri vi sono allora in una figura?
- Si chiama *cifra* (!) un insieme di numeri in cui appare una stessa cifra. Ad esempio 3 appare nei numeri 3, 13, 23, ..., 83, 30, 31, 32, ..., 38, 39 e quindi questi numeri formano una cifra. Supponiamo $c \neq 9$. La cifra c appare nei dieci numeri della decina avente come prima cifra c e nei nove numeri della cadenza avente come seconda cifra c , ma il numero gemello cc appare sia nella decina che nella cadenza. Quindi in una cifra vi sono generalmente 18 numeri.

Fa eccezione 9, la cui cifra è {9, 19, 29, ..., 89, 90} e ha quindi 10 elementi. Nel Lotto in base b quanti numeri vi sono in una cifra?

- (h) Si chiama insieme di numeri *complementari* un insieme di due numeri della forma $\{n, m\}$ con $n + m = 91$. Nel Lotto in base b chiamiamo insieme di numeri *complementari* un insieme di due numeri della forma $\{n, m\}$ con $n + m = (b - 1)b + 1$. Quanti insiemi di numeri complementari ci sono nel Lotto in base b ?
- (i) Si chiama insieme di numeri *diametrali* un insieme di due numeri della forma $\{n, m\}$ con $|n - m| = 45$. Per capire l'origine di questa terminologia si immagini di scrivere i numeri da 1 a 90 lungo una circonferenza a distanza regolare. Nel Lotto in base b chiamiamo insieme di numeri *diametrali* un insieme di due numeri della forma $\{n, m\}$ con $|n - m| = (b - 1)b/2$. Quanti insiemi di numeri diametrali ci sono nel Lotto in base b ?

9.19. Nel gioco del Superenalotto si devono indovinare 6 numeri scelti tra 1 e 90. Quante possibilità di scelta vi sono?

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

Appendice 9.1. Complementi sugli insiemi numerabili

9.19 PROPOSIZIONE. *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:

$$\varphi_S(0) = \min S,$$

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

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 φ_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 $n \in \psi^{-1}(B)$ (ψ' si dice l'applicazione ottenuta da ψ 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. Pertanto anche B è finito o numerabile. \square

9.20 LEMMA. *Sia A un insieme non vuoto. Esiste un'applicazione suriettiva $\psi: \mathbb{N} \rightarrow A$ 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 $\psi: \mathbb{N} \rightarrow A$ definita, per ogni $i \in \mathbb{N}$, da $\psi(i) = a_{i+1}$ se $i < n$ e $\psi(i) = a_n$ se $i \geq n$. Se A è un insieme numerabile, esiste per definizione un'applicazione biiettiva $\psi: \mathbb{N} \rightarrow A$. Questo dimostra una delle due implicazioni dell'enunciato del lemma.

Per dimostrare l'altra implicazione supponiamo invece che esista un'applicazione suriettiva $\psi: \mathbb{N} \rightarrow A$. Per l'esercizio 3.4 esiste un'applicazione $\varphi: A \rightarrow \mathbb{N}$ tale che $\psi \circ \varphi = \iota_A$. Dato che l'applicazione composta $\psi \circ \varphi = \iota_A$ è iniettiva, anche l'applicazione φ è iniettiva (vedi proposizione 3.2(a)). Quindi l'applicazione $\varphi': A \rightarrow \varphi(A)$ definita da $\varphi'(a) = \varphi(a)$ per ogni $a \in A$ (φ' è l'applicazione ottenuta da φ restringendo il codominio a $\varphi(A)$) è una biiezione. Ma allora A è equipotente a $\varphi(A)$, e per la proposizione 9.19 $\varphi(A) \subseteq \mathbb{N}$ deve essere finito o numerabile. Quindi anche A è finito o numerabile. \square

9.21 PROPOSIZIONE. *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 9.20 esiste per ogni $i \in I$ un'applicazione suriettiva $\psi_i: \mathbb{N} \rightarrow A_i$ ed esiste un'applicazione suriettiva $\varphi: \mathbb{N} \rightarrow I$. 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 $f(p_k^{t+1}) = \psi_{\varphi(k)}(t)$. Allora f è un'applicazione suriettiva che manda le potenze di p_k in $A_{\varphi(k)}$. Per la proposizione 9.19 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 9.20. \square

9.22 ESEMPIO. Nella dimostrazione della proposizione 9.17 abbiamo visto che l'insieme $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ è numerabile. Dimostriamo questo stesso fatto come applicazione della proposizione 9.21.

Per ogni $n \in \mathbb{N}^*$ sia

$$A_n = \left\{ \frac{1}{n}, \frac{2}{n-1}, \frac{3}{n-2}, \dots, \frac{n}{1} \right\}$$

l'insieme dei numeri razionali positivi che possono essere scritti come quoziente di due interi positivi la cui la somma 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 9.21. \square

9.23 ESEMPIO. Abbiamo già visto che \mathbb{Q} è numerabile (proposizione 9.17). Questo stesso risultato può essere dimostrato anche partendo da quanto visto nell'esempio 9.22 (\mathbb{Q}^+ è numerabile) e nella proposizione 9.21. Infatti 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 9.21. \square

Altri esercizi

9.21. Si dimostri che se A e B sono insiemi numerabili, anche $A \times B$ è un insieme numerabile.
 [Suggerimento: proposizione 9.21.]

9.22. Si dimostri che se A è un insieme finito o numerabile, allora l'insieme W_A delle parole nell'alfabeto A è numerabile.

§10. Ordinamenti

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

10.1 ESEMPIO. 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 in 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

10.2 ESEMPIO. 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 $y|z$, allora 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

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

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

Un insieme A su cui è definito un ordinamento parziale ϱ si dice un *insieme parzialmente ordinato* (o *semiordinato*). Come mostrano gli esempi 10.1, 10.2 e 10.3, 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 ϱ indicheremo talvolta tale insieme ordinato come (A, ϱ) . Quindi nell'esempio 10.1 abbiamo considerato l'insieme parzialmente ordinato (\mathbb{N}^*, \leq) , nell'esempio 10.2 l'insieme parzialmente ordinato $(\mathbb{N}^*, |)$, nell'esempio 10.3 l'insieme parzialmente ordinato (\mathbb{N}^*, ϱ) . Quando però sarà ben chiaro quale ordinamento ϱ si sta considerando su un insieme A , continueremo a dire che A è un insieme parzialmente ordinato invece di specificare che (A, ϱ) è l'insieme parzialmente ordinato, sottointendendo così l'ordinamento ϱ . Diremo, ad esempio, che x appartiene all'insieme parzialmente ordinato A , ecc.

I simboli più usati per denotare gli ordinamenti sono \leq , \preceq , \sqsubseteq .

Un ordinamento parziale \leq su un insieme A si dice un *ordinamento totale* (o un *ordine totale* o *lineare*) se per ogni $a, b \in A$ si ha $a \leq b$ oppure $b \leq a$, cioè se due elementi $a, b \in A$ sono sempre *confrontabili*. Se (A, \leq) è un insieme parzialmente ordinato e l'ordinamento parziale \leq su A è totale diremo che (A, \leq) è un *insieme totalmente ordinato* (o *linearmente ordinato*, o una *catena*). Negli esempi visti prima si ha che (\mathbb{N}^*, \leq) e (\mathbb{N}^*, ϱ) sono insiemis totalmente ordinati, mentre $(\mathbb{N}^*, |)$ non è un insieme totalmente ordinato in quanto, ad esempio, 2 non divide 3 e 3 non divide 2.

Siano (A, \leq) , (A', \preceq) insiemis parzialmente ordinati. Un *omomorfismo di insiemis ordinati* φ di A in A' è un'applicazione $\varphi: A \rightarrow A'$ tale che $x \leq y$ implica $\varphi(x) \preceq \varphi(y)$ per ogni $x, y \in A$.

10.4 LEMMA. *Siano (A, \leq) , (A', \preceq) due insiemis parzialmente ordinati e $\varphi: A \rightarrow A'$ una biiezione. Le seguenti affermazioni sono equivalenti:*

- (a) *entrambe le applicazioni φ e φ^{-1} sono omomorfismi di insiemis ordinati;*
- (b) *per ogni $x, y \in A$ si ha $x \leq y$ se e solo se $\varphi(x) \preceq \varphi(y)$.*

Dimostrazione. (a) \Rightarrow (b) Supponiamo che valga l'affermazione (a). Siano $x, y \in A$. Dato che φ è un omomorfismo di insiemis ordinati, se $x \leq y$, allora $\varphi(x) \preceq \varphi(y)$. Viceversa, da $\varphi(x) \preceq \varphi(y)$ segue che $\varphi^{-1}(\varphi(x)) \preceq \varphi^{-1}(\varphi(y))$ perché φ^{-1} è omomorfismo di insiemis ordinati, e quindi $x \leq y$.

(b) \Rightarrow (a) Dato che per ogni $x, y \in A$ si ha che $x \leq y$ implica $\varphi(x) \preceq \varphi(y)$, l'applicazione φ è un omomorfismo di insiemis ordinati. Mostriamo che anche l'applicazione $\varphi^{-1}: A' \rightarrow A$ è un omomorfismo di insiemis ordinati. Se $x', y' \in A'$ e $x' \preceq y'$, allora $\varphi(\varphi^{-1}(x')) = \iota_{A'}(x') = x' \preceq y' = \iota_{A'}(y') = \varphi(\varphi^{-1}(y'))$. Ma dato che per ogni $x, y \in A$ si ha che $\varphi(x) \preceq \varphi(y)$ implica $x \leq y$, prendendo $x = \varphi^{-1}(x')$ e $y = \varphi^{-1}(y')$ si ricava che $\varphi^{-1}(x') \preceq \varphi^{-1}(y')$. Questo dimostra che anche $\varphi^{-1}: A' \rightarrow A$ è un omomorfismo di insiemis ordinati. \square

Una biiezione $\varphi: A \rightarrow A'$ tra due insiemis parzialmente ordinati (A, \leq) e (A', \preceq) che soddisfi ad una delle proprietà equivalenti del lemma 10.4, e quindi a entrambe, si dice un *isomorfismo di insiemis ordinati*. Se esiste un isomorfismo di insiemis ordinati di A in A' gli insiemis parzialmente ordinati A e A' si dicono *isomorfi* (o *ordinatamente isomorfi*).

10.5 ESEMPIO. Si consideri l'applicazione identica $\iota_{\mathbb{N}^*}: \mathbb{N}^* \rightarrow \mathbb{N}^*$, dove il dominio si suppone parzialmente ordinato dalla relazione $|$ dell'esempio 10.2 e il codominio si suppone ordinato dall'ordinamento usuale \leq dei numeri naturali positivi (vedi esempio 10.1). Allora $\iota_{\mathbb{N}^*}$ è un omomorfismo di insiemi ordinati perché se $x, y \in \mathbb{N}^*$ e $x|y$ allora $x \leq y$. Invece la biiezione $\iota_{\mathbb{N}^*}$ non è un isomorfismo, in quanto non è vero che se $x, y \in \mathbb{N}^*$ e $x \leq y$ allora $x|y$. \square

10.6 ESEMPIO. È facile dimostrare che per ogni insieme X l'insieme delle parti $\mathcal{P}(X)$ è un insieme parzialmente ordinato dalla relazione di inclusione \subseteq (si veda l'esercizio 10.1). Siano ora $X \subseteq Y$ insiemi. Definiamo $\varphi: \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ ponendo $\varphi(Z) = X \cap Z$ per ogni $Z \in \mathcal{P}(Y)$. Allora φ è un omomorfismo di insiemi ordinati. Infatti se $Z, Z' \in \mathcal{P}(Y)$ e $Z \subseteq Z'$, allora $X \cap Z \subseteq X \cap Z'$, cioè $\varphi(Z) \subseteq \varphi(Z')$. Si osservi anche che φ è un isomorfismo se e solo se $X = Y$. Infatti se φ è un isomorfismo, dato che $X, Y \in \mathcal{P}(Y)$ e $\varphi(X) = \varphi(Y) = X$, per l'iniettività di φ si deve avere $X = Y$. Viceversa, se $X = Y$ si ha $\varphi(Z) = X \cap Z = Z$ per ogni $Z \in \mathcal{P}(Y)$, e quindi φ è l'applicazione identica di $\mathcal{P}(X)$, e questa è certamente un isomorfismo. \square

Se (A, \leq) è un insieme parzialmente ordinato e $B \subseteq A$, allora anche B risulta essere un insieme parzialmente ordinato (se $b \leq b'$ nell'insieme parzialmente ordinato A e $b, b' \in B$ si pone $b \leq b'$ anche nell'insieme parzialmente ordinato B). Si dice in questo caso che B è l'insieme parzialmente ordinato ottenuto *restringendo* l'ordinamento parziale di A a B , o anche che l'ordinamento di A ha *indotto* un ordinamento su B . In questo caso diremo che B è un *sottoinsieme ordinato* di A . Volendo essere più precisi e guardando l'ordinamento \leq su A come relazione, cioè come sottoinsieme di $A \times A$, si ha che l'ordinamento indotto su B è $\leq \cap (B \times B)$.

10.7 ESEMPIO. Se $A = \mathbb{R}$ è l'insieme dei numeri reali ordinato mediante l'ordinamento usuale \leq (cioè l'ordine totale su \mathbb{R} con cui si considerano usualmente ordinati i numeri reali) e $B = \mathbb{N}^*$, allora l'ordinamento indotto su \mathbb{N}^* dall'ordinamento totale di \mathbb{R} è l'ordinamento usuale di \mathbb{N}^* da noi già studiato nell'esempio 10.1. \square

10.8 ESEMPIO. Siano \mathbb{N}^* l'insieme dei numeri naturali positivi e $|$ l'ordinamento parziale su \mathbb{N}^* definito nell'esempio 10.2. Sia

$$B = \{2^n \mid n \in \mathbb{N}^*\} \subseteq \mathbb{N}^*$$

l'insieme delle potenze di 2 a esponente intero positivo. Allora:

- (a) l'ordinamento indotto su B restringendo l'ordinamento $|$ di \mathbb{N}^* è un ordinamento totale;
- (b) l'ordinamento indotto su B dall'ordinamento $|$ di \mathbb{N}^* coincide con l'ordinamento indotto su B dall'ordinamento usuale \leq di \mathbb{N}^* ;
- (c) l'applicazione $\varphi: \mathbb{N}^* \rightarrow B$ definita da $\varphi(n) = 2^n$ per ogni $n \in \mathbb{N}^*$ è un isomorfismo di insiemi ordinati tra l'insieme ordinato (\mathbb{N}^*, \leq) e il sottoinsieme ordinato B di $(\mathbb{N}^*, |)$. \square

Se (A, \leq) è un insieme parzialmente ordinato, definiamo una relazione ϱ su A ponendo, per ogni $a, b \in A$, $a \varrho b$ se $b \leq a$. Allora ϱ è un ordine parziale su A in quanto:

- (1) ϱ è riflessiva (perché per ogni $a \in A$ si ha $a \leq a$ e quindi $a \varrho a$).
- (2) ϱ è antisimmetrica (perché se $a, b \in A$, $a \varrho b$ e $b \varrho a$, allora $b \leq a$ e $a \leq b$; ne segue che $a = b$ per l'antisimmetria di \leq).
- (3) ϱ è transitiva (perché se $a, b, c \in A$, $a \varrho b$ e $b \varrho c$, allora $b \leq a$ e $c \leq b$ e quindi $c \leq a$. Ne segue che $a \varrho c$).

L'ordinamento ϱ su A viene usualmente denotato con \geq ed è detto l'*ordine parziale inverso* di \leq .

Sia (A, \leq) un insieme parzialmente ordinato, sia $a \in A$ e sia $B \subseteq A$. Diremo che

- $\triangleright a$ è il *minimo* di A se $a \leq x$ per ogni $x \in A$;
- $\triangleright a$ è il *massimo* di A se $a \geq x$ per ogni $x \in A$;
- $\triangleright a$ è un *elemento minimale* di A se per ogni $x \in A$ si ha che $x \leq a$ implica $x = a$;
- $\triangleright a$ è un *elemento massimale* di A se per ogni $x \in A$ si ha che $a \leq x$ implica $x = a$;
- $\triangleright a$ è un *minorante* di B (o un *minorante di B in A*) se $a \leq b$ per ogni $b \in B$;
- $\triangleright a$ è un *maggiorante* di B (o un *maggiorante di B in A*) 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 (in A) se a è il massimo dell'insieme dei minoranti di B in A ; 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 (in A) se a è il minimo dell'insieme dei maggioranti di B in A ; 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 $a' \geq a$.

Naturalmente non è detto che per ogni insieme parzialmente ordinato A e per ogni suo sottoinsieme B esistano sempre massimo, minimo, elementi massimali o minimali, maggioranti, ecc.

10.9 ESEMPIO. \mathbb{N}^* con il suo ordinamento usuale (esempio 10.1) non ha massimo e ha 1 come minimo; \mathbb{Z} e \mathbb{Q} con l'ordinamento usuale non hanno né massimo né minimo. \square

10.10 ESEMPIO. Se $A = \{a\}$ ha un unico elemento e \leq è l'unico ordine possibile su A , allora chiaramente a è sia massimo che minimo di A . \square

10.11 ESEMPIO. Sia $(\mathbb{N}^*, |)$ l'insieme parzialmente ordinato che abbiamo già considerato nell'esempio 10.2. Allora \mathbb{N}^* ha un minimo (il numero 1, in quanto $1 | n$ per ogni $n \in \mathbb{N}^*$), e non ha massimo (perché non esiste nessun $n_0 \in \mathbb{N}^*$ tale che $n | n_0$ per ogni $n \in \mathbb{N}^*$). Inoltre 1 è un elemento minimale di \mathbb{N}^* (perché se $n \in \mathbb{N}^*$ e $n | 1$, allora $n = 1$), mentre

\mathbb{N}^* non ha elementi massimali (perché per ogni $n_0 \in \mathbb{N}^*$ esiste $n_1 \in \mathbb{N}^*$ tale che $n_0 | n_1$ e $n_0 \neq n_1$). Cerchiamo l'estremo inferiore in \mathbb{N}^* dell'insieme $P^+ = \{2t \mid t \in \mathbb{N}^*\}$ dei numeri pari positivi: i minoranti di P^+ in \mathbb{N}^* sono i numeri $n \in \mathbb{N}^*$ che dividono tutti i numeri pari, e quindi sono solo 1 e 2. Nell'insieme {1, 2} il numero 2 è il massimo perché $1 \nmid 2$. Quindi 2 è l'estremo inferiore di P^+ in \mathbb{N}^* . Invece non esistono $n \in \mathbb{N}^*$ che sono divisibili per tutti gli elementi di P^+ ; pertanto P^+ non ha maggioranti in \mathbb{N}^* , e quindi, a maggior ragione, P^+ non ha un estremo superiore in \mathbb{N}^* .

Sia ora $D_{>1} = \{2t + 1 \mid t \in \mathbb{N}^*\}$ l'insieme dei numeri dispari maggiori di 1, sia $A = D_{>1} \cup \{2\}$, e supponiamo che A abbia l'ordine indotto da $(\mathbb{N}^*, |)$. 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 $2|x$ allora $x = 2$. Invece gli elementi di $D_{>1}$ non sono elementi massimali di A , perché per ogni $n \in D_{>1}$ si ha $n | n^2$ 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 \mathbb{N}^* . I minoranti di A in \mathbb{N}^* sono gli $n \in \mathbb{N}^*$ 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 \mathbb{N}^* . In particolare 1 è l'estremo inferiore di A in \mathbb{N}^* . \square

Nell'esercizio 10.2 dimostreremo che se un insieme parzialmente ordinato A ha un minimo a , allora a è l'unico minimo di A . Analogamente se un insieme parzialmente ordinato ha un massimo, tale massimo è unico.

Il minimo di A è un elemento minimale di A . Infatti sia a il minimo di A . Sia $x \in A$ tale che $x \leq a$. Dato che a è minimo sappiamo che $a \leq x$, e quindi per l'antisimmetria $x = a$. Quindi a è un elemento minimale di A . Analogamente, il massimo è massimale. Non vale il viceversa, cioè A può avere un elemento minimale che non è il minimo di A . Ad esempio l'insieme parzialmente ordinato A dell'esempio 10.11 ha esattamente un elemento massimale ma non ha massimo.

Un insieme parzialmente ordinato (A, \leq) può essere talvolta rappresentato in un piano nel modo seguente: gli elementi di A sono 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 $x \leq y$.

10.12 ESEMPIO. Si considerino gli insiemi parzialmente ordinati rappresentati nella figura 10.1. Nell'insieme parzialmente ordinato A si ha $a \leq c, c \leq e, c \leq g$. 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'ordine 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. \square

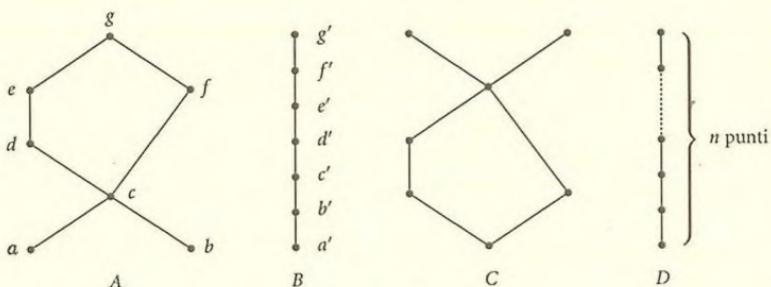


FIGURA 10.1.

Un insieme parzialmente ordinato A si dice *bene ordinato* se ogni sottoinsieme non vuoto di A ha minimo. Ad esempio \mathbb{N} con l'ordine usuale è un insieme bene ordinato, mentre \mathbb{Z} , \mathbb{Q} ed \mathbb{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 $\mathcal{P}(A)$.

- Si dimostri che $(\mathcal{P}(A), \subseteq)$ è un insieme parzialmente ordinato.
- 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 $X \subseteq X$;

antisimmetrica, perché se $X, Y \in \mathcal{P}(A)$, $X \subseteq Y$ e $Y \subseteq X$, allora $X = Y$;

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 $\mathcal{P}(A) = \{\emptyset, A\}$, 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. Si dica se i seguenti sono insiemi parzialmente ordinati (totalmente ordinati):

- L'insieme dei numeri complessi \mathbb{C} dotato della relazione \lesssim definita da $z \lesssim z'$ se $|z| \leq |z'|$, $z, z' \in \mathbb{C}$;
- (\mathbb{Z}, \leq) , ove \leq è definita da $x \leq y$ se $x + z = y$ per qualche $z \in \mathbb{Z}$;
- (\mathbb{Z}, \leq) , ove \leq è definita da $x \leq y$ se $x + n = y$ per qualche $n \in \mathbb{N}$.

10.5. Se $\mathbb{Z}^{\mathbb{N}}$ è l'insieme di tutte le applicazioni di \mathbb{N} in \mathbb{Z} ed $f, g \in \mathbb{Z}^{\mathbb{N}}$, definiamo $f \lesssim g$ se $f(n) \leq g(n)$ per ogni $n \in \mathbb{N}$. Si dimostri che $(\mathbb{Z}^{\mathbb{N}}, \lesssim)$ è un insieme parzialmente ordinato che non è totalmente ordinato.

10.6. Si provi che se (A, \leq) è totalmente ordinato, allora (A, \geq) è totalmente ordinato.

10.7. 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:

- la relazione \preceq è un ordinamento totale su $\mathbb{N} \times \mathbb{N}$;
- 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;
- l'applicazione φ 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 .

10.8. Si rappresenti nel piano:

- l'insieme parzialmente ordinato \mathbb{N} con l'ordine usuale;
- l'insieme parzialmente ordinato $(\mathcal{P}(\{0, 1, 2\}), \subseteq)$ (vedi esercizio 10.1);
- l'insieme parzialmente ordinato $(\{1, 2, 3, 6\}, |)$.

10.9. 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):

- 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;
- il sottoinsieme $\{a, b, c\}$ di A con l'ordine indotto dall'ordine di A non è totalmente ordinato;
- il sottoinsieme $\{a, c, d\}$ di A con l'ordine indotto dall'ordine di A è totalmente ordinato;
- l'elemento g è il massimo di A , mentre A non ha minimo;
- 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 .

10.10. Si consideri l'insieme parzialmente ordinato rappresentato nella figura 10.2.

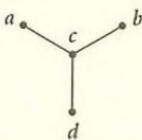


FIGURA 10.2.

Si dica se l'insieme è totalmente ordinato, quali sono gli elementi massimali, qual è il massimo, quali sono gli elementi minimali, qual è il minimo, quali sono gli estremi superiore e inferiore e il massimo e il minimo dell'insieme $\{a, b\}$, quali sono i maggioranti dell'insieme $\{c, d\}$.

10.11. Sia $A = \{a, b, c, d\}$ l'insieme parzialmente ordinato rappresentato nella figura 10.2 e sia $B = (\{0, 1, 2, 3\}, \leq)$, sottoinsieme ordinato di (\mathbb{N}, \leq) . Sia $\varphi: A \rightarrow B$ definita da $\varphi(a) = 3$, $\varphi(b) = 2$, $\varphi(c) = 1$, $\varphi(d) = 0$. Si faccia vedere che φ è un omomorfismo di insiemi parzialmente ordinati, che φ è biiettivo, e che φ non è un isomorfismo.

10.12. Si considerino gli insiemi parzialmente ordinati $(\mathcal{P}(\{a, b\}), \subseteq)$ (vedi esercizio 10.1) e $(\{1, 2, 3, 6\}, |)$, ove quest'ultimo insieme è sottoinsieme ordinato di $(\mathbb{N}^*, |)$ (vedi esempio 10.2). Si determini un isomorfismo di insiemi ordinati $\varphi: \mathcal{P}(\{a, b\}) \rightarrow \{1, 2, 3, 6\}$. Si determinino tutti gli isomorfismi di insiemi ordinati $\varphi: \mathcal{P}(\{a, b\}) \rightarrow \{1, 2, 3, 6\}$. [Suggerimento: si rappresentino nel piano i due insiemi parzialmente ordinati.]

10.13. Siano X un insieme con almeno due elementi e $(\mathcal{P}(X), \subseteq)$ l'insieme delle parti di X ordinato mediante l'inclusione. Si consideri il sottoinsieme ordinato $A = \mathcal{P}(X) \setminus \{\emptyset\}$ di $(\mathcal{P}(X), \subseteq)$. Si dimostri che A non ha minimo e che i suoi elementi minimali sono esattamente gli $\{x\} \in A$, dove $x \in X$. Si osservi che A non ha un unico elemento minimale perché X ha almeno due elementi.

10.14. Si provi che se A è totalmente ordinato e $a \in A$, allora a è massimo di A se e solo se a è un elemento massimale di A .

10.15. Si provi che ogni insieme parzialmente ordinato finito ha almeno un elemento massimale (minimale).

10.16. Quali sono gli elementi minimali, massimali, minimi e massimi degli esempi visti in questo §10? E di $\mathbb{N}^* \setminus \{1\}$ con l'ordine indotto da $(\mathbb{N}^*, |)$ (vedi esempio 10.2)?

10.17. Sia \mathbb{Q} l'insieme dei numeri razionali dotato dell'ordine usuale. Si dica se esistono ed eventualmente quali sono gli estremi superiore ed inferiore dei seguenti sottoinsiemi di \mathbb{Q} :

- (a) $\{x \in \mathbb{Q} \mid x \geq 0\}$;
 (b) $\{x \in \mathbb{Q} \mid 0 < x \leq \sqrt{2}\}$;

- (c) $\{x \in \mathbb{Q} \mid x \geq \pi\}$;
- (d) \mathbb{Q} ;
- (e) $\{x \in \mathbb{Q} \mid x^2 \leq 4\}$;
- (f) $\{x \in \mathbb{Q} \mid x^2 < 4\}$.

10.18. Sia (A, \leq) parzialmente ordinato, $B \subseteq A$. Si provi che se $b \in B$ è il massimo di B , allora b è l'estremo superiore di B in A .

10.19. Si provi che ogni sottoinsieme ordinato di un insieme bene ordinato è bene ordinato.

10.20. Siano $(A, \leq), (B, \leq)$ insiemi parzialmente ordinati. Definiamo la relazione \leq su $A \times B$ in questo modo:

$$(a, b) \leq (a', b') \text{ se e solo se o } a \neq a' \text{ e } a \leq a', \text{ oppure } a = a' \text{ e } b \leq b'.$$

Si provi che:

- (a) $(A \times B, \leq)$ è un insieme parzialmente ordinato (detto il *prodotto lessicografico* di (A, \leq) e (B, \leq));
- (b) se A e B sono totalmente (bene) ordinati, allora $A \times B$ è totalmente (bene) ordinato.

10.21. 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 $X = A$.

10.22. 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.

10.23. Nell'esempio 10.12 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 $A = \{1/z \mid z \in \mathbb{Z}, z \neq 0\} \subseteq \mathbb{R}$ 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 .

10.24. Sia (\mathcal{F}, \leq) l'insieme parzialmente ordinato dell'esercizio 10.21 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 $f(a) = g(a)$. Si

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

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 φ è ben definita, e che la coppia (S, φ) 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 $f(a) = g(a)$.

10.25. 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 $\mathcal{P}(X)$.

10.26. 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 minimi del sottoinsieme ordinato A di P .
 (b) Si consideri il sottoinsieme $B = \{\mathbb{N} \setminus \{n\} \mid n \in \mathbb{N}\}$ di A . Si calcolino, se esistono, l'estremo inferiore e l'estremo superiore di B in A .

§11. Reticoli, reticoli booleani

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 superiore e inferiore 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 $z \leq x \wedge y$.

11.1 ESEMPIO. 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 $z \in A$, $z \leq x$ e $z \leq y$, allora $z \leq x$. 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

In particolare si ha $x \wedge x = x \vee x = x$ per ogni elemento x di un insieme parzialmente ordinato A .

11.2 ESEMPIO. 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 11.1. 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

11.3 ESEMPIO. 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

$$(f \vee g)(x) = \max\{f(x), g(x)\}$$

e

$$(f \wedge g)(x) = \min\{f(x), g(x)\}$$

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

11.4 ESEMPIO. Sia $\mathcal{P}_{\infty}(\mathbb{Z})$ l'insieme di tutti i sottoinsiemi infiniti di \mathbb{Z} . Ad esempio se $\mathbb{P} = \{2z \mid z \in \mathbb{Z}\}$ e $\mathbb{D} = \{2z + 1 \mid z \in \mathbb{Z}\}$ sono gli insiemi dei numeri interi pari e dispari rispettivamente, allora $\mathbb{P} \in \mathcal{P}_{\infty}(\mathbb{Z})$ e $\mathbb{D} \in \mathcal{P}_{\infty}(\mathbb{Z})$, 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 $\mathbb{P} \wedge \mathbb{D}$. Cerchiamo infatti l'estremo inferiore di $\{\mathbb{P}, \mathbb{D}\}$ in $\mathcal{P}_\infty(\mathbb{Z})$. I minoranti di $\{\mathbb{P}, \mathbb{D}\}$ in $\mathcal{P}_\infty(\mathbb{Z})$ sono i sottoinsiemi infiniti di \mathbb{Z} che sono contenuti sia in \mathbb{P} che in \mathbb{D} . Dato che non esistono sottoinsiemi infiniti contenuti sia in \mathbb{P} che in \mathbb{D} , se ne deduce che l'estremo inferiore di $\{\mathbb{P}, \mathbb{D}\}$ 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

11.5 ESEMPIO. Ogni insieme totalmente ordinato è un reticolo, in quanto se $x, y \in T$ e (T, \leq) è totalmente ordinato, allora o $x \leq y$ oppure $x \geq y$. Se $x \leq y$, per l'esempio 11.1 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

11.6 ESEMPIO. Consideriamo la relazione $|$ su \mathbb{N} definita, per ogni $x, y \in \mathbb{N}$, da $x|y$ se esiste $z \in \mathbb{N}$ tale che $y = xz$. Allora $(\mathbb{N}, |)$ è un insieme parzialmente ordinato che ha il numero 1 come minimo e il numero 0 come massimo. Inoltre $(\mathbb{N}, |)$ è un reticolo. In questo caso per ogni $x, y \in \mathbb{N}$, $x \wedge y$ e $x \vee y$ sono rispettivamente il massimo comun divisore ≥ 0 e il minimo comune multiplo ≥ 0 di x e y . \square

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

11.7 ESEMPIO. 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 sia 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

Se (L, \leq) è un reticolo, allora anche (L, \geq) , ossia L con l'ordine inverso (§10, pagina 90) è un reticolo. L'estremo inferiore di due elementi x, y in (L, \leq) è il loro estremo superiore in (L, \geq) , e l'estremo superiore in (L, \leq) è l'estremo inferiore in (L, \geq) . Supponiamo di aver dimostrato che un qualche enunciato A è vero per ogni reticolo (L, \leq) . Allora l'enunciato A vale anche per il reticolo (L, \geq) . Ma l'enunciato A riferito al reticolo (L, \geq) è l'enunciato A^* che si ottiene da A scambiando \leq con \geq e \vee con \wedge , cioè è l'enunciato duale di A , riferito al reticolo (L, \leq) . Quindi se A è un enunciato vero per ogni reticolo, anche l'enunciato duale A^* è vero per ogni reticolo. Abbiamo così dimostrato il seguente

11.8 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.

11.9 ESEMPIO. Siano A, B, C, D, E gli enunciati dell'esempio 11.7. Allora: A è vero per ogni reticolo (basta prendere come y lo stesso elemento x), e quindi anche A^* è vero per ogni reticolo per il principio di dualità dei reticolli; l'enunciato B è vero per ogni reticolo (perché $x \wedge y \neq x$ equivale a $x \not\leq y$ in base a quanto abbiamo dimostrato nell'esempio 10.1), e quindi anche B^* è vero per il principio di dualità dei reticolli; nella proposizione 11.13 vedremo che C è vero per ogni reticolo, e quindi il suo duale C^* è vero. Anche D è vero per ogni reticolo (proposizione 11.12(a)), e quindi D^* è vero per ogni reticolo, ma questo è evidente perché D è autoduale. Invece E non è vero per ogni reticolo, ma solo per gli insiemi totalmente ordinati. \square

11.10 ESEMPIO. Si dimostri per esercizio che se L è un reticolo, $a, b, c, d \in L$, $a \leq b$ e $c \leq d$, allora $a \vee c \leq b \vee d$. Quindi ci troviamo di fronte a un enunciato vero per ogni reticolo. Per il principio di dualità dei reticolli si ha che se $a, b, c, d \in L$, $a \geq b$ e $c \geq d$, allora $a \wedge c \geq b \wedge d$. \square

11.11 ESEMPIO. Attenzione, è errato enunciare il principio di dualità per i reticolli 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

11.12 PROPOSIZIONE. Sia (L, \leq) un reticolo. Allora

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

Dimostrazione. (a) Segue immediatamente dalla definizione di estremo superiore e inferiore.

(b) Dimostriamo la prima. Si ha $x \leq x \vee (y \vee z)$ e $y \vee z \leq x \vee (y \vee z)$. Ma $y \leq y \vee z$ e $z \leq y \vee z$. Quindi $y \leq x \vee (y \vee z)$ e $z \leq x \vee (y \vee z)$; pertanto $x \vee y \leq x \vee (y \vee z)$, e allora $(x \vee y) \vee z \leq x \vee (y \vee z)$. Similmente si dimostra che $x \vee (y \vee z) \leq (x \vee y) \vee z$. Per l'antisimmetria $x \vee (y \vee z) = (x \vee y) \vee z$.

La seconda uguaglianza di (b) segue dalla prima per il principio di dualità dei reticolli.

(c) Dato che $x \wedge y \leq x$, si ha $x \vee (x \wedge y) = x$ per l'esempio 11.1. La seconda uguaglianza segue dalla prima per il principio di dualità. \square

Si noti che in generale non è vero che $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ e che $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ per ogni $a, b, c \in L$, ossia che valgono le due proprietà distributive. Ad

esempio se L è il reticolo della figura 11.1, detto il reticolo M_3 , allora $a \wedge (b \vee c) = a \wedge e = a$ e $(a \wedge b) \vee (a \wedge c) = d \vee d = d$.

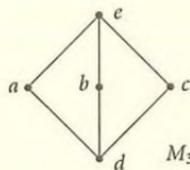


FIGURA 11.1.

È vero comunque che ognuna delle due proprietà distributive implica l'altra:

11.13 PROPOSIZIONE. *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 $a, b, c \in L$.

Dimostrazione. (a) \Rightarrow (b)

$$\begin{aligned}
 a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) && \text{per la (c) della proposizione 11.12} \\
 &= a \vee [(a \wedge c) \vee (b \wedge c)] && \text{per la (b) della proposizione 11.12} \\
 &= a \vee [(c \wedge a) \vee (c \wedge b)] && \text{per la (a) della proposizione 11.12} \\
 &= a \vee [c \wedge (a \vee b)] && \text{per l'ipotesi (a)} \\
 &= a \vee [(a \vee b) \wedge c] && \text{per la (a) della proposizione 11.12} \\
 &= [a \wedge (a \vee b)] \vee [(a \vee b) \wedge c] && \text{per la (c) della proposizione 11.12} \\
 &= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] && \text{per la (a) della proposizione 11.12} \\
 &= (a \vee b) \wedge (a \vee c) && \text{per l'ipotesi (a).}
 \end{aligned}$$

(b) \Rightarrow (a) Segue da (a) \Rightarrow (b) e dal principio di dualità per i reticolati. \square

Un reticolo L si dice *distributivo* se soddisfa alle proprietà equivalenti della proposizione 11.13.

11.14 ESEMPIO. Sappiamo (vedi esempio 1.3) 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 11.2 è un reticolo distributivo. \square

Si è visto sopra che il reticolo M_3 non è distributivo. L'esempio che segue fornisce un altro esempio di reticolo non distributivo.

11.15 ESEMPIO. Se N_5 è l'insieme parzialmente ordinato disegnato nella figura 11.2, 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

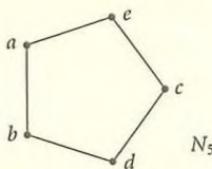
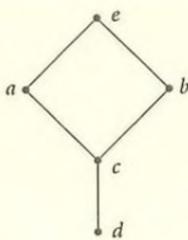
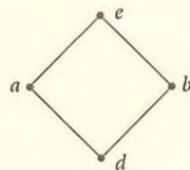


FIGURA 11.2.

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 $x, y \in L'$. Ad esempio se L è il reticolo della figura 11.3(a), allora $L' = L \setminus \{c\}$ non è sottoreticolo di L (perché $a \wedge b = c \notin L'$), mentre $L \setminus \{d\}$ è sottoreticolo di L . Si noti tuttavia che L' è il reticolo della figura 11.3(b), e quindi (L', \leq) , sottoinsieme ordinato di (L, \leq) , è un reticolo, pur non essendo un sottoreticolo di (L, \leq) .



(a)



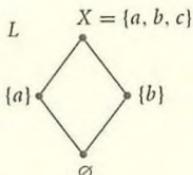
(b)

FIGURA 11.3. (a) Reticolo L ; (b) reticolo L' .

Siano (L, \leq) e (L', \leq) due reticoli. Un *omomorfismo di reticoli* φ 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 $x, y \in L$. Un omomorfismo biettivo 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 .

11.16 ESEMPIO. 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 φ 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 φ 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. Consideriamo l'applicazione $\varepsilon: L \rightarrow \mathcal{P}(X)$ definita da $\varepsilon(A) = A$ per ogni $A \in L$; l'applicazione ε 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 ε non è un omomorfismo di reticolli, 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

Si vede facilmente che un'applicazione tra due reticolli è un isomorfismo di reticolli se e solo se è un isomorfismo di insiemi parzialmente ordinati. Se esiste un isomorfismo di reticolli di L in L' , i reticolli L ed L' si dicono *isomorfi*.

Se L è un reticolo distributivo, ogni sottoreticolo di L è distributivo. Quindi L non può contenere sottoreticolli isomorfi a M_3 o a N_5 , perché questi non sono distributivi. Abbiamo così dimostrato il "solo se" del teorema che segue. La dimostrazione del "se" non è elementare, e la omettiamo.

11.17 TEOREMA. *Un reticolo è distributivo se e solo se non ha sottoreticolli isomorfi ai reticolli M_3 e N_5 .*

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 $a \in L$ si dice un *complemento* di un elemento $b \in L$ se $a \vee b = 1$ e $a \wedge b = 0$. È chiaro che se a è un complemento di b allora b è un complemento di a . In genere un elemento può non avere complementi o averne più di uno. Ad esempio nel reticolo non distributivo M_3 sia b che c sono complementi di a . Un reticolo si dice *complementato* se è limitato ed ogni suo elemento ha almeno un complemento.

11.18 PROPOSIZIONE. *Se in un reticolo distributivo e limitato un elemento ha un complemento, allora tale complemento è unico.*

Dimostrazione. Siano b_1 e b_2 due complementi di a . Allora

$$b_1 = b_1 \wedge 1 = b_1 \wedge (a \vee b_2) = (b_1 \wedge a) \vee (b_1 \wedge b_2) = 0 \vee (b_1 \wedge b_2) = b_1 \wedge b_2.$$

Similmente $b_2 = b_1 \wedge b_2$ e quindi $b_1 = b_2$. \square

Un reticolo distributivo complementato è detto un *reticolo di Boole* (o *reticolo booleano*). Dalla proposizione 11.18 segue che in un reticolo di Boole ogni elemento ha esattamente un complemento. Se L è un reticolo di Boole e $a \in L$, l'unico complemento di a viene di solito denotato con a' .

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

11.20 ESEMPIO. Il reticolo $(\mathcal{P}(A), \subseteq)$ degli esempi 11.2 e 11.14 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 11.14 tale reticolo è anche distributivo, e quindi $(\mathcal{P}(A), \subseteq)$ è un reticolo di Boole. \square

11.21 ESEMPIO.

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 11.5 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

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 11.1 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 11.1.

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 11.1. 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

$$\begin{aligned} (a' \wedge b') \vee (a \vee b) &= (a' \vee (a \vee b)) \wedge (b' \vee (a \vee b)) && \text{per la proprietà distributiva} \\ &= ((a' \vee a) \vee b) \wedge (a \vee (b' \vee b)) && \text{per le proprietà associative} \\ &= (1 \vee b) \wedge (a \vee 1) && \text{e commutativa (proposizione 11.12)} \\ &= 1 \wedge 1 && \text{per la definizione di complemento} \\ &= 1 && \text{perché } b \leq 1 \text{ e } a \leq 1 \end{aligned}$$

e similmente

$$\begin{aligned}(a' \wedge b') \wedge (a \vee b) &= ((a' \wedge b') \wedge a) \vee ((a' \wedge b') \wedge b) \\&= ((a' \wedge a) \wedge b') \vee (a' \wedge (b' \wedge b)) \\&= (0 \wedge b') \vee (a' \wedge 0) = 0 \vee 0 = 0.\end{aligned}$$

Questo dimostra la prima formula. Per la seconda si procede 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. Si dimostri che i reticolli (\mathbb{N}, \leq) e (\mathbb{N}^*, \leq) sono isomorfi.

11.7. Si dimostri che ogni insieme totalmente ordinato è un reticolo distributivo. [Suggerimento: per la distributività usare il teorema 11.17.]

11.8. Il reticolo (\mathbb{N}, \leq) è un reticolo complementato? È un reticolo distributivo? È un reticolo di Boole?

11.9. Si dimostri che un insieme totalmente ordinato è un reticolo di Boole se e solo se ha al più due elementi.

11.10. Il reticolo limitato $(\mathbb{N}, |)$ è complementato?

11.11. Il reticolo $(\mathbb{N}^*, |)$ è limitato?

11.12. L'insieme parzialmente ordinato (\mathbb{N}^*, ϱ) dell'esempio 10.3 è totalmente ordinato, e quindi è un reticolo. Si tratta di un reticolo limitato? complementato? distributivo? di Boole?

11.13. Si è visto nell'esempio 10.5 che l'applicazione identica $\iota_{\mathbb{N}^*} : \mathbb{N}^* \rightarrow \mathbb{N}^*$ è un omomorfismo di insiemi parzialmente ordinati quando il dominio si suppone parzialmente ordinato dalla relazione $|$ e il codominio si suppone ordinato dall'ordinamento usuale \leq . Si tratta di un omomorfismo di reticolli?

11.14. Nell'esempio 10.6 si è visto che l'applicazione $\varphi : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ definita da $\varphi(Z) = X \cap Z$ per ogni $Z \in \mathcal{P}(Y)$ è un omomorfismo di insiemi ordinati. Qui $X \subseteq Y$, e $\mathcal{P}(X), \mathcal{P}(Y)$ si suppongono parzialmente ordinati dall'inclusione \subseteq . L'applicazione φ è un omomorfismo di reticolli?

11.15. Si dia un esempio di un reticolo che ha un sottoinsieme ordinato che non è un reticolo.

11.16. Sia \leq l'ordine usuale sull'insieme dei numeri reali \mathbb{R} . Il reticolo (\mathbb{R}, \leq) è limitato? Si considerino l'intervallo aperto $]0, 1[= \{\alpha \in \mathbb{R} \mid 0 < \alpha < 1\}$ e l'intervallo chiuso $[0, 1] = \{\alpha \in \mathbb{R} \mid 0 \leq \alpha \leq 1\}$ con l'ordine indotto dall'ordine \leq di \mathbb{R} . I reticolli $]0, 1[$ e $[0, 1]$ sono limitati?

11.17. Si costruisca un esempio di un insieme parzialmente ordinato (A, \leq) in cui $\{x, y\}$ ha estremo superiore per ogni $x, y \in A$, ma che non è un reticolo.

11.18. 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 .

11.19. Si dica quali delle seguenti affermazioni sono vere:

(a) un sottoreticolo di un reticolo distributivo è distributivo;

(b) un sottoreticolo di un reticolo limitato è limitato;

(c) un sottoreticolo di un reticolo complementato è complementato;

(d) un sottoreticolo di un reticolo di Boole è di Boole.

11.20. 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 φ è un omomorfismo di reticolli. Si dimostri poi che le seguenti affermazioni sono equivalenti:

(a) φ è un isomorfismo di reticolli;

(b) L ha minimo e a è tale minimo;

(c) $\varphi: L \rightarrow L$ è l'applicazione identica.

11.21. Sia $D = \{z \mid z \in \mathbb{Z}, z > 0, z|70\}$ l'insieme dei divisori interi positivi di 70, | la relazione d'ordine in D definita, per ogni $z, z' \in \mathbb{Z}$ da $z|z'$ se z divide z' (cioè se esiste $k \in \mathbb{Z}$ tale che $z' = zk$.)

(a) Si definisca un isomorfismo tra i reticolli $(D, |)$ e $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.

(b) Il reticolo $(D, |)$ è distributivo?

11.22. Si dica se può esistere un insieme X tale che il reticolo $\mathcal{P}(X)$ sia isomorfo al reticolo di figura 11.4.

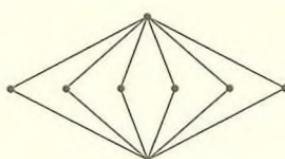


FIGURA 11.4.

11.23. 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, \leq) 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, \leq) 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 $\mathbb{D} = \{2z + 1 \mid z \in \mathbb{Z}\}$. Si dimostri che $(2\mathbb{Z}_{\geq 0} \wedge 2\mathbb{Z}_{\leq 0}) \vee \mathbb{D} = \mathbb{D}$ e $(2\mathbb{Z}_{\geq 0} \vee \mathbb{D}) \wedge (2\mathbb{Z}_{\leq 0} \vee \mathbb{D}) = \mathbb{D} \cup \{0\}$. Pertanto il reticolo (L, \leq) non è distributivo.

11.24. 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.

11.25. Sia X un insieme infinito e sia $\mathcal{P}_{cof}(X)$ 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 $\mathcal{P}_{cof}(X)$ mediante l'inclusione \subseteq . Si dimostri che $(\mathcal{P}_{cof}(X), \subseteq)$ è un reticolo distributivo che non è limitato.

11.26. 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 $(X, Y), (X', Y') \in A$,

$$(X, Y) \leq (X', Y') \quad \text{se} \quad X \subseteq X' \quad \text{e} \quad Y \subseteq Y'.$$

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 $(\mathcal{P}(\{a, b, c\}), \subseteq)$?

11.27. 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?

11.28. Sia A un insieme. Ricordiamo che un'equivalenza su A è una particolare relazione su A , cioè un sottoinsieme di $A \times A$. Pertanto l'insieme \mathcal{E}_A di tutte le equivalenze su A è un sottoinsieme di $\mathcal{P}(A \times A)$. In particolare l'ordinamento \subseteq su $\mathcal{P}(A \times A)$ induce un ordinamento su \mathcal{E}_A . Si provi che:

- (a) Se $\varrho, \varrho' \in \mathcal{E}_A$, allora $\varrho \cap \varrho' \in \mathcal{E}_A$ e $\varrho \cap \varrho'$ è l'estremo inferiore di $\{\varrho, \varrho'\}$ in $(\mathcal{E}_A, \subseteq)$.
 (b) Se $\varrho, \varrho' \in \mathcal{E}_A$, non è detto che $\varrho \cup \varrho' \in \mathcal{E}_A$.
 (c) Se $\varrho, \varrho' \in \mathcal{E}_A$, $\varrho \circ \varrho'$ è la relazione composta (esercizio 7.17) e $(\varrho \circ \varrho')^*$ è la chiusura transitiva di $\varrho \circ \varrho'$ (esercizio 7.15), allora $(\varrho \circ \varrho')^* \in \mathcal{E}_A$ e $(\varrho \circ \varrho')^*$ è l'estremo superiore di $\{\varrho, \varrho'\}$ in $(\mathcal{E}_A, \subseteq)$.

Pertanto $(\mathcal{E}_A, \subseteq)$ è un reticolo, detto il *reticolo delle equivalenze* su A . Se ne trovi 0 e 1. [Suggerimento: si vedano l'esempio 7.10 e l'esercizio 7.8.]

11.29. Si provi che se (L, \leq) è un reticolo, allora per ogni $a, b, c \in L$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) \quad \text{e} \quad (a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

[Suggerimento: per dimostrare che $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ è sufficiente dimostrare che $(a \vee b) \wedge (a \vee c)$ è un maggiorante di $\{a, b \wedge c\}$, perché per la definizione di estremo superiore $a \vee (b \wedge c)$ è il minimo ...]

11.30. Si provi che ogni reticolo finito (L, \leq) (vale a dire tale che l'insieme L sia finito) è limitato.

11.31. Si provi che se (L, \leq) è un reticolo distributivo (limitato, complementato, booleano), allora (L, \geq) è un reticolo distributivo (limitato, complementato, booleano). Naturalmente lo 0 di (L, \geq) è l'1 di (L, \leq) , e l'1 di (L, \geq) è lo 0 di (L, \leq) . Se $a, b \in L$, b è un complemento di a in (L, \geq) se e solo se è un complemento di a in (L, \leq) . Il principio di dualità per i reticolli si specializza quindi al seguente:

PRINCIPIO DI DUALITÀ PER I RETICOLI DI BOOLE. *Se A è un enunciato vero per ogni reticolo di Boole, allora anche l'enunciato duale A^* , ottenuto da A scambiando $\leq, \wedge, 0$ con $\geq, \vee, 1$ rispettivamente, è vero per ogni reticolo di Boole.*

Si noti ad esempio che le due formule di De Morgan per i reticolli booleani dimostrate nell'esercizio 11.3 sono una duale dell'altra.

11.32. Siano (B, \leq) e (C, \leq) due reticolli di Boole ed $f: B \rightarrow C$ un omomorfismo di reticolli 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 .

11.33. 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.

11.34. Sia (L, \leq) un insieme totalmente ordinato. Si provi che le seguenti condizioni sono equivalenti:

- L è un reticolo di Boole;
- L è un reticolo complementato;
- L ha al più due elementi.

§12. Grafi

Un insieme non vuoto V con una relazione simmetrica ϱ su V tale che $v \notin v$ per ogni $v \in V$ si dice un *grafo*. Come già fatto nel §7 rappresenteremo gli elementi dell'insieme V come punti, e se v, w sono due elementi di V tali che $v \varrho w$ disegneremo un arco di curva dal punto che rappresenta v a quello che rappresenta w . (C'è una lieve differenza tra la rappresentazione del §7 e quella di questo §12. Nel §7 rappresentavamo un insieme A e una qualunque relazione ϱ su A disegnando un arco *orientato* da a a b ogniqualvolta $a \varrho b$; si aveva così la nozione di grafo *orientato*. Nel caso di un grafo la relazione ϱ è simmetrica, quindi $v \varrho w$ se e solo se $w \varrho v$, e pertanto risulta molto più comodo disegnare un unico arco non orientato da v a w ogniqualvolta $v \varrho w$.)

Sia V un grafo e ϱ la sua relazione. Se $v, w \in V$ e $v \varrho w$, chiameremo il sottoinsieme $\{v, w\}$ di V di cardinalità 2 il *lato* da v a w . Chiameremo invece gli elementi di V i *vertici* del grafo. Quindi, dato un qualunque grafo, resta individuato l'insieme V dei suoi vertici e l'insieme $L = \{\{v, w\} \mid v, w \in V, v \varrho w\}$ dei suoi lati. Viceversa supponiamo che V sia un insieme non vuoto ed L un insieme di sottoinsiemi di V di cardinalità 2. Sull'insieme V definiamo una relazione ϱ ponendo, per ogni $v, w \in V$, $v \varrho w$ se $\{v, w\} \in L$. È chiaro che la relazione ϱ su V è simmetrica e che $v \notin v$ per ogni $v \in V$. È quindi equivalente definire un grafo come insieme $V \neq \emptyset$ con una relazione simmetrica ϱ su V tale che $v \notin v$ per ogni $v \in V$ oppure come coppia di insiemi (V, L) dove $V \neq \emptyset$ ed L è un insieme di sottoinsiemi di cardinalità 2 di V .

Denoteremo in genere un grafo G con il simbolo (V, L) , ossia con la coppia ordinata in cui il primo elemento è V , l'insieme dei vertici di G , e il cui secondo elemento è L , l'insieme dei lati di G .

12.1 ESEMPIO. 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 in uno dei tre modi indicati nella figura 12.1.

In pratica per descrivere un grafo conviene spesso disegnarne il diagramma invece che elencare tutti i suoi vertici e tutti i suoi lati. \square

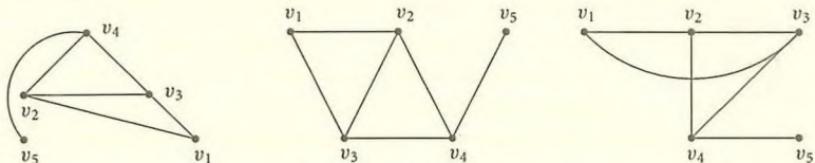


FIGURA 12.1.

Se v e w sono vertici distinti di un grafo ed $\ell = \{v, w\}$ è un lato del grafo, diremo che v e w sono *adiacenti*. Se ℓ e ℓ' sono lati distinti con un vertice in comune (cioè $\ell \cap \ell' \neq \emptyset$), diremo che ℓ e ℓ' sono *incidenti*.

Siano $G = (V, L)$ e $G' = (V', L')$ due grafi. Un *isomorfismo* (di grafi) 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 deve essere finito (perché se V è finito, allora $\mathcal{P}(V)$ è finito, e quindi $L \subseteq \mathcal{P}(V)$ è finito).

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*.

12.2 ESEMPIO. Il grafo dell'esempio 12.1 è un grafo finito. Il vertice v_1 ha grado 2, e quindi è un vertice pari. Invece v_2, v_3 e v_4 hanno grado 3, e quindi sono vertici dispari. Il grafo non ha vertici isolati. \square

12.3 LEMMA. *Il numero di lati di un grafo finito è*

$$|L| = \frac{1}{2} \sum_{v \in V} d(v).$$

Dimostrazione. Consideriamo il numero t di "estremi di lati". Chiaramente ogni lato ha due estremi, e quindi $t = 2|L|$. D'altra parte ogni vertice $v \in V$ è "estremo" di $d(v)$ lati, e quindi $t = \sum_{v \in V} d(v)$. Ne segue che $|L| = \frac{1}{2} \sum_{v \in V} d(v)$. \square

12.4 COROLLARIO. *Ogni grafo finito ha un numero pari di vertici dispari.*

Dimostrazione. Per il lemma precedente $2|L| = \sum_{v \in V} d(v)$ e quindi $\sum_{v \in V} d(v)$ è un numero pari. Se V_p e V_d sono l'insieme dei vertici pari e quello dei vertici dispari, si ha ovviamente che $\sum_{v \in V_p} d(v)$ è pari, e quindi $\sum_{v \in V_d} d(v) = \sum_{v \in V} d(v) - \sum_{v \in V_p} d(v)$ è pari. Si conclude che V_d ha un numero pari di elementi. \square

Un grafo in cui tutti i vertici hanno lo stesso grado d si dice *regolare* di grado d . Nella figura 12.2 sono riportati quattro esempi di grafi regolari di grado 1, 2, 3 e 4 rispettivamente.

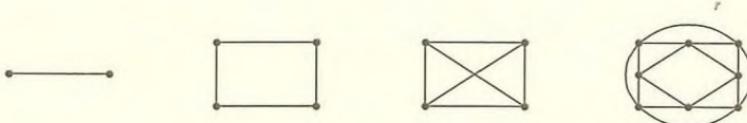


FIGURA 12.2.

12.5 COROLLARIO. Un grafo finito regolare di grado d con n vertici ha $\frac{1}{2}dn$ lati.

Dimostrazione. Segue subito dal lemma 12.3. \square

Avevamo già parlato di grafi orientati nel §7, quando avevamo visto che le relazioni su un insieme potevano essere rappresentate mediante grafi orientati, ossia da insiemi di punti collegati da archi 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 *digraphi*. Sia la nozione di grafo orientato che quella di grafo non orientato si possono generalizzare al caso di grafi in cui due vertici possono essere eventualmente uniti da più lati, cioè ai *multigrafi*. Nella figura 12.3 sono rappresentati i diagrammi di un multigrafo e di un multigrafo orientato.



FIGURA 12.3.

Ecco come si possono dare delle definizioni rigorose (anche se un po' pedanti). 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 ℓ 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 ℓ 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 φ 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 ri-

spettivamente 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 ℓ è un *lato* da v a w , e che v, w sono gli *estremi* di ℓ . Talvolta per dire che ci sono più lati aventi gli stessi estremi v e w si dice che c'è un *lato multiplo* tra v e 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 successione finita $\ell_1 = \{z_1, z_2\}, \ell_2 = \{z_2, z_3\}, \dots, \ell_n = \{z_n, z_{n+1}\}$ 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. Si noti che in un cammino lati consecutivi sono incidenti. 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*.

12.6 ESEMPIO. Il grafo dell'esempio 12.1 è connesso. Non è invece connesso il grafo con otto vertici riportato nella figura 12.4, in quanto, ad esempio, non esiste nessun cammino da v_2 a v_6 . Si osservi il vertice isolato v_8 . \square

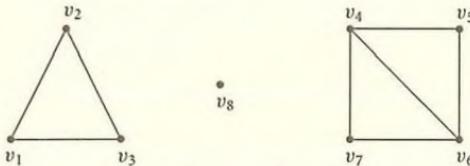


FIGURA 12.4.

Se $v \in V$, l'insieme C_v i cui elementi sono tutti i vertici $w \in V$ 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 connessa 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 in G 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 . Ne segue che le componenti connesse formano una partizione dell'insieme V dei vertici, e ovviamente non vi è alcun lato che colleghi vertici appartenenti a componenti connesse distinte.

12.7 ESEMPIO. 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 12.5 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 12.5 il grafo completo K_n ha $n(n - 1)/2$ lati. \square

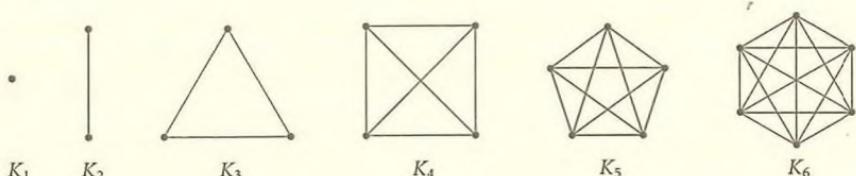
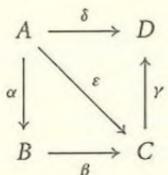


FIGURA 12.5.

La maggior parte delle nozioni viste in questo §12 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 $\ell_1 = (z_1, z_2)$, $\ell_2 = (z_2, z_3), \dots, \ell_n = (z_n, z_{n+1})$ 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. Un grafo orientato G si dice *connesso* se il grafo non orientato G' a lui associato è connesso.

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 $d^+(v) = |\{(w, v) \mid w \in V, (w, v) \in L\}|$. Analogamente il *grado di uscita* $d^-(v)$ di v è il numero di lati orientati che iniziano in v , cioè $d^-(v) = |\{(v, w) \mid w \in V, (v, w) \in L\}|$. Il *grado complessivo* $d(v)$ di v è $d^+(v) - d^-(v)$. Ovviamente, ma lo vedremo in dettaglio nell'esercizio 12.2, $|L| = \sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v)$.

I grafi orientati servono anche a rappresentare i diagrammi di insiemi e applicazioni. Se $G = (V, L)$ è un grafo orientato, un *diagramma* (di insiemi e applicazioni) consiste nell'associare ad ogni vertice $v \in V$ un insieme A_v e a ogni lato $\ell = (v, w) \in L$ un'applicazione $\varphi_\ell: A_v \rightarrow A_w$. Si dice che tale diagramma *commuta* (o che è *commutativo*) se per ogni $v, w \in V$ le composizioni delle applicazioni lungo tutti i cammini orientati da v a w coincidono. Ad esempio siano A, B, C, D insiemi e $\alpha, \beta, \gamma, \delta, \varepsilon$ applicazioni. Il diagramma



commuta se e solo se $\beta\alpha = \varepsilon$ e $\gamma\varepsilon = \delta$.

Un'altra facile estensione delle nozioni incontrate in questo §12 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 *moltelicità* 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 terza 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 $g(\varphi^{-1}(v, w)) = \varphi'^{-1}(v, w)$ per ogni $v, w \in V$, e quindi se $\ell \in L$ e $\varphi(\ell) = (v, w)$ 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 $\varphi'(g(\ell)) = (v, w)$. 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

$$\sum_{v \in V} d(v) = \sum_{v \in V} (d^+(v) - d^-(v)) = \left(\sum_{v \in V} d^+(v) \right) - \left(\sum_{v \in V} d^-(v) \right) = |L| - |L| = 0. \quad \square$$

12.3. I due grafi della figura 12.6 sono isomorfi?

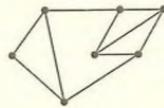
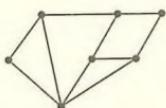


FIGURA 12.6.

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. Sia $G = (V, L)$ un grafo. Si consideri l'insieme $\overline{L} = \{(v, w) \mid v, w \in V, v \neq w, \{v, w\} \notin L\} \subseteq \mathcal{P}(V)$. Allora $\overline{G} = (V, \overline{L})$ è un grafo, detto il *grafo complementare* di G . Si noti che $L \cap \overline{L} = \emptyset$ e che $(V, L \cup \overline{L})$ è un grafo completo. Si provi che se $d(v), \overline{d}(v)$ sono i gradi di $v \in V$ in G, \overline{G} rispettivamente, allora $d(v) + \overline{d}(v) + 1 = |V|$. Si provi che $|L| + |\overline{L}| = \frac{1}{2} |V|(|V| - 1)$.

12.8. Si provi che i tre grafi della figura 12.7 sono a due a due isomorfi tra loro.

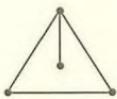
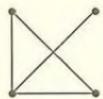
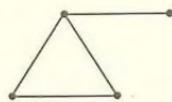


FIGURA 12.7.

12.9. I due grafi della figura 12.8 sono isomorfi?

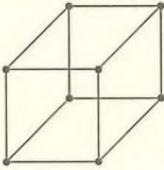
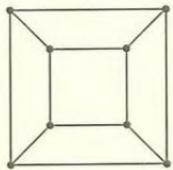


FIGURA 12.8.

12.10. I due grafi della figura 12.9 sono isomorfi?

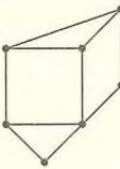
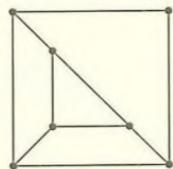


FIGURA 12.9.

12.11. (a) I grafi della figura 12.10 sono isomorfi?

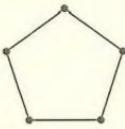
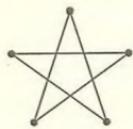


FIGURA 12.10.

(b) I grafi della figura 12.11 sono isomorfi?

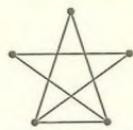


FIGURA 12.11.

(c) Si determinino tutti gli automorfismi del grafo della figura 12.12.

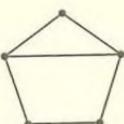


FIGURA 12.12.

12.12. Si provi che se due grafi sono isomorfi, anche i loro grafi complementari (vedi esercizio 12.7) sono isomorfi.

12.13. Sia G un grafo con n vertici tale che G e \overline{G} siano isomorfi (vedi esercizio 12.7). Quanti lati ha G ? Se ne deduca che 4 divide $n(n - 1)$. Poiché o n o $n - 1$ è dispari, ne segue che 4 divide n oppure 4 divide $n - 1$. Quindi $n = 4h$ oppure $n = 4h + 1$, con h intero non negativo. Si trovi un grafo G con 4 vertici tale che G e \overline{G} siano isomorfi. [Suggerimento: si calcoli prima quanti lati deve avere G .]

12.14. 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 .

12.15. Il lettore provi a dire quale potrebbe essere, secondo lui, la definizione di isomorfismo di grafi orientati.

12.16. 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 §7. Data una relazione ϱ su un insieme V , (cioè $\varrho \subseteq V \times V$), definiamo *grafo di ϱ* il grafo orientato $G_\varrho = (V, \varrho)$, ossia il grafo in cui l'insieme dei lati è lo stesso insieme ϱ .

- (a) Si dimostri che per la relazione di uguaglianza $=$ su V , il grafo di $=$ è $G_{} = (V, D_V)$.
- (b) Si dimostri che se ϱ è un'equivalenza su V , il suo grafo è $G_\varrho = (V, L)$, dove $L = (\pi \times \pi)^{-1}(D_{V/\varrho})$. Qui $\pi: V \rightarrow V/\varrho$ è la proiezione canonica, e $\pi \times \pi: V \times V \rightarrow V/\varrho \times V/\varrho$ è definita da $(\pi \times \pi)(v, v') = (\pi(v), \pi(v'))$ per ogni $(v, v') \in V \times V$.

12.17. Sia $n \geq 3$. Si disegnino tutti i grafi orientati connessi con n vertici tali che $d^+(v) = d^-(v) = 1$ per ogni vertice v .

12.18. 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 $G_f = G$.

§13. Cammini e circuiti euleriani

Sia $G = (V, L, \varphi)$ un multigrafo non orientato *finito*, cioè un multigrafo per il quale entrambi gli insiemi V dei vertici ed L dei lati sono finiti. Qui $\varphi: L \rightarrow \mathcal{P}_2(V)$ è l'applicazione che associa ad ogni lato $\ell \in L$ il sottoinsieme di cardinalità 2 di V i cui elementi sono gli estremi di ℓ . Un *cammino* nel multigrafo G consiste di una successione finita $\ell_1, \ell_2, \dots, \ell_n$ di lati distinti di G tale che $\varphi(\ell_i) = \{z_i, z_{i+1}\}$ per opportuni $z_1, z_2, \dots, z_{n+1} \in V$, $i = 1, 2, \dots, n$. 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 e senza ripassare sullo stesso lato.

13.1 TEOREMA DI EULERO (1736). *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.*

Dimostrazione. Sia $G = (V, L, \varphi)$ un multigrafo finito, privo di vertici isolati, con un circuito euleriano. Mostriamo che G è connesso. Siano $v, w \in V$. Dato che G è privo di vertici isolati, i vertici v e w appartengono a due lati di G , e quindi il circuito euleriano attraversa tutti i vertici di G . Ne segue che G è connesso. Fissiamo ora un vertice v_0 e percorriamo tutto il circuito euleriano partendo da v_0 . Ogni volta che si incontra un vertice, si entra e si esce dal vertice per due lati che non erano stati percorsi precedentemente, e quindi è chiaro che tutti i vertici eccetto al più v_0 sono pari. Lo stesso ragionamento vale per v_0 , solo che ora si ha anche il primo lato percorso (quello percorso quando si era partiti da v_0 lungo il circuito) e l'ultimo lato (quello percorso arrivando a v_0). Quindi anche v_0 è pari.

Viceversa supponiamo che G sia un multigrafo finito, privo di vertici isolati, connesso, e con tutti i vertici pari. Fissiamo un qualunque vertice v_0 . Dato che questo vertice non è isolato, esiste un lato a cui questo vertice appartiene. Partiamo da v_0 e percorriamo il lato. Ogni volta che arriviamo ad un nuovo vertice, questo vertice appartiene ad un numero pari di lati, e quindi possiamo scegliere un lato che non abbiamo ancora percorso (se abbiamo trovato un lato per entrare nel vertice, troviamo sempre un lato diverso per uscirne). In questo modo ogni volta che passiamo per un vertice usiamo due lati incidenti nel vertice, e quindi il numero dei suoi lati non ancora percorsi resta sempre pari. Il processo potrà finire solo quando si raggiungerà l'unico vertice lasciato momentaneamente con un numero dispari di lati, cioè v_0 . Abbiamo così visto che esiste un cammino da v_0 a v_0 , cioè un circuito C_1 .

Una volta costruito questo primo circuito C_1 , consideriamo il sottomultigrafo ottenuto da G togliendo tutti i lati appartenenti al circuito C_1 . Ci rimane così un multigrafo che non sarà più necessariamente connesso, ma che avrà ancora tutti i vertici pari. Possiamo quindi ripetere il procedimento, costruendo un altro circuito C_2 . Continuando con questa costruzione, si può quindi trovare una sequenza finita C_1, C_2, \dots, C_k di circuiti aventi a due

a due nessun lato in comune e tali che tutti i lati del multigrafo appartengono ad uno di questi circuiti (cioè i circuiti individuano una partizione dell'insieme L dei lati).

Ora almeno due di questi circuiti C_1, C_2, \dots, C_k si incontrano in qualche vertice, altrimenti il multigrafo G non sarebbe连通的. Se ad esempio C_i e C_j passano entrambi per il vertice w , percorrendo prima C_i da w a w e poi C_j da w a w si ottiene un unico circuito C_{ij} da w a w . Sostituendo in C_1, C_2, \dots, C_k i due circuiti C_i e C_j con il nuovo circuito C_{ij} , si ottiene una partizione dell'insieme L dei lati in $k - 1$ circuiti. Iterando questo procedimento otteniamo infine un unico cammino C che è ovviamente un circuito euleriano. \square

13.2 COROLLARIO. *Sia G un multigrafo finito privo di vertici isolati. Il multigrafo G ha un cammino euleriano se e solo se è连通的 e ha zero o due vertici dispari.*

Dimostrazione. Supponiamo che $G = (V, L, \varphi)$ abbia un cammino euleriano $\ell_1, \ell_2, \dots, \ell_m$ con $\varphi(\ell_i) = \{v_i, v_{i+1}\}$ per ogni $i = 1, 2, \dots, m$. Se questo cammino è un circuito, cioè se $v_1 = v_{m+1}$, si conclude per il teorema 13.1. Se invece il cammino non è un circuito, cioè se $v_1 \neq v_{m+1}$, allora ragionando come nel teorema 13.1 ("ogni volta che si entra in un vertice, poi lo si lascia, e quindi ci sono un numero pari di lati"), si vede che tutti i vertici del multigrafo, eccetto al più v_1 e v_{m+1} , sono pari. Un ragionamento simile vale anche per v_1 , solo che ora da v_1 si è usciti una volta di più (quando si è partiti), e pertanto v_1 è dispari. Similmente, anche v_{m+1} è dispari. Quindi v_1 e v_{m+1} sono i due soli vertici dispari.

Viceversa, se G ha zero vertici dispari, G ha un circuito euleriano per il teorema 13.1. Se invece $G = (V, L)$ ha due vertici dispari v_1 e v_2 possiamo considerare il multigrafo $G' = (V \cup \{v_0\}, L \cup \{\ell, \ell'\}, \varphi')$ ove v_0 è un vertice non appartenente a V , ℓ, ℓ' sono due lati non appartenenti a L , e $\varphi': L \cup \{\ell, \ell'\} \rightarrow \mathcal{P}_2(V \cup \{v_0\})$ è definita da $\varphi'(x) = \varphi(x)$ per ogni $x \in L$, $\varphi'(\ell) = \{v_0, v_1\}$, $\varphi'(\ell') = \{v_0, v_2\}$. Quindi G' si ottiene da G aggiungendogli un vertice v_0 e due lati: uno da v_0 a v_1 e uno da v_0 a v_2 .

In G' tutti i vertici sono pari, e quindi, per il teorema 13.1, G' ha un circuito euleriano. Poiché ℓ_0 ed ℓ_1 sono gli unici due lati a cui v_0 appartiene, essi devono essere percorsi consecutivamente nel circuito euleriano. Sopprimendo ℓ_0 ed ℓ_1 si ottiene un cammino euleriano avente v_1 e v_2 come estremi. \square

Si osservi che le dimostrazioni del teorema 13.1 e del corollario 13.2 danno dei procedimenti effettivi per costruire il circuito (o il cammino) euleriano cercato. Inoltre si noti come nella dimostrazione si è visto che se vi sono due vertici dispari questi debbono essere necessariamente gli estremi del cammino euleriano.

Un *cammino hamiltoniano* in un multigrafo finito è un cammino che passa esattamente una volta per ogni vertice del multigrafo.

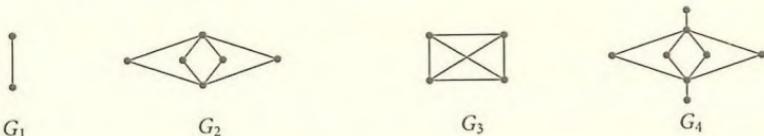


FIGURA 13.1.

13.3 ESEMPIO. 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 .

13.4 TEOREMA. *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 $d + 1 < n$. Sotto queste ipotesi esiste un vertice $v \in V$ distinto da $v_1, v_2, \dots, v_d, v_{d+1}$. Si avrà allora uno dei seguenti tre casi:

- (1) *Esiste un lato ℓ 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 ℓ 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 ℓ' 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 multigrafo c'è in G un lato ℓ 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

13.5 ESEMPIO. 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 13.4 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 $\{d(v, w) \mid v, w \in L\}$.

13.6 ESEMPIO. Nel multigrafo della figura 13.2 la distanza tra i vertici v e w è 2. Il diametro del multigrafo è 3. \square

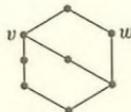


FIGURA 13.2.

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.

13.7 ESEMPIO. Siano m, n interi positivi. Il *grafo bipartito completo* $K_{m,n} = (V, L)$ è il grafo tale che

$$\begin{aligned} V &= \{v_1, v_2, \dots, v_m, w_1, w_2, \dots, w_n\}, \\ L &= \{\ell_{i,j} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\} \end{aligned}$$

ed $\ell_{i,j} = \{v_i, w_j\}$. 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

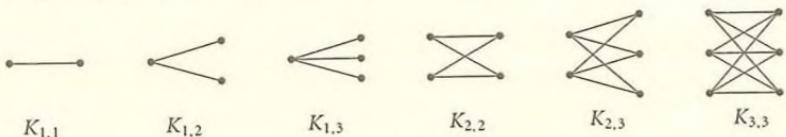


FIGURA 13.3.

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

$$\ell_1 = \{z_1, z_2\}, \quad \ell_2 = \{z_2, z_3\}, \dots, \quad \ell_n = \{z_n, z_{n+1}\}$$

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.

13.8 TEOREMA. *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 sottomultigrafo di G che si ottiene togliendo v e tutti i lati incidenti a v , cioè il sottomultigrafo di G generato da $V \setminus \{v\}$, è sconnesso.

13.9 TEOREMA. *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 sottomultigrafo G' di G generato da $V \setminus \{v\}$ è sconnesso. Siano $U \subseteq V$ e $W \subseteq V$ due componenti connesse distinte di questo sottomultigrafo 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 sottomultigrafo di G generato da $V \setminus \{v\}$. Allora in G' non ci sono cammini da u a v . Quindi G' è sconnesso, e v è un punto di taglio per G . \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 su 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 §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 $P_{f^{-1}}$ hanno lo stesso elemento di posto (i, j) per ogni i e ogni j , è quindi coincidono.

(c) Per quanto dimostrato in (a) e (b) si ha $P_f^t P_f = P_{f^{-1}} P_f = P_{f^{-1} f} = P_i$, dove $i: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ è l'applicazione identica, e similmente $P_f P_f^t = P_i$. Quindi basta provare che P_i è la matrice identica. Ma P_i ha come elemento di posto (i, j) il numero 1 se $i = i(j)$, e 0 altrimenti. Quindi P_i ha come elemento di posto (i, j) il numero 1 se $i = j$, e 0 altrimenti. Pertanto $P_i = I_{n \times n}$.

(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 al più 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连通的, 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 13.1 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,连通的 e con tutti i vertici pari. Dal teorema 13.1 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. Il teorema 13.1 è l'atto di nascita della teoria dei grafi. Fu dimostrato da Eulero per risolvere il seguente problema, detto il *problema dei ponti di Königsberg*. Königsberg era una città della Prussia (oggi si chiama Kaliningrad ed è in Russia) ed è situata su entrambe le sponde e su due isole del fiume Pregel (Pregolja). Il tutto è collegato da sette ponti:

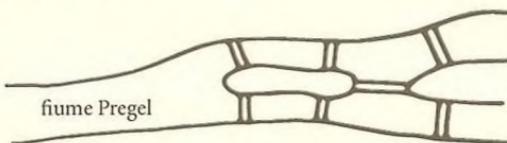


FIGURA 13.4.

Il problema era se fosse possibile fare la passeggiata domenicale partendo da casa propria e ritornandovi dopo aver percorso esattamente una volta i sette ponti della città.

Il problema è quindi equivalente a chiedersi se il multigrafo della figura 13.5 ha un circuito euleriano.

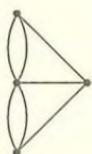


FIGURA 13.5.

Qual è la soluzione data da Eulero al problema dei ponti di Königsberg?

13.4. Sia $n \geq 2$ un numero intero. Si dimostri che un grafo completo con n vertici ha un cammino euleriano se e solo se n è dispari oppure $n = 2$.

13.5. Si provi il seguente corollario al teorema 13.1: *Sia G un grafo. G ha un cammino euleriano se e solo se ha zero o due vertici dispari e tutte le componenti connesse di G , eccetto al più una, consistono di vertici isolati.*

13.6. Sia $G = (V, L, \varphi)$ un multigrafo finito orientato completo. Si dimostri che $|L| \geq |V|(|V| - 1)/2$.

13.7. Siano $G = (V, L)$ 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 $G' = (V \cup \{v_0\}, L \cup L')$.

- Si dimostri che il grafo G' è connesso.
- Si dimostri che il vertice v_0 di G' ha grado pari.
- Si dimostri che il grafo G' ha un circuito euleriano.
- Se ne deduca che ogni grafo finito connesso è un sottografo di un grafo con un circuito euleriano.

13.8. 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.

13.9. Si consideri il grafo con 12 vertici rappresentato nella figura 13.6(a).

- Tale grafo ha un cammino euleriano?
- Ha un circuito euleriano?
- Si calcoli il diametro del grafo.

13.10. 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 $K_{k, n-k}$.

13.11.

- Determinare tutte le coppie (m, n) , con $1 \leq m \leq n$ numeri interi, per le quali il grafo bipartito completo $K_{m,n}$ ha un circuito euleriano.
- Determinare tutte le coppie (m, n) , con $1 \leq m \leq n$ numeri interi, per le quali il grafo bipartito completo $K_{m,n}$ ha un cammino euleriano.

13.12. Il lettore provi a definire cosa si intende per matrice di adiacenza di un grafo finito orientato, e adatti il teorema 13.8 al caso dei grafi finiti orientati.

13.13. 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 ℓ .

- 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 .

- (b) Si dimostri che il grafo con 17 vertici rappresentato nella figura 13.6(b) è connesso, se ne determinino le classi di equivalenza modulo \approx , e si dica se tale grafo è doppiamente connesso.



FIGURA 13.6.

§14. Alberi e grafi piani

In questo §14, 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. Ecco alcuni esempi di alberi:



FIGURA 14.1.

Spieghiamo subito il motivo del nome “albero”. Vedremo nel teorema 14.1 che in un albero esiste solamente un cammino tra due vertici qualunque v e w . Se $\ell_1, \ell_2, \dots, \ell_t$ è l’unico cammino da v a w , la distanza tra v e w è t , $d(v, w) = t$.

Fissiamo arbitrariamente un vertice v_0 . Disegniamo il grafo disponendo i vertici su righe successive: nella prima riga disegniamo l’unico vertice che ha distanza 0 da v_0 (cioè v_0 stesso), nella seconda riga disponiamo tutti i vertici che hanno distanza 1 da v_0 , nella terza disponiamo i vertici che hanno distanza 2 da v_0 , eccetera. Ad esempio i primi quattro grafi della figura 14.1 diventano come in figura 14.2.

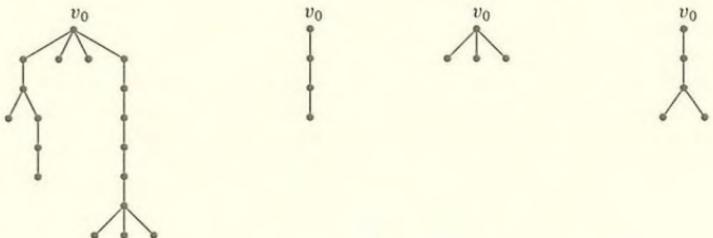


FIGURA 14.2.

Il nome di *alberi* deriva dalla somiglianza di questi grafi con gli alberi (questi alberi però hanno la radice in alto e i rami in basso). È ora naturale chiamare *foreste* i grafi le cui componenti connesse sono alberi.

14.1 TEOREMA. *Sia $G = (V, L)$ un grafo (non necessariamente finito). Le seguenti affermazioni sono equivalenti:*

- G è un albero;*
- per ogni $v, w \in V$ esiste un unico cammino da v a w ;*
- G è connesso e per ogni $\ell \in L$ il grafo $G' = (V, L \setminus \{\ell\})$ è un grafo sconnesso;*
- 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 percorrendo il primo cammino da v a w e poi il secondo da w a v , si potrebbe trovare un circuito in G . Questa è una contraddizione perché un albero non ha circuiti.

(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 ℓ . 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 ℓ 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 contraddirrebbe (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 ℓ 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 14.3, 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.

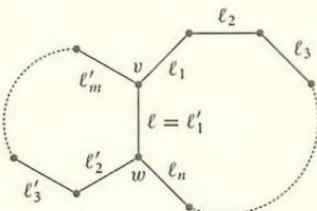


FIGURA 14.3.

(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 ℓ . 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

In tutto il resto del libro considereremo sempre alberi, grafi e multigrafi finiti, cioè con un numero finito di vertici e di lati.

14.2 PROPOSIZIONE. *Sia G un albero finito con almeno due vertici. Allora G ha almeno un vertice di grado uno.*

Dimostrazione. Ragioniamo per assurdo e supponiamo che G sia un albero con almeno due vertici e privo di vertici di grado 1. Dato che G è connesso ed ha almeno due vertici, G deve avere almeno un lato $\ell_1 = \{v_1, v_2\}$. Dato che G non ha vertici di grado 1, si ha che $d(v_2) \geq 2$, e quindi esiste un altro lato $\ell_2 = \{v_2, v_3\}$. Analogamente si ha che $d(v_3) \geq 2$ e quindi esiste un altro lato $\ell_3 = \{v_3, v_4\}$. In questo modo si costruisce una successione infinita di lati $\ell_1, \ell_2, \dots, \ell_n, \dots$ di G dove $\ell_i \neq \ell_{i+1}$ ed ℓ_i è incidente ad ℓ_{i+1} per ogni $i \in \mathbb{N}$. Ma dato che G è un grafo finito, G possiede solo un numero finito di lati distinti, e quindi $\ell_n = \ell_m$ per qualche $n, m \geq 1, n \neq m$. Se ne deduce che G possiede un circuito, assurdo perché G è un albero. \square

Nel caso dei grafi finiti, gli alberi, oltre che nei modi visti nel teorema 14.1, possono essere caratterizzati anche mediante le seguenti condizioni.

14.3 TEOREMA. *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_i ha n_i 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 è privo di circuiti. Si supponga per assurdo che G abbia un circuito. Sia ℓ_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 ℓ_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: si ottiene 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.

14.4 COROLLARIO. *Ogni grafo (o multigrafo) finito connesso con n vertici ha almeno $n - 1$ lati.*

Un *multigrafo piano* è un multigrafo $G = (V, L, \varphi)$ dove V è un insieme di punti di un piano π , L è un insieme di archi di curve del piano π , se $\ell \in L$ e $\varphi(\ell) = \{v, w\}$ allora l'arco di curva ℓ ha v e w come estremi e non passa per nessun altro punto di V , e due lati distinti $\ell, \ell' \in L$ si intersecano al più nei loro estremi. Ad esempio i multigrafi di figura 14.4 sono piani.

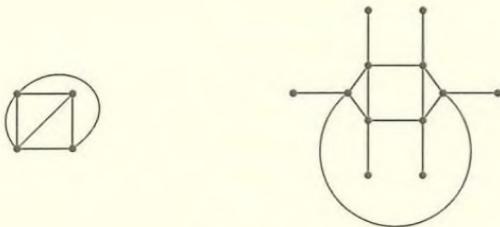


FIGURA 14.4.

Un multigrafo piano finito suddivide il piano in regioni. Ad esempio il multigrafo di figura 14.5 suddivide il piano in sei regioni.

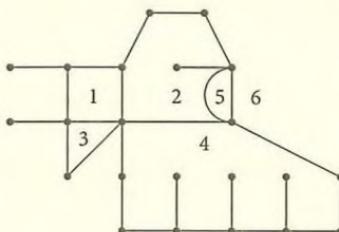


FIGURA 14.5.

Si noti la regione illimitata numerata con 6. Si noti anche che ognuna di queste regioni è limitata da un circuito del multigrafo. Chiameremo *facce* del multigrafo queste regioni.

Un multigrafo si dice *planare* se è isomorfo a un multigrafo piano. Ovviamente ogni albero finito è un multigrafo planare. Un albero piano ha un'unica faccia.

14.5 TEOREMA. *Sia G un multigrafo piano finito connesso con $|V|$ vertici, $|L|$ lati e $|F|$ facce. Allora*

$$|V| - |L| + |F| = 2 \quad (\text{Formula di Eulero}).$$

Dimostrazione. Induzione sul numero $|L|$ dei lati. Se $|L| = 0$, allora $|V| = 1$ e $|F| = 1$, e il teorema è vero. Consideriamo ora un multigrafo $G = (V, L, \varphi)$ con $|L| \geq 1$ lati, distinguendo due casi a seconda che G abbia o non abbia un circuito. Se G non ha un circuito, allora in particolare G ha tutti i lati semplici, cioè l'applicazione φ è iniettiva, e quindi G può essere visto come un grafo. Dato che G è connesso e privo di circuiti, cioè è un albero, allora per il teorema 14.3 si ha che $|L| = |V| - 1$ e $|F| = 1$, e quindi $|V| - |L| + |F| = 2$.

Supponiamo invece che G abbia un circuito. Sia G' il sottomultigrafo di G ottenuto togliendo un lato di questo circuito. Allora G' è piano, connesso, ha $|V|$ vertici, $|L| - 1$ lati e $|F| - 1$ facce in quanto due delle facce di G sono state riunite in un'unica faccia di G' rimuovendo il lato dal circuito. Per l'ipotesi induttiva applicata a G' si ha $|V| - (|L| - 1) + (|F| - 1) = 2$, cioè $|V| - |L| + |F| = 2$. \square

Abbiamo già osservato che ogni grafo $G = (V, L)$ può essere visto come multigrafo (V, L, φ) (è sufficiente prendere come $\varphi: L \rightarrow \mathcal{P}_2(V)$ l'applicazione definita da $\varphi(\{v, w\}) = \{v, w\}$ per ogni $\{v, w\} \in L$). Ha quindi senso parlare di grafi planari.

14.6 COROLLARIO. *Sia $G = (V, L)$ un grafo planare finito. Allora $|L| \leq 3|V| - 6$.*

Dimostrazione. Siano $G_i = (V_i, L_i)$, $i = 1, \dots, t$ le componenti connesse di G . Dato che $|L| = \sum_{i=1}^t |L_i|$ e $|V| = \sum_{i=1}^t |V_i|$, è sufficiente dimostrare che il corollario vale per le componenti connesse $G_i = (V_i, L_i)$ di G .

Per la formula di Eulero applicata al grafo $G_i = (V_i, L_i)$ si ha $|V_i| - |L_i| + |F_i| = 2$, dove $|F_i|$ è il numero di facce di G_i . Dato che ogni lato separa al più due facce, e ogni faccia è limitata da un circuito di lunghezza ≥ 3 , ne segue che $2|L_i| \geq 3|F_i|$ per ogni i . Quindi $|V_i| = |L_i| - |F_i| + 2 \geq |L_i| - \frac{2}{3}|L_i| + 2 = \frac{1}{3}|L_i| + 2$, da cui $|L_i| \leq 3|V_i| - 6$. \square

14.7 COROLLARIO. *Il grafo completo K_5 non è planare.*

Dimostrazione. Per il grafo K_5 non vale la disegualanza $|L| \leq 3|V| - 6$, in quanto $|V| = 5$ e $|L| = \binom{5}{2} = 10$. \square

Si noti invece che il grafo completo K_4 è planare in quanto è isomorfo al grafo di figura 14.6.



FIGURA 14.6.

Se ne deduce che K_n è planare per $n \leq 4$ e non è planare per $n \geq 5$. È chiaro poi 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 planare. Vale il seguente teorema la cui dimostrazione non è elementare.

14.8 TEOREMA DI KURATOWSKI. *Un grafo finito è planare se e solo se non contiene sottografi isomorfi a K_5 o a $K_{3,3}$.*

Concludiamo questo §14 con un famosissimo teorema di teoria dei grafi detto il *teorema dei quattro colori*.

Sia $k \geq 1$ un intero. Una k -colorazione di un multigrafo $G = (V, L, \varphi)$ è un'applicazione $\chi: V \rightarrow \{1, 2, \dots, k\}$ tale che $\chi(v) \neq \chi(w)$ per ogni coppia di vertici adiacenti $v, w \in V$.

14.9 TEOREMA DEI QUATTRO COLORI. *Ogni multigrafo planare finito ha una 4-colorazione.*

La dimostrazione di questo teorema è tutt'altro che elementare. La storia del teorema dei quattro colori comincia circa un secolo e mezzo fa, quando Francis Guthrie, colorando una carta delle contee inglesi nel 1852, osservò che bastavano quattro colori per dipingere una carta politica dell'Inghilterra. Da allora fu tutto un susseguirsi di dimostrazioni che confermavano la validità di quanto osservato da Francis Guthrie per una qualunque carta geografica politica (ma che si dimostravano in seguito imprecise). Supponiamo di avere una qualunque carta geografica politica, ossia una carta piana di regioni connesse, e di volerla colorare con il minor numero possibile di colori in modo che due regioni con un tratto di frontiera comune (non ridotta a un solo punto) siano dipinte con colori differenti. Per il teorema dei quattro colori quattro colori sono sufficienti per dipingere una qualunque carta di questo tipo. Infatti, data una carta geografica politica, scegliamo per ogni regione un capoluogo (un punto arbitrario nella regione) e tracciamo un lato tra due capoluoghi se e solo se le rispettive regioni sono confinanti. Otterremo un grafo piano finito. Per il teorema dei quattro colori il grafo ha una 4-colorazione. Scegliendo quattro colori distinti e colorando di conseguenza ogni regione con il colore corrispondente al capoluogo si avrà una colorazione della carta politica del tipo desiderato. La prima dimostrazione corretta del teorema dei quattro colori è dovuta ad Appel e Haken e risale al 1977.

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 planare? 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 è un grafo planare e, rappresentato nel piano, ha ovviamente 0 lati, 1 faccia ed n componenti connesse. Per un tale grafo si ha $|V| - |L| + |F| = n + 1$. Se $n = 1$, allora G è un grafo piano连通的 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 planare G non è连通的 e quindi ad esso non si applicano le ipotesi del teorema 14.5 (e in tal caso si ha $|V| - |L| + |F| = n + 1 \geq 3$). \square

Altri esercizi

14.2. Si disegnino tutti gli alberi con 5 vertici a meno di isomorfismi (ossia in modo che ogni albero con 5 vertici sia isomorfo a uno di questi, e che questi non siano isomorfi a due a due tra loro).

14.3. Si provi che in un albero con n vertici la somma dei gradi $\sum_{v \in V} d(v)$ è $2n - 2$.

14.4. Se un albero ha due vertici di grado 2, tre vertici di grado 3, quattro vertici di grado 4 e nessun vertice di grado maggiore, quanti vertici di grado 1 ha?

14.5. Siano n_2, n_3, \dots, n_k numeri naturali non tutti nulli. Se un albero ha n_2 vertici di grado 2, n_3 vertici di grado 3, ..., n_k vertici di grado k e nessun vertice di grado maggiore, quanti vertici di grado 1 ha?

14.6. Si formalizzi meglio la dimostrazione dell'implicazione (a) \Rightarrow (b) del teorema 14.1 facendo attenzione che se $\ell_1, \ell_2, \dots, \ell_s$ e $\ell'_1, \ell'_2, \dots, \ell'_t$ sono due cammini distinti da v a w , allora $\ell_1, \ell_2, \dots, \ell_s, \ell'_1, \ell'_2, \dots, \ell'_t$ non è necessariamente un circuito perché potrebbe contenere dei lati ripetuti.

14.7. Siano n, m numeri interi positivi fissati. Si consideri il grafo G con nm vertici disegnato nella figura 14.7.

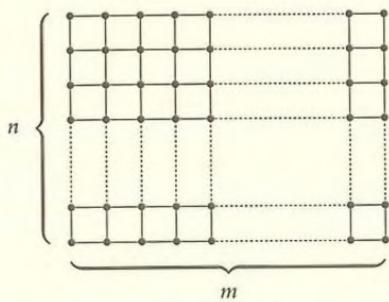


FIGURA 14.7.

- (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?

14.8. Si dimostri il seguente corollario al teorema di Kuratowski (teorema 14.8): *Ogni grafo finito con t lati, ove $t < 9$, è planare.*

14.9.

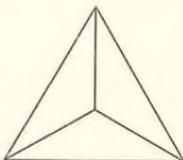
- (a) È possibile disegnare un grafo连通的 con 5 vertici, 8 lati e con un cammino euleriano?
 (b) È possibile disegnare un grafo planare connesso con 5 vertici e 8 lati?

14.10. Si dimostri che togliendo un lato qualunque al grafo K_5 o al grafo $K_{3,3}$ si ottiene sempre un grafo planare.

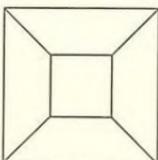
Appendice 14.1. I solidi platonici

Determiniamo, come applicazione del teorema 14.5, tutti i *solidi platonici*, ossia i poliedri regolari, cioè quelli le cui facce sono poligoni regolari tutti congruenti tra loro e nei vertici dei quali incidono sempre lo stesso numero di lati. Sono ad esempio solidi platonici il tetraedro, il cubo, l'ottaedro, il dodecaedro e l'icosaedro. Dimostreremo in questa appendice che questi cinque sono tutti i solidi platonici.

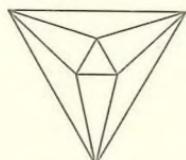
Proiettando da un punto opportuno i lati di un poliedro regolare su un piano si ottiene un grafo piano. Ad esempio ecco cosa si ottiene proiettando i cinque solidi elencati prima:



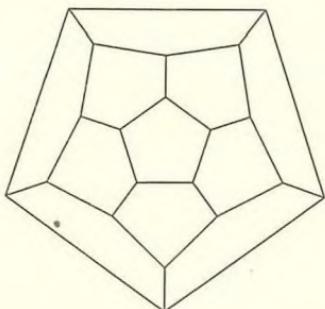
TETRAEDRO



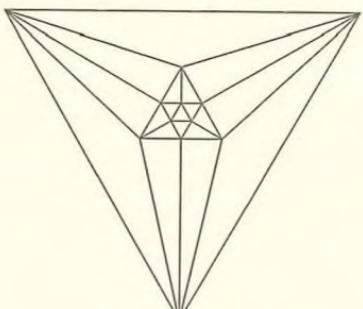
CUBO



OTTAEDRO



DODECAEDRO



ICOSAEDRO

FIGURA 14.8.

Supponiamo quindi di voler determinare i solidi platonici le cui facce sono p -agoni (poligoni con p angoli) e in ogni vertice del quale incidono q lati. Nel grafo piano corrispondente si ha allora $|L| = \frac{1}{2} q |V|$ (ogni vertice ha grado q). Ogni faccia ha p lati, e quindi

le facce sono delimitate complessivamente da $p|F|$ "lati", però in questo modo ogni lato è contato due volte, perché ogni lato separa esattamente due facce. Pertanto $|L| = \frac{1}{2}p|F|$. Infine si ha la formula di Eulero: $|V| - |L| + |F| = 2$. Sostituendo:

$$\frac{2|L|}{q} - |L| + \frac{2|L|}{p} = 2, \quad \text{ossia} \quad \frac{2p - pq + 2q}{pq} |L| = 2.$$

In particolare $2p - pq + 2q > 0$, ossia $4 > 4 - (2p - pq + 2q) = (p-2)(q-2)$. Quindi $p-2$ e $q-2$ sono interi il cui prodotto è < 4 . Ora un poligono ha almeno 3 angoli, $p \geq 3$, e similmente in un vertice devono incidere almeno 3 lati, $q \geq 3$. Quindi $p-2$ e $q-2$ sono interi positivi il cui prodotto è < 4 . Ci sono allora solo cinque casi possibili:

$p-2$	$q-2$	
1	1	tetraedro
1	2	ottaedro
1	3	icosaedro
2	1	cubo
3	1	dodecaedro

Si noti che per i primi tre $p = 3$, cioè le facce sono triangoli, per il cubo $p = 4$, cioè le facce sono quadrati, e per il dodecaedro $p = 5$, cioè le facce sono pentagoni.

Il teorema che abbiamo appena dimostrato, "Esistono solo cinque solidi platonici", è l'ultimo risultato dei 13 libri degli *Elementi* di Euclide. Naturalmente la dimostrazione data da Euclide era differente.

Appendice 14.2. Grafi e colorazioni

La dimostrazione del teorema dei quattro colori è lunga centinaia di pagine, considera migliaia tra diagrammi e verifiche di singole affermazioni, e alcune sue parti sono trattate mediante l'uso del computer. Tale dimostrazione esula quindi di gran lunga dallo scopo del presente volume. Dimostreremo qui invece il seguente teorema più debole:

14.10 TEOREMA. *Ogni multgrafo planare finito ha una 5-colorazione.*

Premettiamo la dimostrazione del lemma che segue:

14.11 LEMMA. *Ogni grafo planare finito ha un vertice di grado ≤ 5 .*

Dimostrazione. Supponiamo per assurdo che esista un grafo planare finito $G = (V, L)$ con $d(v) \geq 6$ per ogni vertice $v \in V$. Per il lemma 12.3 si avrebbe allora

$$|L| = \frac{1}{2} \sum_{v \in V} d(v) \geq \frac{1}{2} 6|V| = 3|V| > 3|V| - 6,$$

e questo contraddice il corollario 14.6. \square

Dimostrazione del teorema 14.10. Sia $G = (V, L, \varphi)$ un multigrafo piano finito. Qui V è un insieme di punti del piano, L è un insieme di archi (lati), e $\varphi: L \rightarrow \mathcal{P}_2(V)$ è l'applicazione che ad ogni lato associa l'insieme dei suoi due estremi. Dimostriamo il teorema per induzione su $|V| + |L|$. Se $|V| + |L| = 1$ si dovrà avere $|V| = 1$ e $|L| = 0$, e in questo caso il teorema è banale. Sia quindi $G = (V, L, \varphi)$ un multigrafo piano finito con $|V| + |L| > 1$. Se in G ci sono lati che non sono semplici, ossia in G ci sono due vertici u, v collegati da più lati, allora cancellando uno di questi lati si ottiene un sottomultigrafo che ha una 5-colorazione per l'ipotesi induttiva, e questa è anche una 5-colorazione di G . Possiamo quindi supporre che in G vi sia sempre al più un lato tra due vertici qualunque, ossia che G sia un grafo. Per il lemma 14.11 il grafo G ha allora un vertice $v_0 \in V$ di grado $d(v_0) \leq 5$.

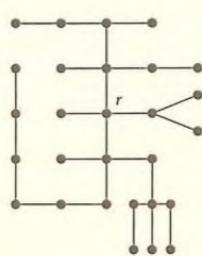
Se $d(v_0) \leq 4$, consideriamo il sottografo G' ottenuto da G cancellando v_0 e tutti i lati incidenti a v_0 . Allora G' è un grafo piano finito con un vertice in meno di G , e quindi per l'ipotesi induttiva G' ha una 5-colorazione $\chi': V \setminus \{v_0\} \rightarrow \{1, 2, \dots, 5\}$. Dato che $d(v_0) \leq 4$, ci sono al più quattro vertici adiacenti a v_0 in G , e quindi esiste $\bar{\iota} \in \{1, 2, 3, 4, 5\}$ tale che $\chi'(v) \neq \bar{\iota}$ per ogni $v \in V$ adiacente a v_0 . È quindi possibile estendere la 5-colorazione $\chi': V \setminus \{v_0\} \rightarrow \{1, 2, \dots, 5\}$ a una 5-colorazione $\chi: V \rightarrow \{1, 2, \dots, 5\}$ ponendo $\chi(v_0) = \bar{\iota}$.

Possiamo supporre quindi $d(v_0) = 5$. Siano v_1, \dots, v_5 i vertici adiacenti a v_0 in G e sia G'' il sottografo di G generato da $V'' = \{v_1, \dots, v_5\}$. Dato che G'' è un grafo planare, G'' non è il grafo completo con 5 vertici (corollario 14.7). Quindi esistono $v_k, v_l \in \{v_1, \dots, v_5\}$ che non sono adiacenti in G'' . Ne segue che v_k e v_l non sono adiacenti nemmeno in G . Costruiamo ora un multigrafo piano G''' nel modo seguente. Supponiamo che il piano su cui giace G sia realizzato in un materiale deformabile. Ritagliamo innanzitutto dal piano una regione contenente il solo vertice v_0 e tutti i lati incidenti a v_0 , ottenendo così un sottografo G' di G (G' è il sottografo di G generato da $V \setminus \{v_0\}$). Deformiamo ora con continuità e senza strappi la parte restante di piano su cui giace G' trascinando prima il vertice v_k fino al punto v_0 facendogli percorrere tutto il lato da v_k a v_0 , e poi trascinando il vertice v_l fino al punto v_0 facendogli percorrere il lato da v_l a v_0 . Si ottiene così un multigrafo piano G''' a partire da G' , deformando G' fino a far coincidere i due vertici v_k e v_l in un unico vertice situato ove prima si trovava il vertice v_0 (l'insieme dei vertici di G''' è $V \setminus \{v_k, v_l\}$ e i lati di G''' sono tanti quanti i lati di G'). Si osservi che dato che in G non c'era nessun lato da v_k a v_l , nemmeno in G' non c'è nessun lato da v_k a v_l , e quindi nel multigrafo deformato G''' non c'è nessun cappio da v_0 a v_0 . Pertanto G''' è veramente quello che abbiamo chiamato un multigrafo, eventualmente con più lati congiungenti v_0 e un medesimo vertice v (in G' c'è sempre al più un lato tra due vertici, ma se in G' c'è un lato da un vertice v a v_k e un altro lato da v a v_l , in G''' ci saranno ora due lati da v a v_0). Per l'ipotesi induttiva G''' ha una 5-colorazione $\chi'': V \setminus \{v_k, v_l\} \rightarrow \{1, 2, \dots, 5\}$. Compiamo ora la deformazione inversa riottenendo il grafo G' a partire da G''' . La 5-colorazione $\chi'': V \setminus \{v_k, v_l\} \rightarrow \{1, 2, \dots, 5\}$ di G''' diventa quindi una 5-colorazione $\chi': V \setminus \{v_0\} \rightarrow \{1, 2, \dots, 5\}$ di G' tale che $\chi'(v_k) = \chi'(v_l)$. Quindi $\{\chi(v_1), \dots, \chi(v_5)\}$ ha al più 4 elementi, e pertanto esiste $\bar{\iota} \in \{1, 2, \dots, 5\} \setminus \{\chi(v_1), \dots, \chi(v_5)\}$. La 5-colorazione $\chi': V \setminus \{v_0\} \rightarrow \{1, 2, \dots, 5\}$ di G' si estende pertanto ad una 5-colorazione $\chi: V \rightarrow \{1, 2, \dots, 5\}$ di G ponendo $\chi(v_0) = \bar{\iota}$, in quanto $\chi(v_0) \neq \chi(v_i)$ per tutti i cinque vertici v_i adiacenti a v_0 ($i = 1, 2, \dots, 5$). \square

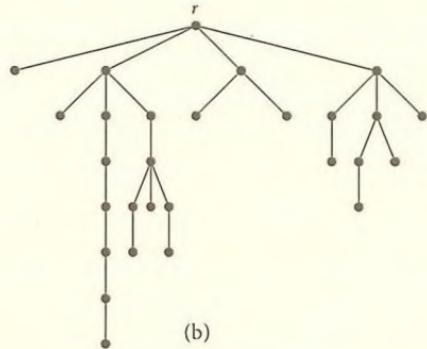
Appendice 14.3. Alberi con radice, notazione polacca

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 si dicono le *foglie* dell'albero.

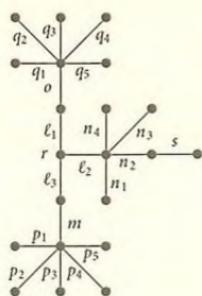
Dato un albero con radice r , si dice *livello* di un qualunque vertice v dell'albero la distanza $d(v, r)$. Si noti che i livelli di due vertici adiacenti differiscono di uno. Dato un albero con radice r è possibile orientare in modo naturale i lati dell'albero: se $\{v, w\}$ è un lato dell'albero si 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.



(a)



(b)



(c)

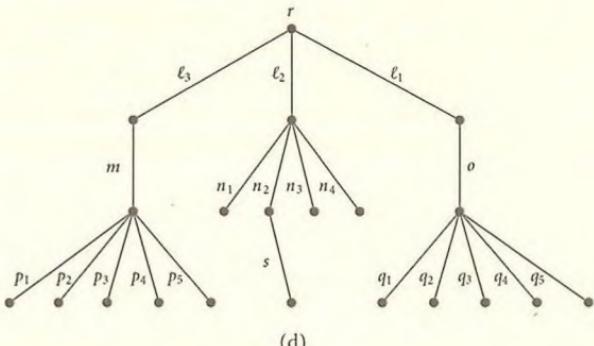


FIGURA 14.9.

Rappresenteremo un albero con radice come abbiamo fatto all'inizio del §14, 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 14.9(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 ℓ nella $(\ell + 1)$ -esima riga. Si ottiene allora il diagramma della figura 14.9(b).

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 rappresenteremo i lati uscenti da un qualunque vertice secondo l'ordine totale fissato in cui si succedono.

14.12 ESEMPIO. Consideriamo l'albero con radice disegnato nella figura 14.9(c). Rappresentiamolo disponendo i vertici di livello ℓ nella $(\ell + 1)$ -esima riga. Otteniamo il diagramma della figura 14.9(d). Tale albero con radice diventa poi un albero ordinato con radice se fissiamo 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 14.10. \square

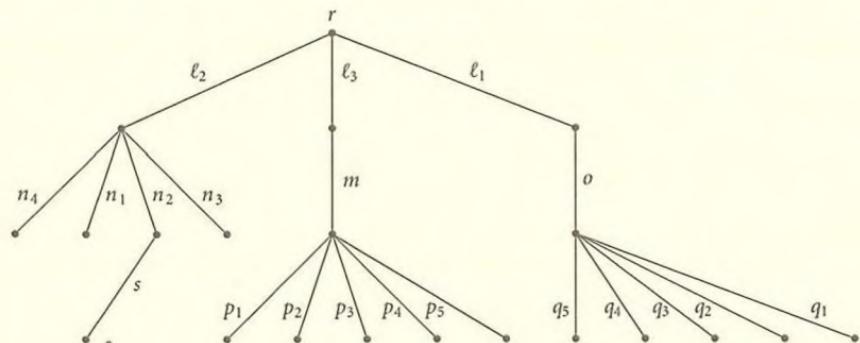


FIGURA 14.10.

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 v è l'estremo del k -esimo lato che esce da u , si assegna a v come indice la successione $S(v)$ ottenuta dalla giustapposizione della successione $S(u)$ e del numero naturale k . L'esempio seguente servirà a capire questo concetto.

14.13 ESEMPIO. Nell'esempio 14.12 abbiamo studiato l'albero ordinato con radice r rappresentato nella figura 14.10. Gli indici assegnati ai vertici nel modo appena descritto sono quelli della figura 14.11. \square

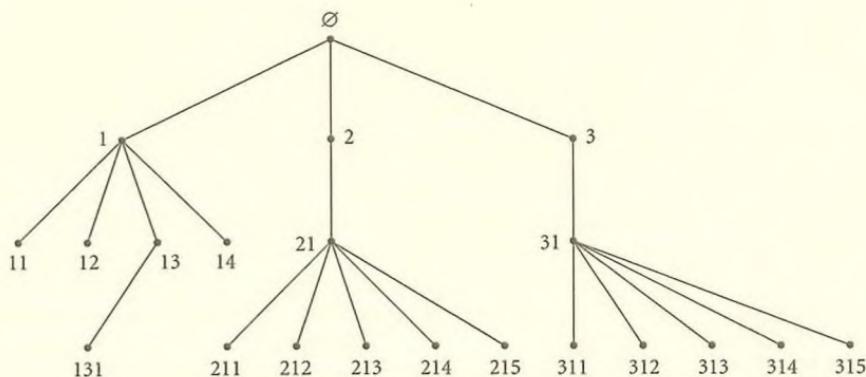


FIGURA 14.11.

14.14 ESEMPIO. 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 14.12(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 14.12(b), ottenuto dall'albero ordinato della figura 14.12(a) invertendo gli ordini sugli insiemi dei lati che escono da due vertici, è l'albero ordinato associato all'espressione $c + \sqrt{a / (d - (bc + a))}$.

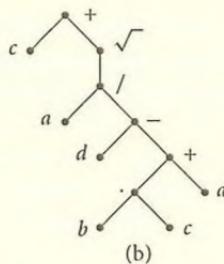
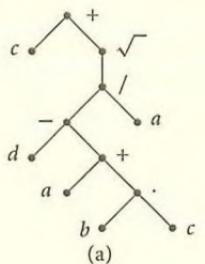


FIGURA 14.12.

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 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 $\sqrt{}$ si applica ad un solo operando, ossia l'estrazione di radice quadrata è un'operazione unaria).² □

Esercizi svolti

14.11. 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 14.13, 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 14.13(a), e la stessa espressione in notazione polacca è $+c\sqrt{-d+a \cdot bca}$.

²Nel §15 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.

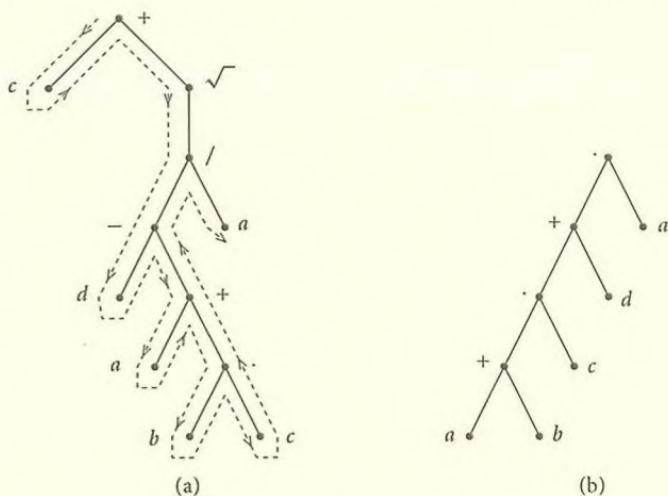


FIGURA 14.13.

- (a) Si disegni l'albero ordinato associato all'espressione algebrica in notazione a infixo $((a + ab) + (ab)c) + ((ab)c)d$ e la si scriva in notazione polacca.

(b) Si scriva l'espressione algebrica associata al grafo della figura 14.13(b) sia in notazione a infixo che in notazione polacca.

(c) Si rappresenti l'albero ordinato associato all'espressione algebrica che in notazione polacca si scrive $\cdot - ab + ab$ e la si scriva in notazione ad infixo (qui i simboli $+, -, \cdot$ indicano tutte operazioni binarie).

Soluzione. (a) L'albero è quello disegnato nella figura 14.14(a). L'espressione in notazione polacca è $+ + a \cdot ab \cdots abc \cdots abcd$.

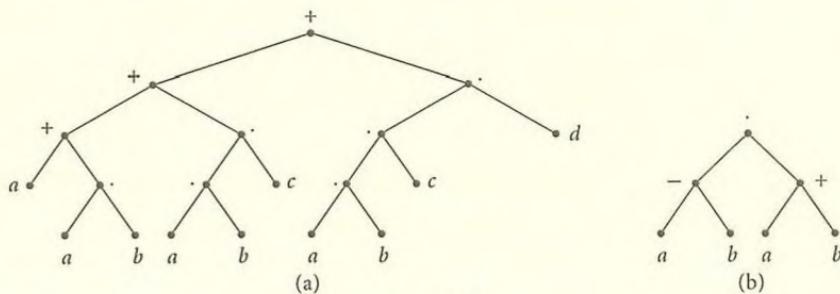


FIGURA 14.14.

- (c) L'albero ordinato è quello della figura 14.14(b). L'espressione in notazione a infisso è $(a - b)(a + b)$. \square

Capitolo 3

INSIEMI DOTATI DI UN'OPERAZIONE

§15. Semigruppi

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 $\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}} \rightarrow A$. Il numero naturale n si dice la *arietà* dell'operazione.

15.1 ESEMPIO. 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} in base alla definizione appena data, perché α / β è definito solo quando $\beta \neq 0$. \square

15.2 ESEMPIO. 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 si denotano in genere con simboli del tipo $+$, $-$, \cdot , \times , $*$, \circ ; se ω 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 α e β . In realtà sappiamo che si suole scrivere $\alpha + \beta$ in luogo di $+(\alpha, \beta)$. Similmente nell'esempio 15.2 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.

Studieremo nel seguito insiemi dotati di operazioni, cioè insiemi su cui sono definite delle operazioni. Un insieme su cui sono definite delle operazioni è detto anche una *struttura algebrica*. Se A è un insieme e $*: A \times A \rightarrow A$ è un'operazione, useremo la notazione $(A, *)$ per indicare l'insieme A dotato dell'operazione $*$. Nell'esempio 15.1 avevamo quindi considerato $(\mathbb{R}, +)$ e (\mathbb{R}, \cdot) , mentre nell'esempio 15.2 avevamo considerato $(\mathcal{P}(A), \cap)$. Questo è del tutto analogo a quanto avevamo fatto in precedenza, quando facevamo uso del simbolo (A, \leq) per mettere in evidenza che si stava considerando l'insieme A parzialmente ordinato dalla relazione \leq .

Un *semigruppo* $(S, *)$ è un insieme S dotato di un'operazione *associativa* $*$, cioè un'operazione $*$ tale che $(a * b) * c = a * (b * c)$ per ogni $a, b, c \in S$. Ad esempio $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) sono semigruppi, mentre se $-$ denota la sottrazione tra numeri interi ($-$ è un'operazione su \mathbb{Z}), allora $(\mathbb{Z}, -)$ non è un semigruppo, perché in generale $(a - b) - c \neq a - (b - c)$, $a, b, c \in \mathbb{Z}$. Un semigruppo $(S, *)$ si dice un *semigruppo commutativo* se $a * b = b * a$ per ogni $a, b \in S$. I quattro semigruppi $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) sono tutti commutativi.

15.3 ESEMPIO. Se A è un insieme, definiamo un'operazione $*$ su A ponendo $a * b = a$ per ogni $a, b \in A$. Allora $(A, *)$ è un semigruppo, 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 semigruppo $(A, *)$ 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

15.4 ESEMPIO. Se A è un insieme, allora $(\mathcal{P}(A), \cup)$ e $(\mathcal{P}(A), \cap)$ sono semigruppi commutativi. \square

La notazione più usata per denotare l'operazione in un semigruppo è quella *moltiplicativa*; in tal caso l'operazione è detta *moltiplicazione* ed è denotata con \cdot ; se a, b sono due elementi del semigruppo, si dice allora che $a \cdot b$ è il *prodotto* di a e b (e spesso si scrive ab in luogo di $a \cdot b$). Per i soli 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 .

Se (S, \cdot) è un semigruppo e $a, b, c \in S$, dato che $(ab)c$ è uguale a $a(bc)$ si può scrivere semplicemente abc , senza ambiguità di notazione; analogamente si può scrivere $abcd, \dots$. Se (S, \cdot) è un semigruppo, diremo a volte che S è un semigruppo, sottointendendo l'operazione \cdot . Questa convenzione è simile a quella già adottata per gli insiemi ordinati (vedi § 10).

Sia A un insieme e sia $*$ un'operazione su A . Un sottoinsieme B di A si dice un *sottoinsieme chiuso per l'operazione $*$* se $x * y \in B$ per ogni $x, y \in B$. Ad esempio \mathbb{N} è un sottoinsieme chiuso di \mathbb{Z} per le operazioni $+$ e \cdot , mentre non è un sottoinsieme chiuso di \mathbb{Z} per l'operazione $-$. Il sottoinsieme $\mathbb{Z}_{\leq 0} = \{z \mid z \in \mathbb{Z}, z \leq 0\}$ di \mathbb{Z} non è chiuso per l'operazione \cdot , ma è chiuso per l'operazione $+$.

Se $*$ è un'operazione su un insieme A e B è un sottoinsieme di A chiuso per l'opera-

zione $*$, è possibile definire un'applicazione $B \times B \rightarrow B$ ponendo $(x, y) \mapsto x * y$ per ogni $x, y \in B$. Questa applicazione $B \times B \rightarrow B$ è quindi un'operazione su B , detta l'operazione *indotta da $*$ su B* . Si osservi che questo è possibile solo perché B è un sottoinsieme chiuso per l'operazione $*$. 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 .

15.5 ESEMPIO. L'addizione $+$ e la moltiplicazione \cdot su \mathbb{Z} inducono l'addizione e la moltiplicazione su \mathbb{N} . \square

Se S è un semigruppo e T è un sottoinsieme chiuso di S , allora T con l'operazione indotta dall'operazione di S è a sua volta un semigruppo (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 *sottosemigruppo* di S .

15.6 ESEMPIO. Il semigruppo $(\mathbb{N}, +)$ è un sottosemigruppo di $(\mathbb{Z}, +)$. Se $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, (\mathbb{Z}^*, \cdot) è un sottosemigruppo di (\mathbb{Z}, \cdot) . Se $A \subseteq B$, allora $(\mathcal{P}(A), \cup)$ è un sottosemigruppo 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

Sia S un semigruppo in cui l'operazione è denotata come moltiplicazione \cdot , e sia a un elemento di S . 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 semigruppo $(S, +)$, in cui si fa uso della notazione additiva per indicare l'operazione, 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 intero positivo n .

15.7 PROPOSIZIONE. *Sia (S, \cdot) un semigruppo. 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 elemento a di un semigruppo S e 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 intero positivo m .

Dimostriamo poi per induzione su m che $(a^n)^m = a^{nm}$. Per $m = 1$ si ha $(a^n)^1 = a^n = a^{n+1}$, 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 $ab^{n+1} = ab^n b = b^n ab = b^n ba = b^{n+1} a$. 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 $(ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^n ab^n b = a^{n+1} b^{n+1}$. Questo conclude la dimostrazione. \square

Per un semigruppo additivo $(S, +)$ valgono per i multipli le analoghe delle proprietà viste nella proposizione 15.7 per le potenze. Per ogni $a, b \in S$ e per ogni intero positivo n, m si ha quindi $(n+m)a = na + ma$, $(nm)a = n(ma)$, e, infine, se $a + b = b + a$ allora $n(a+b) = na + nb$. Non c'è nulla da dimostrare, si è solamente cambiato la notazione.

Esercizi svolti

15.1. 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 semigruppo;
- se A ha almeno due elementi, allora il semigruppo (A^A, \circ) non è commutativo;
- se $B \subseteq A$, l'insieme delle applicazioni $f: A \rightarrow A$ tali che $f(B) \subseteq B$ è un sottosemigruppo 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 semigruppo 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 insiemi ordinati di A in A . Si dimostri che $\text{End}(A)$ è un sottosemigruppo di (A^A, \circ) .

Soluzione. (a) Si è visto nel §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) Supponiamo che A abbia almeno due elementi. Denotiamo, per ogni $t \in A$, con $f_t: A \rightarrow A$ l'applicazione definita da $f_t(x) = t$ per ogni $x \in A$ (f_t è l'applicazione costante uguale a t). Se a, b sono due elementi distinti di A , allora $f_a \circ f_b = f_a$, $f_b \circ f_a = f_b$ e $f_a \neq f_b$. Quindi il semigruppo (A^A, \circ) non è commutativo.

(c) 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 $f \circ g \in S_B$.

(d) 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 $n > 1$ e $f^{n-1} = f$, 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 $n \geq 1$.

(e) 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

15.2. Siano (S, \cdot) un semigruppo e T_1, T_2 due suoi sottosemigruppi. 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 sottosemigruppo 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 $xy = (t_1 t_2)(t'_1 t'_2) = t_1(t_2(t'_1 t'_2)) = t_1((t_2 t'_1) t'_2) = t_1((t'_1 t_2) t'_2) = t_1(t'_1(t_2 t'_2)) = (t_1 t'_1)(t_2 t'_2) \in T_1 T_2$. \square

15.3. Siano (S, \cdot) un semigruppo e T_1, T_2 due suoi sottosemigruppi. Si dimostri che $T_1 \cap T_2$ è un sottosemigruppo 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 sottosemigruppi 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

15.4. Si osservi che se α e β sono numeri reali positivi, il quoziente α/β 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 semigruppo?

15.5. 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 semigruppo commutativo.

15.6. Siano (S, \cdot) un semigruppo 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 semigruppo.

(b) Si dimostri che se (S, \cdot) è un semigruppo commutativo allora anche $(S^X, *)$ è un semigruppo commutativo.

15.7. Si provi che se A è un sottoinsieme di B , allora $(\mathcal{P}(A), \cap)$ è un sottosemigruppo di $(\mathcal{P}(B), \cap)$.

15.8. Sia $t \in \mathbb{N}$ e sia $\mathbb{N}_{\geq t} = \{n \mid n \in \mathbb{N}, n \geq t\}$. Si provi che $\mathbb{N}_{\geq t}$ è un sottoinsieme chiuso di \mathbb{N} sia rispetto all'addizione + che rispetto alla moltiplicazione ·.

15.9. Si dimostri che l'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottoinsieme chiuso di \mathbb{Z} per le tre operazioni +, · e -.

15.10. Si dimostri che $\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ è un sottosemigruppo sia di $(\mathbb{C}, +)$ che di (\mathbb{C}, \cdot) .

15.11. Siano A un insieme e (A^A, \circ) il semigruppo di tutte le applicazioni di A in A (si veda l'esercizio 15.1). Siano \mathcal{I}_A , \mathcal{S}_A e \mathcal{B}_A l'insieme di tutte le applicazioni $A \rightarrow A$ iniettive, suriettive e biettive rispettivamente. Si provi che (\mathcal{I}_A, \circ) , (\mathcal{S}_A, \circ) e (\mathcal{B}_A, \circ) sono sottosemigruppi di (A^A, \circ) .

15.12. Si provi che se (S, \cdot) è un semigruppo e T_λ è un suo sottosemigruppo per ogni $\lambda \in \Lambda$, allora $\bigcap_{\lambda \in \Lambda} T_\lambda$ è un sottosemigruppo di S . [Questo generalizza quanto visto nell'esercizio 15.3.]

15.13. Siano $(S, *)$ e (T, \circ) due semigruppi. Sul prodotto cartesiano $S \times T$ si definisca un'operazione \cdot ponendo $(s, t) \cdot (s', t') = (s * s', t \circ t')$ per ogni $(s, t), (s', t') \in S \times T$. Si provi che $(S \times T, \cdot)$ è un semigruppo (detto il *prodotto diretto* dei semigruppi S e T).

15.14. Con le notazioni dell'esercizio 15.13 si provi che il prodotto diretto di due semigruppi commutativi è un semigruppo commutativo.

15.15. Sul prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ si definisca un'operazione $*$ ponendo, per ogni $(a, b), (a', b') \in \mathbb{R} \times \mathbb{R}$, $(a, b) * (a', b') = (aa', ab' + b)$.

- (a) Si dimostri che $(\mathbb{R} \times \mathbb{R}, *)$ è un semigruppo.
- (b) Il semigruppo $(\mathbb{R} \times \mathbb{R}, *)$ è commutativo?
- (c) Si dimostri che $\{1\} \times \mathbb{R}$ e $\mathbb{R} \times \{0\}$ sono due sottosemigruppi di $(\mathbb{R} \times \mathbb{R}, *)$.
- (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 $a, b \in \mathbb{R}$.

15.16. Sia $\{0, 1\}^\mathbb{R}$ l'insieme di tutte le applicazioni di \mathbb{R} nell'insieme con due elementi $\{0, 1\}$. Sul l'insieme $\{0, 1\}^\mathbb{R}$ si definisca, per ogni $f, g \in \{0, 1\}^\mathbb{R}$, $(f * g)(x) = f(x) + g(x) - f(x)g(x)$ per ogni $x \in \mathbb{R}$.

- (a) Si dimostri che $f * g \in \{0, 1\}^\mathbb{R}$ per ogni $f, g \in \{0, 1\}^\mathbb{R}$, e che $(\{0, 1\}^\mathbb{R}, *)$ è un semigruppo.
- (b) Per ogni sottoinsieme A di \mathbb{R} sia

$$S_A = \{f \mid f \in \{0, 1\}^\mathbb{R}, f(a) = 0 \text{ per ogni } a \in A\}.$$

Si dimostri che S_A è un sottosemigruppo di $\{0, 1\}^\mathbb{R}$.

- (c) Si dimostri che se $A \subseteq B \subseteq \mathbb{R}$ allora $S_A \supseteq S_B$, e che $S_\emptyset = \{0, 1\}^\mathbb{R}$.
- (d) Si dimostri che nel semigruppo $(\{0, 1\}^\mathbb{R}, *)$ si ha $f^2 = f$ per ogni $f \in \{0, 1\}^\mathbb{R}$.
- (e) Si deduca da (d) che nel semigruppo $(\{0, 1\}^\mathbb{R}, *)$ si ha $f^n = f$ per ogni $f \in \{0, 1\}^\mathbb{R}$ e ogni intero $n \geq 1$.

15.17. Se $M_n(\mathbb{R})$ è l'insieme delle matrici $n \times n$ e \cdot è il prodotto righe per colonne, $(M_n(\mathbb{R}), \cdot)$ è un semigruppo per l'esercizio 6.2. Si dimostri che nel semigruppo $(M_2(\mathbb{R}), \cdot)$ si ha

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

per ogni intero positivo m .

15.18. Si considerino il semigruppo $(M_2(\mathbb{R}), \cdot)$ (vedi esercizio 15.17) e i suoi elementi

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

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 15.7 è essenziale per la validità della proposizione stessa.]

15.19. Sia $X = \{1, 2, 3\}$ e siano a, b gli elementi di X^X (cioè le applicazioni $X \rightarrow X$) definiti da $a(1) = 1, a(2) = 3, a(3) = 2, b(1) = 2, b(2) = 1, b(3) = 3$. Si provi che nel semigruppo (X^X, \circ) si ha $(ab)^2 \neq a^2b^2$.

15.20. Sia S il prodotto cartesiano $\mathbb{R}^* \times \mathbb{N}$. 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 semigruppo.
- (b) Il semigruppo S è commutativo?
- (c) Se $a = (2, 2)$ e $b = (1, 2)$ si calcolino $(ab)^2$ e a^2b^2 dimostrando che $(ab)^2 \neq a^2b^2$.

§16. Monoidi

Siano (S, \cdot) un semigruppo, $e \in S$. L'elemento e si dice un'*identità sinistra* di S se $ea = a$ per ogni $a \in S$. Analogamente, e si dice un'*identità destra* di S se $ae = a$ per ogni $a \in S$. Se e è sia un'*identità sinistra* che un'*identità destra*, e si dice un'*identità* (o un *elemento neutro*) di S .

16.1 ESEMPIO. Sia $S = \mathbb{R} \times \mathbb{R}$ il semigruppo 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 semigruppo. 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 $a, b \in \mathbb{R}$. Ovviamente non esiste alcun numero reale x tale che $bx = a$ per ogni $a, b \in \mathbb{R}$. Quindi il semigruppo 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 $c, d \in \mathbb{R}$, ossia se e solo se $yc = c$ per ogni $c \in \mathbb{R}$ e $yd = d$ per ogni $d \in \mathbb{R}$. 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 $x \in \mathbb{R}$. In particolare S ha infinite identità sinistre. \square

16.2 LEMMA. *Se in semigruppo ci sono un'*identità sinistra* e un'*identità destra* e' , allora $e = e'$.*

Dimostrazione. Si ha $e = ee' = e'$. \square

16.3 COROLLARIO. *In un semigruppo l'*identità*, se esiste, è unica.*

Dimostrazione. Se e, e' sono due identità, allora e è un'*identità sinistra* ed e' è un'*identità destra*. Si conclude per il lemma 16.2. \square

Abbiamo visto però nell'esempio 16.1 che esistono semigruppi con identità sinistre (anche infinite) e nessuna identità destra. Per un altro esempio si veda l'esercizio 16.5.

Un *monoide* è un semigruppo nel quale esiste un'identità. Quindi un monoide (M, \cdot) è un insieme M dotato di un'operazione \cdot che soddisfa alle seguenti proprietà:

- (a) *associatività*: $(ab)c = a(bc)$ per ogni $a, b, c \in M$;
- (b) *identità*: esiste un elemento $e \in M$ tale che $ea = ae = a$ per ogni $a \in M$.

In un monoide moltiplicativo (M, \cdot) l'identità si indica di solito con 1 o con 1_M . In un monoide additivo $(M, +)$ l'identità si indica di solito con 0 o con 0_M (e si dice lo *zero* del monoide).

16.4 ESEMPIO. I semigruppi $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono monoidi; la loro identità è il numero 0.

I semigruppi (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) sono monoidi; la loro identità è il numero 1. \square

16.5 ESEMPIO. Sia $n \geq 1$ un numero intero. L'insieme $M_n(\mathbb{R})$ delle matrici $n \times n$ ad elementi reali è un monoide rispetto alla moltiplicazione righe per colonne. La sua identità è la matrice $I_{n \times n}$. \square

16.6 ESEMPIO. 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 semigruppo 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 $a * (b * c) = a * (bc - b - c + 2) = abc - ab - ac + 2a - a - bc + b + c - 2 + 2 = abc - ab - ac - bc + a + b + c$. 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 semigruppo è commutativo, e ovviamente in un semigruppo commutativo un'identità sinistra è un'identità. Quindi $(\mathbb{Z}, *)$ è un monoide avente 2 come identità. \square

16.7 ESEMPIO. 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 11.12 (A, \vee) è un semigruppo commutativo. Vediamo se nel semigruppo 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 11.1) se e solo se $e \leq a$ per ogni $a \in A$, ossia se e solo 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 semigruppo 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

Per un monoide (M, \cdot) le potenze n -esime di un elemento $a \in M$ si possono definire per ogni intero $n \geq 0$, ponendo $a^0 = 1_M$ e $a^{n+1} = a^n a$ per ogni $n \geq 0$. In tal caso le formule della proposizione 15.7 valgono qualsiasi siano gli interi non negativi m ed n .

16.8 ESEMPIO. 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

16.9 ESEMPIO. Sia A un insieme. È facile verificare (si veda l'esercizio 15.1) 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

Sia M un monoide. Un sottomonoido N di M è un sottoinsieme chiuso N di M tale che $1_M \in N$. Ad esempio, per ogni monoide M i suoi sottoinsiemi $\{1_M\}$ ed M sono sottomonoidi. Il sottomonodo M di M si dice il sottomonodo *improprio*; tutti gli altri sottomonoidi di M si dicono *propri*.

16.10 ESEMPIO. Fissato $n \in \mathbb{N}$ poniamo $\mathbb{N}_{\geq n} = \{a \mid a \in \mathbb{N}, a \geq n\}$; è facile verificare che $\mathbb{N}_{\geq n} \cup \{0\}$ è un sottomonodo di $(\mathbb{N}, +)$ e che $\mathbb{N}_{\geq n} \cup \{1\}$ è un sottomonodo di (\mathbb{N}, \cdot) . Infatti $\mathbb{N}_{\geq n} \cup \{0\}$ è un sottomonodo di $(\mathbb{N}, +)$ perché $0 \in \mathbb{N}_{\geq n} \cup \{0\}$ e perché se $a, b \in \mathbb{N}_{\geq n} \cup \{0\}$ anche $a + b \in \mathbb{N}_{\geq n} \cup \{0\}$; analogamente $\mathbb{N}_{\geq n} \cup \{1\}$ è un sottomonodo di (\mathbb{N}, \cdot) perché $1 \in \mathbb{N}_{\geq n} \cup \{1\}$ e perché se $a, b \in \mathbb{N}_{\geq n} \cup \{1\}$ anche $ab \in \mathbb{N}_{\geq n} \cup \{1\}$. \square

16.11 ESEMPIO. Se $a \in \mathbb{Z}$ e $a\mathbb{Z} = \{az \mid z \in \mathbb{Z}\}$, è facile verificare che $a\mathbb{Z}$ è un sottomonodo di $(\mathbb{Z}, +)$ e che $a\mathbb{Z} \cup \{1\}$ è un sottomonodo di (\mathbb{Z}, \cdot) . \square

16.12 ESEMPIO. Sia M un monoide e per ogni $\lambda \in \Lambda$ sia M_λ un sottomonodo di M . Allora $\bigcap_{\lambda \in \Lambda} M_\lambda$ è un sottomonodo 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_λ è un sottomonodo 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 sottomonodo di M (vedi esempio 16.12), ed è ovviamente il più piccolo sottomonodo di M che contiene X . Si chiama il sottomonodo 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 $[\emptyset] = \{1_M\}$ e $[\{1_M\}] = \{1_M\}$.

Se $X = \{a\}$ ha un solo elemento si scrive spesso $[a]$ in luogo di $\{[a]\}$ e si dice che $[a]$ è il sottomonoide 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 .

16.13 PROPOSIZIONE. Siano M un monoide e X un suo sottoinsieme non vuoto. Allora $[X] = \{1_M, x_1x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X\}$. In particolare, se $X = \{a\}$, allora $[a] = \{a^n \mid n \in \mathbb{N}\}$.

Dimostrazione. Sia $N = \{1_M, x_1x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X\}$. È sufficiente dimostrare che N è un sottomonoide di M , che N contiene X , e che N è contenuto in ogni sottomonoide di M contenente X . Ora N è un sottomonoide di M perché è chiaramente un sottoinsieme chiuso; ovviamente $N \supseteq X$; se infine P è un sottomonoide di M contenente X , allora $1_M \in P$ e $x_1x_2 \cdots x_n \in P$ per ogni $x_i \in X$, e quindi $N \subseteq P$. Ciò prova che $[X] = N$.

La seconda parte della proposizione segue immediatamente dalla prima. \square

16.14 ESEMPIO. Si consideri il monoide (\mathbb{N}, \cdot) . Sia $X = \{2, 3, 4\}$. Il sottomonoide di (\mathbb{N}, \cdot) generato da X è

$$\begin{aligned}[X] &= \{1, x_1x_2 \cdots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{2, 3, 4\}\} \\ &= \{1, 2^a 3^b 4^c \mid a, b, c \in \mathbb{N}\} = \{2^a 3^b 4^c \mid a, b, c \in \mathbb{N}\} = \{2^a 3^b \mid a, b \in \mathbb{N}\}.\end{aligned}$$

(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

16.15 ESEMPIO. Si consideri il monoide $(\mathbb{N}, +)$. Sia $X = \{2, 3, 4\}$. Il sottomonoide di $(\mathbb{N}, +)$ generato da X è

$$\begin{aligned}[X] &= \{0, x_1 + x_2 + \cdots + x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{2, 3, 4\}\} \\ &= \{0, 2a + 3b + 4c \mid a, b, c \in \mathbb{N}\} = \mathbb{N} \setminus \{1\}.\end{aligned}$$

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

16.16 ESEMPIO. Sia A un insieme e si consideri il monoide (A^A, \circ) (vedi l'esempio 16.9 e l'esercizio 15.1). 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

$$\begin{aligned}[X] &= \{\iota_A, \xi_1 \circ \xi_2 \circ \cdots \circ \xi_n \mid n \in \mathbb{N}^*, \xi_1, \xi_2, \dots, \xi_n \in X\} \\ &= \{\iota_A, \varphi_{a_1} \circ \varphi_{a_2} \circ \cdots \circ \varphi_{a_n} \mid n \in \mathbb{N}^*, a_1, a_2, \dots, a_n \in A\} \\ &= \{\iota_A, \varphi_a \mid a \in A\} = \{\iota_A\} \cup X.\end{aligned}$$

La penultima uguaglianza segue dal fatto che ovviamente $\varphi_{a_1} \circ \varphi_{a_2} \circ \cdots \circ \varphi_{a_n} = \varphi_{a_1}$. \square

Per la proposizione 16.13 un monoide (M, \cdot) è ciclico se e solo se esiste un elemento $a \in M$ tale che $M = \{a^n \mid n \in \mathbb{N}\}$. Ad esempio il monoide (\mathbb{N}, \cdot) non è ciclico, perché non esiste nessun numero naturale a di cui ogni altro numero naturale è una potenza. Ovviamente un monoide additivo $(M, +)$ è ciclico se e solo se esiste un elemento $a \in M$ tale che $M = \{na \mid n \in \mathbb{N}\}$. Ad esempio il monoide $(\mathbb{N}, +)$ è ciclico generato da 1, mentre il monoide $(\mathbb{Z}, +)$ non è un monoide ciclico.

Siano $(S, *)$, (S', \circ) due semigruppi. Un *omomorfismo di semigruppi* φ 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* φ di S in S' è un omomorfismo di semigruppi tale che $\varphi(1_S) = 1_{S'}$.

Concludiamo con un po' di nomenclatura riguardante gli omomorfismi (di semigruppi o di monoidi) e con alcuni esempi. Un *isomorfismo* (di semigruppi o di monoidi) è un omomorfismo che è anche una biiezione. Un *endomorfismo* di S è un omomorfismo di S in S . Un *automorfismo* di S è un endomorfismo che è anche una biiezione (\circ , equivalentemente, un isomorfismo di S in S). Due semigruppi (o due monoidi) S ed S' si dicono *isomorfi* se esiste un isomorfismo di S in S' . Per indicare che due semigruppi o due monoidi S, S' sono isomorfi scriviamo $S \cong S'$.

16.17 ESEMPIO. 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

16.18 ESEMPIO. 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 $\sigma(zz') = zz'/|zz'| = (z/|z|)(z'/|z'|) = \sigma(z)\sigma(z')$ 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

16.19 ESEMPIO. 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 φ_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 φ_k è un automorfismo di $(\mathbb{Q}, +)$ in quanto:

- (1) φ_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) φ_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 $\varphi_k(k^{-1}x) = kk^{-1}x = x$. \square

16.20 ESEMPIO. Sia $\mu: \mathbb{C} \rightarrow \mathbb{R}$ l'applicazione definita da $\mu(z) = |z|$ per ogni $z \in \mathbb{C}$. Allora μ è un omomorfismo del monoide (\mathbb{C}, \cdot) nel monoide (\mathbb{R}, \cdot) , come è facile verificare. \square

16.21 ESEMPIO. 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 ψ 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 ψ è un omomorfismo di semigruppi 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 ψ 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

16.22 ESEMPIO. L'applicazione $\varphi: \mathbb{N} \rightarrow \mathbb{N}$, $\varphi(n) = 2^n$ per ogni $n \in \mathbb{N}$, è un omomorfismo di monoidi di $(\mathbb{N}, +)$ in (\mathbb{N}, \cdot) . \square

16.23 ESEMPIO. L'applicazione $\psi: \mathbb{N} \rightarrow \mathbb{Z}$, $\psi(n) = -n$ per ogni $n \in \mathbb{N}$, è un omomorfismo di monoidi additivi. \square

16.24 ESEMPIO. Se (S, \cdot) è un semigruppo ed $a \in S$, l'applicazione $\varphi_a: \mathbb{N}^* \rightarrow S$ definita da $\varphi_a(n) = a^n$ per ogni $n \in \mathbb{N}^*$ è un omomorfismo di semigruppi di $(\mathbb{N}^*, +)$ in (S, \cdot) . \square

16.25 ESEMPIO. L'applicazione $i: \mathbb{R} \rightarrow M_2(\mathbb{R})$ definita da

$$i(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

per ogni $\alpha \in \mathbb{R}$ è un omomorfismo di monoidi di (\mathbb{R}, \cdot) in $(M_2(\mathbb{R}), \cdot)$. \square

16.26 ESEMPIO. L'applicazione $\mu: \mathbb{Z} \rightarrow \mathbb{N}$ definita da $\mu(a) = |a|$ per ogni $a \in \mathbb{Z}$ è un omomorfismo del monoide (\mathbb{Z}, \cdot) nel monoide (\mathbb{N}, \cdot) ; non è un omomorfismo di $(\mathbb{Z}, +)$ in $(\mathbb{N}, +)$. \square

Esercizi svolti

16.1. Siano S e T due semigruppi. Sul prodotto cartesiano $S \times T$ si definisca un'operazione di moltiplicazione ponendo $(s, t)(s', t') = (ss', tt')$ per ogni $(s, t), (s', t') \in S \times T$. L'insieme $S \times T$ con questa operazione è un semigruppo, detto il *prodotto diretto* di S per T , come si è dimostrato nell'esercizio 15.13.

- (a) 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.
- (b) Sia $S \times S$ il prodotto diretto di un semigruppo 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 semigruppi.
- (c) 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) Abbiamo già visto nell'esercizio 15.13 che l'operazione su $S \times T$ è associativa. Dimostriamo che $S \times T$ 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 sottomonoido 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 sottomonoido di $S \times T$. Analogamente si vede che $\{1_S\} \times T$ è un sottomonoido 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 φ 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 φ è un isomorfismo di monoidi. In modo analogo si vede che i monoidi T e $\{1_S\} \times T$ sono isomorfi.

(b) Per ogni $(s, t), (s', t') \in S \times S$ si ha

$$\mu((s, t)(s', t')) = \mu(ss', tt') = (ss')(tt') = s(s't)t' = s(ts')t' = (st)(s't') = \mu(s, t)\mu(s', t').$$

(c) Si osservi intanto che da (a) 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 (b) si è già dimostrato che μ è un omomorfismo di semigruppi. Per far vedere che μ 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 $\mu(a, 1_S) = a \cdot 1_S = a$. \square

16.2. 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 $M = [a]$, 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

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx. \quad \square$$

16.3. 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 sottomonoido $[X]$ di $\mathcal{P}(A)$ generato da X .
- (b) Se $a_0 \in A$ è un elemento fissato, si determini il sottomonoido ciclico $[\{a_0\}]$ 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 sottomonoido di $(\mathcal{P}(A), \cup)$ generato da X è l'insieme dei sottoinsiemi finiti di A .

(b) Per quanto riguarda $[\{a_0\}]$ 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 $[\{a_0\}] = \{\{a_0\}^n \mid n \in \mathbb{N}\} = \{\emptyset, \{a_0\}\}$ è il sottomonoido di $(\mathcal{P}(A), \cup)$ avente come soli elementi \emptyset e $\{a_0\}$. \square

Altri esercizi

16.4. Sia A un insieme e Δ la differenza simmetrica. Da quanto si è visto nell'esercizio 1.24 segue che $(\mathcal{P}(A), \Delta)$ è un semigruppo commutativo. È un monoide? Qual è la sua identità?

16.5. Sia A un insieme non vuoto. Quali sono le identità sinistre e le identità destre nel semigruppo $(A, *)$ dell'esempio 15.3? Si dimostri che $(A, *)$ è un monoide se e solo se $|A| = 1$.

16.6. Si dimostri che il semigruppo $(\mathbb{R} \times \mathbb{R}, \star)$ dell'esercizio 15.15 è un monoide. Quale elemento di $\mathbb{R} \times \mathbb{R}$ è l'identità del monoide?

16.7. Si dimostri che il semigruppo $(\{0, 1\}^{\mathbb{R}}, *)$ dell'esercizio 15.16 è un monoide. Quale applicazione di \mathbb{R} in $\{0, 1\}$ è l'identità di questo monoide?

16.8. Si dimostri che se $f: S \rightarrow T$ è un omomorfismo di semigruppi (monoidi), allora $f(S)$ è un sottosemigruppo (rispettivamente sottomonoide) di T .

16.9. Mostriamo che ogni semigruppo è sottosemigruppo di un monoide. Sia (S, \cdot) un semigruppo e sia e un oggetto non appartenente ad S . Poniamo $M = S \cup \{e\}$ e definiammo $*: M \times M \rightarrow M$ ponendo per ogni $m, m' \in M$

$$m * m' = \begin{cases} mm' & \text{se } m \neq e, m' \neq e, \\ m & \text{se } m' = e, \\ m' & \text{se } m = e. \end{cases}$$

Si provi che $(M, *)$ è un monoide e che e ne è l'identità. (Si noti che se S è un monoide con identità 1_S , allora $1_S \neq 1_M$.)

16.10. 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 sottomonoide di A^A generato da f . Quanti elementi ha $[f]$? Quali sono?

[*Suggerimento:* si dimostri per induzione che $f^n = f^2$ per ogni $n \geq 2$.]

16.11. Sia (M, \cdot) un monoide commutativo, n un intero non negativo. Si provi che $\varphi_n: M \rightarrow M$, $\varphi_n(a) = a^n$ per ogni $a \in M$, è un omomorfismo di monoidi.

16.12. Si provi che se $\varphi: S \rightarrow S'$, $\psi: S' \rightarrow S''$ sono omomorfismi di semigruppi (di monoidi), allora $\psi \varphi$ è un omomorfismo di semigruppi (di monoidi).

16.13. Sia \mathbb{C} l'insieme dei numeri complessi e sia $c: \mathbb{C} \rightarrow \mathbb{C}$ l'applicazione definita da $c(\alpha + i\beta) = \alpha - i\beta$ per ogni $\alpha, \beta \in \mathbb{R}$. Si provi che c è un automorfismo sia del monoide additivo $(\mathbb{C}, +)$ che del monoide moltiplicativo (\mathbb{C}, \cdot) . (L'automorfismo c è detto il *coniugio*.)

16.14. Sia $v: \mathbb{C} \rightarrow \mathbb{R}$ l'applicazione definita da $v(\alpha + i\beta) = \alpha^2 + \beta^2$ per ogni $\alpha, \beta \in \mathbb{R}$. Si provi che v è un omomorfismo del monoide (\mathbb{C}, \cdot) nel monoide (\mathbb{R}, \cdot) . (Il numero reale $v(\alpha + i\beta)$ è detto la *norma* di $\alpha + i\beta$.)

16.15. Sia $\varphi: M \rightarrow M'$ un omomorfismo suriettivo di monoidi. Si provi che se M è ciclico, allora M' è ciclico.

16.16. Si provi che $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ è un sottomonoide di (\mathbb{R}, \cdot) . Si provi che l'applicazione log: $\mathbb{R}^+ \rightarrow \mathbb{R}$ definita da $x \mapsto \log x$ per ogni $x \in \mathbb{R}^+$ è un isomorfismo di monoidi di (\mathbb{R}^+, \cdot) in $(\mathbb{R}, +)$. (Ovviamente con $\log x$ abbiamo indicato il *logaritmo* di x .)

16.17. Sia S un semigruppo, e sia $\text{End}(S)$ l'insieme di tutti gli endomorfismi di S . Si provi che $(\text{End}(S), \circ)$, ove \circ è la composizione di applicazioni, è un monoide.

16.18. Sia $f: S \rightarrow S'$ un omomorfismo di semigruppi. 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 .

16.19. Sia $f: M \rightarrow M'$ un omomorfismo di monoidi. Allora:

- (a) se N è un sottomonoide di M , $f(N)$ è un sottomonoide di M' ;
- (b) se N' è un sottomonoide di M' , $f^{-1}(N')$ è un sottomonoide di M .

16.20. Sia $M = \mathbb{N} \times \mathbb{N}$ il prodotto diretto del monoide $(\mathbb{N}, +)$ per sé stesso (vedi esercizio 16.1). 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.

16.21 (TEOREMA DI CAYLEY PER I MONOIDI). Ogni monoide è isomorfo ad un sottomonoide del monoide (X^X, \circ) per un opportuno insieme X . [Suggerimento: se (M, \cdot) è un monoide, si ponga $X = M$ e si consideri per ogni $a \in M$ l'applicazione $f_a: M \rightarrow M$ definita da $f_a(x) = ax$ per ogni $x \in M$. Si provi che $M' = \{f_a \mid a \in M\}$ è un sottomonoide di (M^M, \circ) e che l'applicazione $\varphi: M \rightarrow M'$ definita da $\varphi(a) = f_a$ per ogni $a \in M$ è un isomorfismo di monoidi.]

16.22. Si consideri il monoide moltiplicativo (\mathbb{R}, \cdot) . Sia $S = \{-1, 0\}$ il sottomonoide 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 φ del monoide (\mathbb{R}, \cdot) tale che $\varphi(0) = 0$ e $\varphi(\alpha) = -1$ per ogni numero reale negativo α .
- (c) Si provi che $\varphi(\mathbb{R}) = S$.

[Suggerimento per la parte (b): per capire come deve essere definito φ si osservi che ogni numero reale positivo è il quadrato di un numero reale negativo. Una volta definita opportunamente l'applicazione φ 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.]

16.23. Si consideri il monoide $(\mathbb{Q}, +)$. Sia $M = \mathbb{N} \setminus \{1\}$.

- (a) Si dimostri che M è un sottomonoide di \mathbb{Q} .
- (b) Si dimostri che il monoide M non è ciclico.

§17. Quozienti

Sia (S, \cdot) un semigruppo e sia \sim una relazione di equivalenza sull'insieme S . Diremo che l'operazione \cdot e l'equivalenza \sim sono *compatibili* (tra loro) se $a \sim b$ e $c \sim d$ implicano $ac \sim bd$ per ogni $a, b, c, d \in S$.

Ecco un tipico esempio di operazione ed equivalenza tra loro compatibili: siano (S, \cdot) , (S', \cdot) due semigruppi e sia $f: S \rightarrow S'$ un omomorfismo di semigruppi; la relazione di equivalenza \sim_f sull'insieme S associata ad f è definita ponendo $a \sim_f b$ se $f(a) = f(b)$, $a, b \in S$ (esempio 7.11). Dato che f è un omomorfismo, l'operazione \cdot su S e l'equivalenza \sim_f sono compatibili: infatti se $a, b, c, d \in S$ e $a \sim_f b$ e $c \sim_f d$, allora $f(a) = f(b)$ e $f(c) = f(d)$, e quindi $f(ac) = f(a)f(c) = f(b)f(d) = f(bd)$, cioè $ac \sim_f bd$.

Supponiamo che (S, \cdot) sia un semigruppo e che \sim sia una relazione di equivalenza su S compatibile con \cdot . Possiamo allora considerare l'insieme quoziente S/\sim i cui elementi sono le classi di equivalenza $[a]$ al variare di a in S . È possibile definire un'operazione (che denoteremo ancora con \cdot) su S/\sim ponendo

$$[a] \cdot [b] = [ab] \quad \text{per ogni } [a], [b] \in S/\sim.$$

È necessario verificare immediatamente che in questo modo si è data una *buona definizione*: infatti potrebbe accadere che variando la scelta dei rappresentanti a, b delle classi $[a], [b]$ cambi la classe di equivalenza del prodotto ab ; ma ciò non accade proprio perché \sim e \cdot sono compatibili. Infatti se $a, a', b, b' \in S$, $[a] = [a']$ e $[b] = [b']$, allora $a \sim a'$ e $b \sim b'$, e quindi $ab \sim a'b'$, vale a dire $[ab] = [a'b']$.

Quindi dato il semigruppo (S, \cdot) e l'equivalenza \sim compatibile con \cdot abbiamo definito un'operazione \cdot su S/\sim . Ebbene $(S/\sim, \cdot)$ è un semigruppo, perché se $[a], [b], [c] \in S/\sim$, allora $([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a][b][c]$. Inoltre se S è un monoide con identità 1_S , anche S/\sim è un monoide con identità $1_{S/\sim} = [1_S]$, perché $[a][1_S] = [1_S][a] = [a]$ per ogni $[a] \in S/\sim$. Similmente se S è un semigruppo commutativo anche S/\sim è un semigruppo commutativo, perché $[a][b] = [ab] = [ba] = [b][a]$ per ogni $[a], [b] \in S/\sim$. Se (S, \cdot) è un semigruppo (monoide) e \sim è una relazione di equivalenza sull'insieme S compatibile con l'operazione \cdot , allora $(S/\sim, \cdot)$ è detto il *semigruppo (monoide) quoziente di S modulo \sim* . Si osservi che la *proiezione canonica* $\pi: S \rightarrow S/\sim$, definita da $\pi(a) = [a]$ per ogni $a \in S$, è un omomorfismo di semigruppi (monoidi) in quanto $\pi(ab) = [ab] = [a][b] = \pi(a)\pi(b)$ per ogni $a, b \in S$ (e se S è un monoide con identità 1_S , allora $\pi(1_S) = [1_S] = 1_{S/\sim}$).

17.1 ESEMPIO. 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 8.2). Sull'insieme quoziente \mathbb{Z}/\equiv_n è pertanto definita un'operazione di moltiplicazione, che verrà denotata ancora con \cdot , nel modo seguente:

$$[a] \cdot [b] = [ab] \quad \text{per ogni } a, b \in \mathbb{Z}.$$

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

17.2 ESEMPIO. 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 8.2). Sull'insieme quoziante \mathbb{Z}/\equiv_n c'è pertanto un'ulteriore operazione, che verrà denotata ancora con $+$, definita nel modo seguente:

$$[a] + [b] = [a + b] \quad \text{per ogni } a, b \in \mathbb{Z}.$$

Con questa operazione \mathbb{Z}/\equiv_n diventa un monoide con n elementi, diverso ovviamente da quello dell'esempio 17.1 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

Nell'enunciato del teorema che segue si osservi che se $f: S \rightarrow T$ è un omomorfismo di semigruppi (monoidi), allora $f(S)$ è un sottosemigruppo (sottomonoide) di T , come si è visto nell'esercizio 16.8.

17.3 TEOREMA FONDAMENTALE DI OMOMORFISMO PER I SEMIGRUPPI E I MONOIDI. Siano S e T semigruppi (monoidi) e sia $f: S \rightarrow T$ un omomorfismo di semigruppi (monoidi). Sia \sim_f la relazione di equivalenza su S associata ad f , cioè l'equivalenza su S compatibile con l'operazione di S definita da $a \sim_f b$ se $f(a) = f(b)$, $a, b \in S$. Allora i semigruppi (monoidi) S/\sim_f e $f(S)$ sono isomorfi.

Dimostrazione. Definiamo un'applicazione $g: S/\sim_f \rightarrow f(S)$ ponendo $g([s]_{\sim_f}) = f(s)$ per ogni $[s]_{\sim_f} \in S/\sim_f$. Dobbiamo dimostrare che g è ben definita, cioè che $g([s]_{\sim_f}) = f(s)$ non dipende dalla scelta del particolare rappresentante s della classe $[s]_{\sim_f}$ ma solamente dalla classe $[s]_{\sim_f}$, ossia che se $s, s' \in S$ e $[s]_{\sim_f} = [s']_{\sim_f}$, allora $f(s) = f(s')$. Ora se $s, s' \in S$ e $[s]_{\sim_f} = [s']_{\sim_f}$, allora $s \sim_f s'$, cioè $f(s) = f(s')$. Quindi g è un'applicazione ben definita. Facciamo vedere che g è un omomorfismo di semigruppi (monoidi). Per ogni $s, s' \in S$ si ha $g([s]_{\sim_f}[s']_{\sim_f}) = g([ss']_{\sim_f}) = f(ss') = f(s)f(s') = g([s]_{\sim_f})g([s']_{\sim_f})$, e quindi g è un omomorfismo di semigruppi. Se poi S e T sono monoidi ed $f: S \rightarrow T$ è un omomorfismo di monoidi, si ha anche che $g(1_{S/\sim_f}) = g([1_S]) = f(1_S) = 1_T = 1_{f(S)}$, e quindi g risulta essere anche un omomorfismo di monoidi. Mostriamo che g è iniettiva. Se $s, s' \in S$ e $g([s]_{\sim_f}) = g([s']_{\sim_f})$, allora $f(s) = f(s')$, cioè $s \sim_f s'$, da cui $[s]_{\sim_f} = [s']_{\sim_f}$. Questo dimostra che g è iniettiva. Infine $g: S/\sim_f \rightarrow f(S)$ è suriettiva, perché un generico elemento del suo codominio $f(S)$ è del tipo $f(s)$ per qualche $s \in S$, e quindi $f(s) = g([s]_{\sim_f})$ è l'immagine mediante g dell'elemento $[s]_{\sim_f}$ di S/\sim_f . Quindi g è un isomorfismo, e pertanto S/\sim_f ed $f(S)$ sono isomorfi. \square

Esercizi svolti

17.1. Siano S un insieme e $*$ l'operazione su S definita da $x * y = x$ per ogni $x, y \in S$. Si è visto nell'esempio 15.3 che $(S, *)$ è un semigruppo. Se T è un sottoinsieme non vuoto di S si definisca

una relazione \sim_T su S ponendo, per ogni $x, y \in S$,

$$x \sim_T y \quad \text{se} \quad \begin{cases} x = y \\ \text{oppure} \\ x \in T \text{ e } y \in T. \end{cases}$$

- (a) Si dimostri che \sim_T è un'equivalenza su S e si determini S/\sim_T .
- (b) Si dimostri che $*$ e \sim_T sono tra loro compatibili.
- (c) Si dimostri che ogni sottoinsieme di S è un sottosemigruppo di S .
- (d) Si dimostri che se $t_0 \in T$, allora il semigruppo quoziante S/\sim_T e il sottosemigruppo $\{t_0\} \cup (S \setminus T)$ 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

$$S/\sim_T = \{[s]_{\sim_T} \mid s \in S\} = \{[s]_{\sim_T} \mid s \in T\} \cup \{[s]_{\sim_T} \mid s \in S \setminus T\} = \{T\} \cup \{\{s\} \mid s \in S \setminus T\}.$$

- (b) Siano $x, y, x', y' \in S$ tali che $x \sim_T y$ e $x' \sim_T y'$. Allora $x * x' = x \sim_T y = y * y'$.
- (c) Sia S' un qualunque sottoinsieme di S . Da $x, y \in S'$ segue che $x * y = x \in S'$. Quindi S' è un sottosemigruppo di S .
- (d) 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 semigruppo S nel suo sottosemigruppo $\{t_0\} \cup (S \setminus T)$, 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 i semigruppi S/\sim_T e $f(S) = \{t_0\} \cup (S \setminus T)$ sono isomorfi. 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 semigruppi $S/\sim_T = S/\sim_f$ e $\{t_0\} \cup (S \setminus T)$ sono isomorfi. □

17.2. 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 $z = \rho(\cos \varphi + i \sin \varphi)$ per qualche $\rho, \varphi \in \mathbb{R}$, $\rho \geq 0$. Allora $z' = \sqrt{\rho}(\cos(\varphi/2) + i \sin(\varphi/2))$ 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 i monoidi moltiplicativi \mathbb{C}/\sim_f e $f(\mathbb{C}) = \mathbb{C}$ sono isomorfi. \square

17.3. 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 $f(z) = z/|z|$ 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 $f(zz') = zz'/|zz'| = (z/|z|)(z'/|z'|) = f(z)f(z')$ per ogni $z, z' \in \mathbb{C}^*$ e $f(1) = 1/|1| = 1$. 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 $z/|z| = z'/|z'|$. Ne segue che $z = (|z|/|z'|)z'$ con $|z|/|z'| \in \mathbb{R}$ e $|z|/|z'| > 0$.

Viceversa supponiamo che esista $\alpha \in \mathbb{R}$ tale che $\alpha > 0$ e $z = \alpha z'$. Allora $f(z) = f(\alpha z') = \alpha z'/|\alpha z'| = \alpha z'/\alpha|z'| = z'/|z'| = f(z')$. 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 i monoidi moltiplicativi \mathbb{C}^*/\sim_f e $f(\mathbb{C}^*) = \mathbb{T}$ sono isomorfi. \square

Altri esercizi

17.4. 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.

17.5. Nell'insieme \mathbb{R} si consideri la relazione \sim definita, per ogni $\alpha, \beta \in \mathbb{R}$, da $\alpha \sim \beta$ se $\alpha - \beta \in \mathbb{Z}$. Si provi che \sim è una relazione di equivalenza in \mathbb{R} . Si denoti con \mathbb{R}/\sim l'insieme quoziente. L'operazione $+$ in \mathbb{R}/\sim definita da $[\alpha] + [\beta] = [\alpha + \beta]$ per ogni $\alpha, \beta \in \mathbb{R}$ è ben definita? L'operazione \cdot in \mathbb{R}/\sim definita da $[\alpha] \cdot [\beta] = [\alpha\beta]$ per ogni $\alpha, \beta \in \mathbb{R}$ è ben definita?

17.6. 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 $x \in M$, $m \in \mathbb{N}^*$ e $x^m \sim 1_M$, allora $x \sim 1_M$.

17.7. 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 quoziante \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 φ è un isomorfismo di monoidi.

17.8. Sia $(\mathbb{R} \times \mathbb{R}, *)$ il monoide dell'esercizio 15.15.

- (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 $(\mathbb{R} \times \mathbb{R}, *)$ 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 $(\mathbb{R} \times \mathbb{R}, *)$ 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_{π_1} , associata a π_1 coincidono.
- (d) Si dimostri che il monoide quoziante $\mathbb{R} \times \mathbb{R}/\sim$ 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 φ è un omomorfismo iniettivo del monoide $(\mathbb{R} \times \mathbb{R}, *)$ nel monoide $(\mathbb{R}^\mathbb{R}, \circ)$ di tutte le applicazioni di \mathbb{R} in \mathbb{R} dotato della composizione di applicazioni.

17.9. 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 φ 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_φ associata a φ coincidono.
- (d) Si dimostri che i monoidi moltiplicativi \mathbb{R}/\sim e $\mathbb{R}_{\geq 0}$ sono isomorfi.

17.10. Siano A un insieme e (A^A, \circ) il monoide di tutte le applicazioni di A in A . Sia $B \subseteq A$.

- Si dimostri che $S = \{f \mid f \in A^A, f(B) \subseteq B\}$ è un sottomonoide di A^A .
- 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 φ è un omomorfismo suriettivo di monoidi di S nel monoide (B^B, \circ) .
- 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_φ associata all'applicazione φ coincidono.
- Si dimostri che i monoidi S/\sim e B^B sono isomorfi.

17.11 (COSTRUZIONE DI \mathbb{Z}). Nell'insieme $\mathbb{N} \times \mathbb{N}$ definiamo la relazione \sim ponendo, per $(n, m), (n', m') \in \mathbb{N} \times \mathbb{N}$, $(n, m) \sim (n', m')$ se $n + m' = m + n'$. Siano $+ e \cdot$ le operazioni in $\mathbb{N} \times \mathbb{N}$ definite da $(n, m) + (n', m') = (n + n', m + m')$ e $(n, m) \cdot (n', m') = (nn' + mm', nm' + mn')$ rispettivamente. Si provi che:

- \sim è un relazione di equivalenza su $\mathbb{N} \times \mathbb{N}$;
- \sim e $+$ sono compatibili;
- \sim e \cdot sono compatibili;
- $(\mathbb{N} \times \mathbb{N}, +)$ è un monoide;
- $(\mathbb{N} \times \mathbb{N}, \cdot)$ è un monoide.

Sia $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$ definita da $f(n, m) = n - m$ per ogni $(n, m) \in \mathbb{N} \times \mathbb{N}$. Si dimostri che:

- \sim è la relazione di equivalenza associata ad f ;
- f è un omomorfismo di monoidi di $(\mathbb{N} \times \mathbb{N}, +)$ in $(\mathbb{Z}, +)$;
- f è un omomorfismo di monoidi di $(\mathbb{N} \times \mathbb{N}, \cdot)$ in (\mathbb{Z}, \cdot) ;
- i monoidi $(\mathbb{N} \times \mathbb{N}/\sim, +)$ e $(\mathbb{Z}, +)$ sono isomorfi; [Suggerimento: usare (f), (g) e il teorema fondamentale di omomorfismo per i monoidi.]
- i monoidi $(\mathbb{N} \times \mathbb{N}/\sim, \cdot)$ e (\mathbb{Z}, \cdot) sono isomorfi.

Questo è il modo rigoroso in cui si costruisce l'insieme \mathbb{Z} e si definiscono le operazioni di addizione e di moltiplicazione su \mathbb{Z} a partire da \mathbb{N} e dalle operazioni di addizione e moltiplicazione su \mathbb{N} .

17.12. Sia \sim la relazione di equivalenza sull'insieme $\mathbb{N} \times \mathbb{N}$ definita nell'esercizio 17.11. Sia $*$ l'operazione in $\mathbb{N} \times \mathbb{N}$ definita da $(n, m) * (n', m') = (nn', mm')$ per ogni $(n, m), (n', m') \in \mathbb{N} \times \mathbb{N}$. Allora $(\mathbb{N} \times \mathbb{N}, *)$ è un monoide. Si dimostri che \sim e $*$ non sono tra loro compatibili.

17.13 (COSTRUZIONE DI \mathbb{Q}). Siano \mathbb{Z} l'insieme dei numeri interi e $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Si provi che:

- \mathbb{Z}^* è un sottomonoide di (\mathbb{Z}, \cdot) ;
- nell'insieme $\mathbb{Z} \times \mathbb{Z}^*$, prodotto cartesiano degli insiemi \mathbb{Z} e \mathbb{Z}^* , la relazione \sim definita da $(z, w) \sim (z', w')$ se $zw' = wz'$, $(z, w), (z', w') \in \mathbb{Z} \times \mathbb{Z}^*$, è una relazione di equivalenza;
- se $+$ è l'operazione in $\mathbb{Z} \times \mathbb{Z}^*$ definita da $(z, w) + (z', w') = (zw' + wz', ww')$ per ogni $(z, w), (z', w') \in \mathbb{Z} \times \mathbb{Z}^*$, allora \sim e $+$ sono compatibili;
- se \cdot è l'operazione in $\mathbb{Z} \times \mathbb{Z}^*$ definita da $(z, w) \cdot (z', w') = (zz', ww')$ per ogni $(z, w), (z', w') \in \mathbb{Z} \times \mathbb{Z}^*$, allora \sim e \cdot sono compatibili;
- $(\mathbb{Z} \times \mathbb{Z}^*, +)$ è un monoide;
- $(\mathbb{Z} \times \mathbb{Z}^*, \cdot)$ è un monoide.

Sia $f: \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ l'applicazione definita da $f(z, w) = z/w$ per ogni $(z, w) \in \mathbb{Z} \times \mathbb{Z}^*$. Si dimo-

stri che:

- (g) \sim è la relazione di equivalenza associata ad f ;
- (h) f è un omomorfismo di monoidi di $(\mathbb{Z} \times \mathbb{Z}^*, +)$ in $(\mathbb{Q}, +)$;
- (i) f è un omomorfismo di monoidi di $(\mathbb{Z} \times \mathbb{Z}^*, \cdot)$ in (\mathbb{Q}, \cdot) ;
- (j) i monoidi $(\mathbb{Z} \times \mathbb{Z}^*/\sim, +)$ e $(\mathbb{Q}, +)$ sono isomorfi;
- (k) i monoidi $(\mathbb{Z} \times \mathbb{Z}^*/\sim, \cdot)$ e (\mathbb{Q}, \cdot) sono isomorfi.

Questo è il modo rigoroso in cui si costruisce l'insieme \mathbb{Q} e si definiscono le operazioni di addizione e di moltiplicazione su \mathbb{Q} a partire da \mathbb{Z} e dalle operazioni di addizione e moltiplicazione su \mathbb{Z} .

§18. Il monoide delle parole

Ricordiamo (vedi pagina 81) che se A è un insieme, una *parola nell'alfabeto* A è una qualunque sequenza $a_1 a_2 \dots a_n$ di n elementi di A . Per ogni $n \geq 0$ 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 . La *parola vuota* è l'unica parola di lunghezza 0; la si indica con w_0 , di modo che $W_0 = \{w_0\}$. Per ogni $n \geq 1$ c'è una biiezione canonica $\varphi_n: A^n \rightarrow W_n$. Poniamo $W_A = \bigcup_{n \in \mathbb{N}} W_n$.

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 .

18.1 TEOREMA (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, \cdot) e per ogni applicazione $f: A \rightarrow M$ esiste un unico omomorfismo di monoidi $\widehat{f}: W \rightarrow M$ che rende commutativo il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{f} & M \\ & \varphi \searrow & \nearrow \widehat{f} \\ & W & \end{array}$$

cioè tale che $\widehat{f} \circ \varphi = f$.

Dimostrazione. *Esistenza:* Sia $f: A \rightarrow M$ un'applicazione dell'insieme A nel monoide M . Mostriamo che esiste un omomorfismo di monoidi $\widehat{f}: W \rightarrow M$ tale che $\widehat{f} \circ \varphi = f$. Po-

niamo $\widehat{f}(w_0) = 1_M$ e, per ogni parola $w = a_1 a_2 \dots a_n \in W$ di lunghezza $n \geq 1$, poniamo

$$\widehat{f}(w) = f(a_1) \cdot f(a_2) \cdot \dots \cdot f(a_n).$$

Verifichiamo che $\widehat{f}: W \rightarrow M$ è un omomorfismo di monoidi. Siano $w, w' \in W$. Se w ha lunghezza zero allora

$$\widehat{f}(w \circ w') = \widehat{f}(w') = 1_M \cdot \widehat{f}(w') = \widehat{f}(w) \cdot \widehat{f}(w');$$

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

$$\widehat{f}(w \circ w') = f(a_1) \cdot f(a_2) \cdot \dots \cdot f(a_n) \cdot f(b_1) \cdot f(b_2) \cdot \dots \cdot f(b_m) = \widehat{f}(w) \cdot \widehat{f}(w').$$

Quindi \widehat{f} è un omomorfismo di monoidi, e per ogni $a \in A$ si ha $(\widehat{f} \circ \varphi)(a) = \widehat{f}(a) = f(a)$, cioè $\widehat{f} \circ \varphi = f$.

Unicità: Mostriamo che $\widehat{f}: W \rightarrow M$ è l'unico omomorfismo di monoidi tale che $\widehat{f} \circ \varphi = f$. Sia $f': W \rightarrow M$ un altro omomorfismo di monoidi tale che $f' \circ \varphi = f$. Allora $f'(w_0) = 1_M = \widehat{f}(w_0)$, 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

$$\begin{aligned} f'(w) &= f'(\varphi(a_1) \circ \varphi(a_2) \circ \dots \circ \varphi(a_n)) = f'(\varphi(a_1)) \cdot f'(\varphi(a_2)) \cdot \dots \cdot f'(\varphi(a_n)) \\ &= (f' \circ \varphi)(a_1) \cdot (f' \circ \varphi)(a_2) \cdot \dots \cdot (f' \circ \varphi)(a_n) \\ &= f(a_1) \cdot f(a_2) \cdot \dots \cdot f(a_n) = \widehat{f}(w). \end{aligned}$$

Quindi $f' = \widehat{f}$. Questo prova che \widehat{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 λ 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 $w, w' \in W$.

18.2 LEMMA. *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 $n \in \mathbb{N}$, $n \geq 1$, $\underbrace{aa \dots a}_{n \text{ volte}}$ è l'unica parola di

lunghezza n nell'alfabeto A , si conclude che λ 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 delle parole nell'alfabeto A non è commutativo.

Esercizi svolti

18.1. 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 18.1) 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

$$\begin{array}{ccc} M & \xrightarrow{\quad i \quad} & M \\ & \searrow \varphi & \nearrow \hat{i} \\ & W & \end{array}$$

cioè tale che $\hat{i} \circ \varphi = i$. Dato che $\hat{i} \circ \varphi = i$ è suriettiva, per la proposizione 3.2(b) 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 i monoidi W/\sim e $\hat{i}(W) = M$ sono isomorfi. \square

18.2. Si dimostri il seguente corollario del teorema 18.1: *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*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ \varphi_A \downarrow & & \downarrow \varphi_B \\ W_A & \xrightarrow{\quad \bar{f} \quad} & W_B \end{array}$$

Soluzione. Si applichi la proprietà universale dei monoidi liberi (teorema 18.1) al monoide 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

18.3. Se A è l'insieme vuoto, cos'è il monoide libero su A ? Quanti elementi ha?

18.4. Siano M un monoide, A un insieme, (W, \circ) il monoide 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.

18.5. Siano M un monoide, 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 2.20). Si denoti con W il monoide 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 $\widehat{\varepsilon}: W \rightarrow M$ tale che $\widehat{\varepsilon} \circ \varphi = \varepsilon$. Si dimostri che l'immagine $\widehat{\varepsilon}(W)$ dell'omomorfismo $\widehat{\varepsilon}$ coincide con il sottomonoide $[X]$ di M generato da X .

18.6. Sia A un insieme fissato e sia $W' = \bigcup_{n \geq 1} W_n$ l'insieme di tutte le parole di lunghezza ≥ 1 nell'alfabeto A . Allora W' è un semigruppo rispetto alla concatenazione di parole, detto il *semigruppo 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 semigruppi liberi:

Siano A un insieme, (W', \circ) il semigruppo libero su A, e $\varphi: A \rightarrow W'$ l'applicazione canonica di A in W' . Allora per ogni semigruppo S e ogni applicazione $f: A \rightarrow S$ esiste un unico omomorfismo di semigruppi $\widehat{f}: W' \rightarrow S$ che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{f} & S \\ & \varphi \searrow & \nearrow \widehat{f} \\ & W' & \end{array}$$

cioè tale che $\widehat{f} \circ \varphi = f$.

18.7. Si dimostri che se $|A| = 1$, il semigruppo libero W' su A (vedi esercizio 18.6) è isomorfo al semigruppo $(\mathbb{N}^*, +)$.

Appendice 18.1. Alfabeti valutati

Abbiamo chiamato *parola* nell'alfabeto A una qualunque sequenza $a_1 a_2 \dots a_n$ di elementi di A . Ad esempio le espressioni algebriche che si imparano a calcolare alle scuole elementari sono delle parole nell'alfabeto $A = \mathbb{R} \cup \{+, -, \cdot, :, =\}$. Però non tutte le parole in questo alfabeto A sono delle espressioni algebriche, esattamente come non tutte le sequenze di lettere dell'alfabeto italiano sono parole che hanno significato in italiano. Vediamo un primo modo per aggirare tale difficoltà.

Un *alfabeto valutato* è una coppia ordinata (A, τ) , 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 .

18.3 ESEMPIO. 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, τ) è un alfabeto valutato. Come si può intravedere in questo esempio, nell'alfabeto valutato (A, τ) converrà pensare $\tau(a)$ come il "numero di simboli a cui si applica a ". \square

Se (A, τ) 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, τ) ed un insieme X (i cui elementi saranno detti *variabili*). Le *parole generate da (A, τ) e X* sono definite nel modo seguente:

- (a) gli elementi di $A_0 \cup X$ sono parole;
- (b) se $n \geq 1$, $a \in A_n$ e w_1, w_2, \dots, w_n sono parole, anche $aw_1w_2 \dots w_n$ è una parola;
- (c) sono parole solo le espressioni che si ottengono applicando un numero finito di volte (a) e (b).

18.4 ESEMPIO. Sia (A, τ) l'alfabeto valutato dell'esempio 18.3 e sia $X = \{x, y, z\}$. Sono parole x , $+xy$, 2 , $- + xy$, $.2 - + xy$. Le parole generate da (A, τ) e X sono quindi tutte e sole 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 $\underbrace{X \times X \times \cdots \times X}_{n \text{ volte}} \rightarrow X$. 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 nel §14 (in cui spiegando la notazione polacca denotavamo con $-$ la sottrazione che è un'operazione binaria) e gli esempi 18.3 e 18.4 (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.

§19. Gruppi

Sia (M, \cdot) un monoide con identità 1 , e sia $a \in M$. L'elemento 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.

19.1 ESEMPIO. 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 φ 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 3.3, se e solo se l'applicazione φ è iniettiva. Analogamente, per l'esercizio 3.4, un elemento φ 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 biiezioni $A \rightarrow A$. \square

19.2 LEMMA. Sia M un monoide, e sia a un elemento invertibile a sinistra e a destra. Se $b, c \in M$ sono tali che $ba = ac = 1$, allora $b = c$.

Dimostrazione. Si ha $b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$. \square

Per il lemma 19.2 un elemento invertibile $a \in M$ ha un unico *inverso* (o *reciproco*) sia a sinistra che a destra; denoteremo tale inverso con a^{-1} .

19.3 LEMMA. 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 $(a^{-1})^{-1} = a$.

Dimostrazione. Si ha $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1$ e similmente $(ab)(b^{-1}a^{-1}) = 1$. Quindi ab è invertibile e $b^{-1}a^{-1}$ è il suo inverso. Inoltre a è l'inverso di a^{-1} perché $aa^{-1} = a^{-1}a = 1$. \square

Se nel monoide M l'operazione è scritta in notazione additiva, si preferisce chiamare l'inverso di un elemento invertibile a 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 che soddisfa alle proprietà seguenti:

- (a) *associatività*: $(ab)c = a(bc)$ per ogni $a, b, c \in G$;
- (b) *identità*: esiste un elemento $1_G \in G$ tale che $a1_G = 1_Ga = a$ per ogni $a \in G$;
- (c) *inverso*: per ogni $a \in G$ esiste $b \in G$ tale che $ab = ba = 1_G$.

In questa definizione di gruppo abbiamo usato la notazione moltiplicativa. Nulla vieta naturalmente di fare uso della notazione additiva, nel qual caso la definizione diventa la seguente:

Un gruppo $(G, +)$ è un insieme G dotato di un'operazione $+$ che soddisfa alle proprietà seguenti:

- (a) *associatività*: $(a + b) + c = a + (b + c)$ per ogni $a, b, c \in G$;
- (b) *zero*: esiste un elemento $0_G \in G$ tale che $a + 0_G = 0_G + a = a$ per ogni $a \in G$;
- (c) *oppuesto*: per ogni $a \in G$ esiste $b \in G$ tale che $a + b = b + a = 0_G$.

Torniamo ad usare la nozione moltiplicativa. Un gruppo (G, \cdot) tale che $ab = ba$ per ogni $a, b \in G$ si dice un *gruppo abeliano* (o *commutativo*). La notazione additiva si usa generalmente solo per i gruppi abeliani, mentre quella moltiplicativa si usa sia per i gruppi abeliani che per quelli non abeliani.

19.4 ESEMPIO. I monoidi $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) non sono gruppi; infatti in $(\mathbb{N}, +)$ l'unico elemento invertibile è lo 0, in (\mathbb{N}, \cdot) l'unico elemento invertibile è 1, in (\mathbb{Z}, \cdot) gli unici elementi invertibili sono 1 e -1 , in (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) tutti gli elementi sono invertibili eccetto lo 0. \square

19.5 ESEMPIO. I monoidi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi abeliani. Se $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, allora i monoidi (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{C}^*, \cdot) sono gruppi abeliani. \square

19.6 ESEMPIO. Se (M, \cdot) è un monoide e $U(M)$ è l'insieme degli elementi invertibili di M , mostriamo che $U(M)$ è un sottomonoide 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 19.3. 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 sottomonoide 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 19.3 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

19.7 ESEMPIO. Applicando quanto abbiamo dimostrato nell'esempio 19.6 (cioè che se M è un monoide $U(M)$ risulta essere un gruppo) ai monoidi visti nell'esempio 19.4 troviamo che i gruppi degli elementi invertibili dei monoidi $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) sono rispettivamente i gruppi $(\{0\}, +)$, $(\{1\}, \cdot)$, $(\{1, -1\}, \cdot)$, (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{C}^*, \cdot) . \square

19.8 ESEMPIO. Il monoide (X^X, \circ) , ove X è un insieme con almeno due elementi, non è un gruppo. Il gruppo $U(X^X)$ si suole indicare con S_X , ed è detto il *gruppo simmetrico* su X . I suoi elementi sono le biiezioni di X in X . \square

19.9 ESEMPIO. $(\{1\}, \cdot)$ è un gruppo con un solo elemento. L'operazione è definita da $1 \cdot 1 = 1$. È un gruppo abeliano. \square

Se (G, \cdot) è un gruppo e g è un suo elemento, si può definire la *potenza n-esima* di g per ogni $n \in \mathbb{Z}$ ponendo

$$g^n = \begin{cases} 1_G & \text{se } n = 0, \\ (g^{n-1})g & \text{se } n > 0, \\ (g^{-1})^{-n} & \text{se } n < 0. \end{cases}$$

Quindi $g^n = g \cdot g \cdots g$ (n fattori) se $n > 0$ e $g^n = g^{-1} \cdot g^{-1} \cdots g^{-1}$ ($-n$ fattori) se $n < 0$. Continuano a valere le formule della proposizione 15.7, che raccogliamo nella proposizione seguente; ne omettiamo la dimostrazione.

19.10 PROPOSIZIONE. 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 $(gh)^n = g^n h^n$.

Similmente, se G è un gruppo additivo, si definiscono i multipli.

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) *inverso*: $a^{-1} \in H$ 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*). Tutti i sottogruppi di G che sono diversi da G si chiamano *sottogruppi propri* di G . Chiaramente ogni sottogruppo di un sottogruppo abeliano è abeliano.

19.11 ESEMPIO. 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 $H \supsetneq \{0\}$. 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 numero 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 $x = \underbrace{n + n + \cdots + n}_{z \text{ volte}} \in H$ 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 $x = nz = \underbrace{(-n) + (-n) + \cdots + (-n)}_{-z \text{ volte}} \in H$. 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

19.12 LEMMA. *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 $a, b \in H$.*

Dimostrazione. Supponiamo $H \leq G$. Allora $H \neq \emptyset$, perché $1_G \in H$. Inoltre se $a, b \in H$, allora $b^{-1} \in H$ e quindi, essendo H sottoinsieme chiuso, $ab^{-1} \in H$. Viceversa sia $H \neq \emptyset$ e $ab^{-1} \in H$ per ogni $a, b \in H$. Dato che $H \neq \emptyset$, esiste $h \in H$. Ma allora $1_G = hh^{-1} \in H$. Quindi per ogni $a \in H$ si ha $a^{-1} = 1_G a^{-1} \in H$. Infine per ogni $a, b \in H$ si ha $b^{-1} \in H$ e quindi $ab = a(b^{-1})^{-1} \in H$. Pertanto $H \leq G$. \square

19.13 ESEMPIO. Abbiamo già visto nell'esempio 19.5 che $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ è un gruppo rispetto alla moltiplicazione. Consideriamo il sottoinsieme \mathbb{T} di \mathbb{C}^* costituito dai numeri complessi di modulo 1:

$$\mathbb{T} = \{z \mid z \in \mathbb{C}, |z| = 1\}.$$

Mostriamo che \mathbb{T} è un sottogruppo di (\mathbb{C}^*, \cdot) facendo uso del lemma 19.12. Osserviamo intanto che $\mathbb{T} \neq \emptyset$ perché ad esempio $1 \in \mathbb{T}$. Poi se $z, z' \in \mathbb{T}$ allora $zz'^{-1} \in \mathbb{C}$ e $|zz'^{-1}| = |z||z'|^{-1} = 1/1 = 1$, e quindi $zz'^{-1} \in \mathbb{T}$. Pertanto \mathbb{T} è sottogruppo di \mathbb{C}^* . \square

19.14 ESEMPIO. Sia $n \geq 1$ un numero naturale fissato. Osserviamo che se $z \in \mathbb{C}$ è una radice n -esima dell'unità allora $z \neq 0$ (perché $0^n = 0 \neq 1$). Quindi se

$$C_n = \{z \mid z \in \mathbb{C}, z^n = 1\}$$

è l'insieme delle radici n -esime dell'unità, allora $C_n \subseteq \mathbb{C}^*$. Mostriamo che C_n è un sottogruppo di (\mathbb{C}^*, \cdot) . Intanto $C_n \neq \emptyset$, anzi abbiamo visto nel §5 che $|C_n| = n$. Poi se $z, z' \in C_n$, allora $zz'^{-1} \in \mathbb{C}$ e si ha $(zz'^{-1})^n = z^n(z'^{-1})^n = 1 \cdot 1^{-1} = 1$. Quindi $zz'^{-1} \in C_n$. Pertanto per il lemma 19.12 C_n è un sottogruppo di (\mathbb{C}^*, \cdot) . Dato che la moltiplicazione tra numeri complessi è commutativa, il gruppo C_n , detto il *gruppo delle radici n -esime dell'unità*, è abeliano. \square

Siano G, H gruppi. Un omomorfismo di semigruppi $\varphi: G \rightarrow H$, ossia un'applicazione tale che $\varphi(ab) = \varphi(a)\varphi(b)$ per ogni $a, b \in G$, si dice anche un *omomorfismo di gruppi*.

19.15 LEMMA. *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 φ 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

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H \quad \text{e} \quad \varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1_G) = 1_H.$$

(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

$$\varphi(g^z) = \varphi((g^{-1})^{-z}) = (\varphi(g^{-1}))^{-z} = ((\varphi(g))^{-1})^{-z} = (\varphi(g))^z. \quad \square$$

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 . Se esiste un isomorfismo del gruppo G nel gruppo H si dice che i gruppi G e H sono *isomorfi*, e si scrive $G \cong H$. Un'ultima definizione: se G è un gruppo, la cardinalità dell'insieme G si dice *l'ordine* di G . Ad esempio l'ordine del gruppo C_n delle radici n -esime dell'unità (esempio 19.14) è proprio n .

Esercizi svolti

19.1. Sull'insieme $\mathbb{R}^* \times \mathbb{R} = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{R}, \alpha \neq 0\}$ si definisca un'operazione · ponendo $(\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \alpha\beta' + \beta/\alpha')$ 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 $\alpha\alpha', \alpha\beta' + \beta/\alpha' \in \mathbb{R}$ 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

$$\begin{aligned} ((\alpha, \beta)(\alpha', \beta'))(\alpha'', \beta'') &= \left(\alpha\alpha', \alpha\beta' + \frac{\beta}{\alpha'} \right) (\alpha'', \beta'') = \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \frac{\alpha\beta' + \beta/\alpha'}{\alpha''} \right) \\ &= \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \frac{\alpha\beta'}{\alpha''} + \frac{\beta}{\alpha'\alpha''} \right) \end{aligned}$$

e

$$\begin{aligned} (\alpha, \beta)((\alpha', \beta')(\alpha'', \beta'')) &= (\alpha, \beta) \left(\alpha'\alpha'', \alpha'\beta'' + \frac{\beta'}{\alpha''} \right) = \left(\alpha\alpha'\alpha'', \alpha \left(\alpha'\beta'' + \frac{\beta'}{\alpha''} \right) + \frac{\beta}{\alpha'\alpha''} \right) \\ &= \left(\alpha\alpha'\alpha'', \alpha\alpha'\beta'' + \frac{\alpha\beta'}{\alpha''} + \frac{\beta}{\alpha'\alpha''} \right). \end{aligned}$$

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 $(x\alpha, x\beta + y/\alpha) = (\alpha, \beta)$ per ogni $(\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R}$. Questo accade se e solo se $x\alpha = \alpha$ e $x\beta + y/\alpha = \beta$ 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 $(1, 0)(\alpha, \beta) = (1 \cdot \alpha, 1 \cdot \beta + 0/\alpha) = (\alpha, \beta)$ e $(\alpha, \beta)(1, 0) = (\alpha \cdot 1, \alpha \cdot 0 + \beta/1) = (\alpha, \beta)$. 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 (α, β) . Allora si deve avere $(x, y)(\alpha, \beta) = (1, 0)$, cioè $(x\alpha, x\beta + y/\alpha) = (1, 0)$, vale a dire $x\alpha = 1$ e $x\beta + y/\alpha = 0$. Quindi se (x, y) è l'inverso di (α, β) si deve avere $x = 1/\alpha$ e $y = -\beta$. Questo dimostra che l'inverso di (α, β) , se esiste, deve essere $(1/\alpha, -\beta)$.

Mostriamo che $(1/\alpha, -\beta)$ è proprio l'inverso di (α, β) : si ha

$$(\alpha, \beta)(1/\alpha, -\beta) = (\alpha(1/\alpha), \alpha(-\beta) + \beta\alpha) = (1, 0)$$

e

$$(1/\alpha, -\beta)(\alpha, \beta) = ((1/\alpha)\alpha, (1/\alpha)\beta + (-\beta)/\alpha) = (1, 0). \quad \square$$

19.2. 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 insiemi 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 φ 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 φ è un isomorfismo tra G_1 e G_2 . \square

19.3. Siano \mathbb{R} il gruppo additivo dei numeri reali,

$$\mathbb{T} = \{z \mid z \in \mathbb{C}, |z| = 1\}$$

il gruppo moltiplicativo dei numeri complessi di modulo 1, $\varphi: \mathbb{R} \rightarrow \mathbb{T}$ l'applicazione definita da $\varphi(x) = \cos x + i \sin x$ per ogni $x \in \mathbb{R}$. Si dimostri che φ 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

19.4. Si dica quali dei seguenti monoidi sono gruppi: (\mathbb{R}^+, \cdot) , $(\mathcal{P}(X), \cap)$, $(\{0\}, \cdot)$, $(\{0, 1\}, \cdot)$, $(\{1, -1\}, \cdot)$, ove \cdot indica la moltiplicazione usuale, $\mathbb{R}^+ = \{\alpha \in \mathbb{R} \mid \alpha > 0\}$, e X è un insieme.

19.5. Si dimostri che il semigruppo $(\mathbb{R} \times \mathbb{R}, *)$ dell'esercizio 15.15 è un monoide e se ne determinino gli elementi invertibili.

19.6. Se W è il monoide libero su un insieme A , quali sono gli elementi invertibili di W ? invertibili a destra? invertibili a sinistra?

19.7. Siano G, H gruppi e $G \times H$ il prodotto diretto di G ed H (esercizi 15.13 e 16.1). Si provi che $G \times H$ è un gruppo.

19.8. 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?

19.9. Siano m, n numeri naturali. Si dimostri che $m\mathbb{Z} \supseteq n\mathbb{Z}$ se e solo se $m \mid n$.

19.10. Sia $(G, +)$ un gruppo abeliano.

- (a) Si dimostri che se H, H' sono sottogruppi di G , allora $H + H' = \{h + h' \mid h \in H, h' \in H'\}$ è sottogruppo di G .
- (b) Si dimostri che se H, H' sono sottogruppi di G , allora $H \cap H'$ è sottogruppo di G .
- (c) Siano $a, b \in \mathbb{Z}$ e si consideri il gruppo abeliano $(\mathbb{Z}, +)$. Si dimostri che se d è massimo comun divisore di a e b , ed m è loro minimo comune multiplo, allora $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ e $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

19.11. 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

$$G[mn] = G[m] + G[n] \quad \text{e} \quad G[m] \cap G[n] = \{0_G\}.$$

[Suggerimento per (b): corollario 4.5.]

19.12. Un elemento e di un semigruppo (S, \cdot) si dice *idempotente* se $e^2 = e$.

- (a) Si dimostri che se A è un insieme, nel semigruppo $(A, *)$ studiato nell'esempio 15.3 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 sottosemigruppo di M ed eMe è un monoide.

19.13. 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 .

- 19.14. Sia (M, \cdot) un monoide. Diremo che nel monoide M vale la proprietà di cancellazione se per ogni $x, y, z \in M$ si ha che $xz = yz$ implica $x = y$, e che $zx = xy$ implica $x = y$. Si provi che:
- nel monoide $(\mathbb{N}, +)$ vale la proprietà di cancellazione (attenzione alla notazione);
 - nel monoide (\mathbb{N}, \cdot) non vale la proprietà di cancellazione;
 - in ogni gruppo G vale la proprietà di cancellazione;
 - se G è un gruppo ed M è un sottomonoide di G , allora in M vale la proprietà di cancellazione.

- 19.15. Sia (M, \cdot) un monoide commutativo in cui vale la proprietà di cancellazione (vedi esercizio 19.14). Si provi che:

- nel monoide $M \times M$, prodotto diretto di M per M , la relazione \sim definita da $(a, b) \sim (a', b')$ per ogni $(a, b), (a', b') \in M \times M$, è una relazione di equivalenza compatibile con l'operazione del monoide $M \times M$;
- il monoide $M \times M / \sim$ è un gruppo abeliano;
- l'applicazione $\varepsilon: M \rightarrow M \times M / \sim$, definita da $\varepsilon(a) = [(a, 1)]_\sim$ per ogni $a \in M$, è un omomorfismo iniettivo di monoidi.

Quindi ogni monoide commutativo in cui vale la proprietà di cancellazione è isomorfo ad un sottomonoide di un gruppo abeliano.

- 19.16. Sia (A, \leq) un insieme parzialmente ordinato, e sia $\text{Aut } A$ l'insieme degli automorfismi di A , cioè degli isomorfismi di insieme ordinato $A \rightarrow A$. Si provi che $(\text{Aut } A, \circ)$, ove \circ è la composizione di applicazioni, è un gruppo, detto il gruppo degli automorfismi di A . Si definiscano analogamente i gruppi $\text{Aut } G$ degli automorfismi di un grafo G , $\text{Aut } S$ degli automorfismi di un semigruppo S , $\text{Aut } M$ degli automorfismi di un monoide M , $\text{Aut } H$ degli automorfismi di un gruppo H .

- 19.17. Sia G un gruppo, e sia $g \in G$. Definiamo l'applicazione $\sigma_g: G \rightarrow G$ ponendo $\sigma_g(x) = gxg^{-1}$ per ogni $x \in G$. Si provi che σ_g è un automorfismo di g (detto l'*automorfismo interno indotto da g*).

- 19.18. 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 .

- 19.19. 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 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 .]

19.20. (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 sottomonoide 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 $v: M_n(\mathbb{R}) \rightarrow M_n(0, 1)$ ponendo $v((a_{ij})) = (a'_{ij})$, 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 $A, B \in M_n(0, 1)$, $A * B = v(AB)$, 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 ϱ (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 $(M_n(0, 1), *)$.

§20. Equivalenze compatibili con l'addizione in \mathbb{N} e in \mathbb{Z}

20.1 PROPOSIZIONE. *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 8.2 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 $-b \sim -a$ (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 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, $x - y + nq + r \sim y - y + r$, 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 $x, y \in \mathbb{N}$

$$x \sim_{k,n} y \text{ se } \begin{cases} x = y \\ \text{oppure} \\ x \geq k, y \geq k \text{ e } x \equiv y \pmod{n}. \end{cases}$$

20.2 ESEMPIO. Si ha

$$\begin{array}{lll} 0 \sim_{4,9} 9, & 2 \sim_{4,9} 11, & 3 \sim_{4,9} 12, \\ 4 \sim_{4,9} 13, & 5 \sim_{4,9} 14, & 100 \sim_{4,9} 10. \end{array} \quad \square$$

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 $x \equiv y \pmod{n}$. Ma allora $x \equiv z \pmod{n}$, da cui $x \sim_{k,n} z$.

È quindi possibile costruire l'insieme quoziante

$$\mathbb{N}/\sim_{k,n} = \{[x]_{\sim_{k,n}} \mid x \in \mathbb{N}\}.$$

20.3 LEMMA. Siano $k, n \in \mathbb{N}$ e $n \geq 1$. 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 $k+r \geq k$ 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 $i \equiv j \pmod{n}$. 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:

$$[0]_{\sim_{k,n}} = \{0\},$$

$$[1]_{\sim_{k,n}} = \{1\},$$

$$[2]_{\sim_{k,n}} = \{2\},$$

\vdots

$$[k-2]_{\sim_{k,n}} = \{k-2\},$$

$$[k-1]_{\sim_{k,n}} = \{k-1\},$$

$$[k]_{\sim_{k,n}} = \{k, k+n, k+2n, k+3n, \dots\},$$

$$[k+1]_{\sim_{k,n}} = \{k+1, k+1+n, k+1+2n, k+1+3n, \dots\},$$

\vdots

$$[k+n-2]_{\sim_{k,n}} = \{k+n-2, k+n-2+n, k+n-2+2n, k+n-2+3n, \dots\},$$

$$[k+n-1]_{\sim_{k,n}} = \{k+n-1, k+n-1+n, k+n-1+2n, k+n-1+3n, \dots\}.$$

Nel §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'analogia rappresentazione di $\mathbb{N}/\sim_{k,n}$ è quella della figura 20.1.

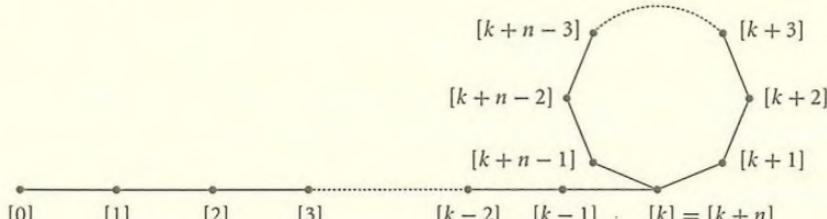


FIGURA 20.1.

20.4 PROPOSIZIONE. *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 20.4 viene omessa per brevità (si veda comunque l'esercizio 20.13). 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 16.13 si ha $[[1]_{\sim_{k,n}}] = \{t[1]_{\sim_{k,n}} \mid t \in \mathbb{N}\} = \{[t]_{\sim_{k,n}} \mid t \in \mathbb{N}\} = \mathbb{N}/\sim_{k,n}$.

20.5 PROPOSIZIONE. *Ogni monoide ciclico 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 $M = [a] = \{a^t \mid t \in \mathbb{N}\}$. Consideriamo l'applicazione $\varphi: \mathbb{N} \rightarrow M$ definita da $\varphi(t) = a^t$ per ogni $t \in \mathbb{N}$. L'applicazione φ è un omomorfismo suriettivo del monoide $(\mathbb{N}, +)$ nel monoide (M, \cdot) . Per il teorema fondamentale di omomorfismo si ha un isomorfismo di monoidi $\mathbb{N}/\sim_\varphi \cong M$, ove \sim_φ è la relazione di equivalenza su \mathbb{N} associata a φ . Tale equivalenza è compatibile con l'addizione di \mathbb{N} perché φ è un omomorfismo di monoidi (§17), e quindi per la proposizione 20.4 la relazione \sim_φ è una delle relazioni $\sim_{k,n}$ per qualche $k \geq 0$ e qualche $n \geq 1$ oppure è l'uguaglianza $=$. Se \sim_φ è una delle relazioni $\sim_{k,n}$, allora $M \cong \mathbb{N}/\sim_\varphi = \mathbb{N}/\sim_{k,n}$. Se invece φ è la relazione di uguaglianza, allora φ 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_φ e $=$ coincidono. Quindi in questo caso φ è una biiezione, e quindi un isomorfismo, e pertanto $(\mathbb{N}, +)$ e (M, \cdot) sono isomorfi. \square

Esercizi svolti

20.1. 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 8.4. Per il teorema fondamentale di omomorfismo per i monoidi (teorema 17.3), se \sim_f è la relazione di equivalenza su \mathbb{N} associata ad f , allora i monoidi \mathbb{N}/\sim_f e \mathbb{Z}/\equiv_n sono isomorfi. 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

20.2. Si dimostri che se (G, \cdot) è un gruppo e \sim è un'equivalenza su G compatibile con l'operazione \cdot , allora il monoide quoziante $(G/\sim, \cdot)$ 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 al-

lora $[g^{-1}]_{\sim}$ appartiene a G/\sim e si ha $[g]_{\sim}[g^{-1}]_{\sim} = [gg^{-1}]_{\sim} = [1_G]_{\sim} = 1_{G/\sim}$ e analogamente $[g^{-1}]_{\sim}[g]_{\sim} = 1_{G/\sim}$. Quindi $[g^{-1}]_{\sim}$ è l'inverso di $[g]_{\sim}$ in G/\sim . \square

20.3. Tra i monoidi $(\mathbb{N}, +)$ e $(\mathbb{N}/\sim_{k,n}, +)$, $k, n \in \mathbb{N}$, $n \geq 1$, quali sono gruppi e quali non lo sono?

Soluzione. Il monoide $(\mathbb{N}, +)$ non è un gruppo, in quanto il suo unico elemento invertibile è 0.

Cerchiamo gli elementi invertibili di $(\mathbb{N}/\sim_{k,n}, +)$ quando entrambi i numeri naturali n e k sono ≥ 1 . Lo zero di $\mathbb{N}/\sim_{k,n}$ è $[0]_{\sim_{k,n}}$. Se $[x]_{\sim_{k,n}} \in \mathbb{N}/\sim_{k,n}$ è un elemento invertibile, esiste un $[y]_{\sim_{k,n}} \in \mathbb{N}/\sim_{k,n}$ tale che $[x]_{\sim_{k,n}} + [y]_{\sim_{k,n}} = [0]_{\sim_{k,n}}$, cioè tale che $x + y \sim_{k,n} 0$. Si deve quindi avere $x + y \in [0]_{\sim_{k,n}}$. Ma abbiamo visto che essendo $k \geq 1$ si ha $[0]_{\sim_{k,n}} = \{0\}$. Pertanto $x + y = 0$, ed essendo x e y numeri naturali si deve avere $x = y = 0$. Abbiamo così dimostrato che quando $k \geq 1$ l'unico elemento invertibile di $\mathbb{N}/\sim_{k,n}$ è $[0]_{\sim_{k,n}}$, ed avendo $\mathbb{N}/\sim_{k,n}$ $n+k \geq 2$ elementi, se ne deduce che $\mathbb{N}/\sim_{k,n}$ non è un gruppo.

Resta da esaminare il caso in cui $k = 0$. Ma in questo caso i monoidi $(\mathbb{N}/\sim_{0,n}, +)$ e $(\mathbb{Z}/\equiv_n, +)$ sono isomorfi per l'esercizio 20.1. Inoltre $(\mathbb{Z}/\equiv_n, +)$ è un gruppo perché $(\mathbb{Z}, +)$ è un gruppo (esercizio 20.2). Pertanto $(\mathbb{N}/\sim_{0,n}, +)$ è un gruppo.

Abbiamo così dimostrato che il monoide $(\mathbb{N}, +)$ non è un gruppo, mentre il monoide $(\mathbb{N}/\sim_{k,n}, +)$, $k, n \in \mathbb{N}$, $n \geq 1$, è un gruppo se e solo se $k = 0$. \square

Altri esercizi

20.4. Si considerino le seguenti tre relazioni sull'insieme \mathbb{Z} :

ϱ definita, per ogni $a, b \in \mathbb{Z}$ da $a \varrho b$ se $a = b$ oppure $a = -b$;
 σ definita, per ogni $a, b \in \mathbb{Z}$ da $a \sigma b$ se $a = b$ oppure $2a = b$;
 τ definita, per ogni $a, b \in \mathbb{Z}$ da $a \tau b$ se $a = b$ oppure $ab = 5$.

- (a) Si dica quali tra le relazioni ϱ , σ e τ sono equivalenze.
- (b) Tra le equivalenze trovate in (a) si dica quali sono compatibili con l'addizione tra numeri interi.
- (c) Tra le equivalenze trovate in (a) si dica quali sono compatibili con la moltiplicazione tra numeri interi.

20.5. Si consideri la relazione ϱ sull'insieme \mathbb{Z} definita, per ogni $a, b \in \mathbb{Z}$, da $a \varrho b$ se $(ab - 3)(a - b) = 0$.

- (a) Si dimostri che ϱ è un'equivalenza sull'insieme \mathbb{Z} .
- (b) Per ogni $a \in \mathbb{Z}$ quanti elementi ha la classe di equivalenza $[a]_{\varrho}$?
- (c) L'equivalenza ϱ è compatibile con l'addizione tra numeri interi?

20.6. Determinare tutte le relazioni di equivalenza \sim sull'insieme \mathbb{Z} tali che \sim sia compatibile con l'addizione tra numeri interi e $2 \sim 3$.

20.7. Determinare tutte le relazioni di equivalenza \sim sull'insieme \mathbb{Z} tali che \sim sia compatibile con l'addizione tra numeri interi e $2 \sim 8$.

20.8. Determinare tutte le relazioni di equivalenza \sim sull'insieme \mathbb{N} tali che \sim sia compatibile con l'addizione tra numeri naturali e $2 \sim 3$.

20.9. Determinare tutte le relazioni di equivalenza \sim sull'insieme \mathbb{N} tali che \sim sia compatibile con l'addizione tra numeri naturali e $2 \sim 8$.

20.10. Siano m, n, q numeri interi positivi tali che $m = nq$.

- Si definisca $\varphi: \mathbb{Z}/\equiv_n \rightarrow \mathbb{Z}/\equiv_m$ ponendo $\varphi([x]_{\equiv_n}) = [qx]_{\equiv_m}$ per ogni $x \in \mathbb{Z}$. Si provi che φ è un'applicazione ben definita¹ e che è un omomorfismo di gruppi additivi.
- Si dimostri che l'omomorfismo φ è iniettivo.
- 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 .

20.11. 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.

20.12. 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 $(\mathbb{N}/\sim_{k,n}, +)$.

20.13. (a) Si dimostri che le relazioni di equivalenza $\sim_{k,n}$ (dove $k \geq 0$ e $n \geq 1$) sono compatibili con l'addizione.

(b) Si dimostri che per ogni equivalenza \sim su \mathbb{N} compatibile con $+$ e diversa dall'uguaglianza $=$, esistono $k \geq 0$ ed $n \geq 1$ tali che \sim coincide con $\sim_{k,n}$.

Questo dimostra la proposizione 20.4.

[Suggerimento per (b): sia \sim compatibile con $+$ e diverso dall'uguaglianza $=$. Poniamo $\ell = \min\{y \in \mathbb{N} \mid \text{esiste } x \in \mathbb{N}, x < y \text{ e } x \sim y\}$. Allora $0, 1, \dots, \ell - 1$ sono a due a due non equivalenti tra loro (nell'equivalenza \sim). Sia $k \in \mathbb{N}$ l'unico elemento tale che $k < \ell$ e $k \sim \ell$. Poniamo $n = \ell - k$ e proviamo che $\sim \sim \sim_{k,n}$ coincidono. Dato che $k \sim \ell$, cioè $k \sim k + n$, ne segue che $k + t \sim k + n + t$ per ogni $t \in \mathbb{N}$. Ora le classi $[0]_\sim, [1]_\sim, \dots, [n+k-1]_\sim$ sono distin-

¹ Nota sul concetto di buona definizione di un'applicazione. Abbiamo già visto in alcuni esercizi (ad esempio nell'8.4, 8.12, 8.13, 10.24 e in altri) e vedremo ancora negli esercizi 22.19, 23.8 e 23.14 che è necessario assicurarsi talvolta che un'applicazione sia ben definita. Questo capita quando si vuole definire un'applicazione $\varphi: A \rightarrow B$ (e quindi per ogni $a \in A$ si vuol specificare un elemento $\varphi(a)$ di B) e per farlo si sceglie in corrispondenza di a un qualche oggetto a' (magari in un altro insieme A') e poi si dice cosa sarà $\varphi(a)$ in funzione di a' . Dobbiamo controllare pertanto che l'applicazione sia ben definita, cioè che se in corrispondenza dello stesso elemento $a \in A$ si sceglie un altro oggetto $a'' \in A'$, l'elemento che si vuole sia $\varphi(a)$ non cambi. Ad esempio nell'esercizio 20.10 l'applicazione $\varphi: \mathbb{Z}/\equiv_n \rightarrow \mathbb{Z}/\equiv_m$ è definita ponendo $\varphi([x]_{\equiv_n}) = [qx]_{\equiv_m}$ per ogni $x \in \mathbb{Z}$. Ora un elemento a del dominio $A = \mathbb{Z}/\equiv_n$ di φ è del tipo $[x]_{\equiv_n}$ per qualche $x \in \mathbb{Z}$. Ma l'elemento $x \in \mathbb{Z}$ tale che $a = [x]_{\equiv_n}$ non è unico: si ha che $a = [x']_{\equiv_n}$ anche per ogni altro elemento $x' \in \mathbb{Z}$ congruo a x modulo n . Ponendo $\varphi(a) = [qx]_{\equiv_m}$ è necessario assicurarsi che si è data una buona definizione, cioè che se al posto di x si sceglie un altro elemento $x' \in \mathbb{Z}$ tale che $a = [x']_{\equiv_n}$ si ha sempre $[qx]_{\equiv_m} = [qx']_{\equiv_m}$.

Spesso il caso in cui è necessario assicurarsi di aver dato una buona definizione è il seguente: si hanno due insiemi B e C , un'equivalenza \sim su C e un'applicazione $f: C \rightarrow B$, e si vuole definire un'applicazione $\varphi: C/\sim \rightarrow B$, dove C/\sim denota l'insieme quoziente. In questo caso per definire l'applicazione φ si deve specificare per ogni $a \in C/\sim$ un elemento $\varphi(a)$ di B . Ora un qualunque elemento $a \in C/\sim$ è una classe di equivalenza $[c]$ per un opportuno elemento $c \in C$. Per definire l'applicazione φ ponendo $\varphi(a) = f(c)$ è necessario assicurarsi che $f(c)$ non dipende dal particolare $c \in C$ scelto, cioè che se $c' \in C$ è un altro elemento tale che $a = [c']$, allora $f(c) = f(c')$. Solo così sarà definita bene l'applicazione φ .

Facciamo un altro esempio. Nell'esercizio 10.24 si avevano due insiemi non vuoti A e B e un insieme \mathcal{G} di coppie (X, f) dove per ogni $(X, f) \in \mathcal{G}$ si aveva che X era un sottoinsieme di A ed f un'applicazione di X in B . Si supponeva poi di sapere che per ogni $(X, f), (Y, g) \in \mathcal{G}$ e ogni $a \in X \cap Y$ si aveva $f(a) = g(a)$. Posto $S = \bigcup_{(X, f) \in \mathcal{G}} X$, si definiva un'applicazione $\varphi: S \rightarrow B$ nel modo seguente: per ogni $a \in S$ se $(X, f) \in \mathcal{G}$ era una coppia tale che $a \in X$ si poneva $\varphi(a) = f(a)$. Era necessario quindi verificare di aver ben definito l'applicazione φ , cioè di avere dato una buona definizione di φ , in quanto fissato un elemento $a \in S$ possono esistere altre coppie $(Y, g) \in \mathcal{G}$ tali che $a \in Y$. Ma è sufficiente osservare che per ogni tale altra eventuale coppia (Y, g) si ha sempre $g(a) = f(a)$. Quindi l'elemento $f(a)$ di B non dipende dalla coppia scelta $(X, f) \in \mathcal{G}$ con la proprietà che $a \in X$, ma solo dall'elemento a .

te tra loro (e quindi a due a due disgiunte), e risulta $[0]_{\sim} \supseteq \{0\}$, $[1]_{\sim} \supseteq \{1\}, \dots, [k-1]_{\sim} \supseteq \{k-1\}$, $[k]_{\sim} \supseteq \{k, k+n, k+2n, k+3n, \dots\}$, $[k+1]_{\sim} \supseteq \{k+1, k+1+n, k+1+2n, \dots\}, \dots, [k+n-1]_{\sim} \supseteq \{(k+n-1), (k+n-1)+n, (k+n-1)+2n, \dots\}$. Se ne deduca che tutte queste inclusioni sono uguaglianze, e quindi che $\sim = \sim_{k,n}$.

20.14. 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 circolare, 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 20.5). 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 $M \cong \mathbb{N}/\sim_{k,n}$.

20.15. 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 circolare $[Y]$ di $\mathcal{P}(X)$ generato da Y .

20.16. 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 circolare $[i]$ di (\mathbb{C}, \cdot) generato da i .

20.17. 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 circolare $[i]$ di $(\mathbb{C}, +)$ generato da i .

20.18. 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 circolare $[f]$ di X^X generato da f .

20.19. 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 $a/b \in \mathbb{R}$.

- (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 considerino il monoide quoziente $(\mathbb{C}^*/\sim, \cdot)$ e il suo elemento $[i\sqrt{2}]_{\sim}$. Quanti elementi ha il sottomonoido circolare $[(i\sqrt{2})_{\sim}]$ 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 $[(i\sqrt{2})_{\sim}]$.

§21. Permutazioni

In questo §21 studieremo un esempio particolare di gruppo. Fissiamo un intero $n \geq 1$ e poniamo $X_n = \{1, 2, \dots, n\}$. Nel §9 abbiamo già incontrato le permutazioni di X_n , cioè le biiezioni $X_n \rightarrow X_n$, e abbiamo imparato a denotare le permutazioni $f : X_n \rightarrow X_n$ nella forma

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

L'insieme di tutte le permutazioni di X_n è un gruppo rispetto alla composizione di applicazioni \circ . Denoteremo tale gruppo con S_n , e lo chiameremo il *gruppo simmetrico su n oggetti* o il *gruppo delle permutazioni di n oggetti*. Per il corollario 9.9 l'ordine del gruppo S_n è $n!$.

Data una permutazione f di X_n , il *grafo orientato della permutazione* f è il grafo orientato G_f che ha come insieme V dei vertici l'insieme X_n e come insieme L dei lati l'insieme $f = \{(i, f(i)) \mid i \in X_n\}$. Quindi i vertici di G_f sono $1, 2, \dots, n$, e c'è un lato orientato da i a j se e solo se $f(i) = j$.

21.1 ESEMPIO. Il grafo orientato G_f della permutazione

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 3 & 7 & 1 & 5 & 8 & 2 & 9 \end{pmatrix}$$

è il grafo riportato nella figura 21.1. \square

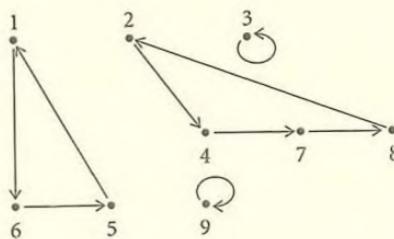


FIGURA 21.1.

Si ha ovviamente $d^+(v) = d^-(v) = 1$ per ogni $v \in X_n$ (si veda anche l'esercizio 12.18). È facile convincersi che ogni grafo orientato finito connesso $G = (V, L)$ con $d^+(v) = d^-(v) = 1$ per ogni $v \in V$ è necessariamente isomorfo a



FIGURA 21.2.

Dato che ogni grafo è unione disgiunta delle sue componenti connesse, ne segue che ogni grafo orientato finito con $d^+(v) = d^-(v) = 1$ per ogni vertice v è necessariamente isomorfo a un grafo del tipo

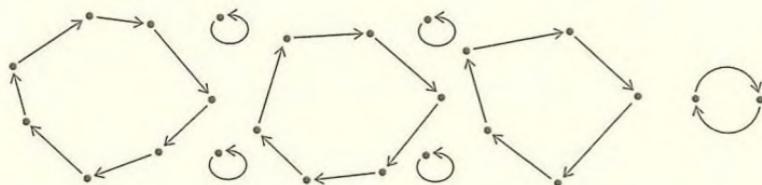


FIGURA 21.3.

Questo ci suggerisce di rivolgere la nostra attenzione a un tipo particolare di permutazioni. 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 $i = 1, 2, \dots, d-1$, $f(a_d) = a_1$, e $f(k) = k$ per ogni $k \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_d\}$. Quindi un ciclo di lunghezza n "permette ciclicamente" d elementi di $\{1, 2, \dots, n\}$ lasciando fissi gli altri $n-d$ elementi. Denoteremo il ciclo che "permette ciclicamente" a_1, a_2, \dots, a_d con il simbolo $(a_1 \ a_2 \ \dots \ a_d)$. Si osservi che la notazione $(a_1 \ a_2 \ \dots \ a_d) = f$ non è univocamente determinata da f . È chiaro infatti che f si potrà anche scrivere come $(a_2 \ a_3 \ \dots \ a_d \ a_1)$ oppure $(a_3 \ a_4 \ \dots \ a_d \ a_1 \ a_2)$.

21.2 ESEMPIO. 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

$$(1 \ 2 \ 6 \ 3) = (2 \ 6 \ 3 \ 1) = (6 \ 3 \ 1 \ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}. \quad \square$$

21.3 ESEMPIO. Le permutazioni

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (2 \ 3 \ 4) = (3 \ 4 \ 2) = (4 \ 2 \ 3)$$

e

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1 \ 2) = (2 \ 1)$$

sono cicli di lunghezza 3 e 2 rispettivamente. \square

Il grafo orientato G_f del ciclo $f = (a_1 \ a_2 \ \dots \ a_d)$ è quindi del tipo

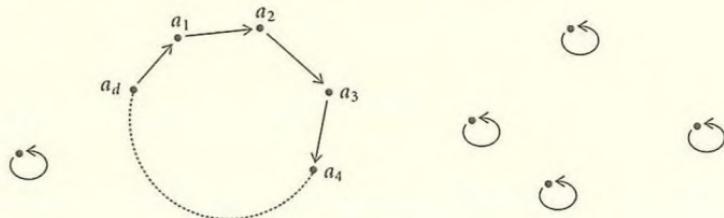


FIGURA 21.4.

Il lettore osservi che i cicli di lunghezza 1 sono tutti uguali all'identità di S_n , e che, viceversa, l'identità di S_n può essere considerata un ciclo di lunghezza 1. Denoteremo quindi talvolta l'identità di S_n con (1).

Due cicli $(a_1 \ a_2 \ \dots \ a_d)$, $(b_1 \ b_2 \ \dots \ b_t)$ di S_n si dicono *disgiunti* se $\{a_1, a_2, \dots, a_d\} \cap \{b_1, b_2, \dots, b_t\} = \emptyset$.

Se $f = (a_1 \ a_2 \ \dots \ a_d)$, $g = (b_1 \ b_2 \ \dots \ b_t)$ sono due cicli disgiunti, allora il grafo orientato $G_{f \circ g}$ della permutazione composta $f \circ g$ è

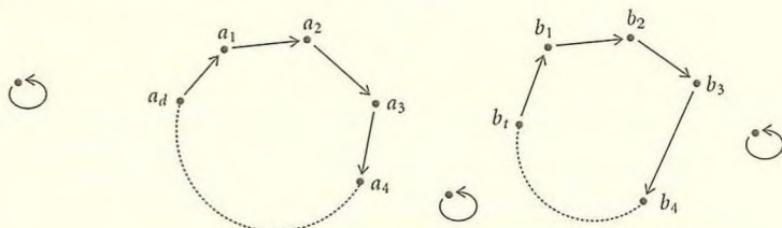


FIGURA 21.5.

Si ottiene lo stesso grafo orientato anche con la permutazione composta $g \circ f$. Infatti f e g permutano insiemi disgiunti, e quindi l'ordine in cui queste permutazioni vengono effettuate non modifica il risultato. Si ha pertanto che

21.4 LEMMA. Se $f = (a_1 \ a_2 \ \dots \ a_d)$ e $g = (b_1 \ b_2 \ \dots \ b_t)$ sono cicli disgiunti, allora $f \circ g = g \circ f$.

Si osservi che se f e g sono due cicli non disgiunti, può risultare $f \circ g \neq g \circ f$. Ad esempio in S_3 se $f = (1 \ 2 \ 3)$ e $g = (1 \ 2)$, allora

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{e} \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Se f è una permutazione, allora il suo grafo orientato G_f è unione disgiunta in modo unico delle sue componenti connesse, ciascuna delle quali è un grafo del tipo



FIGURA 21.6.

Se ne ricava che

21.5 TEOREMA. *Ogni permutazione può essere scritta come prodotto di cicli a due a due disgiunti. Tale scrittura è unica a meno dell'ordine dei fattori.*

Per scrivere una permutazione $f \in S_n$ come prodotto di cicli a due a due disgiunti si procede nel modo seguente. Si comincia con lo scrivere il numero 1:

(1.

Se f manda 1 in un elemento a_2 , si scrive

(1 a_2 .

Ora f manda a_2 in un elemento a_3 , e si scrive

(1 a_2 a_3 .

Continuando con questo procedimento si ritroverà prima o poi un numero ripetuto (al più all' $(n + 1)$ -esimo passo, se non prima). Il primo numero ripetuto deve essere 1. Altrimenti se si avesse $(1 a_2 a_3 \dots a_d a_t)$, ove $1 = a_1, a_2, \dots, a_d$ sono distinti e $1 \neq t \leq d$, allora a_t sarebbe l'immagine dei due elementi distinti a_{t-1} e a_d , e questo contraddirebbe l'iniettività di f . La prima volta che si incontra una ripetizione del numero 1 si chiude la parentesi:

(1 $a_2 a_3 \dots a_d$).

Si comincia poi un altro ciclo partendo dal più piccolo numero non usato nel ciclo precedente. Se un tale numero esiste si ripete il procedimento di prima. Se tutti i numeri da 1 a n sono già stati trovati in cicli precedenti si è terminato. In questo modo ogni permutazione si scrive come prodotto di cicli disgiunti e tale scrittura è unica a meno dell'ordine dei fattori.

21.6 ESEMPIO. Scriviamo 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5$$

Ma f manda 5 in 2 e quindi scriviamo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2$$

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ .$$

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 .$$

La permutazione f manda 3 in 7:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 \quad 7$$

e manda 7 in 3. Quindi anche il secondo ciclo è concluso:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 \quad 7) \circ .$$

Il primo numero che non abbiamo ancora incontrato è 4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 \quad 7) \circ (4 .$$

La f manda 4 in 6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 \quad 7) \circ (4 \quad 6$$

e manda 6 in 8

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 6 & 2 & 8 & 3 & 4 \end{pmatrix} = (1 \quad 5 \quad 2) \circ (3 \quad 7) \circ (4 \quad 6 \quad 8$$

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 completa. Si noti che tale scrittura è unica a meno dell'ordine dei fattori; per il lemma 21.4 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. \square

21.7 ESEMPIO. Il lettore decomponga come 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 5 & 2 & 1 & 4 \end{pmatrix} = (1 \ 6) \circ (2 \ 7 \ 4 \ 5). \quad \square$$

Si osservi un fatto del tutto generale visto nell'esempio 21.7: dato che i cicli di lunghezza 1 sono uguali all'identità, nella scrittura di una permutazione come prodotto di cicli disgiunti si può tralasciare di scrivere i cicli di lunghezza 1.

I cicli di lunghezza 2 si chiamano anche *trasposizioni*.

21.8 TEOREMA. *Ogni permutazione può essere scritta come prodotto di trasposizioni.*

Dimostrazione. Segue dal teorema 21.5 osservando che ogni ciclo

$$(a_1 \ a_2 \ \dots \ a_d)$$

è prodotto di trasposizioni in quanto

$$(a_1 \ a_2 \ \dots \ a_d) = (a_1 \ a_d)(a_1 \ a_{d-1}) \cdots (a_1 \ a_3)(a_1 \ a_2). \quad \square$$

21.9 ESEMPIO. In S_8 si ha

$$(2 \ 4 \ 5 \ 6 \ 7) = (2 \ 7) \circ (2 \ 6) \circ (2 \ 5) \circ (2 \ 4). \quad \square$$

Si noti però che una stessa permutazione ha varie fattorizzazioni in prodotto di trasposizioni; ad esempio, si provi per esercizio che le permutazioni $(1 \ 3) \circ (2 \ 4)$, $(1 \ 4) \circ (1 \ 2) \circ (4 \ 3)$, $(4 \ 2) \circ (4 \ 1) \circ (4 \ 3)$, $(4 \ 1)$ coincidono.

21.10 COROLLARIO. 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 sottomonoidi 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,

$$f = (a_{11} \ a_{12} \ \dots \ a_{1d_1}) \circ (a_{21} \ a_{22} \ \dots \ a_{2d_2}) \circ \dots \circ (a_{k1} \ a_{k2} \ \dots \ a_{kd_k});$$

se f è prodotto di k cicli di lunghezza d_1, d_2, \dots, d_k rispettivamente, poniamo

$$\lambda(f) = \left(\sum_{i=1}^k d_i \right) - k.$$

21.11 ESEMPI.

- (a) In S_4 consideriamo $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$; allora $f = (1 \ 2) \circ (3 \ 4)$ e quindi $\lambda(f) = (2+2) - 2 = 2$.
- (b) In S_5 se $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} = (1 \ 2 \ 5)$, allora $\lambda(g) = 3 - 1 = 2$.
- (c) In S_n , se t è una trasposizione, $\lambda(t) = 2 - 1 = 1$. \square

Si definisca ora l'applicazione $\text{sgn}: S_n \rightarrow \{1, -1\}$ ponendo $\text{sgn}(f) = (-1)^{\lambda(f)}$ per ogni $f \in S_n$ ($\text{sgn}(f)$ si dice la *segnatura* di f). Dimostreremo nell'esercizio 21.14 che

21.12 TEOREMA. L'applicazione $\text{sgn}: S_n \rightarrow \{1, -1\}$ è un omomorfismo del gruppo (S_n, \circ) nel gruppo $(\{1, -1\}, \cdot)$.

Per il teorema 21.12, $\text{sgn}(f \circ g) = \text{sgn}(f) \cdot \text{sgn}(g)$ per ogni $f, g \in S_n$. Ora se t è una trasposizione si ha $\text{sgn}(t) = -1$ (esempio 21.11(c)). Quindi se f si scrive come prodotto di ℓ trasposizioni (e questo è possibile per il teorema 21.8), $f = t_1 \circ t_2 \circ \dots \circ t_\ell$, allora $\text{sgn}(f) = \text{sgn}(t_1) \cdot \text{sgn}(t_2) \cdot \dots \cdot \text{sgn}(t_\ell) = \underbrace{(-1)(-1)\dots(-1)}_{\ell \text{ fattori}} = (-1)^\ell$. Quindi $\text{sgn}(f)$ è

1 se e solo se ℓ è pari, e $\text{sgn}(f) = -1$ se solo se ℓ è dispari.

Inoltre se $f = t_1 \circ t_2 \circ \dots \circ t_\ell = t'_1 \circ t'_2 \circ \dots \circ t'_m$ sono due fattorizzazioni di f come prodotto di trasposizioni, allora $(-1)^\ell = \text{sgn}(f) = (-1)^m$, e quindi ℓ e m sono entrambi pari o entrambi dispari. Abbiamo così dimostrato il seguente teorema:

21.13 TEOREMA. Le rappresentazioni di una data permutazione f come prodotto di trasposizioni hanno tutte un numero pari o tutte un numero dispari di fattori.

Se $\text{sgn}(f) = 1$, cioè se f è prodotto di un numero pari di trasposizioni, f si dice *di classe pari*. Altrimenti si dice di *classe dispari*.

Esercizi svolti

21.1. 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 biezione $\{1\} \rightarrow \{1\}$, 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 biezioni $\{1, 2\} \rightarrow \{1, 2\}$, 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

$$\begin{aligned} (1 & \quad 2) \circ (1 \quad 2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} (1 & \quad 2 \quad 3) \circ (1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}. \end{aligned}$$

Quindi $(1 \quad 2) \circ (1 \quad 2 \quad 3) \neq (1 \quad 2 \quad 3) \circ (1 \quad 2)$, e pertanto il gruppo S_n non è abeliano per $n \geq 3$. \square

21.2. 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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 3 & 8 & 7 \end{pmatrix} = (1 \quad 2 \quad 4 \quad 6 \quad 3 \quad 5)(7 \quad 8),$$

e quindi, come si vede facendo uso della formula scritta nella dimostrazione del teorema 21.8, questa permutazione è uguale a

$$(1 \quad 5)(1 \quad 3)(1 \quad 6)(1 \quad 4)(1 \quad 2)(7 \quad 8). \quad \square$$

21.3. 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 $\operatorname{sgn}(f) = (-1)^5 = -1$. Pertanto f è di classe dispari.

(2) Decomporla 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

21.4. (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 $f \circ g = f$.

21.5. 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.

21.6. 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 $f \circ g = g \circ f$?

21.7. 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.

21.8. 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} .

21.9. Si scriva come prodotto di cicli disgiunti, come prodotto di trasposizioni e si calcoli la segnatura delle seguenti permutazioni:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 13 & 10 & 7 & 8 & 9 & 6 & 3 & 1 & 12 & 5 & 11 & 2 & 4 \end{pmatrix}.$$

21.10. Si scriva come prodotto di cicli disgiunti, come prodotto di trasposizioni e si calcoli la segnatura delle permutazioni f, f^2, f^3 ed f^4 dove $f = (1 \ 5) \circ (2 \ 3 \ 4) \in S_5$.

21.11. 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.

21.12. 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 φ 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 $f = \psi^{-1} \varphi \psi$ è una permutazione di X_8 . Si scriva f come prodotto di cicli disgiunti e se ne determini la classe.

21.13. 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 $d/2$.

21.14. Si dimostri il teorema 21.12. [Suggerimento: si deve dimostrare che $\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g)$ per ogni $f, g \in S_n$. Si scriva g come prodotto di trasposizioni, $g = t_1 \circ t_2 \circ \dots \circ t_\ell$; allora è sufficiente dimostrare che $\operatorname{sgn}(h \circ t) = -\operatorname{sgn}(h)$ per ogni $h, t \in S_n$ con t trasposizione, perché allora $\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f \circ t_1 \circ t_2 \circ \dots \circ t_\ell) = -\operatorname{sgn}(f \circ t_1 \circ t_2 \circ \dots \circ t_{\ell-1}) = \dots = \operatorname{sgn}(f) \cdot (-1)^\ell = \operatorname{sgn}(f) \cdot \operatorname{sgn}(t_1) \cdot (-1)^{\ell-1} = \operatorname{sgn}(f) \cdot \operatorname{sgn}(t_1 \circ t_2) \cdot (-1)^{\ell-2} = \dots = \operatorname{sgn}(f) \cdot \operatorname{sgn}(t_1 \circ t_2 \circ \dots \circ t_\ell) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g)$. Per provare che $\operatorname{sgn}(h \circ t) = -\operatorname{sgn}(h)$ ($t = (a \ b)$ trasposizione) decomponiamo h in cicli disgiunti: $h = h_1 h_2 \dots h_k$, h_i ciclo di lunghezza d_i , e in questa fattorizzazione supponiamo di aver scritto anche i cicli di lunghezza 1, di modo che $d_1 + \dots + d_k = n$. Si hanno allora due casi: a e b compaiono nello stesso h_i oppure a e b compaiono in h_i distinti. Nel primo caso permutando gli h_i , si può supporre per il lemma 21.4 che a e b compaiano entrambi in h_k ; poniamo che $h_k = (ae_1 \dots e_r bf_1 \dots f_s)$ con $r+s+2 = d_k$; allora $ht = h_1 h_2 \dots h_{k-1} (ae_1 \dots e_r bf_1 \dots f_s)(ab) = h_1 h_2 \dots h_{k-1} (af_1 \dots f_s)(be_1 \dots e_r)$ è una decomposizione in cicli disgiunti, e quindi $\lambda(ht) = d_1 + \dots + d_{k-1} + (s+1) + (r+1) - (k+1) = \lambda(h) - 1$. Nel secondo caso, se a e b compaiono in h_i distinti, si può supporre come prima che a compaia in h_{k-1} e b in h_k ; poniamo $h_{k-1} = (ae_2 \dots e_{d_{k-1}})$, $h_k = (bf_2 \dots f_{d_k})$; allora $ht = h_1 \dots h_{k-2} (ae_2 \dots e_{d_{k-1}})(bf_2 \dots f_{d_k})(ab) = h_1 \dots h_{k-2} (af_2 \dots f_{d_k} be_2 \dots e_{d_{k-1}})$, e quindi $\lambda(ht) = d_1 + \dots + d_{k-2} + (d_k + d_{k-1}) - (k-1) = \lambda(h) + 1$.]

21.15. Mostrare che $A_n = \{f \in S_n \mid \operatorname{sgn}(f) = 1\}$ è un sottogruppo di S_n (A_n è detto il *gruppo alterno*).

§22. Sottogruppi normali e classi laterali

Sia (G, \cdot) un gruppo, H 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*.

22.1 ESEMPIO. 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 $\alpha = g \cdot (\alpha/g)$ e $\alpha/g \in \mathbb{R}^+$. Quindi $\alpha = g \cdot (\alpha/g) \in g\mathbb{R}^+$).

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 $\alpha/g \in \mathbb{R}^+$, e quindi $\alpha = g \cdot (\alpha/g) \in g\mathbb{R}^+$. Pertanto $\mathbb{R}^- \subseteq g\mathbb{R}^+$. \square

22.2 ESEMPIO. 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 $g_1^{-1}g_2 = 1_H = h \in H$.

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

Dall'esempio precedente si deduce in particolare che se G è un gruppo, $H \leq G$ e $g \in G$, allora $gH = H$ se e solo se $g \in H$.

Per le classi laterali destre si potrebbe dimostrare che $Hg_1 = Hg_2$ se e solo se $g_1g_2^{-1} \in H$.

22.3 LEMMA. Se G è un gruppo, $H \leq G$ e $g \in G$, allora gli insiemi H e gH sono equipotenti.

Dimostrazione. L'applicazione $\varphi: H \rightarrow gH$ definita da $\varphi(h) = gh$ per ogni $h \in H$ è una biiezione. Infatti φ è suriettiva, perché un generico elemento y del suo codominio gH è del tipo $y = gh$ per qualche $h \in H$, e quindi $\varphi(h) = y$. E φ è iniettiva, perché se $h_1, h_2 \in H$ e $\varphi(h_1) = \varphi(h_2)$, allora $gh_1 = gh_2$, e quindi moltiplicando a sinistra per g^{-1} si ha $h_1 = h_2$. \square

22.4 LEMMA. Siano G un gruppo e H un sottogruppo di G . Allora l'insieme $\{gH \mid g \in G\}$ di tutte le classi laterali sinistre di G modulo H è una partizione di G .

Dimostrazione. I sottoinsiemi gH di G ($g \in G$) sono tutti non vuoti, perché $g = g \cdot 1 \in gH$. Poi evidentemente $\bigcup_{g \in G} gH = G$. Infine se $g_1, g_2 \in G$ e $g_1H \neq g_2H$, allora $g_1H \cap g_2H = \emptyset$, perché se così non fosse, cioè se esistesse $x \in g_1H \cap g_2H$, allora $x = g_1h_1 = g_2h_2$ per opportuni $h_1, h_2 \in H$, da cui $g_1 = g_2h_2h_1^{-1}$. Ma allora per ogni $h \in H$ si avrebbe $g_1h = g_2h_2h_1^{-1}h \in g_2H$, cioè $g_1H \subseteq g_2H$. Similmente $g_2H \subseteq g_1H$. Quindi $g_1H = g_2H$, assurdo. \square

22.5 ESEMPIO. Nell'esempio 22.1 abbiamo visto che se $G = \mathbb{R}^*$ e $H = \mathbb{R}^+$, la classe laterale sinistra $g\mathbb{R}^+$ di \mathbb{R}^* modulo \mathbb{R}^+ di rappresentante g è \mathbb{R}^+ se $g > 0$, ed è \mathbb{R}^- se $g < 0$. Si noti che $\{gH \mid g \in G\} = \{\mathbb{R}^+, \mathbb{R}^-\}$ è proprio una partizione di \mathbb{R}^* , in accordo con l'enunciato del lemma 22.4. \square

Il numero di classi laterali sinistre di G modulo H si chiama l'*indice* di H in G , e si indica con $[G : H]$. Quindi $[G : H] = |\{gH \mid g \in G\}|$ se l'insieme $\{gH \mid g \in G\}$ è finito. Se invece $\{gH \mid g \in G\}$ è un insieme infinito diremo che l'indice di H in G è infinito e scriveremo $[G : H] = \infty$. Negli esempi 22.1 e 22.5 abbiamo visto che ci sono esattamente due classi laterali sinistre del gruppo moltiplicativo \mathbb{R}^* modulo il suo sottogruppo \mathbb{R}^+ , formata una da tutti i numeri reali positivi e l'altra da tutti i numeri reali negativi. Quindi $[\mathbb{R}^* : \mathbb{R}^+] = 2$.

È ovvio che se il gruppo G è finito, allora $[G : H]$ è finito qualunque sia il sottogruppo H di G . In questo caso si ha che:

22.6 TEOREMA DI LAGRANGE. L'ordine di ogni sottogruppo di un gruppo finito G divide l'ordine di G .

Dimostrazione. Per il lemma 22.3 si ha che $|H| = |gH|$ per ogni $g \in G$, e per il lemma 22.4 l'insieme $\{gH \mid g \in G\}$ è una partizione di G . Pertanto G è ripartito in $[G : H]$ classi laterali ognuna delle quali contiene $|H|$ elementi. Quindi $|G| = [G : H] \cdot |H|$ e $|H|$ divide $|G|$. \square

Si noti che la formula $[G : H] = |G|/|H|$ ha senso solo quando il gruppo G è finito, perché in questo caso $|G|$, $|H|$ e $[G : H]$ sono tre numeri interi ≥ 1 . Se il gruppo G è infinito la formula $[G : H] = |G|/|H|$ può non avere alcun senso. Ad esempio abbiamo già osservato che se $G = \mathbb{R}^*$ e $H = \mathbb{R}^+$ allora $[G : H] = 2$, e quindi la formula precedente diventerebbe l'espressione $2 = \infty/\infty$ che è ovviamente priva di significato.

Sia G un gruppo. Vogliamo studiare ora le relazioni di equivalenza \sim su G compatibili con l'operazione \cdot del gruppo, cioè le relazioni di equivalenza \sim su G tali che se $a, b, c, d \in G$, $a \sim b$ e $c \sim d$ allora $ac \sim bd$. A questo scopo è conveniente introdurre la nozione di sottogruppo normale. Vedremo negli esercizi 22.1 e 22.5 che possono esistere sottogruppi H di un gruppo G ed elementi $g \in G$ tali che $gH \neq Hg$. Quindi in generale la classe laterale sinistra e la classe laterale destra modulo H di rappresentante g posso-

no essere diverse. Diremo che un sottogruppo H di G è un *sottogruppo normale* di G se $gH = Hg$ per ogni $g \in G$; in tal caso scriveremo $H \trianglelefteq G$. Si ha $G \trianglelefteq G$ e $\{1_G\} \trianglelefteq G$ qualunque sia il gruppo G . Se G è un gruppo abeliano ogni suo sottogruppo H è normale in quanto per ogni $g \in G$ si ha $gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$.

22.7 LEMMA. *Sia H un sottogruppo di G . Allora H è normale in G se e solo se $ghg^{-1} \in H$ per ogni $g \in G$ e ogni $h \in H$.*

Dimostrazione. Siano $H \trianglelefteq G$, $g \in G$ e $h \in H$. Allora $gh \in gH = Hg$, e quindi esiste $h' \in H$ tale che $gh = h'g$. Ma allora $ghg^{-1} = h' \in H$. Viceversa supponiamo che $ghg^{-1} \in H$ per ogni $g \in G$ e $h \in H$. Mostriamo che $gH = Hg$ per ogni $g \in G$. Se $x \in gH$, allora $x = gy$ per un opportuno $y \in H$, e quindi $gyg^{-1} = y'$ per un opportuno $y' \in H$. Ma allora $x = gy = y'g \in Hg$; questo prova che $gH \subseteq Hg$. Similmente se $x \in Hg$, allora $x = zg$ per qualche $z \in H$, e quindi $g^{-1}zg \in H$, cioè $g^{-1}zg = z' \in H$. Pertanto $x = zg = gz' \in gH$. Si conclude che $Hg \subseteq gH$, e quindi $H \trianglelefteq G$. \square

22.8 TEOREMA. *Sia (G, \cdot) un gruppo. Se \sim è una relazione di equivalenza su G compatibile con l'operazione \cdot , allora $[1_G]_\sim$, la classe di equivalenza di 1_G , è un sottogruppo normale di G . Viceversa, se N è sottogruppo normale di G e \sim_N è la relazione sull'insieme G definita, per ogni $a, b \in G$, da $a \sim_N b$ se $a^{-1}b \in N$, allora \sim_N è una relazione di equivalenza su G compatibile con l'operazione \cdot e $[1_G]_\sim = N$.*

Dimostrazione. Supponiamo che \sim sia un'equivalenza su G compatibile con la moltiplicazione. Allora $[1_G]_\sim \neq \emptyset$ perché $1_G \in [1_G]_\sim$; inoltre se $a, b \in [1_G]_\sim$, allora $a \sim 1_G$ e $b \sim 1_G$, da cui $1_G \sim b$ e quindi $a \sim b$. Ma essendo $b^{-1} \sim b^{-1}$, si ha $ab^{-1} \sim bb^{-1} = 1_G$, ossia $ab^{-1} \in [1_G]_\sim$. Per il lemma 19.12 l'insieme $[1_G]_\sim$ è sottogruppo di G . Inoltre se $a \in [1_G]_\sim$ e $g \in G$, allora $g \sim g$, $a \sim 1_G$ e $g^{-1} \sim g^{-1}$, da cui per la compatibilità $gag^{-1} \sim g1_Gg^{-1} = gg^{-1} = 1_G$, ossia $gag^{-1} \in [1_G]_\sim$. Quindi $[1_G]_\sim \trianglelefteq G$.

Viceversa sia $N \trianglelefteq G$ e sia \sim_N definita da $a \sim_N b$ se $a^{-1}b \in N$ ($a, b \in G$). Allora \sim_N è riflessiva, perché $a^{-1}a = 1_G \in N$ per ogni $a \in G$; \sim_N è simmetrica, perché se $a^{-1}b \in N$ allora $b^{-1}a = (a^{-1}b)^{-1} \in N$; \sim_N è transitiva, perché se $a^{-1}b \in N$ e $b^{-1}c \in N$ allora $a^{-1}c = (a^{-1}b)(b^{-1}c) \in N$; infine \sim_N è compatibile con la moltiplicazione \cdot del gruppo, perché se $a \sim_N b$ e $c \sim_N d$ ($a, b, c, d \in G$), allora $a^{-1}b \in N$ e $c^{-1}d \in N$. Ma allora $c^{-1}(a^{-1}b)c \in N$ perché $N \trianglelefteq G$, e quindi $(ac)^{-1}(bd) = c^{-1}a^{-1}bd = (c^{-1}a^{-1}bc)(c^{-1}d) \in N$, ossia $ac \sim_N bd$. Resta da dimostrare che $[1_G]_\sim = N$, ma questo è ovvio perché $[1_G]_\sim = \{a \in G \mid 1_G \sim_N a\} = \{a \in G \mid 1_G^{-1}a \in N\} = \{a \in G \mid a \in N\} = N$. \square

Dal teorema 22.8 si deduce facilmente che se (G, \cdot) è un gruppo, \mathcal{E}_G è l'insieme di tutte le relazioni di equivalenza su G compatibili con l'operazione \cdot , ed $\mathcal{N}_G = \{N \mid N \trianglelefteq G\}$ è l'insieme dei sottogruppi normali di G , allora le applicazioni $\Phi: \mathcal{E}_G \rightarrow \mathcal{N}_G$, definita da $\Phi(\sim) = [1_G]_\sim$ per ogni $\sim \in \mathcal{E}_G$, e $\Psi: \mathcal{N}_G \rightarrow \mathcal{E}_G$, definita da $\Psi(N) = \sim_N$ per ogni $N \in \mathcal{N}_G$, sono due biiezioni una l'inversa dell'altra. Qui, come nell'enunciato del teorema 22.8, con \sim_N abbiamo denotato l'equivalenza su G definita, per ogni $a, b \in G$, da $a \sim_N b$ se $a^{-1}b \in N$.

22.9 ESEMPIO. Sia G un gruppo con p elementi, dove p è un numero primo. Cerchiamo tutte le equivalenze su G compatibili con l'operazione di G . Dato che $|G| = p$, per il teorema di Lagrange tutti i sottogruppi di G hanno come ordine un divisore di p . Ma p è primo, e quindi i sottogruppi di G hanno tutti ordine 1 o p . Dato che 1_G appartiene a ogni sottogruppo di G , c'è un unico sottogruppo di G di ordine 1, vale a dire il gruppo $\{1_G\}$. Dato che $|G| = p$, c'è un unico sottoinsieme di G con p elementi, ossia il gruppo G stesso. Abbiamo così dimostrato che G ha solo i due sottogruppi $\{1_G\}$ e G . Sappiamo anche già che questi due sottogruppi di G sono normali. Quindi G ha esattamente due sottogruppi normali, cioè $\{1_G\}$ e G . Per il teorema 22.8 ci sono esattamente due equivalenze su G compatibili con l'operazione di G , vale a dire $\sim_{\{1_G\}}$ e \sim_G . Ora per ogni $a, b \in G$ si ha $a \sim_{\{1_G\}} b$ se e solo se $a^{-1}b \in \{1_G\}$, ossia se e solo se $a^{-1}b = 1_G$, e quindi (moltiplicando a sinistra per a) se e solo se $a = b$. Questo dimostra che $\sim_{\{1_G\}}$ è la relazione di uguaglianza $=$. Similmente si vede che \sim_G è la relazione di equivalenza banale ω su G . Quindi $=$ e ω sono le due uniche equivalenze su G compatibili con l'operazione del gruppo. \square

Siano G un gruppo e $N \trianglelefteq G$. È facile dimostrare che per ogni $g \in G$ la classe di equivalenza $[g]_{\sim_N}$ nella relazione di equivalenza \sim_N è esattamente la classe laterale sinistra (o destra) $gN = Ng$ di G modulo N (le classi laterali destra e sinistra coincidono perché N è normale in G). Infatti $[g]_{\sim_N} = \{x \in G \mid g \sim_N x\} = \{x \in G \mid g^{-1}x \in N\} = \{x \in G \mid x \in gN\} = gN$. Quindi il quoziente $G/\sim_N = \{[g]_{\sim_N} \mid g \in G\} = \{gN \mid g \in G\}$. Lo denoteremo in genere con G/N . Quindi $G/N = \{gN \mid g \in G\}$ è il monoide in cui l'operazione è definita da $(g_1N)(g_2N) = (g_1g_2)N$ e in cui $1_{G/N} = 1_GN = N$. La proposizione che segue era già stata essenzialmente dimostrata nell'esercizio 20.2.

22.10 PROPOSIZIONE. Se G è un gruppo ed N è un sottogruppo normale di G , allora G/N è un gruppo.

Dimostrazione. È sufficiente dimostrare che nel monoide G/N ogni elemento è invertibile. Ma se $gN \in G/N$, il suo inverso in G/N è $g^{-1}N$ perché $(gN)(g^{-1}N) = gg^{-1}N = N = 1_{G/N}$ e similmente $(g^{-1}N)(gN) = N = 1_{G/N}$. \square

Riassumendo: per ogni gruppo G e ogni suo sottogruppo normale N abbiamo costruito un gruppo G/N , detto il *gruppo quoziente di G modulo N* , i cui elementi sono le classi laterali sinistre (o destre) $gN = Ng$, cioè

$$\bullet \quad G/N = \{gN \mid g \in G\},$$

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 $(gN)^{-1} = g^{-1}N$.

Sia $N \trianglelefteq G$. 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 $\pi(g), \pi(g') = gN, g'N = gg'N = \pi(gg')$.

22.11 ESEMPIO. 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 non nullo $z = \varrho(\cos \theta + i \sin \theta)$ avente argomento θ , la classe laterale sinistra $z\mathbb{R}^+$ è l'insieme degli elementi del tipo $\varrho(\cos \theta + i \sin \theta)t$ con $t \in \mathbb{R}^+$, ossia $z\mathbb{R}^+ = \{\varrho t(\cos \theta + i \sin \theta) \mid t \in \mathbb{R}^+\} = \{r(\cos \theta + i \sin \theta) \mid r \in \mathbb{R}^+\}$. Quindi gli elementi di $z\mathbb{R}^+$ sono tutti i numeri complessi non nulli aventi argomento θ , vale a dire tutti i punti del piano di Argand-Gauss che stanno sulla semiretta aperta (cioè senza l'origine) passante per z e la cui origine è il punto 0. Si noti che queste classi laterali formano una partizione di \mathbb{C}^* . Il gruppo quoziante 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

22.1. Sia $S(\mathbb{R})$ il gruppo di tutte le biiezioni $f: \mathbb{R} \rightarrow \mathbb{R}$ 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 biiezione 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

22.2. 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 19.14). 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 -agono regolare inscritto nella circonferenza C di centro 0 e raggio 1 e avente un vertice nel punto $(1, 0)$ sono anche vertici dell' m -agono regolare inscritto in 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 $[C_m : C_n] = |C_m|/|C_n| = m/n$. \square

Altri esercizi

22.3. Sia \mathbb{C}^* il gruppo moltiplicativo dei numeri complessi non nulli e sia \mathbb{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 $z\mathbb{T}$ è l'insieme dei numeri complessi aventi modulo uguale al modulo di z , cioè è l'insieme dei numeri complessi che rappresentati 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}^* .

22.4. Sia \mathbb{R}^* il gruppo moltiplicativo dei numeri reali 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 αH è l'insieme $\{\alpha, -\alpha\}$. Si noti che anche in questo caso le classi laterali sinistre formano una partizione di \mathbb{R}^* .

22.5. Sia $G = S_3$ il gruppo simmetrico su tre oggetti, e sia $H = \langle (1 \ 2) \rangle = \{(1 \ 2), (1)\}$.

- (a) Si scrivano tutti gli elementi della classe laterale sinistra di S_3 modulo H di rappresentante $(1 \ 2 \ 3)$.
- (b) Si scrivano gli elementi di tutte le classi laterali sinistre di S_3 modulo H (si osservi che le classi laterali sinistre di S_3 modulo H formano una partizione di S_3).
- (c) Qual è l'indice $[S_3 : H]$ di H in S_3 ?
- (d) Si scrivano tutti gli elementi della classe laterale destra di S_3 modulo H di rappresentante $(1 \ 2 \ 3)$.
- (e) Il sottogruppo H di S_3 è normale?

22.6. In questo §22 abbiamo usato sempre la notazione moltiplicativa per i gruppi. Naturalmente se il gruppo G è additivo, la classe laterale sinistra di G modulo H di rappresentante l'elemento $g \in G$ è $g + H = \{g + h \mid h \in H\}$, e se H è sottogruppo normale di G allora $G/H = \{g + H \mid g \in G\}$ e l'operazione sul gruppo G/H è definita da $(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H$ per ogni $g_1, g_2 \in G$. Si osservi che, come abbiamo già fatto notare a pagina 167, usando la notazione additiva si intende di solito che il gruppo G sia abeliano; in tal caso tutti i sottogruppi sono normali, come si è visto a pagina 193. Quali sono le classi laterali di $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$? Qual è l'indice $[\mathbb{C} : \mathbb{R}]$?

22.7. Si provi che \mathbb{Q}^+ è un sottogruppo del gruppo (\mathbb{Q}^*, \cdot) (ove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$) e $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$) e si calcoli l'indice di \mathbb{Q}^+ in \mathbb{Q}^* .

22.8. Sia A un insieme.

- (a) Si dimostri che $(\mathcal{P}(A), \Delta)$ è un gruppo abeliano (si veda l'esercizio 1.24).
- (b) Si dimostri che se B è sottoinsieme di A , allora $\mathcal{P}(B)$ è sottogruppo di $\mathcal{P}(A)$.
- (c) Si dimostri che se $X, Y \in \mathcal{P}(A)$ e $B \subseteq A$, allora le classi laterali sinistre $X \Delta \mathcal{P}(B)$ e $Y \Delta \mathcal{P}(B)$ coincidono se e solo se $X \Delta Y \subseteq B$. [Suggerimento: far uso di quanto dimostrato nell'esempio 22.2.]

22.9. Sia n un intero positivo. Quanti e quali elementi ha il gruppo quoziente $\mathbb{Z}/n\mathbb{Z}$? Qual è l'indice $[\mathbb{Z} : n\mathbb{Z}]$?

22.10. Sia (G, \cdot) un gruppo. Si provi che i gruppi G e $G/\{1_G\}$ sono isomorfi. Si provi che i gruppi G/G e $\{1_G\}$ sono isomorfi.

22.11. Sia G un gruppo, H un sottogruppo di G . Si provi che se $\mathcal{S} = \{gH \mid g \in G\}$ e $\mathcal{D} = \{Hg \mid g \in G\}$ sono l'insieme delle classi laterali sinistre e destre di H in G , allora l'applicazione $\varphi: \mathcal{S} \rightarrow \mathcal{D}$ definita da $\varphi(gH) = Hg^{-1}$ per ogni $g \in G$ è ben definita (ossia se $g_1H = g_2H$, allora $Hg_1^{-1} = Hg_2^{-1}$) ed è una biiezione. Questo implica che $|\mathcal{S}| = |\mathcal{D}|$, e quindi si sarebbe potuto definire l'indice di H in G anche come il numero delle classi laterali destre. Naturalmente anche le classi laterali destre di G modulo H formano una partizione di G .

22.12. Siano G un gruppo, \mathcal{E}_G l'insieme delle equivalenze su G compatibili con l'operazione di G , \mathcal{N}_G l'insieme dei sottogruppi normali di G . Si considerino le applicazioni $\Phi: \mathcal{E}_G \rightarrow \mathcal{N}_G$, $\Phi(\sim) = [1_G]_\sim$ per ogni $\sim \in \mathcal{E}_G$, e $\Psi: \mathcal{N}_G \rightarrow \mathcal{E}_G$, $\Psi(N) = \sim_N$ per ogni $N \in \mathcal{N}_G$ (notazioni come nell'enunciato del teorema 22.8). Si provi che Φ e Ψ sono due biiezioni, una l'inversa dell'altra.

22.13. Sia $f: G \rightarrow G'$ un omomorfismo di gruppi e sia H' un sottogruppo di G' .

- (a) Può essere che $f^{-1}(H') = \emptyset$?
- (b) Se C è una classe laterale sinistra di G' modulo H' , può essere che $f^{-1}(C) = \emptyset$?

22.14. Sia S_{10} il gruppo simmetrico su dieci oggetti e

$$H = \{f \mid f \in S_{10}, f(10) = 10\}.$$

- (a) Si dimostri che H è un sottogruppo di S_{10} .
- (b) Si dimostri che il gruppo H è isomorfo al gruppo simmetrico su nove oggetti S_9 .
- (c) Si calcoli l'indice $[S_{10} : H]$.

22.15. Sia S_8 il gruppo simmetrico su 8 oggetti e sia

$$H = \{f \in S_8 \mid f(4) = 4\}.$$

- (a) Si verifichi che H è un sottogruppo di S_8 .
- (b) Il sottogruppo H è un sottogruppo normale di S_8 ?

22.16. Siano $n \geq 2$ un numero intero, S_n il gruppo delle permutazioni dell'insieme $X_n = \{1, 2, 3, \dots, n\}$, e $G = \{f \mid f \in S_n, f(\{1, 2\}) \subseteq \{1, 2\}\}$.

- (a) Si dimostri che G è un sottogruppo di S_n .
- (b) Si calcoli l'ordine di G .
- (c) Se H è un sottogruppo di G di ordine 2, si calcoli l'indice $[G : H]$.

22.17. 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:

- (a) H è un sottogruppo di G ;
- (b) se H_n è un sottogruppo normale di G per ogni $n \in \mathbb{N}$, allora H è un sottogruppo normale di G .

22.18. 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

$$(\alpha, x)(\beta, y) = (\alpha\beta, x\beta + y) \quad \text{per ogni } (\alpha, x), (\beta, y) \in \mathbb{Q}^* \times \mathbb{Q}.$$

- (a) Si provi che G è un gruppo.
- (b) Il gruppo G è abeliano?

- (c) 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 $(\mathbb{Q}, +)$?
 (d) Il sottoinsieme $H = \mathbb{Q}^* \times \{0\}$ di G è un sottogruppo normale di G ?

22.19. Sia G un gruppo. Per ogni $x \in G$ si ponga

$$C(x) = \{g \mid g \in G, gx = xg\}.$$

- (a) Si dimostri che $C(x)$ è un sottogruppo di G per ogni $x \in G$.
 (b) 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 .
 (c) Per ogni elemento $x \in G$ si denoti con $[x]_\sim$ la classe di equivalenza di x . Sia $\mathcal{D}_x = \{C(x)g \mid g \in G\}$ l'insieme di tutte le classi laterali destre di G modulo $C(x)$, e si definisca $\varphi: \mathcal{D}_x \rightarrow [x]_\sim$ ponendo $\varphi(C(x)g) = g^{-1}xg$ per ogni $g \in G$. Si provi che l'applicazione φ è ben definita.
 (d) Si dimostri che φ è una biiezione.

- (e) 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.]

22.20. Si consideri il gruppo abeliano additivo \mathbb{Z} .

- (a) Se \sim è una relazione di equivalenza su \mathbb{Z} compatibile con l'operazione $+$, allora per la proposizione 20.1 la relazione \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 .
 (b) Se N è un sottogruppo di \mathbb{Z} , allora come si è visto nell'esempio 19.11 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?

22.21. Si dimostri che se G è un gruppo ed N è un sottogruppo normale di G , allora $|G/N| = [G : N]$.

22.22. Si consideri il gruppo $(\mathbb{Q}/\mathbb{Z}, +)$.

- (a) Si dimostri che per ogni elemento $x \in \mathbb{Q}/\mathbb{Z}$ esiste $t \in \mathbb{N}^*$ tale che $tx = 0$.
 (b) Siano a, b due numeri interi non nulli primi tra loro. Se x è l'elemento $a/b + \mathbb{Z}$ di \mathbb{Q}/\mathbb{Z} , si calcoli il più piccolo numero naturale $t \in \mathbb{N}^*$ tale che $tx = 0$.

§23. Omomorfismi di gruppi

Sia $f: G \rightarrow G'$ un omomorfismo di gruppi. Il nucleo di f è l'insieme $f^{-1}(1_{G'}) = \{g \mid g \in G, f(g) = 1_{G'}\}$. Lo si indica con $\ker f$.

23.1 LEMMA. Il nucleo $\ker f$ di un omomorfismo di gruppi $f: G \rightarrow G'$ è un sottogruppo normale di G .

Dimostrazione. Per il lemma 19.15 si ha $f(1) = 1$, cioè $1 \in \ker f$, e quindi $\ker f \neq \emptyset$. Inoltre se $a, b \in \ker f$, allora $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = 1 \cdot 1 = 1$, e quindi $ab^{-1} \in \ker f$. Per il lemma 19.12, $\ker f \leq G$. Infine se $g \in G$ e $a \in \ker f$, allora

$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g) \cdot 1 \cdot f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$, e quindi $gag^{-1} \in \ker f$. Dal lemma 22.7 si conclude che $\ker f \trianglelefteq G$. \square

23.2 ESEMPIO. Consideriamo l'applicazione $\mu: \mathbb{C}^* \rightarrow \mathbb{R}^*$ definita da $\mu(z) = |z|$ per ogni $z \in \mathbb{C}^*$. L'applicazione μ è un omomorfismo del gruppo (\mathbb{C}^*, \cdot) nel gruppo (\mathbb{R}^*, \cdot) , perché per ogni $z, z' \in \mathbb{C}^*$ si ha $\mu(zz') = |zz'| = |z||z'| = \mu(z)\mu(z')$. Il nucleo di μ è

$$\ker \mu = \{z \mid z \in \mathbb{C}^*, \mu(z) = 1\} = \{z \mid z \in \mathbb{C}^*, |z| = 1\} = \mathbb{T},$$

il sottogruppo di \mathbb{C}^* che avevamo già incontrato nell'esempio 19.13. \square

23.3 ESEMPIO. Siano G un gruppo, N un sottogruppo normale di G e $\pi: G \rightarrow G/N$ la proiezione canonica di G nel gruppo quoziante G/N . Abbiamo già osservato che π è un omomorfismo di gruppi. Calcoliamone il nucleo. Si ha

$$\ker \pi = \{g \mid g \in G, \pi(g) = 1_{G/N}\} = \{g \mid g \in G, gN = N\} = \{g \mid g \in G, g \in N\}$$

(si veda l'osservazione dopo l'esempio 22.2). Quindi $\ker \pi = N$. \square

23.4 LEMMA. *Sia $f: G \rightarrow G'$ un omomorfismo di gruppi. Allora f è iniettivo se e solo se $\ker f = \{1_G\}$.*

Dimostrazione. Se f è iniettivo, $\ker f = f^{-1}(1)$ può contenere al più un elemento di G ; dato che $\ker f \supseteq \{1_G\}$ deve quindi essere $\ker f = \{1_G\}$. Viceversa sia $\ker f = \{1_G\}$ e siano $a, b \in G$ tali che $f(a) = f(b)$. Allora $f(ab^{-1}) = f(a)f(b)^{-1} = 1$, e quindi $ab^{-1} \in \ker f = \{1_G\}$. Ne segue che $ab^{-1} = 1_G$, cioè $a = b$. Se ne conclude che f è iniettiva. \square

23.5 PROPOSIZIONE. *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) Dato che $H \neq \emptyset$ si ha $f(H) \neq \emptyset$. Inoltre se $a, b \in f(H)$, allora $a = f(x)$ e $b = f(y)$ per opportuni $x, y \in H$. Quindi $xy^{-1} \in H$ e $ab^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$. Per il lemma 19.12 l'insieme $f(H)$ è un sottogruppo di G' .

(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 19.12 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 nel §48. \square

23.6 TEOREMA FONDAMENTALE DI OMOMORFISMO PER I GRUPPI. Siano G , G' gruppi ed $f: G \rightarrow G'$ un omomorfismo di gruppi. Allora $G/\ker f$ ed $f(G)$ sono gruppi isomorfi.

Prima dimostrazione. Questa dimostrazione è del tutto analoga a quella data per i semigruppi e i monoidi per dimostrare il teorema 17.3.

Definiamo un'applicazione $g: G/\ker f \rightarrow f(G)$ ponendo $g(x\ker f) = f(x)$ per ogni $x \in G$. Dobbiamo dimostrare che g è ben definita, cioè se per qualche $x, y \in G$ si ha $x\ker f = y\ker f$, allora $f(x) = f(y)$. Ora se $x, y \in G$ e $x\ker f = y\ker f$, allora $x^{-1}y \in \ker f$ (esempio 22.2). Quindi $f(x^{-1}y) = 1$. Ma allora $f(x) = f(x) \cdot 1 = f(x)f(x^{-1}y) = f(xx^{-1}y) = f(y)$. Questo prova che l'applicazione g è ben definita. È un omomorfismo di gruppi, perché per ogni $x, y \in G$ si ha $g(x\ker f)g(y\ker f) = f(x)f(y) = f(xy) = g(xy\ker f) = g((x\ker f)(y\ker f))$. È iniettiva perché $\ker g = \{x\ker f \mid x \in G, g(x\ker f) = 1_{G'}\} = \{x\ker f \mid x \in G, f(x) = 1_{G'}\} = \{x\ker f \mid x \in \ker f\} = \{\ker f\} = \{1_{G/\ker f}\}$ (lemma 23.4). Infine $g: G/\ker f \rightarrow f(G)$ è suriettiva, perché un generico elemento di $f(G)$ è del tipo $f(x)$ per qualche $x \in G$, e si ha $g(x\ker f) = f(x)$. Pertanto g è un isomorfismo, e $G/\ker f \cong f(G)$. \square

Seconda dimostrazione. L'omomorfismo di gruppi $f: G \rightarrow G'$ è un omomorfismo di semigruppi, e quindi si può applicare ad esso il teorema 17.3. Quindi G/\sim_f ed $f(G)$ sono semigruppi isomorfi, dove con \sim_f si è indicata l'equivalenza su G definita da $a \sim_f b$ se $f(a) = f(b)$, $a, b \in G$. Gli elementi di $G/\ker f$ sono le classi laterali $a\ker f$, $a \in G$, e gli elementi di G/\sim_f sono le classi di equivalenza $[a]_{\sim_f} = \{x \in G \mid x \sim_f a\} = \{x \in G \mid f(x) = f(a)\} = \{x \in G \mid f(a^{-1}x) = 1\} = \{x \in G \mid a^{-1}x \in \ker f\} = \{x \in G \mid x \in a\ker f\} = a\ker f$, $a \in G$, e in entrambi i casi le operazioni sono quelle indotte dall'operazione di G . Quindi $G/\ker f$ coincide con G/\sim_f e pertanto $G/\ker f$ e $f(G)$ sono isomorfi come semigruppi. Ma ogni isomorfismo di semigruppi tra due gruppi è un isomorfismo di gruppi. Se ne conclude che $G/\ker f$ e $f(G)$ sono isomorfi come gruppi. \square

23.7 ESEMPIO. Consideriamo l'omomorfismo $\text{sgn}: S_n \rightarrow \{1, -1\}$. Il nucleo di 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 sgn , il sottogruppo A_n è normale in S_n per il lemma 23.1. Inoltre osservato che per $n \geq 2$ l'omomorfismo sgn è suriettivo, ossia $\text{sgn}(S_n) = \{1, -1\}$, dal teorema 23.6 si deduce che i gruppi S_n/A_n e $\{1, -1\}$ sono isomorfi per ogni $n \geq 2$. \square

23.8 TEOREMA DI CORRISPONDENZA PER I GRUPPI. Siano G e G' gruppi ed $f: G \rightarrow G'$ un omomorfismo. Siano

$$\mathcal{L} = \{H \mid H \leq G, H \supseteq \ker f\}$$

l'insieme dei sottogruppi di G che contengono il nucleo di f e

$$\mathcal{L}' = \{H' \mid H' \leq f(G)\}$$

l'insieme dei sottogruppi di G' contenuti nell'immagine di f . Allora c'è una biiezione $\Phi: \mathcal{L} \rightarrow \mathcal{L}'$ definita da $\Phi(H) = f(H)$ per ogni $H \in \mathcal{L}$, la cui inversa è la biiezione $\Psi: \mathcal{L}' \rightarrow \mathcal{L}$ definita da $\Psi(H') = f^{-1}(H')$ per ogni $H' \in \mathcal{L}'$. Inoltre:

- (a) se $H \leq G$ e $H \supseteq \ker f$, si ha $H \trianglelefteq G$ se e solo se $\Phi(H) \trianglelefteq f(G)$;
- (b) se $H' \leq f(G)$, si ha $H' \trianglelefteq f(G)$ se e solo se $\Psi(H') \trianglelefteq G$.

Dimostrazione. Si osservi che se $H \in \mathcal{L}$ allora $f(H) \in \mathcal{L}'$ perché $f(H) \leq f(G)$, e che se $H' \in \mathcal{L}'$ allora $f^{-1}(H') \in \mathcal{L}$ perché $f^{-1}(H') \leq G$ e $f^{-1}(H') \supseteq f^{-1}(\{1\}) = \ker f$.

Per mostrare che Φ e Ψ sono due biiezioni l'una inversa dell'altra è sufficiente dimostrare che $\Psi \circ \Phi = \iota_{\mathcal{L}}$ e $\Phi \circ \Psi = \iota_{\mathcal{L}'}$, ossia che $f^{-1}(f(H)) = H$ per ogni $H \in \mathcal{L}$ e $f(f^{-1}(H')) = H'$ per ogni $H' \in \mathcal{L}'$. Questo segue dalla proposizione 23.5, in quanto se $H \in \mathcal{L}$ si ha $f^{-1}(f(H)) = H \cdot \ker f = H$ perché $H \supseteq \ker f$, e se $H' \in \mathcal{L}'$ allora $f(f^{-1}(H')) = H' \cap f(G) = H'$ perché $H' \leq f(G)$.

La dimostrazione delle asserzioni sui sottogruppi normali è lasciata per esercizio al lettore. \square

23.9 ESEMPIO. Torniamo all'omomorfismo $\text{sgn}: S_n \rightarrow \{1, -1\}$ dell'esempio 23.7, e applichiamo ad esso il teorema di corrispondenza. Supponiamo $n \geq 2$. In questo caso si ha che $\ker \text{sgn} = A_n$, $\mathcal{L} = \{H \mid H \leq G, H \supseteq A_n\}$, $\mathcal{L}' = \{H' \mid H' \leq \{1, -1\}\}$. I soli sottoinsiemi di $\{1, -1\}$ che contengono 1 sono $\{1\}$ e $\{1, -1\}$. Se ne deduce che $\{1, -1\}$ ha solamente i due sottogruppi $\{1\}$ e $\{1, -1\}$. In base al teorema di corrispondenza c'è una biiezione $\Psi: \mathcal{L}' \rightarrow \mathcal{L}$ data da $\Psi(H') = \text{sgn}^{-1}(H')$ per ogni $H' \in \mathcal{L}'$. In particolare \mathcal{L} ha esattamente due elementi, che sono $\Psi(\{1\}) = \text{sgn}^{-1}(\{1\}) = \ker \text{sgn} = A_n$ e $\Psi(\{1, -1\}) = \text{sgn}^{-1}(\{1, -1\}) = S_n$. Quindi A_n e S_n sono gli unici due sottogruppi di S_n che contengono A_n . \square

23.10 COROLLARIO. Siano G un gruppo ed N un sottogruppo normale di G . Allora:

- (a) i sottogruppi di G/N sono tutti e soli i gruppi H/N con H sottogruppo di G contenente N ;
- (b) i sottogruppi normali di G/N sono tutti e soli i gruppi H/N con H sottogruppo normale di G contenente N .

Dimostrazione. Applichiamo il teorema di corrispondenza 23.8 alla proiezione canonica $\pi: G \rightarrow G/N$. L'applicazione π è un omomorfismo suriettivo di gruppi e $\ker \pi = N$, e quindi se $\mathcal{L} = \{H \mid H \leq G, H \supseteq N\}$ e $\mathcal{L}' = \{H' \mid H' \leq G/N\}$, l'applicazione $\Phi: \mathcal{L} \rightarrow \mathcal{L}'$ definita da $\Phi(H) = \pi(H)$ per ogni $H \in \mathcal{L}$ è una biiezione. Pertanto i sottogruppi di G/N

sono tutti e soli i gruppi $\pi(H)$ con $H \leq G$ e $H \supseteq N$. Ma $\pi(H) = \{\pi(h) \mid h \in H\} = \{hN \mid h \in H\} = H/N$. Questo dimostra la parte (a).

Per la parte (b) si consideri un qualunque sottogruppo H di G contenente N (di modo che H/N è un generico sottogruppo di G/N). Per il teorema 23.8(a) si ha che $H \trianglelefteq G$ se e solo se $\Phi(H) \trianglelefteq \pi(G)$, cioè se e solo se $\pi(H) = H/N$ è normale in $\pi(G) = G/N$. Quindi i sottogruppi normali di G/N sono tutti e soli del tipo H/N con $H \trianglelefteq G$, $H \supseteq \ker f$. \square

23.11 ESEMPIO. Siano \mathbb{Z} il gruppo additivo degli interi ed $n \geq 1$ un intero. Cerchiamo i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.

In base al corollario 23.10 i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono esattamente i gruppi $H/n\mathbb{Z}$ dove H è un sottogruppo di \mathbb{Z} contenente $n\mathbb{Z}$. Ma abbiamo visto (esempio 19.11) che i sottogruppi H di \mathbb{Z} sono tutti del tipo $m\mathbb{Z}$ con $m \geq 0$ intero. Quindi i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono esattamente i gruppi $m\mathbb{Z}/n\mathbb{Z}$ dove $m \geq 0$ è un intero tale che $m\mathbb{Z} \supseteq n\mathbb{Z}$. Ora sappiamo anche (esercizio 19.9) che $m\mathbb{Z} \supseteq n\mathbb{Z}$ se e solo se $m \mid n$. Quindi i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono esattamente i gruppi $m\mathbb{Z}/n\mathbb{Z}$ con m divisore intero positivo di n .

Ad esempio i sottogruppi di $\mathbb{Z}/12\mathbb{Z}$ sono i sei gruppi seguenti: $1\mathbb{Z}/12\mathbb{Z}, 2\mathbb{Z}/12\mathbb{Z}, 3\mathbb{Z}/12\mathbb{Z}, 4\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}, 12\mathbb{Z}/12\mathbb{Z}$. Si noti anche che $1\mathbb{Z} = \mathbb{Z}$, e quindi $1\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$ è il sottogruppo improprio di $\mathbb{Z}/12\mathbb{Z}$. Inoltre $12\mathbb{Z}/12\mathbb{Z} = \{x + 12\mathbb{Z} \mid x \in 12\mathbb{Z}\} = \{12\mathbb{Z}\} = \{0_{\mathbb{Z}/12\mathbb{Z}}\}$ è il sottogruppo banale di $\mathbb{Z}/12\mathbb{Z}$. \square

Esercizi svolti

23.1 (PROPRIETÀ UNIVERSALE DEL GRUPPO ADDITIVO \mathbb{Z}). Sia \mathbb{Z} il gruppo additivo dei numeri interi. Per ogni gruppo (G, \cdot) e ogni elemento $g \in G$ esiste un unico omomorfismo di gruppi $\varphi_g : \mathbb{Z} \rightarrow G$ tale che $\varphi_g(1) = g$.

Soluzione. Esistenza. Mostriamo che un omomorfismo di gruppi $\varphi_g : \mathbb{Z} \rightarrow G$ tale che $\varphi_g(1) = g$ esiste. Poniamo $\varphi_g(z) = g^z$ per ogni $z \in \mathbb{Z}$ e verifichiamo che φ_g è un omomorfismo di gruppi. Se $z, z' \in \mathbb{Z}$, allora $\varphi_g(z+z') = g^{z+z'} = g^z g^{z'} = \varphi_g(z)\varphi_g(z')$. Quindi φ_g è un omomorfismo di gruppi. Inoltre si ha $\varphi_g(1) = g^1 = g$.

Unicità. Mostriamo che $\varphi_g : \mathbb{Z} \rightarrow G$ definito da $\varphi_g(z) = g^z$ per ogni $z \in \mathbb{Z}$ è l'*unico* omomorfismo di gruppi di \mathbb{Z} in G tale che $\varphi_g(1) = g$. Sia $\psi : \mathbb{Z} \rightarrow G$ un altro omomorfismo di gruppi tale che $\psi(1) = g$. Allora per ogni $z \in \mathbb{Z}$ si ha, in base al lemma 19.15(c),²

$$\psi(z) = \psi(z \cdot 1) = (\psi(1))^z = g^z = \varphi_g(z),$$

e quindi $\psi = \varphi_g$. Questo dimostra che φ_g è l'*unico* omomorfismo di gruppi con le proprietà richieste. \square

23.2. Sia G un gruppo.

- (a) Si dimostri che se G_λ è un sottogruppo di G per ogni $\lambda \in \Lambda$, allora $\bigcap_{\lambda \in \Lambda} G_\lambda$ è un sottogruppo di G .

²Il lemma 19.15(c) dice che un omomorfismo di gruppi $\varphi : G \rightarrow H$ manda la potenza n -esima di $g \in G$ nella potenza n -esima di $\varphi(g)$, cioè $\varphi(g^n) = (\varphi(g))^n$. Qui si è supposto ovviamente che la notazione dell'operazione sia di G che di H sia quella moltiplicativa. Se invece, come nel caso in questione, la notazione dell'operazione è quella additiva su G e quella moltiplicativa su H , un omomorfismo di gruppi $\varphi : G \rightarrow H$ manda il multiplo n -esimo di $g \in G$ nella potenza n -esima di $\varphi(g)$, cioè $\varphi(ng) = (\varphi(g))^n$.

Se X è un sottoinsieme di G , l'intersezione di tutti i sottogruppi di G che contengono X è un sottogruppo di G che è ovviamente il più piccolo sottogruppo di G che contiene X . Si chiama *sottogruppo di G generato da X* , e lo si denota con $\langle X \rangle$. Dato che $\{1_G\}$ è il più piccolo di tutti i sottogruppi di G , si ha quindi ad esempio che $\langle \emptyset \rangle = \{1_G\}$. Se $X = \{g\}$ ha un solo elemento si scrive $\langle g \rangle$ in luogo di $\{\langle g \rangle\}$ e tale sottogruppo di G è detto il *sottogruppo ciclico di G generato da g* . Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che $G = \langle g \rangle$.

(b) Se X è un sottoinsieme di un gruppo G si ponga

$$X^{-1} = \{x^{-1} \mid x \in X\}.$$

Sia $\langle X \rangle$ il sottogruppo di G generato da X , e $[X \cup X^{-1}]$ il sottomonoide 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 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_λ 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 19.12).

(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

$$\begin{aligned} [X \cup X^{-1}] &= \{1_G, x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X \cup X^{-1}\} \\ &= \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in X, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\}. \end{aligned}$$

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 ε_i, η_j sono 1 o -1 per tutti gli i e tutti gli 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 ε_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

$$\begin{aligned} \langle g \rangle &= \langle \{g\} \rangle = [\{g\} \cup \{g\}^{-1}] = [\{g, g^{-1}\}] \\ &= \{1_G, x_1 x_2 \dots x_n \mid n \in \mathbb{N}^*, x_1, x_2, \dots, x_n \in \{g, g^{-1}\}\} \\ &= \{1_G, g^{\varepsilon_1} g^{\varepsilon_2} \dots g^{\varepsilon_n} \mid n \in \mathbb{N}^*, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\} \\ &= \{1_G, g^{\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_n} \mid n \in \mathbb{N}^*, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{1, -1\}\} = \{g^z \mid z \in \mathbb{Z}\}. \quad \square \end{aligned}$$

23.3. Sia C_n il gruppo delle radici n -esime dell'unità, sottogruppo del gruppo moltiplicativo \mathbb{C}^* dei numeri complessi non nulli. Facendo uso dell'applicazione $\varphi_n: \mathbb{C}^* \rightarrow \mathbb{C}^*$ definita da $\varphi_n(x) = x^n$ per ogni $x \in \mathbb{C}^*$, e applicando ad essa il teorema fondamentale di omomorfismo per i gruppi, si dimostri che $\mathbb{C}^*/C_n \cong \mathbb{C}^*$ qualunque sia il numero naturale $n \geq 1$.

Soluzione. L'applicazione $\varphi_n: \mathbb{C}^* \rightarrow \mathbb{C}^*$ definita da $\varphi_n(x) = x^n$ per ogni $x \in \mathbb{C}^*$ è un endomorfismo del gruppo moltiplicativo \mathbb{C}^* , in quanto per ogni $x, y \in \mathbb{C}^*$ si ha $\varphi_n(xy) = (xy)^n = x^n y^n = \varphi_n(x)\varphi_n(y)$.

Mostriamo che φ_n è suriettiva. Sia $y \in \mathbb{C}^*$. 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 φ_n è suriettiva.

Applicando il teorema fondamentale di omomorfismo per i gruppi all'omomorfismo suriettivo $\varphi_n: \mathbb{C}^* \rightarrow \mathbb{C}^*$ si ottiene che $\mathbb{C}^*/\ker \varphi_n \cong \mathbb{C}^*$. Ma

$$\ker \varphi_n = \{x \in \mathbb{C}^* \mid \varphi_n(x) = 1\} = \{x \in \mathbb{C}^* \mid x^n = 1\} = C_n.$$

Quindi $\mathbb{C}^*/C_n = \mathbb{C}^*/\ker \varphi_n \cong \mathbb{C}^*$. \square

Altri esercizi

23.4. 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 ι_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 $G \times \{\iota_G\}$.

[*Suggerimento per (a): dimostrare che $1_L = (1_G, \iota_G)$ e che $(x, \varphi)^{-1} = ((\varphi^{-1}(x))^{-1}, \varphi^{-1})$.*]

23.5. Sia G un gruppo e per ogni $g \in G$ sia $\sigma_g: G \rightarrow G$ l'automorfismo interno indotto da g (esercizio 19.17). Sia $\text{Aut } G$ il gruppo degli automorfismi di G (esercizio 19.16). Si provi che $\sigma: G \rightarrow \text{Aut } G$ definito da $g \mapsto \sigma_g$ per ogni $g \in G$ è un omomorfismo di gruppi. Si provi che $Z(G) = \{g \mid g \in G, gx = xg \text{ per ogni } x \in G\}$ è il nucleo di σ . Quindi $Z(G)$, detto il *centro* di G , insieme di tutti gli elementi di G che commutano con ogni altro elemento di G , è un sottogruppo normale di G .

23.6 (TEOREMA DI CAYLEY PER I GRUPPI (vedi esercizio 16.21)). Ogni gruppo G è isomorfo ad un sottogruppo del gruppo simmetrico (S_G, \circ) (vedi esempio 19.8). In particolare ogni gruppo

finito di ordine n è isomorfo ad un sottogruppo di S_n . [Suggerimento: si ragioni sullo schema dell'esercizio 16.21, dimostrando che se $a \in G$, allora $f_a: G \rightarrow G$, $f_a(x) = ax$ per ogni $x \in G$, è una biiezione e quindi è un elemento di S_G .]

23.7. Sia $(\mathbb{Q}, +)$ il gruppo dei numeri razionali, \mathbb{Z} il sottogruppo dei numeri interi e \mathbb{Q}/\mathbb{Z} il gruppo quoziante. Si definisca $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ ponendo $\varphi(x) = 3x + \mathbb{Z}$ per ogni $x \in \mathbb{Q}$. Si dimostri che

- (a) l'applicazione φ è un omomorfismo di gruppi;
- (b) l'applicazione φ è suriettiva;
- (c) il nucleo di φ è un sottogruppo di \mathbb{Q} contenente \mathbb{Z} ;
- (d) il gruppo $\ker \varphi/\mathbb{Z}$ ha ordine 3.

23.8. Siano (\mathbb{R}^*, \cdot) il gruppo moltiplicativo dei numeri reali non nulli, H il suo sottogruppo $\{1/2^z \mid z \in \mathbb{Z}\}$ ed \mathbb{R}^*/H il gruppo quoziante. Si ponga $\varphi(xH) = x^2H$ per ogni $x \in \mathbb{R}^*$. Si dimostri che

- (a) l'applicazione $\varphi: \mathbb{R}^*/H \rightarrow \mathbb{R}^*/H$ è ben definita;
- (b) l'applicazione φ è un endomorfismo del gruppo \mathbb{R}^*/H ;
- (c) il nucleo di φ è un sottogruppo di \mathbb{R}^*/H di ordine 2.

23.9. 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 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 σ_g è un automorfismo di N .
- (d) Sia $\text{Aut}(N)$ il gruppo degli automorfismi di N con l'operazione di composizione di applicazioni \circ . 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 $\ker \varphi = C_G(N)$.

23.10. Siano G un gruppo e $\iota_G: G \rightarrow G$ l'applicazione identica di G . Qual è il nucleo di ι_G ? Si deduca dal teorema fondamentale di omomorfismo che $G/\{1_G\} \cong G$.

23.11. 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 \mathbb{Q}^* è il gruppo moltiplicativo dei numeri razionali non nulli si calcoli $t(\mathbb{Q}^*)$.
- (d) Se \mathbb{R} è il gruppo additivo dei numeri reali si calcoli $t(\mathbb{R})$.
- (e) Si dimostri che $\mathbb{Q}^*/t(\mathbb{Q}^*) \cong \mathbb{Q}^+$, ove \mathbb{Q}^+ è il gruppo moltiplicativo dei numeri razionali positivi. [Suggerimento: applicare il teorema fondamentale di omomorfismo per i gruppi all'omomorfismo $\varphi: \mathbb{Q}^* \rightarrow \mathbb{Q}^+$ definito da $\varphi(x) = |x|$ per ogni $x \in \mathbb{Q}^*$.]

23.12. 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 φ è un omomorfismo del gruppo $(\mathbb{Z}, +)$ nel gruppo (C_{12}, \cdot) .
- (b) Si calcoli il nucleo di φ .
- (c) Si dimostri che i gruppi C_{12} e $\mathbb{Z}/12\mathbb{Z}$ sono isomorfi.

23.13. 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 φ 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.

23.14. 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 $g \in G$.]

23.15. Siano S_n e A_n il gruppo simmetrico su n oggetti e il sottogruppo alterno rispettivamente.

- (a) Si calcoli l'ordine di A_n .
- (b) Si calcoli l'indice $[S_n : A_n]$.

[Suggerimento: distinguere i casi $n = 1$ e $n \geq 2$.]

23.16. Si dimostri che se G e H sono gruppi ed $f: G \rightarrow H$ è un omomorfismo di gruppi, allora $[G : \ker f] = |f(G)|$.

23.17. 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 $|H|$.

23.18. 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 $|G|$.

23.19. 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 $x \in G$.

23.20. 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 $|G|$.

23.21. 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 $|G|$.

23.22. 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 φ è un endomorfismo del gruppo $\mathbb{Z}^{\mathbb{N}}$.
- (d) Si dica se φ è un automorfismo di $\mathbb{Z}^{\mathbb{N}}$.

23.23. 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 $[G : H]$.

23.24 (PROPRIETÀ UNIVERSALE DEL SEMIGRUPPO $(\mathbb{N}^*, +)$). Sia \mathbb{N}^* il semigruppo additivo dei numeri naturali positivi. Per ogni semigruppo (S, \cdot) e ogni elemento $a \in S$ esiste un unico omomorfismo di semigruppi $\varphi_a: \mathbb{N}^* \rightarrow S$ tale che $\varphi_a(1) = a$. [Suggerimento: si ragioni come nell'esercizio 23.1.]

23.25 (PROPRIETÀ UNIVERSALE DEL MONOIDE $(\mathbb{N}, +)$). Sia \mathbb{N} il monoide additivo dei numeri naturali. Per ogni monoide (M, \cdot) e ogni elemento $a \in M$ esiste un unico omomorfismo di monoidi $\varphi_a: \mathbb{N} \rightarrow M$ tale che $\varphi_a(1) = a$. [Suggerimento: si ragioni come nell'esercizio 23.1.]

23.26. Si dimostri che ogni gruppo ciclico è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ per qualche $n \in \mathbb{N}$. [Suggerimento: per quanto riguarda la nozione di gruppo ciclico si veda l'esercizio 23.2. Per dimostrare che ogni gruppo ciclico è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ per qualche naturale n si ragioni come nella dimostrazione della proposizione 20.5 sostituendo il gruppo $(\mathbb{Z}, +)$ al monoide $(\mathbb{N}, +)$ e facendo uso dell'esercizio 23.1, del teorema fondamentale di omomorfismo per i gruppi e dell'esempio 19.11.]

23.27. Si provi che se G è un gruppo con p elementi, ove p è un numero primo, allora G è ciclico. [Suggerimento: sia $g \in G$, $g \neq 1_G$, e si consideri $\langle g \rangle \leq G$. Per il teorema di Lagrange 22.6 si ha $|\langle g \rangle| \mid p$. Quindi $|\langle g \rangle| = p$ oppure $|\langle g \rangle| = 1$. Dedurre che $\langle g \rangle = G$.]

23.28. Si provi che se G è un gruppo con n elementi, allora $g^n = 1_G$ per ogni $g \in G$. [Suggerimento: se $g \in G$, si consideri l'omomorfismo $\varphi_g: \mathbb{Z} \rightarrow G$ tale che $\varphi_g(1) = g$ (esercizio 23.1). Se $m\mathbb{Z} = \ker \varphi_g$, allora $\mathbb{Z}/m\mathbb{Z} \cong \varphi_g(\mathbb{Z})$ per il teorema fondamentale di omomorfismo per i gruppi.

Ma $\varphi_g(\mathbb{Z})$ è un sottogruppo di G , e quindi per il teorema di Lagrange 22.6 $|\varphi_g(\mathbb{Z})|$ divide $|G|$. Ora $|\varphi_g(\mathbb{Z})| = |\mathbb{Z}/m\mathbb{Z}| = m$ e $|G| = n$, e quindi m divide n , cioè $n = qm$ per qualche $q \in \mathbb{Z}$. Ma allora $n = qm \in \ker \varphi_g$, e quindi $g^n = (\varphi_g(1))^n = \varphi_g(n \cdot 1) = \varphi_g(n) = 1_G$.]

Capitolo 4

INSIEMI DOTATI DI PIÙ OPERAZIONI

§24. Anelli

Le strutture algebriche che abbiamo incontrato finora, semigruppi, monoidi e gruppi, erano insiemi dotati di un'unica operazione; in questo §24 iniziamo lo studio di strutture algebriche dotate di due (o più) operazioni. Un *anello* è un insieme R dotato di due operazioni $+$ e \cdot soddisfacenti alle seguenti condizioni:

- (a) $(R, +)$ è un gruppo abeliano;
- (b) (R, \cdot) è un semigruppo;
- (c) *distributività*: per ogni $a, b, c \in R$ si ha $a(b+c) = ab+ac$, $(b+c)a = ba+ca$.

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.

Un anello $(R, +, \cdot)$ si dice *commutativo* se $ab = ba$ per ogni $a, b \in R$, cioè se il semigruppo (R, \cdot) è commutativo. Si noti che il gruppo $(R, +)$ è sempre commutativo per definizione, qualunque sia l'anello R .

L'identità del gruppo additivo $(R, +)$ si indica, come al solito, con 0 o 0_R e si dice lo *zero* dell'anello.

Se il semigruppo (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 $e_R a = ae_R = a$ per ogni $a \in R$ (ossia che e_R sia l'identità del semigruppo 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 .

24.1 ESEMPIO. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, ove $+$ e \cdot sono le solite operazioni di addizione e moltiplicazione, sono anelli commutativi con identità. L'identità è il numero 1 . \square

24.2 ESEMPIO. Sia $\mathbb{Z} \times \mathbb{Z}$ il prodotto cartesiano di \mathbb{Z} per \mathbb{Z} ; definiamo in $\mathbb{Z} \times \mathbb{Z}$ 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 $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. È facile verificare che $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$ è un anello commutativo con identità. L'identità $1_{\mathbb{Z} \times \mathbb{Z}}$ è $(1, 0)$. Vediamo ad esempio la distributività. Per ogni $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}$ si ha

$$\begin{aligned}(a, b) \circ ((c, d) + (e, f)) &= (a, b) \circ (c + e, d + f) \\&= (a(c + e), a(d + f) + b(c + e)) \\&= (ac + ae, ad + af + bc + be)\end{aligned}$$

e

$$\begin{aligned}(a, b) \circ (c, d) + (a, b) \circ (e, f) &= (ac, ad + bc) + (ae, af + be) \\&= (ac + ae, ad + af + bc + be),\end{aligned}$$

da cui

$$(a, b) \circ ((c, d) + (e, f)) = (a, b) \circ (c, d) + (a, b) \circ (e, f). \quad \square$$

24.3 ESEMPIO. Come nell'esempio 24.2 sia $\mathbb{Z} \times \mathbb{Z}$ il prodotto cartesiano di \mathbb{Z} per \mathbb{Z} e definiamo in $\mathbb{Z} \times \mathbb{Z}$ 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 $(\mathbb{Z} \times \mathbb{Z}, +, *)$ è un anello, che però non è commutativo e non ha identità (in realtà $\mathbb{Z} \times \mathbb{Z}$ ha infinite identità destre $(1, d)$, $d \in \mathbb{Z}$, e non ha identità sinistre). Non è commutativo, in quanto $(1, 1) * (0, 1) = (0, 0)$, mentre $(0, 1) * (1, 1) = (0, 1)$. \square

24.4 LEMMA. Sia R un anello, e siano $a, b \in R$. Allora

$$0a = a0 = 0 \quad e \quad (-a)b = a(-b) = -(ab).$$

Dimostrazione. Si ha $0a = (0 + 0)a = 0a + 0a$, da cui, sommando $-0a$ ad entrambi i membri, si ricava $0 = 0a$; analogamente $0 = a0$.

Poi $ab + (-a)b = (a + (-a))b = 0b = 0$, e quindi $(-a)b$ è l'opposto di ab , ossia $(-a)b = -(ab)$. Analogamente $a(-b) = -(ab)$. \square

Scrivendo, come abbiamo fatto nell'enunciato del lemma 24.4, $(-a)b = -(ab)$, intendiamo naturalmente che l'opposto dell'elemento a moltiplicato per un elemento b è uguale all'opposto dell'elemento ab . Analogamente per $a(-b) = -(ab)$. Indicheremo l'elemento $(-a)b = a(-b) = -(ab)$ con il simbolo $-ab$.

Dato che ogni anello è un gruppo abeliano rispetto all'addizione ed è un semigruppo 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 . Ad esempio se a è un elemento dell'anello R ed n è un intero positivo, allora

$$na = \underbrace{a + a + \cdots + a}_{n \text{ volte}} \quad e \quad a^n = \underbrace{aa \cdots a}_{n \text{ volte}}.$$

24.5 ESEMPIO. Nell'anello $(\mathbb{Z} \times \mathbb{Z}, +, *)$ dell'esempio 24.3 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

$$(2, 1)^3 = (2, 1) * (2, 1) * (2, 1) = (4, 2) * (2, 1) = (8, 4). \quad \square$$

Se R è un anello, un *sottoanello* di R è un sottoinsieme S di R tale che $(S, +)$ sia sottogruppo di $(R, +)$ ed (S, \cdot) sia sottosemigruppo 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 , ossia se (R, \cdot) è un monoide, 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 $a, b \in S$.

24.6 ESEMPIO. Se si considerano gli anelli \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} dell'esempio 24.1, 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

24.7 ESEMPIO. Sia $R = \mathbb{Z} \times \mathbb{Z}$ l'anello dell'esempio 24.2. Abbiamo visto in quell'esempio 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) $1_R = (1, 0) \in S$;
- (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 $(x, 0) \circ (y, 0) = (xy, x \cdot 0 + 0 \cdot y) = (xy, 0) \in S$. \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 $b = 0$.

24.8 ESEMPIO. Gli anelli \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} dell'esempio 24.1 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

24.9 ESEMPIO. Nell'anello commutativo con identità $\mathbb{Z} \times \mathbb{Z}$ dell'esempio 24.2 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 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 19.6, 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.)

24.10 LEMMA. Ogni campo è un dominio di integrità.

Dimostrazione. Sia R un campo. Se R non è un dominio di integrità, allora esistono $a, b \in R$ tali che $ab = 0$, $a \neq 0$, $b \neq 0$; ma a è invertibile in R , e quindi $b = 1b = a^{-1}ab = a^{-1}0 = 0$, assurdo. \square

24.11 ESEMPIO. 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 24.8 che \mathbb{Z} è un dominio di integrità. Quindi \mathbb{Z} è un dominio di integrità che non è un campo. \square

24.12 ESEMPIO. Gli anelli \mathbb{Q}, \mathbb{R} e \mathbb{C} sono campi. \square

Esercizi svolti

24.1. 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

$$(f + f')(x) = f(x) + f'(x), \quad (f \circ f')(x) = f(f'(x)) \text{ per ogni } x \in G.$$

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 della definizione di anello sono soddisfatte. Mostriamone tre, lasciando la verifica delle altre al lettore.

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 $f + g = g + f$.

Associatività della moltiplicazione: Abbiamo già visto nel §3 che la composizione di applicazioni \circ è sempre associativa. Questo ne è un caso particolare.

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

24.2. Si provi che se R è un anello e $a, b \in R$, allora $(-a)(-b) = ab$.

Soluzione. Applicando due volte il lemma 24.4 si ha $(-a)(-b) = -(a(-b)) = -(-(ab))$, e questo è uguale ad ab perché in un gruppo additivo si ha $-(-x) = x$ (lemma 19.3). \square

24.3. 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 τ_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 biettiva. 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

24.4. 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 $a \neq 0$ implicino $b = c$. 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 o $a = 0$ oppure $a \neq 0$. Se $a \neq 0$, per la proprietà di cancellazione da $ab = 0 = a \cdot 0$ si ricava $b = 0$. Quindi o $a = 0$ oppure $b = 0$. \square

Altri esercizi

24.5. Sia $(G, +)$ un gruppo abeliano. Si definisca una moltiplicazione in G ponendo $ab = 0$ per ogni $a, b \in G$. Si provi che $(G, +, \cdot)$ è un anello commutativo.

24.6. 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.

24.7. Sia X un insieme non vuoto e sia \mathbb{R} il campo dei numeri reali. Nell'insieme

$$\mathbb{R}^X = \{f \mid f: X \rightarrow \mathbb{R} \text{ è un'applicazione}\}$$

si definiscano l'addizione e la moltiplicazione ponendo per ogni $f, g \in \mathbb{R}^X$ 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 $(\mathbb{R}^X, +, \cdot)$ è un anello commutativo con identità. L'identità è l'applicazione $e: X \rightarrow \mathbb{R}$ definita da $e(x) = 1$ per ogni $x \in X$.

24.8. Sia $\mathbb{Z}^n = \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{Z}\}$ l'insieme di tutte le n -uple di numeri interi. In \mathbb{Z}^n si definiscano un'operazione di addizione ed un'operazione di moltiplicazione ponendo

$$(x_1, x_2, \dots, x_n) + (x'_1, x'_2, \dots, x'_n) = (x_1 + x'_1, x_2 + x'_2, \dots, x_n + x'_n)$$

$$(x_1, x_2, \dots, x_n)(x'_1, x'_2, \dots, x'_n) = (x_1 x'_1, x_2 x'_2, \dots, x_n x'_n).$$

Si dimostri che \mathbb{Z}^n con queste operazioni è un anello commutativo con identità.

24.9. Siano X un insieme non vuoto e $\mathcal{P}(X)$ l'insieme delle parti di X . Si provi che $(\mathcal{P}(X), \Delta, \cap)$ è un anello commutativo con identità. Qui Δ denota la differenza simmetrica.

24.10. Se R ed S sono anelli, definiamo nel prodotto cartesiano $R \times S$ le due operazioni di addizione e moltiplicazione per componenti:

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{e} \quad (a, b) \cdot (a', b') = (aa', bb')$$

per ogni $(a, b), (a', b') \in R \times S$. Si provi che

- (a) $R \times S$ è un anello;
- (b) se R ed S sono anelli commutativi, allora $R \times S$ è un anello commutativo;
- (c) se R ed S sono anelli con identità, allora $R \times S$ è un anello con identità.

L'anello $R \times S$ si dice il *prodotto diretto* degli anelli R ed S .

24.11. Sia $R = \{a\}$ un insieme con un solo elemento. Si definisca $a + a = a$, $a \cdot a = a$. Allora R è anello commutativo (privo di identità, perché l'identità del monoide (R, \cdot) è uguale a 0), detto l'anello *banale*.

24.12. Sia R un anello. Se il monoide (R, \cdot) ha un'identità e_R ed $e_R = 0_R$, allora $R = \{e_R\}$ (cioè R è un anello banale).

24.13. Sia $(\mathbb{Z} \times \mathbb{Z}, +, *)$ l'anello dell'esempio 24.3 e sia $S = \{(z, 0) \mid z \in \mathbb{Z}\}$. Si provi che S è un sottoanello di $\mathbb{Z} \times \mathbb{Z}$.

24.14. Sia m un intero positivo. Si provi che $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ è sottoanello di \mathbb{R} .

24.15. 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.

24.16. 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.

24.17. 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.

24.18. 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 $(\mathbb{Q}, +, *)$.]

- 24.19. 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 24.2.
- 24.20. Sia R un anello e sia R_λ un sottoanello di R per ogni $\lambda \in \Lambda$. Si dimostri che $\bigcap_{\lambda \in \Lambda} R_\lambda$ è un sottoanello di R .
- 24.21. Calcolare $U(R)$ dove R è l'anello dell'esempio 24.2.

- 24.22. Sia $(\mathbb{R}, +, \cdot)$ l'anello dei numeri reali. Nell'insieme \mathbb{R} si definiscano due operazioni \oplus e \otimes ponendo $x \oplus y = x + y - 2$, $x \otimes y = xy - 2x - 2y + 6$ per ogni $x, y \in \mathbb{R}$. Allora $(\mathbb{R}, \oplus, \otimes)$ è un anello commutativo con identità.
- Si dica qual è lo zero dell'anello $(\mathbb{R}, \oplus, \otimes)$ (cioè l'elemento neutro per l'operazione \oplus).
 - Si dica qual è l'identità dell'anello $(\mathbb{R}, \oplus, \otimes)$.
 - Si dica se $(\mathbb{R}, \oplus, \otimes)$ è un campo.

- 24.23. Si provi per induzione su $n \geq 0$ che se $a, b \in R$ ed R è un anello commutativo, allora $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.

- 24.24. Se $a, b \in R$ ed $n \in \mathbb{Z}$ si faccia attenzione a non confondere il multiplo na (i multipli sono definiti in ogni gruppo additivo) con il prodotto ab (che è definito perché R è un anello). Se R è l'anello dell'esempio 24.2, cosa sono $3(1, 2)$, $(3, 0) \circ (1, 2)$, $(0, 3) \circ (1, 2)$?

§25. Ideali

Vogliamo studiare ora le relazioni di equivalenza su un anello R che sono compatibili con entrambe le operazioni di R , cioè le relazioni di equivalenza \sim nell'insieme R tali che se $a \sim b$ e $c \sim d$ allora $a+c \sim b+d$ e $ac \sim bd$. Ricordiamo che l'analogo problema per i gruppi (studiare le relazioni di equivalenza nel gruppo G che sono compatibili con l'operazione di gruppo) aveva portato allo studio dei sottogruppi normali, in quanto le relazioni d'equivalenza \sim su G compatibili con l'operazione di G sono tutte e sole le equivalenze \sim_N , ove N è sottogruppo normale di G e \sim_N è l'equivalenza su G definita da $a \sim_N b$ se e solo se $a^{-1}b \in N$, $a, b \in G$ (teorema 22.8 ed esercizio 22.12).

Il concetto corrispondente per gli anelli è quello di ideale. Sia R un anello. Un *ideale* I di R è un sottoinsieme non vuoto $I \subseteq R$ tale che:

- $x - y \in I$ per ogni $x, y \in I$;
- $rx \in I$ e $xr \in I$ per ogni $r \in R$ e ogni $x \in I$.

La notazione per “ I è ideale di R ” è $I \trianglelefteq R$. Si noti che per la condizione (a) ogni ideale di R è in particolare un sottogruppo del gruppo additivo $(R, +)$.

25.1 ESEMPIO. 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 19.11 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,

- (2) la condizione (a) della definizione di ideale è soddisfatta perché $n\mathbb{Z}$ è un sottogruppo del gruppo $(\mathbb{Z}, +)$, e
 (3) 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

25.2 ESEMPIO. Ogni anello R ha almeno due ideali, che sono R stesso (detto l'ideale *improprio*) e $\{0\}$ (detto l'ideale *nullo*). Tutti gli ideali di un anello R che sono diversi da R si chiamano ideali *propri*. \square

25.3 ESEMPIO. 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

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \dots + b_nx^n) \\ = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n \end{aligned}$$

e

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) \\ = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots + (a_nb_m)x^{n+m}. \end{aligned}$$

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

$$I_t = \{a_{t+1}x^{t+1} + a_{t+2}x^{t+2} + \cdots + a_nx^n \mid n \in \mathbb{N}, n > t\},$$

$$a_i \in R \text{ per ogni } i = t+1, t+2, \dots, n\},$$

cioè I_t è l'insieme di tutti i polinomi $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ con $a_0 = a_1 = \cdots = a_t = 0$, allora I_t è un ideale di $R[x]$. Questo può essere verificato facilmente o in modo diretto oppure osservando che $I_t = \{x^{t+1}f \mid f \in R[x]\}$. \square

25.4 TEOREMA. *Sia R 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 $x, y \in R$ da $x \sim_I y$ se $x - y \in I$, allora \sim_I è una relazione di equivalenza su R compatibile con entrambe le operazioni $+ e \cdot$, e $[0_R]_{\sim_I} = I$.*

Dimostrazione. Sia \sim un'equivalenza su R compatibile con $+ e \cdot$, e dimostriamo che $[0_R]_\sim$ è ideale. Si ha $[0_R]_\sim \neq \emptyset$ perché $0_R \in [0_R]_\sim$. Se $x, y \in [0_R]_\sim$, allora $x \sim 0_R$ e $y \sim 0_R$, da cui $0_R \sim y$ e quindi $x + 0_R \sim 0_R + y$, cioè $x \sim y$; per la proprietà riflessiva si ha $-y \sim -y$, e pertanto $x - y \sim y - y = 0_R$, cioè $x - y \in [0_R]_\sim$. Infine se $r \in R$ e $x \in [0_R]_\sim$, allora $r \sim r$ e $x \sim 0_R$, da cui $rx \sim r0_R = 0_R$, vale a dire $rx \in [0_R]_\sim$. Similmente $xr \in [0_R]_\sim$. Ciò prova che $[0_R]_\sim$ è ideale di R .

Viceversa sia I ideale di R , e definiamo $x \sim_I y$ se $x - y \in I$. Dimostriamo solo che \sim_I è compatibile con la moltiplicazione, lasciando tutte le altre verifiche per esercizio al lettore. Si deve far vedere che se $a, b, c, d \in R$, $a \sim_I b$ e $c \sim_I d$, allora $ac \sim_I bd$. Se $a \sim_I b$ e $c \sim_I d$, allora $a - b \in I$ e $c - d \in I$, da cui $(a - b)c \in I$ e $b(c - d) \in I$, e quindi $ac - bd = (a - b)c + b(c - d) \in I$, vale a dire $ac \sim_I bd$. \square

Si noti che se $r \in R$ e $I \trianglelefteq R$, la classe di equivalenza di r rispetto all'equivalenza \sim_I è $[r]_{\sim_I} = \{x \in R \mid x \sim_I r\} = \{x \in R \mid x - r \in I\} = \{x \in R \mid x \in r + I\} = r + I$, ove $r + I = \{r + i \mid i \in I\}$ è la classe laterale di r modulo 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

$$(r + I) + (r' + I) = (r + r') + I$$

e

$$(r + I) \cdot (r' + I) = rr' + I$$

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'anelli* $\varphi: R \rightarrow S$ 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'anelli $\varphi: R \rightarrow S$ 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'anelli 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 $R \cong S$.

25.5 ESEMPIO. Dato un anello R commutativo e con identità, consideriamo l'applicazione $\varphi: R[x] \rightarrow R$ definita da

$$\varphi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0$$

per ogni $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$. Allora φ è un omomorfismo di anelli con identità in quanto si ha

$$\begin{aligned} & \varphi((a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \cdots + b_nx^n)) \\ &= \varphi((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n) \\ &= a_0 + b_0 \\ &= \varphi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + \varphi(b_0 + b_1x + b_2x^2 + \cdots + b_nx^n), \\ & \varphi((a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)) \\ &= \varphi((a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + (a_nb_m)x^{n+m}) \\ &= a_0b_0 \\ &= \varphi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)\varphi(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m) \end{aligned}$$

e

$$\varphi(1) = 1. \quad \square$$

25.6 ESEMPIO. 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 $\varphi: R \rightarrow S$ è un omomorfismo d'anelli, il *nucleo* di φ è

$$\ker \varphi = \{r \mid r \in R, \varphi(r) = 0_S\}.$$

Si osservi che ogni omomorfismo di anelli è in particolare un omomorfismo di gruppi additivi; quindi un omomorfismo d'anelli $\varphi: R \rightarrow S$ è iniettivo se e solo se è un omomorfismo iniettivo di gruppi additivi, cioè se e solo se $\ker \varphi = \{0\}$.

25.7 ESEMPIO. Sia X un insieme non vuoto. Fissiamo $x_0 \in X$. Se \mathbb{R}^X è l'anello dell'esercizio 24.7, l'applicazione $\varphi: \mathbb{R}^X \rightarrow \mathbb{R}$ definita da $\varphi(f) = f(x_0)$ per ogni $f \in \mathbb{R}^X$ è un omomorfismo d'anelli; il suo nucleo è $\ker \varphi = \{f \in \mathbb{R}^X \mid f(x_0) = 0\}$. \square

25.8 ESEMPIO. Se $\varepsilon: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ è l'applicazione di \mathbb{Z} in $\mathbb{Z} \times \mathbb{Z}$ definita da $\varepsilon(x) = (x, 0)$ per ogni $x \in \mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ è l'anello dell'esempio 24.2, ε è un omomorfismo iniettivo di anelli. \square

25.9 ESEMPIO. Se $\pi_1: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ è la proiezione sul primo fattore, definita da $\pi_1(x, y) = x$ per ogni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, e $\mathbb{Z} \times \mathbb{Z}$ è l'anello dell'esempio 24.2, allora π_1 è un omomorfismo suriettivo di anelli. \square

25.10 ESEMPIO. Se R è un anello, I un ideale di R , R/I l'anello quoziante e $\pi: R \rightarrow R/I$ è la *proiezione canonica*, definita da $\pi(r) = r + I$ per ogni $r \in R$, allora π è un omomorfismo di anelli. \square

25.11 LEMMA. *Se $\varphi: R \rightarrow S$ è un omomorfismo di anelli, il nucleo di φ è un ideale di R .*

Dimostrazione. Si ha che $\ker \varphi \neq \emptyset$, perché $0 \in \ker \varphi$; se $x, y \in \ker \varphi$, allora $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$, e quindi $x - y \in \ker \varphi$; se $r \in R$ e $x \in \ker \varphi$, allora $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0$, e quindi $rx \in \ker \varphi$; analogamente $xr \in \ker \varphi$. \square

Si noti la somiglianza tra il ruolo dei sottogruppi normali in un gruppo e il ruolo degli ideali in un anello. Per un gruppo G si dimostrava che (1) i sottogruppi normali corrispondono alle relazioni di equivalenza compatibili (teorema 22.8), e quindi (2) si definiva il quoziante di G modulo un sottogruppo normale (proposizione 22.10); inoltre (3) i sottogruppi normali sono esattamente i nuclei degli omomorfismi (lemma 23.1). Per un anello R si è dimostrato in questo §25 che (1) gli ideali corrispondono alle relazioni di equivalenza compatibili, e quindi (2) si è definito il quoziante di R modulo un ideale; inoltre (3) gli ideali sono esattamente i nuclei degli omomorfismi di anelli.

Valgono anche per gli anelli il teorema fondamentale di omomorfismo e il teorema di corrispondenza. Ne omettiamo la dimostrazione.

25.12 TEOREMA FONDAMENTALE DI OMOMORFISMO PER GLI ANELLI. *Siano R, R' anelli e $\varphi: R \rightarrow R'$ un omomorfismo di anelli. Allora $\varphi(R)$ è un sottoanello di R' e gli anelli $R/\ker \varphi$ e $\varphi(R)$ sono isomorfi.*

25.13 TEOREMA DI CORRISPONDENZA PER GLI IDEALI. Siano R, R' anelli e $\varphi: R \rightarrow R'$ un omomorfismo di anelli. Siano poi $\mathcal{L} = \{I \mid I \trianglelefteq R, I \supseteq \ker \varphi\}$ l'insieme degli ideali di R che contengono il nucleo di φ ed $\mathcal{L}' = \{J \mid J \trianglelefteq \varphi(R)\}$ l'insieme degli ideali di $\varphi(R)$. Allora c'è una biiezione $\Phi: \mathcal{L} \rightarrow \mathcal{L}'$ definita da $\Phi(I) = \varphi(I)$ per ogni $I \in \mathcal{L}$, la cui inversa è la biiezione $\Psi: \mathcal{L}' \rightarrow \mathcal{L}$ definita da $\Psi(J) = \varphi^{-1}(J)$ per ogni $J \in \mathcal{L}'$.

25.14 ESEMPIO. 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 §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 §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 (δ_{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 φ è un omomorfismo iniettivo di anelli. \square

Esercizi svolti

25.1. 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 $\delta(fg) = \delta(f) + \delta(g)$.

In queste formule si adottano le ovvie convenzioni che $-\infty - \infty = -\infty$, $-\infty + n = -\infty$ e $-\infty < n$ per ogni $n \in \mathbb{N}$.

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 le formule dell'esercizio 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 $\delta(0) = 0$.

25.2. 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 25.1 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

25.3. 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 α . 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 φ_α è l'insieme I_α di tutti i polinomi a coefficienti razionali di cui α è una radice;
- l'insieme I_α è un ideale di $\mathbb{Q}[x]$.

Soluzione. (a) Si ha, per ogni $f, g \in \mathbb{Q}[x]$,

$$\begin{aligned}\varphi_\alpha(f+g) &= (f+g)(\alpha) = f(\alpha) + g(\alpha) = \varphi_\alpha(f) + \varphi_\alpha(g) \\ \varphi_\alpha(fg) &= (fg)(\alpha) = f(\alpha)g(\alpha) = \varphi_\alpha(f)\varphi_\alpha(g) \quad \text{e} \\ \varphi_\alpha(1) &= 1.\end{aligned}$$

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 α è radice.

(c) Segue da (b) e dal lemma 25.11. \square

Altri esercizi

25.4. Siano X un insieme non vuoto ed \mathbb{R}^X l'anello dell'esercizio 24.7.

- Si determinino i divisori dello zero nell'anello \mathbb{R}^X .
- Si determinino gli elementi invertibili nell'anello \mathbb{R}^X .

(c) Per ogni sottoinsieme Y di X sia

$$I_Y = \{f \in \mathbb{R}^X \mid f(y) = 0 \text{ per ogni } y \in Y\}.$$

Si dimostri che I_Y è un ideale di \mathbb{R}^X per ogni $Y \subseteq X$.

25.5. Per ogni anello R sia $Z(R) = \{z \in R \mid zr = rz \text{ per ogni } r \in R\}$.

- (a) Si dimostri che $Z(R)$ è un sottoanello di R e che $Z(R)$ è commutativo.
- (b) Si dimostri che se I è un ideale di R allora $I \cap Z(R)$ è un ideale di $Z(R)$.
- (c) Si dimostri che se J è un ideale di $Z(R)$ e

$$JR = \left\{ \sum_{t=1}^n j_t r_t \mid n \in \mathbb{N}^*, j_1, j_2, \dots, j_n \in J, r_1, r_2, \dots, r_n \in R \right\},$$

allora JR è un ideale di R .

25.6. Si provi che se I e J sono ideali di un anello R , allora $I + J = \{i + j \mid i \in I, j \in J\}$ e $I \cap J$ sono ideali di R .

25.7. 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 $I = R$.

25.8. Si provi che se R è anello commutativo con identità e $a \in R$, allora $Ra = \{ra \mid r \in R\}$ è ideale di R , e per ogni ideale I di R se $a \in I$ allora $Ra \subseteq I$. (L'ideale Ra si indica in genere con (a) e si chiama l'ideale *principale* generato da a .)

25.9. Sia $(R, +, \cdot)$ un anello commutativo con identità e sia a un elemento di R . Si ponga $I(a) = \{x \in R \mid xa = 0\}$.

- (a) Si dimostri che $I(a)$ è un ideale di R .
- (b) 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 $I(a)$.
- (c) 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 $a = (0, 2)$.

25.10. 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 .

25.11. 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 $\mathbb{Z}[x]$.

25.12. 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 $v: \mathbb{Z}[i] \rightarrow \mathbb{Z}$ definita da $v(a + ib) = a^2 + b^2$ per ogni $a, b \in \mathbb{Z}$.

- (a) Si dimostri che v è un omomorfismo del monoide $(\mathbb{Z}[i], \cdot)$ nel monoide (\mathbb{Z}, \cdot) .
- (b) Si deduca da (a) che se $z \in \mathbb{Z}[i]$ è un elemento invertibile dell'anello $\mathbb{Z}[i]$, allora $v(z) = 1$.

- (c) Si deduca da (b) che gli elementi invertibili dell'anello $\mathbb{Z}[i]$ sono tutti e soli gli elementi $1, -1, i, -i$.

25.13. Si provi che se f è un isomorfismo d'anelli, allora anche f^{-1} è un isomorfismo d'anelli.

25.14. Sia $\varphi: R \rightarrow S$ un omomorfismo di anelli. Si provi che

- (a) se R' è sottoanello di R , allora $\varphi(R')$ è sottoanello di S ;
- (b) se S' è sottoanello di S , allora $\varphi^{-1}(S')$ è sottoanello di R ;
- (c) se I è ideale di R , allora $\varphi(I)$ è ideale dell'anello $\varphi(R)$;
- (d) se J è ideale di S , allora $\varphi^{-1}(J)$ è ideale di R ;
- (e) se l'anello R ha identità 1_R , allora $\varphi(1_R)$, che è un sottoanello di S per (a), ha identità $\varphi(1_R)$.
- (f) se R ed S hanno entrambi l'identità, $\varphi(1_R) = 1_S$ ed x è invertibile in R , allora $\varphi(x)$ è invertibile in S e $[\varphi(x)]^{-1} = \varphi(x^{-1})$.

25.15. Sia R un anello e $\iota_R: R \rightarrow R$ l'applicazione identica di R . Qual è il nucleo di ι_R ? Si deduca dal teorema fondamentale di omomorfismo per gli anelli che $R/\{0_R\} \cong R$.

25.16. Facendo uso del teorema di corrispondenza per i gruppi e dell'esercizio 25.14 provare il teorema 25.13 (teorema di corrispondenza per gli ideali). [Suggerimento: restringere la biiezione data dal teorema di corrispondenza per i gruppi all'insieme degli ideali.]

§26. Polinomi

Sia R un anello commutativo con identità 1_R . Nell'esempio 25.3 abbiamo già introdotto l'anello $R[x]$ dei polinomi nell'indeterminata x a coefficienti in R . Nell'esercizio 25.1 abbiamo definito il *grado* $\delta(f)$ di un polinomio $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ e il *coefficiente direttivo* di f . Un polinomio il cui coefficiente direttivo è 1 è un *polinomio monico*; un polinomio del tipo a_nx^n è detto *monomio*.

26.1 TEOREMA (PROPRIETÀ UNIVERSALE DELL'ANELLO DEI POLINOMI). Siano R anello commutativo con identità, x indeterminata su R , $R[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in R . Se T è un anello commutativo, R è sottoanello di T e $t \in T$, esiste un unico omomorfismo $\varphi_t: R[x] \rightarrow T$ tale che $\varphi_t(x) = t$ e $\varphi_t(r) = r$ per ogni $r \in R$.

Dimostrazione. Esistenza: Mostriamo che un omomorfismo φ_t con le proprietà richieste esiste. Definiamo $\varphi_t(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) = a_0 + a_1t + a_2t^2 + \dots + a_nt^n$ per ogni $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$. Allora $\varphi_t(x) = t$, $\varphi_t(r) = r$ per ogni $r \in R$ e φ_t è un omomorfismo perché $\varphi_t[(a_0 + a_1x + \dots) + (b_0 + b_1x + \dots)] = \varphi_t[(a_0 + b_0) + (a_1 + b_1)x + \dots] = (a_0 + b_0) + (a_1 + b_1)t + \dots = (a_0 + a_1t + \dots) + (b_0 + b_1t + \dots) = \varphi_t(a_0 + a_1x + \dots) + \varphi_t(b_0 + b_1x + \dots)$ e similmente per la moltiplicazione.

Unicità: Mostriamo che φ_t così definito è l'unico omomorfismo con le proprietà richieste. Se anche $\psi: R[x] \rightarrow T$ è un omomorfismo tale che $\psi(x) = t$ e $\psi(r) = r$ per ogni $r \in R$,

allora per ogni $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ si ha

$$\begin{aligned}\psi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \\ &= \psi(a_0) + \psi(a_1x) + \psi(a_2x^2) + \cdots + \psi(a_nx^n) \\ &= \psi(a_0) + \psi(a_1)\psi(x) + \psi(a_2)(\psi(x))^2 + \cdots + \psi(a_n)(\psi(x))^n \\ &= a_0 + a_1t + a_2t^2 + \cdots + a_nt^n = \varphi_t(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n),\end{aligned}$$

cioè $\psi = \varphi_t$. \square

I polinomi si indicano in genere con simboli del tipo f, g o con $f(x), g(x)$. Ciò non vuol dire però che si tratti di funzioni (un polinomio per noi è solo un'espressione del tipo $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$), anche se alcuni vecchi testi chiamano la x *variabile*. Noi l'abbiamo chiamata *indeterminata*, ma ciò non vuol dire che sia un “elemento non determinato”: x è un ben determinato elemento di $R[x]$, è l'unico monomio monico di grado 1. Ecco la ragione di tali simboli e di tale nomenclatura: supponiamo di avere due polinomi $f, g \in R[x]$, e di sapere che $f = g$; allora per ogni anello commutativo $T \supseteq R$ e per ogni $t \in T$ si ha che $\varphi_t(f) = \varphi_t(g)$, ove φ_t è l'omomorfismo del teorema 26.1. Ora, come visto nella dimostrazione del teorema, $\varphi_t(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n$, ossia φ_t è l'applicazione che associa ad un polinomio l'elemento di T che si ottiene sostituendo t ad x ed eseguendo le operazioni. In genere si suole indicare $\varphi_t(f)$ con $f(t)$. Abbiamo così visto che se $f(x), g(x) \in R[x]$ e $f(x) = g(x)$, allora $f(t) = g(t)$ ogniqualvolta si sostituisce a x un elemento t appartenente ad un qualunque sopraanello di R . Questa è la ragione per cui la x viene chiamata indeterminata (o addirittura variabile) e i polinomi vengono denotati con lettere che ricordano le funzioni.

26.2 TEOREMA (DIVISIONE EUCLIDEA FRA POLINOMI). *Sia F un campo e $F[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in F . Siano $f, g \in F[x]$ con $g \neq 0$. Esiste allora una ed una sola coppia (q, r) di polinomi appartenenti ad $F[x]$ tali che*

- (a) $f = gq + r$, e
- (b) il grado di r è minore del grado di g .

Dimostrazione. Esistenza: Siano $\delta(f), \delta(g)$ i gradi dei polinomi f e g . Se $\delta(f) < \delta(g)$, allora non vi è nulla da dimostrare, perché $q = 0$ e $r = f$ soddisfano alla tesi del teorema.

Possiamo quindi supporre $\delta(f) \geq \delta(g)$ e ragionare per induzione sul numero naturale $n = \delta(f)$. Poniamo

$$\begin{aligned}m &= \delta(g), \\ f &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \\ g &= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0\end{aligned}$$

(e quindi $a_n \neq 0$ e $b_m \neq 0$, da cui $b_m^{-1} \in F$). Allora

$$f = a_n b_m^{-1} x^{n-m} g + (f - a_n b_m^{-1} x^{n-m} g);$$

ora

$$\begin{aligned} f - a_n b_m^{-1} x^{n-m} g &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) \\ &\quad - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}) \end{aligned}$$

è un polinomio di grado $< n = \delta(f)$. Per l'ipotesi induttiva si può quindi dividere $f - a_n b_m^{-1} x^{n-m} g$ per g , ottenendo $f - a_n b_m^{-1} x^{n-m} g = q_1 g + r_1$ per opportuni $q_1, r_1 \in F[x]$ tali che il grado di r_1 sia minore del grado di g . Allora $f = (a_n b_m^{-1} x^{n-m} + q_1)g + r_1$, vale a dire $q = a_n b_m^{-1} x^{n-m} + q_1$ e $r = r_1$ hanno le proprietà volute.

Unicità: Supponiamo che $f = qg + r$, $f = q'g + r'$, $\delta(r) < \delta(g)$, $\delta(r') < \delta(g)$. Allora $(q - q')g = r' - r$. Se $q \neq q'$, allora $\delta((q - q')g) \geq \delta(g)$; ma $\delta(r) < \delta(g)$ e $\delta(r') < \delta(g)$, e quindi $\delta(r' - r) < \delta(g)$, contraddizione perché $(q - q')g = r' - r$. Quindi $q = q'$, $0 = (q - q')g = r' - r$ e $r' = r$. \square

La dimostrazione del teorema 26.2 mostra come sia possibile calcolare effettivamente il quoto e il resto della divisione tra due polinomi. Ecco tre esempi da cui è possibile capire come si procede in pratica; nel primo si è diviso $4x^3 + 2x^2 + 3x + 7$ per $2x^2 + 5$ in $\mathbb{Q}[x]$ (quoto = $2x + 1$, resto = $-7x + 2$), nel secondo si è diviso $x^6 + 4x^5 - 12x + 1$ per $x^3 + 4x^2 + 1$ in $\mathbb{R}[x]$ (quoto = $x^3 - 1$, resto = $4x^2 - 12x + 2$), nel terzo si è diviso $2x^3 + x + 1$ per $4x + 1$ in $\mathbb{C}[x]$ (quoto = $\frac{1}{2}x^2 - \frac{1}{8}x + \frac{9}{32}$, resto = $\frac{23}{32}$).

$4x^3 + 2x^2 + 3x + 7$	$2x^2 + 5$	$x^6 + 4x^5$	$-12x + 1$	$x^3 + 4x^2 + 1$
$4x^3$	$+10x$	$2x + 1$	$x^6 + 4x^5$	$x^3 - 1$
$2x^2$	$-7x + 7$		$+x^3$	
$2x^2$	$+5$		$-x^3$	$-12x + 1$
$-7x + 2$			$-x^3 - 4x^2$	-1
			$4x^2 - 12x + 2$	

$2x^3$	$+ x + 1$	$4x + 1$
$2x^3 + \frac{1}{2}x^2$		$\frac{1}{2}x^2 - \frac{1}{8}x + \frac{9}{32}$
$-\frac{1}{2}x^2 + x + 1$		
$-\frac{1}{2}x^2 - \frac{1}{8}x$		
$\frac{9}{8}x + 1$		
$\frac{9}{8}x + \frac{9}{32}$		
$\frac{23}{32}$		

Esercizi svolti

26.1. Si provi che l'anello $R[x]$ non è mai un campo, qualunque sia l'anello commutativo con identità R .

Soluzione. Mostriamo che $R[x]$ non è un campo facendo vedere che il suo elemento x , che è $\neq 0$, non è mai invertibile. Se per assurdo x fosse invertibile, esisterebbe un elemento $f \in R[x]$

tal che $xf = 1$. Prendendo il grado dei due termini di questa uguaglianza si troverebbe che $0 = \delta(1) = \delta(xf) = \delta(x) + \delta(f) = 1 + \delta(f)$. Ma $\delta(f) \in \mathbb{N}$ o $\delta(f) = -\infty$, e non si ha né $0 = 1 + n$ per $n \in \mathbb{N}$ né $0 = 1 - \infty$. Questa contraddizione dimostra quanto asserito. \square

Altri esercizi

26.2. Si provi che in $R[x]$ un polinomio monico non è divisore dello zero.

26.3. Sia R un dominio di integrità, e sia $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$. Si provi che f è un elemento invertibile dell'anello $R[x]$ se e solo se a_0 è invertibile in R e $a_1 = a_2 = \dots = a_n = 0$.

26.4. Sia I l'insieme di tutti i polinomi di $R[x]$ del tipo $a_1x + a_2x^2 + \dots + a_nx^n$ ($n \geq 1, a_i \in R$), cioè i polinomi con "termine noto" nullo. Sappiamo che I è ideale di $R[x]$ (esempio 25.3). Si provi che $R[x]/I$ ed R sono anelli isomorfi.

26.5. Si divida $2x^3 + x + 1$ per $4x + 1$ in $\mathbb{R}[x]$; $x^6 - 1$ per $x - 1$ in $\mathbb{Q}[x]$; $x^4 + 2x^3 + 3x^2 + 1$ per $ix + 1$ in $\mathbb{C}[x]$; $x^5 + 2x^4 - x^3 - x^2$ per $x^2 - 1$ in $\mathbb{R}[x]$.

§27. L'anello delle classi resto e la caratteristica di un anello

Fissiamo un intero $n \geq 0$. Abbiamo già osservato nell'esempio 25.1 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 quoziante $\mathbb{Z}/n\mathbb{Z}$. 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'uguaglianza (esempio 8.2), 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 quoziati 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 spesso $\mathbb{Z}/n\mathbb{Z}$ con \mathbb{Z}_n e i suoi elementi $[a]_{\equiv_n} = a + n\mathbb{Z}$ con \bar{a} , sottointendendo il numero fissato n . Quindi $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$ è un anello con n elementi, e le operazioni di addizione e moltiplicazione in \mathbb{Z}_n sono definite da

$$\bar{a} + \bar{b} = \overline{a + b}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

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 $\bar{1}$. È detto l'anello delle classi resto modulo n .

27.1 PROPOSIZIONE.

- (a) Sia R un anello commutativo con identità e sia $a \in R$. Se a è invertibile, allora a non è divisore dello zero.
- (b) 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 (§24). In vista di (a) dobbiamo quindi dimostrare solamente che se R è un anello commutativo, finito e con identità ed $a \in R$ è $\neq 0$ e non è un divisore dello zero, allora a è invertibile. Consideriamo l'applicazione $\varphi: R \rightarrow R$ definita da $\varphi(r) = ar$ per ogni $r \in R$. Questa φ 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 divisore dello zero, non esiste nessun $b \in R$, $b \neq 0$, tale che $ab = 0$. Quindi $\ker \varphi = \{0\}$, e pertanto φ è iniettiva. Ma R è un insieme finito, e quindi φ è una biiezione. Esiste quindi in particolare un elemento $c \in R$ tale che $\varphi(c) = 1_R$. Ma allora $ac = 1_R$, e pertanto a è invertibile. \square

27.2 COROLLARIO. Se R è un anello commutativo con identità 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 24.10.

Viceversa se R è un dominio d'integrità, R non ha divisori dello zero. Per la proposizione 27.1 ogni elemento $a \neq 0$ di R è invertibile. Quindi R è un campo. \square

27.3 PROPOSIZIONE. 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} è 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 4.5 segue che a ed n sono primi tra loro.

Viceversa supponiamo che a ed n siano primi tra loro. Per il corollario 4.5 esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta n = 1$. Ma allora $\bar{1} = \overline{\alpha a + \beta n} = \bar{\alpha} \cdot \bar{a} + \bar{\beta} \cdot \bar{n} = \bar{\alpha} \cdot \bar{a} + \bar{\beta} \cdot \bar{0} = \bar{\alpha} \cdot \bar{a} + \bar{0} = \bar{\alpha} \cdot \bar{a}$, e quindi $\bar{a} \in \mathbb{Z}_n$ è l'inverso di \bar{a} . In particolare $\bar{a} \in \mathbb{Z}_n$ è invertibile. \square

Dalle proposizioni 27.1 e 27.3 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 $(a, n) \neq 1$.

27.4 COROLLARIO. 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 27.2. Inoltre \mathbb{Z}_n è un campo se e solo se i suoi elementi $\bar{1}, \bar{2}, \bar{3}, \dots, \bar{n-1}$ sono tutti invertibili, ossia, per la proposizione 27.3, 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

27.5 ESEMPIO. 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

27.6 ESEMPIO. 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

27.7 ESEMPIO. 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

27.8 ESEMPIO. 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

27.9 ESEMPIO. Nel teorema 26.2 si è visto che, se F è un campo, è sempre possibile dividere un polinomio $f \in F[x]$ per un polinomio $g \in F[x]$ non nullo. Vediamo come si divide $\bar{2}x^2 + \bar{3}x + \bar{4}$ per $\bar{3}x + \bar{4}$ nell'anello $\mathbb{Z}_7[x]$. (Si noti che $\mathbb{Z}_7[x]$ è un campo.) Un primo modo è quello di effettuare la divisione come se fosse in $\mathbb{Q}[x]$, ricordandosi solo di aggiungere la sbarretta:

$$\begin{array}{r|l} \bar{2}x^2 + \bar{3}x + \bar{4} & \bar{3}x + \bar{4} \\ \bar{2}x^2 + \frac{\bar{8}}{3}x & \bar{\frac{2}{3}}x + \bar{\frac{1}{9}} \\ \hline \bar{\frac{1}{3}}x + \bar{4} & \\ \bar{\frac{1}{3}}x + \bar{\frac{4}{9}} & \\ \hline \bar{\frac{32}{9}} & \end{array}$$

Quindi

$$\bar{2}x^2 + \bar{3}x + \bar{4} = (\bar{3}x + \bar{4}) \left(\frac{\bar{2}}{3}x + \frac{\bar{1}}{9} \right) + \frac{\bar{32}}{9}.$$

Ma cosa sono $\frac{\bar{2}}{3}, \frac{\bar{1}}{9}, \frac{\bar{32}}{9}$ in \mathbb{Z}_7 ? In \mathbb{Z}_7 si ha che $\bar{3} \cdot \bar{5} = \bar{15} = \bar{1}$, e quindi $\bar{\frac{1}{3}} = \bar{5}$, da cui $\bar{\frac{2}{3}} = \bar{10} = \bar{3}$. Similmente $\bar{\frac{1}{9}} = \bar{4}$ e $\bar{\frac{32}{9}} = \bar{2}$. Quindi $\bar{2}x^2 + \bar{3}x + \bar{4} = (\bar{3}x + \bar{4}) \cdot (\bar{3}x + \bar{4}) + \bar{2}$ in $\mathbb{Z}_7[x]$.

Un secondo modo di ottenere questo stesso risultato è quello di scrivere ad ogni passo della divisione il corrispondente valore in \mathbb{Z}_7 già nella forma \bar{a} con $a \in \mathbb{Z}$. Ad esempio il primo passo nella divisione è quello di dividere il monomio $\bar{2}x^2$ per il monomio $\bar{3}x$. Si trova $\bar{\frac{2}{3}}x$. Come abbiamo visto sopra, in \mathbb{Z}_7 si ha $\bar{\frac{2}{3}} = \bar{3}$. Quindi si può già scrivere direttamente al primo passo $\bar{3}x$ in luogo di $\bar{\frac{2}{3}}x$. Ecco tutti i calcoli svolti in questo secondo

modo:

$$\begin{array}{r|l} \overline{2}x^2 + \overline{3}x + \overline{4} & \overline{3}x + \overline{4} \\ \overline{9}x^2 + \overline{12}x & \hline \overline{3}x - \overline{3} \\ \hline -\overline{2}x + \overline{4} & \\ -\overline{9}x - \overline{12} & \\ \hline \overline{2} & \end{array}$$

Quindi $\overline{2}x^2 + \overline{3}x + \overline{4} = (\overline{3}x + \overline{4}) \cdot (\overline{3}x - \overline{3}) + \overline{2}$ in $\mathbb{Z}_7[x]$. Questo è lo stesso risultato di prima in quanto $-\overline{3} = \overline{4}$ in \mathbb{Z}_7 . \square

Vediamo un ulteriore corollario della proposizione 27.3.

27.10 COROLLARIO (TEOREMA CINESE DEL RESTO). *Siano m, n interi positivi primi tra loro, e siano $b, c \in \mathbb{Z}$. Allora il sistema di congruenze*

$$(27.1) \quad \begin{cases} x \equiv b \pmod{m} \\ x \equiv c \pmod{n} \end{cases}$$

ha una soluzione $x \in \mathbb{Z}$. Se $x_0 \in \mathbb{Z}$ è una tale soluzione, le soluzioni del sistema sono tutti e soli gli $x \in \mathbb{Z}$ tali che $x \equiv x_0 \pmod{mn}$.

Dimostrazione. Sia $x \in \mathbb{Z}$. Si ha $x \equiv b \pmod{m}$ se e solo se $x = b + tm$ per qualche $t \in \mathbb{Z}$. Un tale $x = b + tm$ è soluzione del sistema se e solo se $b + tm \equiv c \pmod{n}$. Ora, dato che m ed n sono primi tra loro, l'elemento $\overline{m} \in \mathbb{Z}_n$ è invertibile in \mathbb{Z}_n (proposizione 27.3). Consideriamo l'elemento $(\overline{m})^{-1} \overline{c} - \overline{b} \in \mathbb{Z}_n$. Esiste un $t_0 \in \mathbb{Z}$ tale che $\overline{t}_0 = (\overline{m})^{-1} \overline{c} - \overline{b}$ in \mathbb{Z}_n , ossia tale che $\overline{mt}_0 = \overline{c} - \overline{b}$ in \mathbb{Z}_n . Ma allora $mt_0 \equiv c - b \pmod{n}$, vale a dire $b + mt_0 \equiv c \pmod{n}$. Quindi $x_0 = b + mt_0$ è una soluzione del sistema di congruenze (27.1).

Se $x \in \mathbb{Z}$ e x_0 è una soluzione del sistema (27.1), si ha che x è una soluzione del sistema di congruenze (27.1) se e solo se

$$\begin{cases} x \equiv x_0 \pmod{m} \\ x \equiv x_0 \pmod{n}, \end{cases}$$

ossia se e solo se $m | (x - x_0)$ e $n | (x - x_0)$. Dato che m ed n sono primi tra loro, questo accade se e solo se $mn | (x - x_0)$, ossia se e solo se $x \equiv x_0 \pmod{mn}$. \square

Torniamo alla proposizione 27.3. Essa dice che se a è un numero intero, la congruenza $ax \equiv 1 \pmod{n}$ ha una soluzione $x \in \mathbb{Z}$ se e solo se $(a, n) = 1$, dove con (a, n) si è denotato il massimo comun divisore positivo di a ed n . Vediamo una generalizzazione di questo risultato.

27.11 PROPOSIZIONE. *Siano $a, b, n \in \mathbb{Z}$, $n \geq 1$. La congruenza $ax \equiv b \pmod{n}$ ha una soluzione $x \in \mathbb{Z}$ se e solo se $(a, n) | b$.*

Dimostrazione. Supponiamo che $ax \equiv b \pmod{n}$ con $x \in \mathbb{Z}$. Allora $b = ax + tn$ per qualche $t \in \mathbb{Z}$, e quindi $b \in a\mathbb{Z} + n\mathbb{Z}$. Nell'esercizio 19.10(c) si è visto che $a\mathbb{Z} + n\mathbb{Z} = (a, n)\mathbb{Z}$. Quindi $b \in (a, n)\mathbb{Z}$, ossia $(a, n) | b$.

Viceversa supponiamo che $(a, n) | b$. Allora esistono $a', n', b' \in \mathbb{Z}$ tali che $a = a'(a, n)$, $n = n'(a, n)$ e $b = b'(a, n)$. Inoltre $(a', n') = 1$. Quindi esiste $y \in \mathbb{Z}$ tale che $a'y \equiv 1 \pmod{n'}$, vale a dire $a'y = 1 + dn'$ per qualche $d \in \mathbb{Z}$. Moltiplicando per $b = b'(a, n)$ si trova che $a'(a, n)b'y = b + b'dn'(a, n)$, ossia $ab'y = b + b'dn$, e quindi l'equazione $ax \equiv b \pmod{n}$ ha la soluzione $x = b'y$. \square

Abbiamo già incontrato i multipli di un elemento in un anello (pagina 210). Consideriamo il caso particolare di un anello R con identità 1_R , e studiamo i multipli di 1_R . Si ricordi che per $n > 0$ si ha $n \cdot 1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}}$.

27.12 DEFINIZIONE. Sia R un anello con identità 1_R . Se esiste un intero positivo n tale che

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = 0_R,$$

il più piccolo intero n con tale proprietà si dice la *caratteristica* dell'anello R ; se invece

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} \neq 0_R$$

per ogni $n > 0$, diremo che l'anello R ha *caratteristica zero*. \square

La caratteristica dell'anello R verrà denotata con $\text{char } R$.

27.13 ESEMPIO. Per il campo \mathbb{C} dei numeri complessi si ha $\text{char } \mathbb{C} = 0$. \square

27.14 ESEMPIO. 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

27.15 ESEMPIO. Per ogni $n > 1$ si ha $\text{char } \mathbb{Z}_n = n$. \square

27.16 ESEMPIO. Gli anelli R e $R[x]$ hanno la stessa caratteristica. \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 $1_R \neq 0_R$.

27.17 PROPOSIZIONE. Sia R un anello con identità 1_R e sia

$$P = \{z1_R \mid z \in \mathbb{Z}\}$$

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 $P \cong \mathbb{Z}_n$.

Dimostrazione. Dato che $z1_R + z'1_R = (z + z')1_R$ e $(z1_R)(z'1_R) = (zz')1_R$ per ogni $z, z' \in \mathbb{Z}$ (vedi esercizio 27.9), l'applicazione $\varphi: \mathbb{Z} \rightarrow R$ definita da $\varphi(z) = z1_R$ per ogni $z \in \mathbb{Z}$, è un omomorfismo di anelli e $P = \varphi(\mathbb{Z})$ è un sottoanello di R . Ovviamente $\ker \varphi = \{z \in \mathbb{Z} \mid z1_R = 0_R\}$. Quindi se R ha caratteristica 0, $\ker \varphi$ è un ideale di \mathbb{Z} che non contiene interi positivi, e pertanto $\ker \varphi = \{0\}$; ne segue che φ è iniettivo e $\mathbb{Z} \cong \varphi(\mathbb{Z}) = P$. Se invece R ha caratteristica $n > 0$, n è il più piccolo intero positivo appartenente all'ideale $\ker \varphi = \{z \in \mathbb{Z} \mid z1_R = 0_R\}$ di \mathbb{Z} , e quindi $\ker \varphi = n\mathbb{Z}$. Per il teorema fondamentale di omomorfismo per gli anelli (teorema 25.12) $\mathbb{Z}/\ker \varphi \cong \varphi(\mathbb{Z})$, cioè $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker \varphi \cong \varphi(\mathbb{Z}) = P$. \square

Per la proposizione 27.17 ogni anello R con identità ha un sottoanello isomorfo a \mathbb{Z} (se $\text{char } R = 0$) o a \mathbb{Z}_n (se $\text{char } R = n > 0$).

27.18 COROLLARIO. *Ogni dominio di integrità ha caratteristica 0 oppure un numero primo. In particolare ogni campo ha caratteristica 0 oppure un numero primo.*

Dimostrazione. Sia R un dominio di integrità, e sia P il sottoanello fondamentale di R . Allora P è un dominio di integrità. Se R ha caratteristica $n \neq 0$, allora $P \cong \mathbb{Z}_n$. Quindi \mathbb{Z}_n è un dominio di integrità, e pertanto n è primo (corollario 27.4). Ciò prova che ogni dominio di integrità ha caratteristica 0 o un numero primo. La stessa asserzione per i campi segue dal lemma 24.10. \square

27.19 ESEMPIO. Fissato un numero intero $t > 1$ si consideri l'anello $\mathbb{Z}_t \times \mathbb{Z}_t = \{(a, b) \mid a, b \in \mathbb{Z}_t\}$ con le operazioni definite da

$$(a, b) + (a', b') = (a + a', b + b')$$

$$(a, b)(a', b') = (aa', bb')$$

per ogni $(a, b), (a', b') \in \mathbb{Z}_t \times \mathbb{Z}_t$. L'anello $\mathbb{Z}_t \times \mathbb{Z}_t$ è un anello commutativo con identità. L'identità è $(\bar{1}, \bar{1})$, lo zero è $(\bar{0}, \bar{0})$.

Si ha

$$\star \quad \underbrace{(\bar{1}, \bar{1}) + \cdots + (\bar{1}, \bar{1})}_{n \text{ volte}} = \underbrace{(\bar{1} + \cdots + \bar{1}, \bar{1} + \cdots + \bar{1})}_{n \text{ volte}} = (\bar{n}, \bar{n}),$$

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 $\text{char}(\mathbb{Z}_t \times \mathbb{Z}_t) = t$. In particolare, se t è primo, $\mathbb{Z}_t \times \mathbb{Z}_t$ 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. Denoteremo con $\mathcal{L}(R)$ l'insieme di tutti gli ideali di R . Chiaramente $(\mathcal{L}(R), \subseteq)$ è un insieme parzialmente ordinato dall'inclusione \subseteq .

Possiamo considerare il sottoinsieme ordinato

$$\mathcal{L}_p(R) = \mathcal{L}(R) \setminus \{R\} = \{I \mid I \trianglelefteq R, I \neq R\}$$

i cui elementi sono tutti gli ideali propri di R . Un elemento massimale dell'insieme ordinato $(\mathcal{L}_p(R), \subseteq)$ si chiama un *ideale massimale* di R . Quindi un ideale I di R è massimale se e solo 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 $y \in I$.

27.20 ESEMPIO. 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

27.21 LEMMA. Sia R un anello commutativo con identità. Le seguenti affermazioni sono equivalenti:

- (a) R è un campo;
- (b) $\{0\}$ è ideale massimale di R ;
- (c) gli ideali di R sono solo $\{0\}$ ed R .

Dimostrazione. (a) \Rightarrow (b) Sia R un campo e mostriamo che $\{0\}$ è massimale. Si deve mostrare che se J è ideale di R e $\{0\} \subseteq J \subseteq R$, allora o $J = \{0\}$ oppure $J = R$. Supponiamo $J \neq \{0\}$ e sia $x \in J, x \neq 0$. Allora per ogni $r \in R$ si ha $r = (rx^{-1})x \in J$, cioè $R \subseteq J$. Questo prova che $J = R$.

(b) \Rightarrow (c) Per ogni ideale J di R si ha $\{0\} \subseteq J \subseteq R$. Quindi se $\{0\}$ è massimale, $\{0\}$ ed R sono gli unici ideali di R .

(c) \Rightarrow (a) Siano $\{0\}$ ed R i soli ideali di R e mostriamo che R è un campo. Si deve far vedere che se $r \in R$ e $r \neq 0$, allora r è invertibile. Consideriamo $Rr = \{tr \mid t \in R\}$; è facile verificare che Rr è ideale di R . Inoltre $r = 1r \in Rr$ ed $r \neq 0$. Quindi Rr è un ideale non nullo di R , e pertanto $Rr = R$; in particolare $1 \in Rr$, cioè $1 = tr$ per qualche $t \in R$, e pertanto r è un elemento invertibile. \square

27.22 TEOREMA. Sia R un anello commutativo con identità e sia I un ideale proprio di R . Allora

- (a) I è primo se e solo se R/I è un dominio di integrità;
- (b) I è massimale se e solo se R/I è un campo.

Dimostrazione. (a) (\Rightarrow) Sia I un ideale primo, e supponiamo che $a + I, b + I \in R/I$, $(a + I)(b + I) = 0_{R/I} = I$. Allora $ab + I = I$, da cui $ab \in I$. Essendo I primo, ne segue che $a \in I$ oppure $b \in I$, e quindi $a + I = I$ oppure $b + I = I$. Questo prova che R/I è un dominio di integrità.

(\Leftarrow) Supponiamo che R/I sia un dominio di integrità, e siano $a, b \in R$ tali che $ab \in I$.

Allora $(a+I)(b+I) = ab + I = I = 0_{R/I}$, e quindi, essendo R/I un dominio, $a+I = I$ oppure $b+I = I$. Se ne deduce che $a \in I$ oppure $b \in I$. Questo prova che I è ideale primo di R .

(b) Per il teorema di corrispondenza per gli ideali 25.13 applicato alla proiezione canonica $\pi: R \rightarrow R/I$ c'è una corrispondenza biunivoca tra $\{J \mid I \subseteq J \trianglelefteq R\}$ e $\{J' \mid J' \trianglelefteq R/I\}$. Quindi $\{J \mid I \subseteq J \trianglelefteq R\}$ ha due elementi se e solo se $\{J' \mid J' \trianglelefteq R/I\}$ ha due elementi. Ora $\{J \mid I \subseteq J \trianglelefteq R\}$ ha due elementi se e solo se ci sono solo i due ideali che contengono I (necessariamente I ed R), cioè se e solo se I è ideale massimale. D'altra parte $\{J' \mid J' \trianglelefteq R/I\}$ ha due elementi se e solo se R/I ha solo i due ideali banali $\{0_{R/I}\}$ e R/I , cioè se e solo se R/I è un campo (lemma 27.21). Quindi I è ideale massimale di R se e solo se R/I è un campo. \square

27.23 COROLLARIO. *Ogni ideale massimale è primo.*

Dimostrazione. Sia I ideale massimale di R . Allora R/I è un campo (teorema 27.22) e quindi è un dominio di integrità (24.10). Pertanto I è primo (teorema 27.22). \square

27.24 ESEMPIO. L'anello \mathbb{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 (esempio 27.20 e lemma 27.21). Per l'esempio 25.1 gli altri ideali di \mathbb{Z} sono gli $n\mathbb{Z}$ con $n \geq 1$ intero. Per $n = 1$ si ha l'ideale improprio. Per $n \geq 2$ si ha che $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ è un dominio d'integrità se e solo se $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ è un campo, e questo avviene se e solo se n è un numero primo (corollario 27.4). Dal teorema 27.22 segue che per ogni intero $n \geq 1$ l'ideale $n\mathbb{Z}$ di \mathbb{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 \mathbb{Z} sono l'ideale nullo e gli ideali $n\mathbb{Z}$ con n numero primo;
- (b) gli ideali massimali di \mathbb{Z} sono gli ideali $n\mathbb{Z}$ con n numero primo. \square

Concludiamo con una proposizione di cui omettiamo la dimostrazione.

27.25 PROPOSIZIONE. *Sia t un elemento non invertibile di un anello R commutativo con identità. Allora esiste un ideale massimale di R contenente t .*

Esercizi svolti

27.1. 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 27.2 un suo sottoanello finito R è un campo.

Per risolvere la seconda parte dell'esercizio basta prendere invece come esempio il campo \mathbb{R} e il suo sottoanello \mathbb{Z} , che è un dominio d'integrità ma non è un campo. \square

27.2. Si calcoli la caratteristica dell'anello $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$ dell'esempio 24.2.

Soluzione. Si osservi intanto che $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$ è un anello con identità, e che si ha $0_{\mathbb{Z} \times \mathbb{Z}} = (0, 0)$ e $1_{\mathbb{Z} \times \mathbb{Z}} = (1, 0)$ (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 $(a, b) \in \mathbb{Z} \times \mathbb{Z}$). Inoltre per ogni numero naturale $n > 0$ si ha

$$\underbrace{(1, 0) + (1, 0) + \cdots + (1, 0)}_{n \text{ volte}} = (n, 0) \neq 0_{\mathbb{Z} \times \mathbb{Z}} = (0, 0).$$

Quindi $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$ ha caratteristica 0. \square

27.3. 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 25.14). 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 25.14 avevamo 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

27.4. Si dica quali sono gli elementi invertibili e quali sono i divisori dello zero nell'anello \mathbb{Z}_8 . Idem nell'anello \mathbb{Z}_9 .

27.5. Siano n, m interi positivi e supponiamo che $n \mid m$. Si provi che l'applicazione $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ definita da $f(a + m\mathbb{Z}) = a + n\mathbb{Z}$ per ogni $a + m\mathbb{Z} \in \mathbb{Z}_m$ è un ben definito omomorfismo di anelli. (Per verificare che f è ben definito si deve dimostrare che se $a, b \in \mathbb{Z}$ e $a + m\mathbb{Z} = b + m\mathbb{Z}$, allora $a + n\mathbb{Z} = b + n\mathbb{Z}$.) Dove è stata adoperata l'ipotesi che $n \mid m$?

27.6. Sia n un intero, $n > 1$. Quanti elementi ha l'anello $\mathbb{Z}_n[x]$? *

27.7. Si divida $x^7 + \bar{6}$ per $x + \bar{6}$ in $\mathbb{Z}_7[x]$; $x^7 + x^5 + x^3 + x$ per $x + \bar{1}$ in $\mathbb{Z}_2[x]$; $x^4 + x + \bar{1}$ per $\bar{2}x$ in $\mathbb{Z}_3[x]$.

27.8. Si scrivano tutti gli ideali degli anelli \mathbb{Z}_6 , \mathbb{Z}_7 e \mathbb{Z}_8 . [Suggerimento: Far uso del teorema di corrispondenza per gli ideali. Si era visto l'analogico per i gruppi nell'esempio 23.11.]

27.9. Si provi che se $z, z' \in \mathbb{Z}$, allora $(z1_R)(z'1_R) = (zz')1_R$, dove 1_R è l'identità dell'anello R . [Suggerimento: Distinguere i due casi $z' \geq 0$ e $z' < 0$. Nel primo caso procedere per induzione su z' ; nel secondo caso rifarsi al primo.]

27.10. Sia \mathbb{Z}_4 l'anello delle classi resto modulo 4 ed $R = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ l'insieme di tutte le terne di elementi di \mathbb{Z}_4 . Si definiscano su R le operazioni $+ e \cdot$ ponendo

$$(a, b, c) + (a', b', c') = (a + a', b + b', c + c') \quad e \quad (a, b, c)(a', b', c') = (aa', ab' + ba', ac' + ca')$$

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 $\{\bar{0}\} \times \mathbb{Z}_4 \times \mathbb{Z}_4$ è un ideale di R e che tutti gli elementi non nulli di $\{\bar{0}\} \times \mathbb{Z}_4 \times \mathbb{Z}_4$ sono divisori dello zero in R .
- (d) Si determini la caratteristica di R .

27.11. Siano $n \geq 2$ un numero intero, X un insieme non vuoto e \mathbb{Z}_n l'anello delle classi resto degli interi modulo n . L'insieme

$$\mathbb{Z}_n^X = \{f \mid f: X \rightarrow \mathbb{Z}_n\}$$

è un anello se si definiscono le operazioni di addizione e di moltiplicazione ponendo

$$(f + g)(x) = f(x) + g(x) \quad e \quad (fg)(x) = f(x)g(x)$$

per ogni $f, g \in \mathbb{Z}_n^X$ e ogni $x \in X$.

- (a) Qual è il sottoanello fondamentale di \mathbb{Z}_n^X ?
- (b) Qual è la caratteristica di \mathbb{Z}_n^X ?
- (c) Si dimostri che \mathbb{Z}_n^X è un campo se e solo se X ha cardinalità 1 ed n è un numero primo.

27.12. Si dimostri che se R è un anello con identità finito con $|R|$ elementi, allora la caratteristica di R è un divisore di $|R|$.

27.13. 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.

27.14. Si provi che se R è un anello di caratteristica n , allora $na = 0$ per ogni $a \in R$.

27.15. Si dimostri che se R è un anello con identità avente un numero primo p di elementi, allora R è isomorfo al campo \mathbb{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 .]

27.16. Sia p un numero primo.

- (a) Si provi che se $1 \leq i \leq p-1$, allora p divide $\binom{p}{i}$.
- (b) Si provi che in un anello di caratteristica p si ha $\binom{p}{i}a = 0$ per ogni $a \in R$ ed ogni intero i con $1 \leq i \leq p-1$. [Suggerimento: esercizio 27.14.]
- (c) Si provi che in un anello commutativo di caratteristica p , $(a+b)^p = a^p + b^p$ per ogni $a, b \in R$. [Suggerimento: esercizio 24.23.]
- (d) Si provi che in un anello commutativo di caratteristica p , $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ per ogni $a, b \in R$, $n \geq 1$.

(e) Si provi che se $\pi: R \rightarrow R$ è l'applicazione definita da $\pi(a) = a^p$ per ogni $a \in R$ ed R è un anello commutativo di caratteristica p , allora π è un endomorfismo d'anelli (detto *l'endomorfismo di Frobenius*). Ne segue, più generalmente, che per ogni $n \geq 1$ l'applicazione $\pi^n: R \rightarrow R$, definita da $\pi^n(a) = a^{p^n}$ per ogni $a \in R$, è un endomorfismo di anelli.

27.17. Si provi che ogni anello di caratteristica 0 è infinito.

27.18. Si dia un esempio di un anello di caratteristica $n > 0$ che sia finito e un esempio di un anello di caratteristica n che sia infinito.

27.19. Si provi che ogni anello di caratteristica p (numero primo) contiene un sottoanello che è un campo.

27.20. Si dia un esempio di un anello di caratteristica 0 che non contenga sottoanelli che siano campi.

27.21. Si dimostri che ogni campo finito ha per caratteristica un numero primo.

27.22. Sia R un anello commutativo con identità e $\mathcal{L}(R)$ l'insieme di tutti gli ideali di R . Si dimostri che l'insieme parzialmente ordinato $(\mathcal{L}(R), \subseteq)$ è un reticolo limitato. [Suggerimento: se $I, J \in \mathcal{L}(R)$ l'estremo superiore di $\{I, J\}$ è $I + J = \{i + j \mid i \in I, j \in J\}$ e l'estremo inferiore è $I \cap J$. Si veda l'esercizio 25.6. L'1 di $\mathcal{L}(R)$ è l'ideale improprio e lo 0 di $\mathcal{L}(R)$ è l'ideale nullo $\{0\}$.]

27.23. Si considerino il reticolo $(\mathbb{N}, |)$ e il reticolo $(\mathcal{L}(\mathbb{Z}), \supseteq)$, ossia il reticolo con l'ordine inverso di quello considerato nell'esercizio 27.22. Si dimostri che l'applicazione $\varphi: \mathbb{N} \rightarrow \mathcal{L}(\mathbb{Z})$ definita da $\varphi(n) = n\mathbb{Z}$ per ogni $n \in \mathbb{N}$ è un isomorfismo di reticolli di $(\mathbb{N}, |)$ in $(\mathcal{L}(\mathbb{Z}), \supseteq)$.

27.24. Sia $\varphi: R \rightarrow S$ un omomorfismo suriettivo di anelli. Si provi che:

- se P è un ideale primo di R contenente $\ker \varphi$, allora $\varphi(P)$ è ideale primo di S ;
- se P' è un ideale primo di S , allora $\varphi^{-1}(P')$ è un ideale primo di R ;
- se M è un ideale massimale di R contenente $\ker \varphi$, allora $\varphi(M)$ è ideale massimale di S ;
- se M' è un ideale massimale di S , allora $\varphi^{-1}(M')$ è un ideale massimale di R .

Se ne deduca che nella corrispondenza biunivoca del teorema 25.13 ideali primi corrispondono a ideali primi e ideali massimali corrispondono a ideali massimali (nell'ipotesi che l'omomorfismo φ sia suriettivo).

27.25. Si provi che $I = \{2a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in \mathbb{Z}\}$ è un ideale massimale di $\mathbb{Z}[x]$.

27.26. Sia I l'ideale di $R[x]$ dell'esercizio 26.4. Si provi che I è ideale primo di $R[x]$ se e solo se R è un dominio di integrità. Si provi che I è ideale massimale di $R[x]$ se e solo se R è un campo.

27.27. Si consideri l'anello $\mathbb{Z} \times \mathbb{Z}$ dell'esempio 24.2. Si provi che il suo sottoinsieme $\{0\} \times \mathbb{Z}$ è un ideale primo di $\mathbb{Z} \times \mathbb{Z}$.

27.28. Sia X un insieme non vuoto e sia \mathbb{R}^X l'anello dell'esercizio 24.7. Si fissi $x_0 \in X$, e sia $I_0 = \{f \in \mathbb{R}^X \mid f(x_0) = 0\}$. Si provi che I_0 è ideale massimale di \mathbb{R}^X . [Suggerimento: si faccia uso dell'omomorfismo $\varphi: \mathbb{R}^X \rightarrow \mathbb{R}$ dell'esempio 25.7 e dei teoremi 25.12 e 27.22.]

27.29. Siano R un anello, F un campo e $\varphi: F \rightarrow R$ un omomorfismo di anelli. Si provi che allora o φ è iniettivo oppure $\varphi(a) = 0$ per ogni $a \in F$. [Suggerimento: usare il fatto che $\ker \varphi$ è ideale di F e il lemma 27.21.]

27.30. Sia \mathbb{R} il campo dei numeri reali. Si determinino tutte le equivalenze \sim sull'insieme \mathbb{R} compatibili sia con l'operazione di addizione che con l'operazione di moltiplicazione tra numeri reali.

27.31. Sia $(\mathbb{Q}, +)$ il gruppo additivo dei numeri razionali. Si definisca un'operazione $*$ in \mathbb{Q} ponendo $x * y = \frac{5}{3}xy$ per ogni $x, y \in \mathbb{Q}$. È allora possibile dimostrare che $(\mathbb{Q}, +, *)$ è un anello commutativo con identità.

- Si determini l'identità di $(\mathbb{Q}, +, *)$.
- Si calcoli la caratteristica di $(\mathbb{Q}, +, *)$.
- Si determini il sottoanello fondamentale di $(\mathbb{Q}, +, *)$.
- Si dimostri che $(\mathbb{Q}, +, *)$ è un campo isomorfo al campo $(\mathbb{Q}, +, \cdot)$ dei numeri razionali. Qui \cdot denota la moltiplicazione usuale tra numeri razionali.

27.32. Sia $R = \mathbb{R} \times \mathbb{Z}_8$ il prodotto diretto del campo \mathbb{R} dei numeri reali e dell'anello \mathbb{Z}_8 delle classi resto degli interi modulo 8 (esercizio 24.10). Quindi R è un anello commutativo con identità.

- L'anello R è un dominio d'integrità?
- Si dimostri che $\{0\} \times \mathbb{Z}_8$ è un ideale massimale di R . [Suggerimento: applicare il teorema fondamentale di omomorfismo per gli anelli alla proiezione canonica sul primo fattore $\pi_{\mathbb{R}}: \mathbb{R} \times \mathbb{Z}_8 \rightarrow \mathbb{R}$.]
- Si dimostri che l'ideale $\mathbb{R} \times \{\bar{0}\}$ di R non è un ideale primo.
- Si calcoli la caratteristica di R .

27.33. Siano R un anello commutativo con identità, M un suo ideale massimale e S un sottoanello di R . Si dimostri che:

- il sottoinsieme $S + M = \{s + m \mid s \in S, m \in M\}$ di R è un sottoanello di R ;
- il sottoinsieme M di $S + M$ è un ideale primo di $S + M$.

§28. Domini euclidei e teorema di Ruffini

Se R è un dominio di integrità, indichiamo con R^* l'insieme degli elementi non nulli di R .

Un dominio di integrità R si dice un dominio *euclideo* se esiste un'applicazione $\delta: R^* \rightarrow \mathbb{N}$ tale che:

- $\delta(ab) \geq \delta(a)$ per ogni $a, b \in R^*$;
- se $a, b \in R$ e $b \neq 0$, esistono $q, r \in R$ tali che
 - $a = bq + r$;
 - $r = 0$ oppure $\delta(r) < \delta(b)$.

28.1 ESEMPIO. \mathbb{Z} è un dominio euclideo se si pone $\delta(a) = |a|$ per ogni $a \in \mathbb{Z}^*$. \square

28.2 ESEMPIO. Se F è un campo e $\delta(f)$ è il grado del polinomio f per ogni $f \in F[x]^*$, $F[x]$ è un dominio euclideo per il teorema 26.2. \square

Se R è un dominio euclideo e $a \in R^*$, $\delta(a)$ si chiama il *grado* di a , e i q ed r della condizione (b) della definizione si chiamano il *quofo* e il *resto* della divisione di a per b . (Non sono necessariamente unici: dividendo 7 per 3 in \mathbb{Z} si ha $7 = 3 \cdot 2 + 1 = 3 \cdot 3 - 2$.)

Se R è un anello commutativo con identità 1_R , un ideale I di R si dice *principale* se esiste $a \in R$ tale che $I = \{ra \mid r \in R\}$. L'ideale $\{ra \mid r \in R\}$ si indica in genere con (a) o con Ra , e si dice l'*ideale principale generato da a* (vedi esercizio 25.8).

28.3 TEOREMA. Sia R un dominio euclideo. Allora ogni ideale di R è principale.

Dimostrazione. Sia I ideale di R . Se $I = \{0\}$, I è l'ideale principale generato da 0. Supponiamo $I \neq \{0\}$ e consideriamo l'insieme $G = \{\delta(x) \mid x \in I, x \neq 0\}$. Allora G è un sottoinsieme non vuoto di \mathbb{N} , e quindi ha un minimo. Pertanto esiste $a \in I$, $a \neq 0$, tale che $\delta(a) \leq \delta(x)$ per ogni $x \in I$, $x \neq 0$. Mostriamo che $I = (a)$. Dato che $a \in I$, si ha $ra \in I$ per ogni $r \in R$, e quindi $(a) \subseteq I$.

Viceversa sia $x \in I$. Dividiamo x per a ; allora $x = qa + r$ con $r = 0$ oppure $\delta(r) < \delta(a)$. Ne segue che $r = x - qa$ è differenza di due elementi di I , e quindi $r \in I$. Se fosse $r \neq 0$, allora $\delta(r) \in G$ e $\delta(r) < \delta(a)$, assurdo perché $\delta(a)$ è il minimo di G . Pertanto deve essere $r = 0$ e $x = qa \in (a)$. Ciò prova che $I \subseteq (a)$. Quindi $I = (a)$ è l'ideale principale generato da a . \square

Sia R un dominio di integrità. Se $a, b \in R$, diremo che a divide b (o che a è un *divisore* di b , o che b è un *multiplo* di a) se esiste $c \in R$ tale che $b = ac$. Se a divide b scriveremo $a \mid b$. Un elemento u è invertibile se e solo se $u \mid 1$. Chiaramente un elemento invertibile divide ogni elemento di R . Se $a, b \in R^*$, $a \mid b$ e $b \mid a$, diremo che a e b sono *associati* e scriveremo $a \sim b$; in tal caso si ha $b = ac$ e $a = bd$ per certi $c, d \in R$, da cui $a = acd$. Ne segue che $a(1 - cd) = 0$, ed essendo $a \neq 0$ ed R un dominio di integrità, si deve avere $1 - cd = 0$, cioè $cd = 1$, e quindi a e b differiscono per un fattore invertibile. Viceversa, è immediato che se a e b differiscono per un fattore invertibile, cioè $a = bu$ con u invertibile, essi sono associati.

28.4 ESEMPIO. Mostriamo che se $a, b \in R$, dove R è un dominio di integrità, si ha $a \mid b$ se e solo se $(a) \supseteq (b)$.

Supponiamo che $a \mid b$. Allora $b = ac$ per qualche $c \in R$. Se $x \in (b)$, allora $x = bx'$ per qualche $x' \in R$, e quindi $x = bx' = acx' = (ax')c \in (a)$.

Viceversa, se $(a) \supseteq (b)$, allora $b \in (b) \subseteq (a)$, e quindi $b = ad$ per qualche $d \in R$, e pertanto $a \mid b$. \square

28.5 ESEMPIO. Mostriamo che se $a, b \in R^*$, dove R è un dominio di integrità, si ha $a \sim b$ se e solo se $(a) = (b)$.

Si ha $a \sim b$ se e solo se $a \mid b$ e $b \mid a$, ossia, per l'esempio precedente, se e solo se $(a) \supseteq (b)$ e $(b) \supseteq (a)$, vale a dire se e solo se $(a) = (b)$. \square

28.6 ESEMPIO. Mostriamo che se $a \in R^*$, dove R è un dominio di integrità, si ha che a è invertibile se e solo se $(a) = R$.

Infatti supponiamo a invertibile. Allora $aa^{-1} = 1$ con $a^{-1} \in R$. Ma allora per ogni $x \in R$ si ha $x = 1x = a(a^{-1}x) \in (a)$. Questo dimostra che $R \subseteq (a)$. Dato che certamente si ha $(a) \subseteq R$, ne segue che $(a) = R$.

Viceversa, se $(a) = R$, allora $1 \in (a)$ e quindi $1 = ab$ per qualche $b \in R$. Quindi a è invertibile in R . \square

È chiaro che tutti gli elementi invertibili e tutti gli elementi associati ad a sono divisori di a ; questi sono detti i divisori *impropri* di a ; tutti gli altri si dicono divisori *propri*. Un elemento $a \in R^*$ è detto *irriducibile* se non è invertibile e non ha divisori propri. Equivalentemente $a \in R$ è irriducibile se e solo se $a \neq 0$, a non è invertibile, e per ogni $b, c \in R^*$, da $a = bc$ segue che b è invertibile o c è invertibile (e pertanto l'altro elemento sarà associato ad a).

28.7 ESEMPIO. Nel dominio euclideo \mathbb{Z} gli unici elementi invertibili sono 1 e -1 ; due elementi $a, b \in \mathbb{Z}$ sono associati se e solo se $|a| = |b|$; i divisori impropri di $a \in \mathbb{Z}$ sono $1, -1, a, -a$; e un elemento $a \in \mathbb{Z}$ è irriducibile se e solo se a è un numero primo. \square

28.8 ESEMPIO. Se F è un campo, nel dominio euclideo $F[x]$ gli elementi invertibili sono gli elementi di F^* ; due polinomi $f, g \in F[x]$ sono associati se e solo se differiscono per una costante moltiplicativa non nulla, cioè se e solo se $f = ag$ per qualche $a \in F^*$; i divisori impropri di $f \in F[x]$ sono gli $a \in F^*$ e gli af con $a \in F^*$; un elemento $f \in F[x]$ è irriducibile se e solo se $\delta(f) \geq 1$ ed f non può essere scritto come prodotto di due polinomi appartenenti a $F[x]$ di grado $< \delta(f)$. \square

28.9 PROPOSIZIONE. Sia R un dominio euclideo, e sia $a \in R$, $a \neq 0$. Allora l'ideale (a) è massimale se e solo se a è un elemento irriducibile.

Dimostrazione. L'ideale (a) è massimale se e solo se $(a) \neq R$ e non esistono ideali I di R tali che $I \supseteq (a)$, $I \neq (a)$, $I \neq R$. Ma in un dominio euclideo gli ideali sono tutti principali (teorema 28.3). Quindi (a) è massimale se e solo se a non è invertibile e non esistono elementi $b \in R$ tali che $b \mid a$, $b \not\sim a$ e b non è invertibile, ossia se e solo se a non è invertibile e non ha divisori propri, vale a dire se e solo se a è irriducibile. \square

Dalla proposizione 28.9 si deduce immediatamente che se R è un dominio euclideo, $a \in R$ e $a \neq 0$, allora $R/(a)$ è un campo se e solo se a è un elemento irriducibile di R .

Omettiamo la dimostrazione del teorema che segue.

28.10 TEOREMA (FATTORIZZAZIONE UNICA NEI DOMINI EUCLIDEI). In un dominio euclideo R ogni elemento non nullo e non invertibile è prodotto di elementi irriducibili (non necessariamente distinti). Tale fattorizzazione è essenzialmente unica nel senso seguente: se $a = p_1 p_2 \cdots p_r$ e $a = q_1 q_2 \cdots q_s$ sono due fattorizzazioni dell'elemento $a \in R$ con $p_1, \dots, p_r, q_1, \dots, q_s$ elementi irriducibili, allora $r = s$ e si possono riordinare i fattori in modo che $p_1 \sim q_1, p_2 \sim q_2, \dots, p_r \sim q_r$.

Consideriamo ora in particolare il dominio euclideo $F[x]$, ove F è un campo ed x è

una indeterminata su F . Se $f \in F[x]$ ed $a \in F$, a si dice una *radice* (o uno *zero*) di f se $f(a) = 0$.

28.11 TEOREMA DI RUFFINI. *Sia F un campo, $f \in F[x]$ ed $a \in F$. Allora a è radice di f se e solo se il polinomio $x - a$ divide f nell'anello $F[x]$.*

Dimostrazione. Supponiamo che a sia radice di f . Dividiamo f per $x - a$. Allora $f = (x - a)q + r$, ove $q, r \in F[x]$ e $\delta(r) < \delta(x - a)$ (teorema 26.2). Ora $\delta(x - a) = 1$, e quindi $\delta(r) \leq 0$, cioè $r \in F$. Pertanto $f = (x - a)q + r$ con $q \in F[x]$ e $r \in F$. Dato che a è radice di f si ha $0 = f(a) = (a - a)q(a) + r = r$. Ne segue che $f = (x - a)q$, cioè che $(x - a) | f$.

Viceversa supponiamo che $(x - a) | f$. Allora $f = (x - a)q$ per un opportuno $q \in F[x]$, e quindi $f(a) = (a - a)q(a) = 0$, cioè a è radice di f . \square

28.12 COROLLARIO. *Un polinomio $f \in F[x]$ di grado $n \geq 0$ a coefficienti in un campo F ha al più n radici distinte.*

Dimostrazione. Induzione su n . Se $n = 0$, allora $f \in F$ e $f \neq 0$, e quindi f non ha radici. Supponiamo il risultato vero per i polinomi di grado $n - 1$. Se il polinomio f di grado n non ha radici, il risultato è vero; se invece f ha una radice $a \in F$, si ha $f = (x - a)q$ con $q \in F[x]$ per il teorema di Ruffini. Allora q ha grado $n - 1$, e quindi per l'ipotesi induttiva q ha al più $n - 1$ radici distinte. Ma $b \in F$ è radice di f se e solo se $b = a$ oppure b è radice di q . Quindi f ha al più n radici distinte. \square

Se $f(x) \in F[x]$ e a è radice di $f(x)$, il massimo intero n tale che $(x - a)^n | f(x)$ si dice la *moltiplicità* della radice a di $f(x)$.

Esercizi svolti

28.1. Si dimostri che $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (*anello degli interi di Gauss*) è un dominio euclideo.

Soluzione. Dato che $\mathbb{Z}[i]$ è un sottoanello di \mathbb{C} , $\mathbb{Z}[i]$ è certamente un dominio d'integrità. Sia $\delta: \mathbb{C} \rightarrow \mathbb{R}$ l'applicazione definita da $\delta(a + ib) = a^2 + b^2$ per ogni $a, b \in \mathbb{R}$. (Il numero reale $\delta(a + ib)$ si chiama la *norma* di $a + ib$.) È facile verificare che $\delta(xy) = \delta(x)\delta(y)$ per ogni $x, y \in \mathbb{C}$. Inoltre $\delta(\mathbb{Z}[i]^*) \subseteq \mathbb{N}^*$ e quindi $\delta(xy) \geq \delta(x)$ per ogni $x, y \in \mathbb{Z}[i]^*$. Per verificare la (b) della definizione di dominio euclideo prendiamo $a + ib, c + id \in \mathbb{Z}[i]$ con $c + id \neq 0$. Allora

$$\frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + i \frac{bc - ad}{c^2 + d^2}.$$

Poniamo

$$a' = \frac{ac + bd}{c^2 + d^2}, \quad b' = \frac{bc - ad}{c^2 + d^2},$$

di modo che $a', b' \in \mathbb{Q}$. Siano $e, f \in \mathbb{Z}$ tali che $|a' - e| \leq 1/2$ e $|b' - f| \leq 1/2$. Poniamo $e' = a' - e$, $f' = b' - f$. Si ha che $e', f' \in \mathbb{Q}$ e $|e'|, |f'| \leq 1/2$, da cui

$$\begin{aligned} a + ib &= (a' + ib')(c + id) = [(e + e') + i(f + f')](c + id) \\ &= (e + if)(c + id) + (e' + if')(c + id). \end{aligned}$$

Allora $e + if$ è il quoto della divisione di $a + ib$ per $c + id$, ed $(e' + if')(c + id)$ è il resto, in quanto

$$\begin{aligned} \delta[(e' + if')(c + id)] &= \delta(e' + if') \delta(c + id) = (e'^2 + f'^2) \delta(c + id) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) \delta(c + id) = \frac{1}{2} \delta(c + id) < \delta(c + id). \quad \square \end{aligned}$$

28.2. Si provi che in un dominio euclideo ogni ideale primo $\neq \{0\}$ è massimale.

Soluzione. Sia $P \neq \{0\}$ un ideale primo di un dominio euclideo R . Per il teorema 28.3 l'ideale P è principale, diciamo $P = (p)$ con $p \in R$, $p \neq 0$. L'elemento p non è invertibile in R , perché se p fosse invertibile, allora $P = (p) = R$ non sarebbe un ideale proprio, e quindi P non sarebbe primo, contraddizione. Fattorizziamo p : si ha $p = q_1 \cdots q_m$ per opportuni elementi $q_i \in R$ irriducibili (teorema 28.10). Dato che P è primo, uno dei q_i deve appartenere a P . Supponiamo che $q_t \in P$. Allora $q_t | p$, e quindi $(p) \subseteq (q_t)$. Ma $q_t \in P$ implica che $(q_t) \subseteq P$. Quindi $P = (p) \subseteq (q_t) \subseteq P$, da cui $P = (q_t)$. Per la proposizione 28.9 l'ideale P è massimale. \square

28.3. Siano a, b due elementi di un dominio di integrità R . Un elemento $d \in R$ si dice un *massimo comun divisore* di a e b se valgono le seguenti proprietà:

- (a) $d | a, d | b$;
- (b) se $c \in R$, $c | a$ e $c | b$, allora $c | d$.

Si noti che il massimo comun divisore non è unico, perché se d è un massimo comun divisore di a e b anche ogni altro elemento associato a d è un massimo comun divisore di a e b .

Se a e b sono elementi di un dominio euclideo R si provi che d è un massimo comun divisore di a e b se e solo se l'ideale (d) è uguale all'ideale $(a) + (b) = \{xa + yb \mid x, y \in R\}$. Se ne deduca che se d è massimo comun divisore di a e b , allora esistono $\alpha, \beta \in R$ tali che $d = \alpha a + \beta b$.

Soluzione. Per l'esempio 28.4 si ha che d è un massimo comun divisore di a e b se e solo se $(d) \supseteq (a), (d) \supseteq (b)$ e per ogni $c \in R$ da $(c) \supseteq (a)$ e $(c) \supseteq (b)$ segue che $(c) \supseteq (d)$.

Supponiamo quindi che d sia un massimo comun divisore di a e b . Allora $(d) \supseteq (a)$ e $(d) \supseteq (b)$, e quindi $(d) \supseteq (a) + (b)$. Dato che l'ideale $(a) + (b)$ è principale (teorema 28.3), esiste $c \in R$ tale che $(c) = (a) + (b)$. Ma allora $(c) \supseteq (a)$ e $(c) \supseteq (b)$, da cui $(c) \supseteq (d)$. Quindi $(a) + (b) \supseteq (d)$. Questo prova che $(d) = (a) + (b)$.

Viceversa supponiamo che $(d) = (a) + (b)$, Allora $(d) \supseteq (a), (d) \supseteq (b)$, e per ogni $c \in R$ tale che $(c) \supseteq (a)$ e $(c) \supseteq (b)$ si ha $(c) \supseteq (a) + (b)$, e quindi $(c) \supseteq (d)$. Questo dimostra che d è massimo comun divisore di a e b . \square

Altri esercizi

28.4. Sia R dominio di integrità euclideo, e siano $a, b \in R^*$. Si provi che:

- (a) Se $a \sim b$, allora $\delta(a) = \delta(b)$.
- (b) Se $a | b$ e $\delta(a) = \delta(b)$, allora $a \sim b$. [Suggerimento: Sia $b = ac$. Si divida a per b . Allora $a = bq + r$ con $r = 0$ o $\delta(r) < \delta(b)$. Se $r \neq 0$, allora $\delta(r) = \delta(a - bq) = \delta[a(1 - cq)] \geq \delta(a) = \delta(b) > \delta(r)$, assurdo. Quindi $r = 0$ e $b | a$.]
- (c) $\delta(a) \geq \delta(1)$.
- (d) $\delta(a) = \delta(1)$ se e solo se a è invertibile in R .

28.5. Si provi che ogni campo è un dominio euclideo. [Suggerimento: porre $\delta(a) = 0$ per ogni $a \neq 0$.]

28.6. È facile vedere che l'algoritmo di Euclide studiato nel §4 vale non solo in \mathbb{Z} ma in qualsiasi dominio euclideo R . Ad esempio la successione dell'algoritmo di Euclide termina perché $\delta(b) > \delta(r_1) > \delta(r_2) > \dots$ Facendo uso dell'algoritmo di Euclide trovare il massimo comun divisore di

- (a) $4x^3 + 2x^2 + 3x + 7$ e $2x^2 + 5$ nell'anello $\mathbb{Q}[x]$;
- (b) $x^6 + \bar{4}x^5 - \bar{1}\bar{2}x + \bar{1}$ e $x^3 + \bar{4}x + \bar{1}$ nell'anello $\mathbb{Z}_5[x]$;
- (c) $\bar{2}x^3 + x + \bar{1}$ e $\bar{4}x + \bar{1}$ nell'anello $\mathbb{Z}_7[x]$;
- (d) $x^4 + x$ e x nell'anello $\mathbb{Z}_3[x]$;
- (e) $2x^3 + x + 1$ e $4x + 1$ nell'anello $\mathbb{R}[x]$.

28.7. Si provi che per un polinomio $f \in F[x]$ di grado $n \geq 0$ a coefficienti in un campo F la somma delle molteplicità delle radici è $\leq n$. [Suggerimento: ragionare come nella dimostrazione del corollario 28.12.]

28.8 (PRINCIPIO DI IDENTITÀ DEI POLINOMI). Siano f, g due polinomi a coefficienti in un campo F . Si provi che se esiste un sottoinsieme infinito $A \subseteq F$ tale che $f(a) = g(a)$ per ogni $a \in A$, allora $f = g$. [Suggerimento: considerare le radici di $f - g$.]

28.9. Se $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in F[x]$ è un polinomio a coefficienti in un campo F , definiamo la *derivata (formale)* di f come il polinomio $f' = a_1 + 2a_2x + 3a_3x^2 + \dots + na_nx^{n-1} \in F[x]$. (Attenzione: se il campo ha caratteristica p e $p \mid i$, allora $ia_i = 0$ in F ; quindi ad esempio la derivata del polinomio $x^{p^2} + x^p - x + \bar{2} \in \mathbb{Z}_p[x]$ è $-\bar{1}$.) Si provi che $(f + g)' = f' + g'$, $(fg)' = f'g + fg'$ e $(f^n)' = nf^{n-1}f'$ per ogni $f, g \in F[x]$ e ogni $n \geq 1$ intero.

28.10. Sia $f \in F[x]$ e sia $\alpha \in F$. Si provi che α è radice di f di molteplicità ≥ 2 se e solo se α è radice sia di f che di f' . [Suggerimento: Si ha $f = (x - \alpha)q$, da cui $f' = q + (x - \alpha)q'$. Quindi $f'(\alpha) = 0$ se e solo se $q(\alpha) = 0$.]

28.11. Siano F un campo di caratteristica zero, $f \in F[x]$, $\alpha \in F$ e d un intero positivo. Si dimostri che α è radice di f di molteplicità $\geq d$ se e solo se $f(\alpha) = 0$ e α è radice di f' di molteplicità $\geq d - 1$. [Suggerimento: (\Leftarrow) induzione su $d \geq 1$.]

28.12. Se $f \in F[x]$, definiamo le derivate successive di f ponendo $f'' = (f')'$, $f''' = (f'')'$, ..., $f^{(d)} = (f^{(d-1)})'$. Siano F un campo di caratteristica zero, $f \in F[x]$, $\alpha \in F$ e d un intero positivo. Si dimostri che α è radice di f di molteplicità $\geq d$ se e solo se α è radice contemporaneamente di $f, f', f'', \dots, f^{(d-1)}$. [Suggerimento: induzione su $d \geq 1$ ed esercizio precedente.]

28.13. Si dimostri che quanto asserito nei due esercizi 28.11 e 28.12 non vale in caratteristica diversa da zero. [Suggerimento: prendere un primo p , $F = \mathbb{Z}/p\mathbb{Z}$, $f = (x - 1)^p$, $\alpha = 1$ e $d > p$.]

§29. Serie di potenze, relazioni di ricorrenza e funzioni generatrici

Sia F un campo. Una *serie formale di potenze* (nell'indeterminata x a coefficienti in F) è un'espressione del tipo

$$a_0 + a_1x + a_2x^2 + \cdots = \sum_{n \geq 0} a_n x^n$$

dove gli a_n sono elementi di F . L'elemento $a_0 \in F$ è detto il *termine costante* della serie. Anche le serie, come i polinomi, si indicano in genere con simboli del tipo f, g o con $f(x), g(x)$. Due serie formali $\sum_{n \geq 0} a_n x^n$ e $\sum_{n \geq 0} b_n x^n$ a coefficienti in F sono uguali se e solo se $a_n = b_n$ per ogni $n \geq 0$.

Sia $F[[x]]$ l'insieme di tutte le serie formali nell'indeterminata x a coefficienti in F . Nell'insieme

$$F[[x]] = \left\{ \sum_{n \geq 0} a_n x^n \mid a_n \in F \text{ per ogni } n \geq 0 \right\}$$

definiamo due operazioni $+$ e \cdot ponendo

$$\left(\sum_{n \geq 0} a_n x^n \right) + \left(\sum_{n \geq 0} b_n x^n \right) = \sum_{n \geq 0} (a_n + b_n) x^n$$

e

$$\left(\sum_{n \geq 0} a_n x^n \right) \cdot \left(\sum_{n \geq 0} b_n x^n \right) = \sum_{n \geq 0} c_n x^n$$

dove

$$c_n = \sum_{i=0}^n a_i b_{n-i}.$$

È possibile dimostrare, anche se non è banalissimo, che $F[[x]]$ con queste due operazioni è un anello commutativo con identità, detto l'*anello delle serie formali nell'indeterminata x a coefficienti in F* .

29.1 ESEMPIO. Se $f = f(x) = \sum_{n \geq 0} a_n x^n$ è un elemento invertibile nell'anello $F[[x]]$ denoteremo il suo inverso con le notazioni f^{-1} o $f(x)^{-1}$ o anche con le notazioni più consuete $\frac{1}{f(x)}$ o $\frac{1}{f}$. Dimostriamo che per ogni $f \in F[[x]]$ la serie $1 - xf$ è invertibile in $F[[x]]$ e che

$$(29.1) \quad \frac{1}{1 - xf} = \sum_{n \geq 0} (xf)^n.$$

Si osservi che nella somma che appare nel termine a destra di questa formula abbiamo scritto una somma di infiniti addendi. Questo non ha in generale alcun significato in

un anello arbitrario, perché in un anello arbitrario è definita la somma di due addendi, e quindi, per induzione e grazie alla proprietà associativa, è definita la somma di un qualunque numero finito di addendi, ma non la somma di infiniti addendi. Nel caso in questione però si osservi che la serie $(xf)^n$ ha i primi n coefficienti tutti uguali a zero, e quindi per ogni $i \geq 0$ il coefficiente di x^i negli addendi $(xf)^n$ è zero per ogni $n > i$. Quindi il calcolo del coefficiente di x^i nella somma $\sum_{n \geq 0} (xf)^n$ involve solo un numero finito di addendi, e pertanto nel caso in questione la scrittura $\sum_{n \geq 0} (xf)^n$ ha senso.

Per verificare ora l'uguaglianza (29.1), ossia che $\sum_{n \geq 0} (xf)^n$ è l'inverso di $1 - xf$, si deve verificare che il loro prodotto è 1. La verifica è molto semplice:

$$(1 - xf) \left(\sum_{n \geq 0} (xf)^n \right) = \sum_{n \geq 0} (xf)^n - \sum_{n \geq 0} (xf)^{n+1} = 1.$$

Come caso particolare importante si osservi che l'inverso di $1 - x$ è la serie

$$\frac{1}{1 - x} = \sum_{n \geq 0} x^n = 1 + x + x^2 + x^3 + \dots,$$

detta la *serie geometrica*. \square

29.2 ESEMPIO. Una serie $f = \sum_{n \geq 0} a_n x^n \in F[[x]]$ è invertibile nell'anello $F[[x]]$ se e solo se $a_0 \neq 0$.

Infatti se $f = \sum_{n \geq 0} a_n x^n$ è una serie invertibile e $g = \sum_{n \geq 0} b_n x^n \in F[[x]]$ è il suo inverso, confrontando i termini costanti nell'uguaglianza $fg = 1$ si ricava che $a_0 b_0 = 1$, e quindi $a_0 \neq 0$. Viceversa se $a_0 \neq 0$, allora $a_0^{-1} \in F$ e si ha che $a_0^{-1} f = 1 - xh$ dove $h = \sum_{n \geq 1} a_0^{-1} a_n x^{n-1}$. Per l'esempio precedente $a_0^{-1} f$ è invertibile in $F[[x]]$, e quindi anche f è invertibile. \square

Nell'esempio 29.1 si è visto che nell'anello $F[[x]]$ è possibile fare una somma di infinite serie purché non si sommino mai infiniti elementi del campo F . Facciamo un altro esempio. Date due serie $h = \sum_{n \geq 0} a_n x^n$ e $g = \sum_{n \geq 0} b_n x^n \in F[[x]]$, se g ha termine costante $b_0 = 0$, è possibile definire la serie

$$(29.2) \quad h(g) = \sum_{n \geq 0} a_n g^n$$

detta la *serie ottenuta sostituendo x con g in h*. Infatti, dato che $b_0 = 0$, la serie g^n ha i coefficienti di x^0, x^1, \dots, x^{n-1} tutti nulli e quindi nella somma (29.2) i coefficienti della potenza x^i in g^n sono tutti nulli per ogni $n > i$. Nell'esempio 29.1 si era sostituito x con la serie xf nella serie geometrica $h = \sum_{n \geq 0} x^n$.

La *derivata formale* di una serie $f = \sum_{n \geq 0} a_n x^n$ è per definizione la serie

$$\sum_{n \geq 1} n a_n x^{n-1}.$$

La si denota con f' , con $f'(x)$, con $\frac{df}{dx}$ o con $\frac{d}{dx} f(x)$. Valgono anche per questa derivata formale le regole per la derivata di una somma, di un prodotto e di un'applicazione

composta che il lettore ha incontrato nel corso di Analisi matematica, ossia

$$\frac{d(f+g)}{dx} = \frac{df}{dx} + \frac{dg}{dx}, \quad \frac{d(fg)}{dx} = \frac{df}{dx}g + f\frac{dg}{dx}$$

per ogni $f, g \in F[[x]]$, e, nel caso in cui g abbia termine costante nullo, $\frac{df(g)}{dx} = f'(g)g'$ (si veda l'esercizio 29.1). Se inoltre il campo F ha caratteristica 0, per ogni $f \in F[[x]]$ si ha $f' = 0$ se e solo se $f \in F$, e, per ogni $f, g \in F[[x]]$ si ha $f' = g'$ se e solo se $f = g + c$ per qualche $c \in F$. In tutto il resto di questo §29 supporremo sempre che il campo F abbia caratteristica 0. Ha allora senso dividere in F per ogni numero intero positivo, e quindi si possono definire due serie particolari, dette l'*esponenziale* e il *logaritmo*:

$$\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!} \quad \text{e} \quad \log(1+x) = \sum_{n \geq 1} \frac{(-1)^{n-1} x^n}{n}.$$

29.3 ESEMPIO. Dimostriamo che $\frac{d}{dx} \exp(x) = \exp(x)$ e $\frac{d}{dx} \log(1+x) = \frac{1}{1+x}$. Si ha

$$\frac{d}{dx} \exp(x) = \frac{d}{dx} \left(\sum_{n \geq 0} \frac{x^n}{n!} \right) = \sum_{n \geq 1} n \frac{1}{n!} x^{n-1} = \sum_{n \geq 1} \frac{1}{(n-1)!} x^{n-1} = \exp(x)$$

e

$$\begin{aligned} \frac{d}{dx} \log(1+x) &= \frac{d}{dx} \left(\sum_{n \geq 1} \frac{(-1)^{n-1} x^n}{n} \right) = \sum_{n \geq 1} n \frac{(-1)^{n-1}}{n} x^{n-1} \\ &= \sum_{n \geq 1} (-x)^{n-1} = \sum_{n \geq 0} (-x)^n = \frac{1}{1+x} \end{aligned}$$

per l'esempio 29.1. \square

29.4 ESEMPIO. Vedremo negli esercizi 29.6 e 29.7 che

- (a) $\exp(-x) = 1/\exp(x)$;
- (b) $\exp(\log(1+x)) = 1+x$. \square

Per ogni $\alpha \in F$ definiamo $(1+x)^\alpha = \exp(\alpha \log(1+x))$. Ad esempio $(1+x)^1 = 1+x$, $(1+x)^0 = 1$ e

$$(1+x)^{-1} = \exp(-\log(1+x)) = \frac{1}{\exp(\log(1+x))} = \frac{1}{1+x}.$$

Si vede facilmente (esercizio 29.2) che si ha

$$(1+x)^\alpha (1+x)^\beta = (1+x)^{\alpha+\beta}$$

per ogni $\alpha, \beta \in F$. Inoltre

$$\begin{aligned} (29.3) \quad \frac{d}{dx} (1+x)^\alpha &= \frac{d}{dx} \exp(\alpha \log(1+x)) = \exp(\alpha \log(1+x)) \alpha \frac{d}{dx} \log(1+x) \\ &= (1+x)^\alpha \alpha \frac{1}{1+x} = \alpha (1+x)^{\alpha-1}. \end{aligned}$$

Per ogni $\alpha \in F$ e ogni $n \in \mathbb{N}$ definiamo il coefficiente binomiale $\binom{\alpha}{n}$ mediante la formula

$$\binom{\alpha}{n} = \frac{\alpha(\alpha - 1) \cdots (\alpha - n + 1)}{n!}$$

(si ha $\binom{\alpha}{0} = 1$ per $n = 0$).

29.5 PROPOSIZIONE (SERIE BINOMIALE). *Si ha*

$$(1+x)^\alpha = \sum_{n \geq 0} \binom{\alpha}{n} x^n.$$

Si osservi che se α è un intero positivo, allora $\binom{\alpha}{n} = 0$ per ogni $n > \alpha$, e quindi la formula della proposizione 29.5 si riduce alla formula del binomio (proposizione 9.14).

Dimostrazione. Per ogni $\alpha \in F$ poniamo $f_\alpha = \sum_{n \geq 0} \binom{\alpha}{n} x^n$. Allora

$$\frac{d}{dx} f_\alpha = \sum_{n \geq 1} n \binom{\alpha}{n} x^{n-1}.$$

Ma

$$n \binom{\alpha}{n} = n \frac{\alpha(\alpha - 1) \cdots (\alpha - n + 1)}{n!} = \frac{\alpha(\alpha - 1) \cdots (\alpha - n + 1)}{(n-1)!} = \alpha \binom{\alpha - 1}{n-1},$$

e quindi

$$(29.4) \quad \frac{d}{dx} f_\alpha = \sum_{n \geq 1} \alpha \binom{\alpha - 1}{n-1} x^{n-1} = \alpha \sum_{m \geq 0} \binom{\alpha - 1}{m} x^m = \alpha f_{\alpha-1}.$$

Dato che

$$\begin{aligned} \binom{\alpha - 1}{n} + \binom{\alpha - 1}{n-1} &= \frac{(\alpha - 1)(\alpha - 2) \cdots (\alpha - n)}{n!} + \frac{(\alpha - 1)(\alpha - 2) \cdots (\alpha - n + 1)}{(n-1)!} \\ &= \frac{(\alpha - 1)(\alpha - 2) \cdots (\alpha - n + 1)}{(n-1)!} \left(\frac{\alpha - n}{n} + 1 \right) \\ &= \frac{(\alpha - 1)(\alpha - 2) \cdots (\alpha - n + 1)}{(n-1)!} \cdot \frac{\alpha}{n} = \binom{\alpha}{n} \end{aligned}$$

per ogni $n \geq 1$, si ha

$$\sum_{n \geq 1} \binom{\alpha - 1}{n} x^n + \sum_{n \geq 1} \binom{\alpha - 1}{n-1} x^n = \sum_{n \geq 1} \binom{\alpha}{n} x^n,$$

ossia $(f_{\alpha-1} - 1) + xf_{\alpha-1} = f_\alpha - 1$, vale a dire $f_{\alpha-1} = \frac{1}{1+x} f_\alpha$. Dalla (29.4) si ricava allora che $\frac{d}{dx} f_\alpha = \frac{\alpha}{1+x} f_\alpha$. Da questa e dalla (29.3) si ha che la derivata della serie

$f_\alpha \cdot (1+x)^{-\alpha}$ è

$$\begin{aligned} \frac{d}{dx} f_\alpha \cdot (1+x)^{-\alpha} + f_\alpha \cdot \frac{d}{dx} (1+x)^{-\alpha} &= \frac{\alpha}{1+x} f_\alpha \cdot (1+x)^{-\alpha} + f_\alpha \cdot (-\alpha)(1+x)^{-\alpha-1} \\ &= f_\alpha \cdot (1+x)^{-\alpha} \left(\frac{\alpha}{1+x} - \alpha(1+x)^{-1} \right) = 0. \end{aligned}$$

Quindi la serie $f_\alpha \cdot (1+x)^{-\alpha}$ è costante, vale a dire $f_\alpha \cdot (1+x)^{-\alpha} = c$ per qualche $c \in F$. Il termine costante di f_α è $\binom{\alpha}{0} = 1$ e il termine costante di $(1+x)^{-\alpha}$ è 1. Quindi il termine costante di $f_\alpha \cdot (1+x)^{-\alpha}$ è 1, cioè $c = 1$. Da $f_\alpha \cdot (1+x)^{-\alpha} = 1$, moltiplicando per $(1+x)^\alpha$ si trova che $f_\alpha = (1+x)^\alpha$, come desiderato. \square

Vogliamo ora applicare le serie formali allo studio delle successioni a_0, a_1, a_2, \dots di elementi a_n appartenenti ad un campo F . A volte può capitare di dover definire una successione a_0, a_1, a_2, \dots mediante una *relazione di ricorrenza*, ossia di definire a_n supponendo noti a_0, a_1, \dots, a_{n-1} . Ad esempio, fissiamo un elemento $a \in F$ e consideriamo la successione a_0, a_1, a_2, \dots definita da $a_0 = a$ e $a_n = -a_{n-1}$ per ogni numero naturale $n > 0$. In questo facile esempio è chiaro che a successione cercata è la successione definita da $a_n = a(-1)^n$ per ogni $n \in \mathbb{N}$. Ma vediamo un altro modo di calcolare gli elementi a_n . Associamo alla successione a_0, a_1, a_2, \dots la serie

$$(29.5) \quad f = \sum_{n \geq 0} a_n x^n \in F[[x]],$$

detta la *funzione generatrice* della successione a_0, a_1, a_2, \dots . In questo modo si associa ad ogni successione di elementi di F un'unica serie appartenente a $F[[x]]$ e, viceversa, ogni serie appartenente a $F[[x]]$ resta associata ad un'unica successione di elementi di F . In altre parole, abbiamo definito una biiezione tra l'insieme delle successioni di elementi di F e $F[[x]]$. Dalla relazione di ricorrenza $a_n = -a_{n-1}$, segue che $a_n x^n = -a_{n-1} x^n$ per ogni numero naturale $n > 0$, e quindi $\sum_{n>0} a_n x^n = -\sum_{n>0} a_{n-1} x^n$. Il termine a sinistra in questa uguaglianza è $f - a_0$ e il termine a destra è $-\sum_{n>0} a_{n-1} x^n = -x \sum_{n>0} a_{n-1} x^{n-1} = -x \sum_{m \geq 0} a_m x^m = -xf$. Dato che $a_0 = a$, si ha quindi $f - a = -xf$. Ne segue che $(1+x)f = a$, e quindi nell'anello $F[[x]]$ si ha $f = a/(1+x) = a \sum_{n \geq 0} (-x)^n$ per quanto visto nell'esempio 29.1. Pertanto $f = \sum_{n \geq 0} a(-1)^n x^n$. Dalla definizione di f (equazione (29.5)) ricaviamo allora che $a_n = a(-1)^n$ per ogni $n \in \mathbb{N}$. Nel resto di questo §29 vedremo numerosi altri esempi di impiego delle funzioni generatrici per determinare successioni a_0, a_1, a_2, \dots di elementi di un campo F .

Numeri di Fibonacci

I numeri che studieremo ora furono introdotti da Leonardo Fibonacci¹ all'inizio del XIII secolo per studiare il seguente problema. Supponiamo di avere una coppia di conigli A e di sapere che a ogni coppia di conigli è necessario un primo mese di vita per divenire fertile, e che poi ad ogni mese successivo ogni coppia di conigli dà alla luce un'altra coppia

¹ Detto anche Leonardo Pisano perché era di Pisa, ma il cui cognome era probabilmente Bigollo.

di conigli. Quante coppie di conigli si avranno dopo n mesi? Vediamo di quali dati disponiamo. Il primo mese abbiamo solo la nostra coppia iniziale di conigli A . Il secondo mese la coppia A è ancora troppo giovane per avere figli, e quindi si ha ancora un'unica coppia di conigli. Il terzo mese alla coppia A si aggiunge la coppia B dei loro figli, e quindi si hanno due coppie. Il quarto mese la coppia A ha un'altra coppia di figli, mentre la coppia B è ancora troppo giovane per averne, e quindi in tutto si hanno tre coppie. Si noti che in questo modello matematico abbiamo volutamente introdotto numerosi semplificazioni, ad esempio supponendo che la nascita dei conigli avvenga sempre in modo così regolare, che nessun coniglio muoia mai e che ogni coppia di conigli generi sempre un coniglio maschio e un coniglio femmina.

In generale ad ogni mese successivo ai primi due si hanno tante coppie di conigli quante ce n'erano il mese precedente più un numero di coppie neonate pari a quante erano le coppie due mesi prima. Se denotiamo con F_n il numero di coppie che si hanno nell' n -esimo mese si ha quindi che $F_n = F_{n-1} + F_{n-2}$ per ogni $n > 2$, oltre alle *condizioni iniziali* $F_1 = 1$ e $F_2 = 1$. I numeri F_n si dicono i *numeri di Fibonacci*. Possiamo porre anche $F_0 = 0$, di modo che la relazione $F_n = F_{n-1} + F_{n-2}$ vale anche per $n = 2$. Abbiamo così visto che

29.6 PROPOSIZIONE. *La relazione di ricorrenza per i numeri di Fibonacci F_n è*

$$F_n = F_{n-1} + F_{n-2} \quad \text{per ogni } n \geq 2.$$

I primi numeri di Fibonacci F_0, F_1, F_2, \dots sono $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$

Vediamo ora di calcolare i numeri F_n mediante il metodo delle funzioni generatrici esposto sopra. Consideriamo la funzione generatrice $f = \sum_{n \geq 0} F_n x^n \in \mathbb{R}[[x]]$.

29.7 PROPOSIZIONE. *La funzione generatrice dei numeri di Fibonacci F_n è*

$$f = \frac{x}{1 - x - x^2}.$$

Dimostrazione. Da $F_n = F_{n-1} + F_{n-2}$ per ogni $n \geq 2$, segue che $F_n x^n = F_{n-1} x^n + F_{n-2} x^n$, e quindi, sommando,

$$(29.6) \quad \sum_{n \geq 2} F_n x^n = \sum_{n \geq 2} F_{n-1} x^n + \sum_{n \geq 2} F_{n-2} x^n.$$

Ora si ha

$$\begin{aligned} \sum_{n \geq 2} F_n x^n &= f - F_0 - F_1 x = f - x, \\ \sum_{n \geq 2} F_{n-1} x^n &= x \sum_{n \geq 2} F_{n-1} x^{n-1} = x(f - F_0) = xf \end{aligned}$$

e

$$\sum_{n \geq 2} F_{n-2} x^n = x^2 \sum_{n \geq 2} F_{n-2} x^{n-2} = x^2 f,$$

e quindi dalla (29.6) si ricava che $f - x = xf + x^2 f$, ossia $(1 - x - x^2)f = x$, da cui $f = x/(1 - x - x^2)$. \square

Dalla funzione generatrice ricaveremo ora un'espressione per i numeri di Fibonacci F_n .

29.8 PROPOSIZIONE. Siano $\alpha = \frac{1 + \sqrt{5}}{2}$, $\beta = \frac{1 - \sqrt{5}}{2}$. Per i numeri di Fibonacci F_n si ha

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

per ogni $n \geq 0$.

Dimostrazione. Scriviamo la frazione $x/(1 - x - x^2)$ nella forma

$$(29.7) \quad \frac{x}{1 - x - x^2} = \frac{ax}{1 - \alpha x} + \frac{bx}{1 - \beta x},$$

ossia determiniamo $a, b, \alpha, \beta \in \mathbb{R}$ per i quali valga la (29.7). Si ha

$$\frac{ax}{1 - \alpha x} + \frac{bx}{1 - \beta x} = \frac{ax(1 - \beta x) + bx(1 - \alpha x)}{(1 - \alpha x)(1 - \beta x)} = \frac{(a + b)x - (a\beta + b\alpha)x^2}{1 - (\alpha + \beta)x + \alpha\beta x^2}.$$

Quindi affinché valga la (29.7) è sufficiente che a, b, α, β siano soluzioni del sistema

$$\begin{cases} a + b = 1 \\ a\beta + b\alpha = 0 \\ \alpha + \beta = 1 \\ \alpha\beta = -1. \end{cases}$$

Dalle ultime due equazioni del sistema si vede che α e β sono le soluzioni dell'equazione $x^2 - x - 1 = 0$. Come soluzioni di questa equazione prendiamo $\alpha = (1 + \sqrt{5})/2$ e $\beta = (1 - \sqrt{5})/2$. Sostituendo questi valori nelle prime due equazioni del sistema si trova un sistema di due equazioni lineari la cui soluzione è $a = \frac{\sqrt{5} + 1}{2\sqrt{5}}, b = \frac{\sqrt{5} - 1}{2\sqrt{5}}$. Ma allora nell'anello $\mathbb{R}[[x]]$ si ha che

$$\begin{aligned} f &= \frac{x}{1 - x - x^2} = \frac{ax}{1 - \alpha x} + \frac{bx}{1 - \beta x} \\ &= ax \sum_{n \geq 0} (\alpha x)^n + bx \sum_{n \geq 0} (\beta x)^n = \sum_{n \geq 0} (a\alpha^n + b\beta^n) x^{n+1}, \end{aligned}$$

e quindi $F_{n+1} = a\alpha^n + b\beta^n$ per ogni $n \geq 0$. Per ogni $n \geq 1$ si ha pertanto che

$$F_n = a\alpha^{n-1} + b\beta^{n-1} = \frac{a}{\alpha} \alpha^n + \frac{b}{\beta} \beta^n = \frac{\alpha^n - \beta^n}{\sqrt{5}}. \quad \square$$

Abbiamo così visto quanto risulta utile associare ad ogni successione a_0, a_1, a_2, \dots la funzione generatrice $\sum_{n \geq 0} a_n x^n$. A volte può capitare che la successione a_0, a_1, a_2, \dots sia nulla da un certo punto in poi, ossia che esista $N \in \mathbb{N}$ tale che $a_n = 0$ per ogni $n > N$. In tal caso la funzione generatrice è ovviamente un polinomio di grado $\leq N$. Vediamo un esempio.

29.9 ESEMPIO. Si supponga di avere n oggetti uguali tra loro e di volerli distribuire in tre scatole etichettate con 1, 2 e 3 in modo che in ogni scatola ci siano almeno due ma non più di otto oggetti. Si calcoli in quanti modi si possono distribuire gli n oggetti nelle tre scatole.

Il problema è equivalente al seguente. Sia $n \in \mathbb{N}$. Si calcoli quante sono le soluzioni $(m_1, m_2, m_3) \in \mathbb{N}^3$ del sistema

$$\begin{cases} m_1 + m_2 + m_3 = n \\ 2 \leq m_i \leq 8 \end{cases} \quad \text{per ogni } i = 1, 2, 3.$$

Sia a_n il numero di modi cercato per ogni $n \in \mathbb{N}$. Se calcoliamo il coefficiente di x^n nel prodotto

$$(x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \cdot (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \cdot (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8)$$

troviamo che il coefficiente di x^n si incrementa di uno per ogni prodotto $x^i x^j x^k$ con $i + j + k = n$. In altre parole, il coefficiente di x^n nel prodotto

$$(x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \cdot (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \cdot (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8) = (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8)^3$$

è esattamente uguale al numero a_n di modi cercato. Quindi $(x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8)^3$ è la funzione generatrice della successione a_0, a_1, a_2, \dots \square

Relazioni di ricorrenza lineari

Sia a_0, a_1, a_2, \dots una successione ad elementi in un campo F . Una relazione di ricorrenza del tipo

$$a_n = c_1(n)a_{n-1} + c_2(n)a_{n-2} + \cdots + c_k(n)a_{n-k},$$

dove k è un intero positivo e c_1, c_2, \dots, c_k sono applicazioni di \mathbb{N} in F , si dice una *relazione di ricorrenza lineare ($k+1$ termini)*. Si dice una relazione di ricorrenza lineare a *coefficienti costanti* se le applicazioni c_1, c_2, \dots, c_k sono costanti, ossia sono elementi di F . Ad esempio la successione costantemente nulla $0, 0, 0, \dots$, ossia la successione a_0, a_1, a_2, \dots in cui $a_n = 0$ per ogni $n \in \mathbb{N}$, soddisfa ogni relazione di ricorrenza lineare.

Osserviamo che data una relazione di ricorrenza lineare a $k+1$ termini

$$(29.8) \quad a_n = c_1(n)a_{n-1} + c_2(n)a_{n-2} + \cdots + c_k(n)a_{n-k}$$

per ogni $n \geq k$ e k elementi $a_0, a_1, \dots, a_{k-1} \in F$, esiste un'unica successione a_0, a_1, a_2, \dots di elementi di F soddisfacente la relazione di ricorrenza i cui primi valori siano proprio i k elementi a_0, a_1, \dots, a_{k-1} di F fissati. Infatti una volta stabiliti i primi k valori

a_0, a_1, \dots, a_{k-1} , la relazione di ricorrenza determina a_k , e quindi anche a_{k+1} , e così via. Chiamiamo i valori fissati per a_0, a_1, \dots, a_{k-1} le *condizioni iniziali*.²

Vediamo ora come si determinano tutte le successioni a_0, a_1, a_2, \dots soddisfacenti una relazione di ricorrenza lineare a coefficienti costanti

$$(29.9) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

dove $c_1, c_2, \dots, c_k \in F$. Ad esempio per i numeri di Fibonacci si aveva la relazione di ricorrenza lineare a 3 termini a coefficienti costanti $a_n = a_{n-1} + a_{n-2}$ per $n \geq 2$. Osserviamo intanto che se t successioni

$$a_{1,n}, \quad n = 0, 1, 2, 3, \dots,$$

$$a_{2,n}, \quad n = 0, 1, 2, 3, \dots,$$

$$a_{3,n}, \quad n = 0, 1, 2, 3, \dots,$$

 \vdots

$$a_{t,n}, \quad n = 0, 1, 2, 3, \dots,$$

sono tutte soluzioni della (29.9) e se $\lambda_1, \lambda_2, \dots, \lambda_t \in F$, anche la successione

$$b_n = \lambda_1 a_{1,n} + \lambda_2 a_{2,n} + \cdots + \lambda_t a_{t,n}, \quad n = 0, 1, 2, 3, \dots,$$

è una soluzione della (29.9), in quanto

$$\begin{aligned} b_n &= \sum_{i=1}^t \lambda_i a_{i,n} = \sum_{i=1}^t \lambda_i (c_1 a_{i,n-1} + c_2 a_{i,n-2} + \cdots + c_k a_{i,n-k}) \\ &= \sum_{i=1}^t (\lambda_1 c_1 a_{i,n-1} + \lambda_2 c_2 a_{i,n-2} + \cdots + \lambda_t c_k a_{i,n-k}) \\ &= c_1 b_{n-1} + c_2 b_{n-2} + \cdots + c_k b_{n-k}. \end{aligned}$$

Per i numeri di Fibonacci, ad esempio, si erano trovate delle soluzioni del tipo $a_n = \lambda_1 \alpha^n + \lambda_2 \beta^n$. Cerchiamo quindi una soluzione della (29.9) del tipo $a_n = \alpha^n$ per ogni $n \in \mathbb{N}$ dove $\alpha \in F$. Per $\alpha = 0$ si ha la soluzione nulla $a_n = 0$ per ogni $n \in \mathbb{N}$, e quindi possiamo supporre $\alpha \neq 0$. Un elemento $\alpha \neq 0$ è tale che la successione $a_n = \alpha^n$ per ogni $n \in \mathbb{N}$ è una soluzione della (29.9) se e solo se $\alpha^n = c_1 \alpha^{n-1} + c_2 \alpha^{n-2} + \cdots + c_k \alpha^{n-k}$ per ogni $n \geq k$, e quindi se e solo se $\alpha^k = c_1 \alpha^{k-1} + c_2 \alpha^{k-2} + \cdots + c_{k-1} \alpha + c_k$, ossia se e solo se α è una soluzione dell'equazione $x^k = c_1 x^{k-1} + c_2 x^{k-2} + \cdots + c_{k-1} x + c_k$, detta l'*equazione caratteristica* della relazione di ricorrenza. Se il polinomio $x^k - c_1 x^{k-1} - c_2 x^{k-2} - \cdots - c_{k-1} x - c_k$ ha k radici distinte $\alpha_1, \alpha_2, \dots, \alpha_k \in F$, allora ogni successione $a_{i,n} = \alpha_i^n$, $n = 0, 1, 2, \dots$, è una soluzione della (29.9), e quindi anche la successione $a_n = \lambda_1 \alpha_1^n + \lambda_2 \alpha_2^n + \cdots + \lambda_k \alpha_k^n$ è una

²In certi problemi si vuole determinare invece una successione a_1, a_2, a_3, \dots di elementi di F soddisfacente a una relazione di ricorrenza lineare a $k+1$ termini come la (29.8). In tal caso le k condizioni iniziali necessarie per determinare univocamente la successione consistono nel fissare i valori di $a_1, a_2, a_3, \dots, a_k$.

soluzione della (29.9) per ogni $\lambda_1, \lambda_2, \dots, \lambda_k \in F$. Ad esempio per i numeri di Fibonacci la relazione di ricorrenza era la $a_n = a_{n-1} + a_{n-2}$ per $n \geq 2$. L'equazione caratteristica è quindi $x^2 = x + 1$, le cui soluzioni sono $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$. Ogni successione a_0, a_1, a_2, \dots di elementi di \mathbb{R} del tipo $a_n = \lambda_1 \alpha^n + \lambda_2 \beta^n$ soddisfa quindi la relazione di ricorrenza $a_n = a_{n-1} + a_{n-2}$. Se invece il polinomio $x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_{k-1} x - c_k$ ha una radice α di molteplicità $d > 1$, sarebbe possibile dimostrare (ma non è immediato e quindi lo tralasciamo) che le d successioni

$$\begin{aligned} a_{1,n} &= \alpha^n, & n &= 0, 1, 2, 3, \dots, \\ a_{2,n} &= n\alpha^n, & n &= 0, 1, 2, 3, \dots, \\ &\vdots \\ a_{d,n} &= n^{d-1}\alpha^n, & n &= 0, 1, 2, 3, \dots, \end{aligned}$$

sono tutte soluzioni della (29.9). Anzi è possibile dimostrare che se F è il campo \mathbb{C} dei numeri complessi, per ogni polinomio $f \in \mathbb{C}[x]$ di grado k la somma delle molteplicità delle radici di f è k (confronta esercizio 28.7 e §46). Se $\alpha_1, \alpha_2, \dots, \alpha_p$ sono le radici distinte del polinomio $x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_{k-1} x - c_k$ e le loro molteplicità sono rispettivamente d_1, d_2, \dots, d_p , si ha quindi che $d_1 + d_2 + \dots + d_p = k$. Le successioni a_0, a_1, a_2, \dots in \mathbb{C} che soddisfano la relazione di ricorrenza lineare a coefficienti costanti (29.9) sono tutte e sole le successioni del tipo $\lambda_1 a_{1,n} + \lambda_2 a_{2,n} + \dots + \lambda_k a_{k,n}$, $n = 0, 1, 2, 3, \dots$, dove $\lambda_1, \lambda_2, \dots, \lambda_k \in \mathbb{C}$ e $a_{1,n}, a_{2,n}, \dots, a_{k,n}$ sono le successioni definite da $a_{i,n} =$

$$\begin{aligned} (29.10) \quad & \alpha_1^n, \quad n\alpha_1^n, \quad n^2\alpha_1^n, \quad \dots, \quad n^{d_1-1}\alpha_1^n \\ & \alpha_2^n, \quad n\alpha_2^n, \quad n^2\alpha_2^n, \quad \dots, \quad n^{d_2-1}\alpha_2^n \\ & \vdots \\ & \alpha_p^n, \quad n\alpha_p^n, \quad n^2\alpha_p^n, \quad \dots, \quad n^{d_p-1}\alpha_p^n \end{aligned}$$

per ogni $n \in \mathbb{N}$. Vedremo nel successivo capitolo di algebra lineare che questo si esprime dicendo che le successioni che soddisfano la relazione di ricorrenza sono tutte e sole le combinazioni lineari delle k successioni (29.10). La dimostrazione di quanto ora asserito viene tralasciata in quanto involve tecniche che sono al di fuori della portata del lettore al momento presente.

29.10 ESEMPIO. Calcoliamo la successione a_0, a_1, a_2, \dots di numeri razionali tale che $a_0 = a_1 = 0$, $\overset{\circ}{a}_2 = 2$ e

$$(29.11) \quad a_n = -4a_{n-1} - 5a_{n-2} - 2a_{n-3} \quad \text{per ogni } n \geq 3.$$

Determiniamo in primo luogo tutte le successioni a_0, a_1, a_2, \dots ad elementi in \mathbb{C} soddisfacenti la relazione di ricorrenza lineare (29.11). L'equazione caratteristica è la $x^3 = -4x^2 - 5x - 2$. Il polinomio $x^3 + 4x^2 + 5x + 2 = (x+2)(x+1)^2$ ha le due radici -2 e -1 di molteplicità 1 e 2 rispettivamente. Le successioni a_0, a_1, a_2, \dots ad elementi in \mathbb{C} soddisfacenti la relazione di ricorrenza (29.11) sono quindi tutte e sole quelle definite da

$a_n = \lambda_1(-2)^n + \lambda_2(-1)^n + \lambda_3n(-1)^n$ per ogni $n \in \mathbb{N}$ al variare di $\lambda_1, \lambda_2, \lambda_3$ in \mathbb{C} . Dalle condizioni iniziali $a_0 = a_1 = 0$ e $a_2 = 2$ segue che $\lambda_1, \lambda_2, \lambda_3$ devono soddisfare il sistema

$$\begin{cases} 0 = \lambda_1 + \lambda_2 \\ 0 = -2\lambda_1 - \lambda_2 - \lambda_3 \\ 2 = 4\lambda_1 + \lambda_2 + 2\lambda_3. \end{cases}$$

Risolvendo questo sistema si trova $\lambda_1 = 2$, $\lambda_2 = \lambda_3 = -2$, e quindi la successione a_n definita da $a_n = 2(-2)^n - 2(-1)^n - 2n(-1)^n = 2(2^n - 1 - n)(-1)^n$ per ogni $n \in \mathbb{N}$ è l'unica successione ad elementi in \mathbb{C} soddisfacente alla relazione di ricorrenza e alle condizioni iniziali date. Dato che questa successione ha elementi tutti razionali, è chiaro allora che tale successione a_n è l'unica successione ad elementi razionali che soddisfa alla relazione (29.11) e tale che $a_0 = a_1 = 0$ e $a_2 = 2$. \square

Numeri di Catalan

Passiamo ora a studiare una successione di numeri introdotti nel 1838 da Catalan per risolvere il seguente problema. Siano A un insieme e \cdot un'operazione non associativa su A . Se $a_1, a_2, \dots, a_n \in A$, scrivere il prodotto $a_1 a_2 \dots a_n$ non ha senso, in quanto il risultato della moltiplicazione dipende dall'ordine in cui vengono moltiplicati tra loro gli elementi. È indispensabile metterci le parentesi, e ci sono varie possibilità. Ad esempio per $n = 3$ ci sono le due possibilità $a_1(a_2a_3)$ e $(a_1a_2)a_3$, e per $n = 4$ ci sono le cinque possibilità $a_1(a_2(a_2a_3))$, $a_1((a_2a_3)a_4)$, $(a_1a_2)(a_3a_4)$, $(a_1(a_2a_3))a_4$ e $((a_1a_2)a_3)a_4$. Indichiamo con C_n il numero di modi in cui è possibile scrivere il prodotto, ossia il massimo numero possibile di differenti risultati della moltiplicazione di n elementi a_1, a_2, \dots, a_n di A , di modo che, come abbiamo visto, $C_3 = 2$, $C_4 = 5$, e, ovviamente, $C_1 = C_2 = 1$. Per calcolare i numeri C_n osserviamo che ogni possibile prodotto di a_1, a_2, \dots, a_n si scrive in modo unico nella forma pq , dove p è un prodotto in qualche ordine di a_1, a_2, \dots, a_i , e q è un prodotto in qualche ordine di $a_{i+1}, a_{i+2}, \dots, a_n$ (il prodotto pq è “l'ultimo prodotto che si esegue”). Qui i è un numero che può variare tra 1 e $n - 1$, $1 \leq i \leq n - 1$. Per ogni tale i esistono quindi C_i modi in cui si può scrivere p e C_{n-i} modi in cui si può scrivere q . Quindi in totale si hanno $C_i C_{n-i}$ modi in cui si può scrivere un tale pq . Al variare di i da 1 a $n - 1$, si trova che

29.11 PROPOSIZIONE. *La relazione di ricorrenza per i numeri di Catalan C_n è*

$$(29.12) \quad C_n = \sum_{i=1}^{n-1} C_i C_{n-i}$$

per ogni $n \geq 2$.

Si osservi che la relazione di ricorrenza (29.12) non è lineare. Calcoliamo i numeri di Catalan facendo uso delle funzioni generatrici.

29.12 PROPOSIZIONE. Si ha

$$C_n = \frac{1}{n} \binom{2n-2}{n-1}.$$

per ogni $n \geq 1$.

Dimostrazione. Consideriamo la funzione generatrice $f = \sum_{n \geq 0} C_n x^n$, dove abbiamo posto $C_0 = 0$. Dalla relazione di ricorrenza (29.12) si ha

$$C_n = \sum_{i=0}^n C_i C_{n-i}$$

per ogni $n \geq 2$, da cui

$$\sum_{n \geq 2} C_n x^n = \sum_{n \geq 2} \sum_{i=0}^n C_i C_{n-i} x^n.$$

Il termine a destra in questa uguaglianza è f^2 , e il termine a sinistra è $f - C_0 - C_1 x = f - x$. Quindi $f - x = f^2$. Se ne ricava che $f^2 - f + x = 0$, e risolvendo questa equazione di secondo grado si trova che deve essere

$$f = \frac{1 + \sqrt{1 - 4x}}{2} \quad \text{oppure} \quad f = \frac{1 - \sqrt{1 - 4x}}{2}.$$

Dato che il termine costante della serie f è $C_0 = 0$, il termine costante della serie $(1 + \sqrt{1 - 4x})/2$ è 1, e quello della serie $(1 - \sqrt{1 - 4x})/2$ è 0, la soluzione cercata è quella con il segno meno, ossia

$$f = \frac{1 - \sqrt{1 - 4x}}{2} = \frac{1}{2} \left(1 - (1 - 4x)^{\frac{1}{2}} \right).$$

Quindi dalla serie binomiale (proposizione 29.5) si ricava che

$$f = \frac{1}{2} \left(1 - \sum_{n \geq 0} \binom{\frac{1}{2}}{n} (-4x)^n \right).$$

Il coefficiente di x^n per $n \geq 1$ è

$$\begin{aligned} C_n &= -\frac{1}{2} \binom{\frac{1}{2}}{n} (-4)^n = -\frac{1}{2} \cdot \frac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-n+1)}{n!} (-4)^n \\ &= -\frac{(-1)(-3)\cdots(-(2n-3))}{2^{n+1}(n!)} (-4)^n. \end{aligned}$$

Dato che il prodotto di tutti i numeri dispari da 1 a $2n-3$ è $\frac{(2n-2)!}{2^{n-1}(n-1)!}$, se ne ricava che

$$C_n = -\frac{(-1)^{n-1}}{2^{n+1}(n!)} \cdot \frac{(2n-2)!}{2^{n-1}(n-1)!} (-1)^n 2^{2n} = \frac{(2n-2)!}{n!(n-1)!} = \frac{1}{n} \binom{2n-2}{n-1}. \quad \square$$

Numeri di Bell

Il numero di Bell B_n è il numero di partizioni di un qualunque insieme di cardinalità n (o equivalentemente, per $n \geq 1$, il numero di partizioni dell'insieme $X_n = \{1, 2, 3, \dots, n\}$). Ad esempio, c'è un'unica partizione dell'insieme $X_1 = \{1\}$ (è la $\{\{1\}\}$), e quindi $B_1 = 1$. Ci sono due partizioni dell'insieme $X_2 = \{1, 2\}$ (sono la $\{\{1, 2\}\}$ e la $\{\{1\}, \{2\}\}$), e quindi $B_2 = 2$. C'è un'unica partizione dell'insieme vuoto (la partizione vuota), e quindi $B_0 = 1$.

29.13 PROPOSIZIONE. *La relazione di ricorrenza per i numeri di Bell B_n è*

$$(29.13) \quad B_n = \sum_{i=1}^n \binom{n-1}{i-1} B_{n-i}$$

per ogni $n \geq 1$.

Dimostrazione. Fissata una partizione \mathcal{F} di $X_n = \{1, 2, 3, \dots, n\}$, il numero n appartiene ad un unico elemento A di \mathcal{F} . Quindi ogni partizione \mathcal{F} di X_n è univocamente determinata dall'elemento A di \mathcal{F} che contiene n e da una partizione di $X_n \setminus A$. Se A ha cardinalità i , si ha che $1 \leq i \leq n$ (perché A è un sottoinsieme non vuoto di X_n), A può essere scelto tra uno qualunque degli $\binom{n-1}{i-1}$ sottoinsiemi di X_n che contengono n , e la partizione di $X_n \setminus A$, essendo una partizione di un insieme di $n - i$ elementi, può essere scelta in B_{n-i} modi. Quindi per ogni i con $1 \leq i \leq n$ ci sono esattamente $\binom{n-1}{i-1} B_{n-i}$ partizioni di X_n per le quali n appartiene ad un elemento A di cardinalità i della partizione. In definitiva su X_n ci sono esattamente $\sum_{i=1}^n \binom{n-1}{i-1} B_{n-i}$ partizioni distinte. \square

Benché la relazione di ricorrenza (29.13) sia una relazione lineare tra i B_n , non si tratta di una relazione di ricorrenza lineare a $k + 1$ termini per nessun k , in quanto per calcolare B_n è necessario conoscere tutti i termini precedenti. Invece di calcolare la funzione generatrice $\sum_{n \geq 0} B_n x^n$, calcoliamo la serie

$$\sum_{n \geq 0} \frac{B_n}{n!} x^n \in \mathbb{R}[[x]],$$

detta la *funzione generatrice esponenziale* dei numeri di Bell. (In generale, data una successione a_0, a_1, a_2, \dots di elementi di un campo F , la serie

$$\sum_{n \geq 0} a_n x^n \in F[[x]],$$

si dice la funzione generatrice *ordinaria* della successione, mentre la serie

$$\sum_{n \geq 0} \frac{a_n}{n!} x^n \in F[[x]],$$

si dice la funzione generatrice *esponenziale* di a_0, a_1, a_2, \dots)

29.14 PROPOSIZIONE. *La funzione generatrice esponenziale dei numeri di Bell B_n è*

$$\sum_{n \geq 0} \frac{B_n}{n!} x^n = \exp(\exp(x) - 1).$$

Dimostrazione. Si consideri la serie $b = \sum_{n \geq 0} (B_n/n!)x^n$. La sua derivata è

$$b' = \sum_{n \geq 1} \frac{B_n}{n!} nx^{n-1},$$

e quindi, per la (29.13),

$$(29.14) \quad b' = \sum_{n \geq 1} \left(\sum_{i=1}^n \binom{n-1}{i-1} B_{n-i} \right) \frac{1}{(n-1)!} x^{n-1}.$$

D'altra parte

$$\exp(x) \cdot b = \left(\sum_{n \geq 0} \frac{x^n}{n!} \right) \left(\sum_{n \geq 0} \frac{B_n}{n!} x^n \right) = \sum_{m \geq 0} \sum_{j=0}^m \frac{1}{j!} \frac{B_{m-j}}{(m-j)!} x^m.$$

Ponendo $i = j + 1$, di modo che quando j varia da 0 a m si ha che i varia da 1 a $m + 1$, si trova che

$$\exp(x) \cdot b = \sum_{m \geq 0} \sum_{i=1}^{m+1} \frac{1}{(i-1)!} \frac{B_{m-i+1}}{(m-i+1)!} x^m.$$

Poniamo ora $n = m + 1$, di modo che quando m varia nei numeri naturali, n varia negli interi positivi. Si ha allora

$$\exp(x) \cdot b = \sum_{n \geq 1} \sum_{i=1}^n \frac{1}{(i-1)!} \frac{B_{n-i}}{(n-i)!} x^{n-1} = \sum_{n \geq 1} \sum_{i=1}^n \binom{n-1}{i-1} \frac{B_{n-i}}{(n-1)!} x^{n-1}.$$

Da questa e dalla (29.14) si vede che $b' = \exp(x) \cdot b$. Ne segue che la derivata della serie prodotto $\exp(1 - \exp(x)) \cdot b$ è 0, e quindi $\exp(1 - \exp(x)) \cdot b = c$ per qualche $c \in \mathbb{R}$. Il termine costante della serie $\exp(1 - \exp(x))$ è 1 e quello della serie b è $B_0 = 1$, e quindi deve essere $c = 1$. Moltiplicando l'uguaglianza $\exp(1 - \exp(x)) \cdot b = 1$ per l'inverso $\exp(\exp(x) - 1)$ di $\exp(1 - \exp(x))$ si trova che $b = \exp(\exp(x) - 1)$. \square

Permutazioni senza punti fissi

Una *permutazione senza punti fissi* è una permutazione σ dell'insieme $X_n = \{1, 2, \dots, n\}$ tale che $\sigma(i) \neq i$ per ogni $i = 1, 2, \dots, n$. Equivalentemente, data una permutazione σ di X_n , decomponiamo σ come prodotto di cicli disgiunti,

$$(29.15) \quad \circ \quad \sigma = (a_{11} a_{12} \dots a_{1d_1}) \circ (a_{21} a_{22} \dots a_{2d_2}) \circ \dots \circ (a_{k1} a_{k2} \dots a_{kd_k}),$$

di modo che σ risulta essere prodotto di k cicli di lunghezza d_1, d_2, \dots, d_k rispettivamente e $d_1 + \dots + d_k = n$; allora σ è senza punti fissi se e solo se tutti i d_1, d_2, \dots, d_k sono ≥ 2 .

29.15 PROPOSIZIONE. Sia s_n il numero di permutazioni senza punti fissi di $X_n = \{1, 2, \dots, n\}$. La relazione di ricorrenza per i numeri s_n è

$$(29.16) \quad s_{n+1} = n(s_n + s_{n-1}).$$

per ogni $n \geq 2$. Inoltre $s_1 = 0$ e $s_2 = 1$.

Dimostrazione. Le condizioni iniziali $s_1 = 0$ e $s_2 = 1$ sono ovvie. Supponiamo quindi $n \geq 2$ e calcoliamo s_{n+1} . Data una qualunque permutazione σ senza punti fissi di X_{n+1} e la sua decomposizione come prodotto di cicli disgiunti (29.15), possiamo supporre senza perdita di generalità che $a_{11} = n + 1$. Ne risulta che $a_{12}, a_{13}, \dots, a_{1d_1}$ sono completamente determinati da σ . Ripartiamo quindi l'insieme di tutte le permutazioni senza punti fissi di X_{n+1} in n sottoinsiemi disgiunti A_i , dove in A_i stanno tutte le permutazioni senza punti fissi di X_{n+1} tali che $a_{12} = i$. Ripartiamo ora ogni insieme A_i in 2 sottoinsiemi disgiunti B_i, C_i dove in B_i stanno tutte le permutazioni appartenenti ad A_i per le quali $d_1 = 2$, e in C_i stanno tutte le permutazioni appartenenti ad A_i per le quali $d_1 > 2$.

Le permutazioni in B_i sono quindi tutte e sole del tipo

$$\sigma = (n+1\ i) \circ (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{k1}a_{k2}\dots a_{kd_k}).$$

Ma allora $\sigma' = (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{k1}a_{k2}\dots a_{kd_k})$ è una permutazione senza punti fissi di $X_{n+1} \setminus \{i, n+1\}$, e anzi l'assegnazione $\sigma \mapsto \sigma'$ è una biiezione tra B_i e l'insieme di tutte le permutazioni senza punti fissi di $X_{n+1} \setminus \{i, n+1\}$. In particolare ogni B_i ha s_{n-1} elementi.

Le permutazioni in C_i sono invece tutte e sole del tipo

$$\sigma = (n+1\ i\ a_{13}\dots a_{1d_1}) \circ (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{k1}a_{k2}\dots a_{kd_k})$$

con $d_1 > 2$. Data una tale permutazione σ si vede che

$$\sigma'' = (i\ a_{13}\dots a_{1d_1}) \circ (a_{21}a_{22}\dots a_{2d_2}) \circ \dots \circ (a_{k1}a_{k2}\dots a_{kd_k})$$

è una permutazione senza punti fissi di $X_{n+1} \setminus \{n+1\} = X_n$, e anzi l'assegnazione $\sigma \mapsto \sigma''$ è una biiezione tra C_i e l'insieme di tutte le permutazioni senza punti fissi di X_n . Quindi ogni C_i ha s_n elementi. La (29.16) segue ora facilmente. \square

Poniamo $s_0 = 1$, di modo che la relazione di ricorrenza (29.16) vale per ogni $n \geq 1$, e calcoliamo la funzione generatrice esponenziale $s = \sum_{n \geq 0} (s_n/n!)x^n$ della successione degli s_n .

29.16 PROPOSIZIONE. Si ha

$$s = \frac{\exp(-x)}{1-x}.$$

Dimostrazione. Moltiplicando la (29.16) per $x^n/n!$ e sommando si trova che

$$(29.17) \quad \sum_{n \geq 1} \frac{s_{n+1}}{n!} x^n = \sum_{n \geq 1} \frac{s_{n-1}}{(n-1)!} x^n + \sum_{n \geq 1} \frac{s_n}{(n-1)!} x^n.$$

Calcoliamo separatamente le tre serie in questa equazione. Si ha

$$\sum_{n \geq 1} \frac{s_{n+1}}{n!} x^n = \sum_{n \geq 2} \frac{s_n}{(n-1)!} x^{n-1} = \sum_{n \geq 2} \frac{s_n}{n!} nx^{n-1} = s' - s_1 = s',$$

$$\sum_{n \geq 1} \frac{s_{n-1}}{(n-1)!} x^n = x \sum_{n \geq 1} \frac{s_{n-1}}{(n-1)!} x^{n-1} = xs,$$

$$\sum_{n \geq 1} \frac{s_n}{(n-1)!} x^n = x \sum_{n \geq 1} \frac{s_n}{n!} n x^{n-1} = xs',$$

e quindi, sostituendo nella (29.17), si ricava $s' = xs + xs'$, cioè

$$(29.18) \quad (1-x)s' = xs.$$

Dato che il termine costante della serie $(1-x)s$ è 1, la serie $(1-x)s$ è invertibile nell'anello $\mathbb{R}[[x]]$ (esempio 29.2), e quindi dividendo la (29.18) per $(1-x)s$ si trova che nell'anello $\mathbb{R}[[x]]$

$$\frac{s'}{s} = \frac{x}{1-x} = -1 + \frac{1}{1-x}.$$

Ora si ha

$$\frac{s'}{s} = \frac{d}{dx}(\log s)^* \quad \text{e} \quad -1 + \frac{1}{1-x} = \frac{d}{dx}(-x - \log(1-x)),$$

e quindi $\log s = -x - \log(1-x) + c$ per qualche $c \in \mathbb{R}$. Per $x=0$, ossia confrontando i termini costanti della due serie, si trova che $c=0$, e quindi $\log s + \log(1-x) = -x$. Ne segue che

$$s = \frac{\exp(-x)}{1-x}. \quad \square$$

Dalla proposizione (29.16) si ha

$$s = \frac{\exp(-x)}{1-x} = \left(\sum_{n \geq 0} \frac{(-1)^n}{n!} x^n \right) \left(\sum_{n \geq 0} x^n \right),$$

da cui, confrontando i coefficienti di x^n , si ricava che $s_n/n! = \sum_{i=0}^n (-1)^i / i!$, e quindi

29.17 COROLLARIO. Il numero di permutazioni senza punti fissi di un insieme di n elementi è

$$s_n = n! \sum_{i=0}^n \frac{(-1)^i}{i!}.$$

Esercizi svolti

29.1. Siano $f, g \in F[[x]]$. Si dimostri che

$$(a) \frac{d(f+g)}{dx} = \frac{df}{dx} + \frac{dg}{dx};$$

$$(b) \frac{d(fg)}{dx} = \frac{df}{dx}g + f\frac{dg}{dx};$$

$$(c) \frac{d(f^n)}{dx} = nf^{n-1}f' \text{ per ogni } n \geq 1;$$

*Noi abbiamo definito la serie $\log(1+x)$, e quindi ha significato sostituire qui x con una qualunque serie g con termine costante nullo, ottenendo la serie $\log(1+g)$. La serie s è del tipo $1+g$ con $g=s-1$ avente termine costante nullo. A rigore avremmo quindi dovuto scrivere $\log(1+(s-1))$ in luogo di $\log s$. Non l'abbiamo fatto per non appesantire ulteriormente le notazioni.

(d) se g ha termine costante nullo, allora $\frac{df(g)}{dx} = f'(g)g'$.

Soluzione. Se $f = \sum_{n \geq 0} a_n x^n$ e $g = \sum_{n \geq 0} b_n x^n$, allora

$$\begin{aligned}\frac{d(f+g)}{dx} &= \frac{d}{dx} \sum_{n \geq 0} (a_n + b_n)x^n = \sum_{n \geq 1} n(a_n + b_n)x^{n-1} \\ &= \sum_{n \geq 1} (na_n + nb_n)x^{n-1} = \sum_{n \geq 1} na_n x^{n-1} + \sum_{n \geq 1} nb_n x^{n-1} = \frac{df}{dx} + \frac{dg}{dx}.\end{aligned}$$

Questo dimostra (a)

Si osservi poi che se $\{f_\lambda \mid \lambda \in \Lambda\}$ è una famiglia di elementi di $F[[x]]$, dove $f_\lambda = \sum_{n \geq 0} a_{\lambda,n} x^n$ e per ogni $n \in \mathbb{N}$ i coefficienti $a_{\lambda,n}$ di x^n sono tutti nulli eccetto che per un numero finito di $\lambda \in \Lambda$, allora è possibile definire la somma $\sum_{\lambda \in \Lambda} f_\lambda$, e si ha

$$\frac{d}{dx} \sum_{\lambda \in \Lambda} f_\lambda = \sum_{\lambda \in \Lambda} f'_\lambda.$$

In base a questa osservazione, per dimostrare che vale la (b) in generale, è sufficiente dimostrarla nel caso di $f_n = a_n x^n$ e $g_m = b_m x^m$, in quanto si ha

$$\frac{d(fg)}{dx} = \frac{d}{dx} \sum_{(n,m) \in \mathbb{N} \times \mathbb{N}} f_n g_m = \sum_{(n,m) \in \mathbb{N} \times \mathbb{N}} \frac{d}{dx} (f_n g_m) = \sum_{(n,m) \in \mathbb{N} \times \mathbb{N}} (f'_n g_m + f_n g'_m) = \frac{df}{dx} g + f \frac{dg}{dx}.$$

Per il caso di f_n e g_m si ha poi

$$\begin{aligned}\frac{d}{dx} (f_n g_m) &= \frac{d}{dx} (a_n b_m x^{n+m}) = (n+m)a_n b_m x^{n+m-1} = n a_n x^{n-1} b_m x^m + a_n x^n m b_m x^{m-1} \\ &= \frac{df_n}{dx} g_m + f_n \frac{dg_m}{dx}.\end{aligned}$$

Questo conclude la dimostrazione di (b).

Mediante induzione su n , (c) segue immediatamente da (b).

Per dimostrare la (d) si ragiona come fatto per la (b): basta dimostrarla nel caso delle $f_n = a_n x^n$, in quanto se è vera la formula per le f_n allora

$$\frac{df(g)}{dx} = \frac{d}{dx} \sum_{n \geq 0} f_n(g) = \sum_{n \geq 0} \frac{d}{dx} (f_n(g)) = \sum_{n \geq 0} f'_n(g) g' = \left(\sum_{n \geq 0} f'_n(g) \right) g' = f'(g)g'.$$

Nel caso delle $f_n = a_n x^n$ si ha dalla (c) che

$$\frac{d}{dx} f_n(g) = \frac{d}{dx} a_n g^n = a_n \frac{d}{dx} g^n = a_n n g^{n-1} g' = f'_n(g) g'. \quad \square$$

29.2. Si dimostri che se $f, g \in F[[x]]$ sono due serie con termine costante nullo, allora $\exp(f) \exp(g) = \exp(f+g)$.

Soluzione. Si ha

$$\exp(f+g) = \sum_{k \geq 0} \frac{(f+g)^k}{k!} = \sum_{k \geq 0} \frac{1}{k!} \sum_{\substack{n \geq 0, m \geq 0 \\ n+m=k}} \frac{k!}{n!m!} f^n g^m,$$

dove l'ultima somma percorre tutte le coppie di numeri naturali (n, m) con $n + m = k$. Al variare di k in \mathbb{N} e di n, m in tutte le coppie di numeri naturali (n, m) con $n + m = k$, i numeri n, m variano in tutto \mathbb{N} , ossia la coppia (n, m) percorre tutto $\mathbb{N} \times \mathbb{N}$. Quindi

$$\exp(f + g) = \sum_{\substack{n \geq 0 \\ m \geq 0}} \frac{1}{n!m!} f^n g^m = \left(\sum_{n \geq 0} \frac{f^n}{n!} \right) \left(\sum_{m \geq 0} \frac{g^m}{m!} \right) = \exp(f) \exp(g). \quad \square$$

Altri esercizi

29.3. Si scrivano come serie formali

- (a) $\frac{1}{2+x};$
- (b) $\frac{1}{(2+x)^2};$
- (c) $\frac{1}{(2+x)^3}.$

29.4. Siano $f, g \in F[[x]]$ e si supponga g invertibile nell'anello $F[[x]]$ (di modo che $\frac{1}{g} \in F[[x]]$). Si dimostri che

- (a) $\frac{d}{dx} \left(\frac{1}{g} \right) = -\frac{g'}{g^2};$
- (b) $\frac{d}{dx} \left(\frac{f}{g} \right) = \frac{f'g - fg'}{g^2}.$

29.5. Si scrivano come serie formali

- (a) $\exp(x^2);$
- (b) $\exp(-x^2).$

29.6. Si verifichi che $\exp(-x) = 1/\exp(x).$

29.7. Si verifichi che $\exp(\log(1+x)) = 1+x$. [Suggerimento: si ponga $\exp(\log(1+x)) = \sum_{n \geq 0} a_n x^n$. Confrontando i termini costanti di questa uguaglianza si trova che $1 = a_0$, mentre derivandola si trova che... Si conclude che $a_0 = a_1 = 1$ e $a_n = 0$ per ogni $n \geq 2$.]

29.8. Si dimostri che $\log(1 + (\exp(x) - 1)) = x$. (Il lettore osservi che è possibili effettuare la sostituzione in quanto la serie $\exp(x) - 1$ ha termine costante nullo.)

29.9. Si dimostri che

$$\frac{1}{(1-x)^n} = \sum_{i \geq 0} \binom{n+i-1}{i} x^i$$

per ogni intero positivo n .

29.10. Siano $a_0 = 0$ e $a_n = 1 + 2 + \dots + n$ per ogni $n \geq 1$. Si calcoli la funzione generatrice della successione a_0, a_1, a_2, \dots

29.11. Siano $a_0 = 0$ e $a_n = 1^2 + 2^2 + \dots + n^2$ per ogni $n \geq 1$. Si calcoli la funzione generatrice della successione a_0, a_1, a_2, \dots e se ne ricavi il valore di a_n .

29.12. Si determinino le funzioni generatrici delle successioni di numeri razionali a_0, a_1, a_2, \dots definite da

$$(a) \quad a_n = \begin{cases} -1 & \text{se } 0 \leq n \leq 2, \\ 0 & \text{se } n = 3, \\ 1 & \text{se } 4 \leq n \leq 6, \\ 0 & \text{se } n \geq 7; \end{cases}$$

- (b) $a_n = (-1)^n$ per ogni $n \geq 0$;
 (c) $a_n = c$, dove $c \in \mathbb{Q}$ è una costante.

29.13. Si determini il numero di n -uple (c_1, c_2, \dots, c_n) dove c_i è uguale a 0 o a 1 per ogni $i = 1, 2, \dots, n$ e in cui non appaiono due zeri consecutivi. [Suggerimento: una tale n -upla termina con 1 o con 1,0. Si determini una relazione di ricorrenza. La risposta è (quasi) i numeri di Fibonacci.]

29.14. Si dimostri che per la successione F_0, F_1, F_2, \dots dei numeri di Fibonacci si ha $F_0 + F_1 + F_2 + \dots + F_n = F_{n+2} - 1$ per ogni $n \geq 0$. [Suggerimento: la relazione di ricorrenza dei numeri di Fibonacci si può riscrivere $F_i = F_{i+2} - F_{i+1}$. Si sommi per $i = 0, 1, \dots, n$.]

29.15. Si risolva l'esercizio 29.14 usando l'induzione su $n \geq 0$.

29.16. La formula già dimostrata negli esercizi 29.14 e 29.15 può essere verificata anche usando la funzione generatrice f dei numeri di Fibonacci. Vediamolo.

- (a) Si osservi che quanto enunciato nell'esercizio 29.14 equivale all'uguaglianza delle due serie $\sum_{n \geq 0} (F_0 + F_1 + \dots + F_n)x^n$ e $\sum_{n \geq 0} (F_{n+2} - 1)x^n$.
 (b) Si dimostri che le due serie in (a) sono uguali rispettivamente a

$$f \frac{1}{1-x} \quad \text{e} \quad \frac{f - F_1x - F_0}{x^2} - \frac{1}{1-x}.$$

(c) Si dimostri facendo uso della proposizione 29.7 che le due serie in (a) sono uguali.

29.17. Si dimostri che per la successione F_0, F_1, F_2, \dots dei numeri di Fibonacci si ha $F_n^2 = F_{n-1}F_{n+1} + (-1)^{n-1}$ per ogni $n \geq 1$.

29.18. Si determini la successione a_0, a_1, a_2, \dots tale che $a_0 = a_1 = 1, a_2 = 0$ e $a_n = 3a_{n-2} - 2a_{n-3}$ per ogni $n \geq 3$.

29.19. Supponiamo di avere n oggetti uguali tra loro e di volerli distribuire in quattro scatole etichettate da 1 a 4 in modo che in ogni scatola ci siano almeno tre oggetti e nella scatola etichettata da 1 ce ne siano almeno otto. In quanti modi a_n possiamo allora distribuire i nostri n oggetti nelle quattro scatole? Si calcoli una funzione generatrice della successione a_0, a_1, a_2, \dots

29.20. Per ogni $n \geq 0$ e ogni $k \geq 0$ sia $a_{n,k}$ il numero di sottoinsiemi di k elementi di un insieme di n elementi. Verifichiamo ancora una volta che $a_{n,k} = \binom{n}{k}$, questa volta facendo uso delle funzioni generatrici.

- (a) Si osservi innanzitutto che $a_{n,k} = 0$ se $n < k$.
 (b) Si dimostri che $a_{n,k} = a_{n-1,k} + a_{n-1,k-1}$ se $n \geq k \geq 1$.

Per ogni $k \in \mathbb{N}$ sia $f_k = \sum_{n \geq k} a_{n,k}x^n$ la funzione generatrice della successione $a_{0,k}, a_{1,k}, a_{2,k}, \dots$

- (c) Si dimostri che $f_0 = \frac{1}{1-x}$.
- (d) Si deduca da (b) che $f_k = \frac{x f_{k-1}}{1-x}$ per ogni $k \geq 1$.
- (e) Da (c) e (d) si deduca che $f_k = \frac{x^k}{(1-x)^{k+1}}$ per ogni $k \geq 0$.
- (f) Da (e) e dall'esercizio 29.9 di deduca che $a_{n,k} = \binom{n}{k}$ per ogni $n \geq k$.

29.21. Sia $A = \{x_1, x_2, \dots, x_t\}$ un alfabeto (cioè un insieme) di $t \geq 1$ lettere. Sia a_n il numero di parole nell'alfabeto A di lunghezza n con un numero pari di x_1 .

- (a) Si determini una relazione di ricorrenza per gli a_n .
- (b) Si determini la funzione generatrice f .
- (c) Nel caso particolare di $t = 1$, cioè di un alfabeto con una sola lettera, si ha ovviamente $a_n = 1$ per n pari e $a_n = 0$ per n dispari. Si dimostri che questo è in accordo con la funzione generatrice f trovata in (b).
- (d) Si determini a_n nel caso particolare di $t = 2$.

29.22. In questo esercizio troveremo una formula per calcolare i numeri di Bell B_n . Fissiamo una partizione \mathcal{F} dell'insieme $X_n = \{1, 2, \dots, n\}$. Per ogni $i = 1, 2, \dots, n$ denotiamo con k_i il numero di elementi $X \in \mathcal{F}$ con $|X| = i$.

- (a) Si dimostri che $1 \cdot k_1 + 2 \cdot k_2 + 3 \cdot k_3 + \dots + n \cdot k_n = n$.

Fissiamo quindi $k_1, k_2, \dots, k_n \in \mathbb{N}$ tali che $1 \cdot k_1 + 2 \cdot k_2 + \dots + n \cdot k_n = n$. Sia T_{k_1, \dots, k_n} l'insieme di tutte le partizioni \mathcal{F} di X_n aventi esattamente k_i elementi X tali che $|X| = i$ per ogni $i = 1, 2, \dots, n$. Siano S_n il gruppo simmetrico su n oggetti e $\Phi: S_n \rightarrow T_{k_1, \dots, k_n}$ l'applicazione che manda un qualunque elemento

$$\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix} \in S_n$$

nella partizione $\{\{\sigma(1)\}, \{\sigma(2)\}, \dots, \{\sigma(k_1)\}, \{\sigma(k_1 + 1), \sigma(k_1 + 2)\}, \{\sigma(k_1 + 3), \sigma(k_1 + 4)\}, \dots, \{\sigma(k_1 + 2k_2 - 1), \sigma(k_1 + 2k_2)\}, \dots\}$ (cioè che manda la permutazione σ nella partizione in cui i primi k_1 elementi della successione $\sigma(1), \sigma(2), \dots, \sigma(n)$ stanno in insiemi di un solo elemento, i successivi $2k_2$ elementi stanno in insiemi di due elementi, e così via). L'applicazione Φ è chiaramente suriettiva.

- (b) Si dimostri che l'antiimmagine di un qualunque elemento di T_{k_1, \dots, k_n} ha cardinalità

$$k_1!(1!)^{k_1} k_2!(2!)^{k_2} \dots k_n!(n!)^{k_n}.$$

- (c) Si deduca da (b) che

$$B_n = \sum_{\substack{k_1 \geq 0, \dots, k_n \geq 0 \\ 1 \cdot k_1 + \dots + n \cdot k_n = n}} \frac{n!}{k_1!(1!)^{k_1} k_2!(2!)^{k_2} \dots k_n!(n!)^{k_n}}.$$

§30. 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.

30.1 LEMMA. *Ogni anello booleano è un anello commutativo di caratteristica 2.*

Dimostrazione. Sia R un anello booleano. Allora per ogni $a \in R$ si ha che $-a = (-a)(-a) = a^2 = a$. In particolare $-1_R = 1_R$, e quindi $1_R + 1_R = 0$, cioè R ha caratteristica 2. Inoltre se $a, b \in R$, $a + b = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$, da cui $ab + ba = 0$, e pertanto $ab = -ba = ba$. \square

30.2 ESEMPIO. Siano X un insieme, $\mathcal{P}(X)$ l'insieme delle parti di X , Δ 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 Δ 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* (si veda, ad esempio, l'esercizio 16.4). 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

30.3 ESEMPIO. Il campo \mathbb{Z}_2 è un anello booleano. Viceversa per il lemma 30.1 e la proposizione 27.17, 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

30.4 TEOREMA. *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.*

Dimostrazione. L'insieme R ha almeno due elementi perché $1_R \neq 0_R$. La dimostrazione consiste nel verificare che \leq è riflessiva, antisimmetrica e transitiva, che $a + b + ab$ e ab sono rispettivamente l'estremo superiore e inferiore di $\{a, b\}$ per ogni $a, b \in R$, che 0_R e 1_R sono proprio lo 0 e l'1 del reticolo, che il reticolo è distributivo, e che per ogni $a \in R$ $1 + a$ è il complemento di a .

\leq è riflessiva: per ogni $a \in R$ si ha $a^2 = a$, e quindi $a \leq a$.

\leq è antisimmetrica: se $a, b \in R$, $a \leq b$ e $b \leq a$, allora $ab = a$, $ba = b$; per la commutatività $a = ab = ba = b$.

\leq è transitiva: se $a, b, c \in R$, $a \leq b$ e $b \leq c$, allora $ab = a$ e $bc = b$, e pertanto $ac = (ab)c = a(bc) = ab = a$, vale a dire $a \leq c$.

$a + b + ab = a \vee b$: si ha $a \leq a + b + ab$ perché $a(a + b + ab) = a + ab + ab = a$ dato che R ha caratteristica due. Similmente $b \leq a + b + ab$. Inoltre se $c \in R$, $a \leq c$ e $b \leq c$, allora $ac = a$, $bc = b$ e pertanto $(a + b + ab)c = ac + bc + abc = a + b + ab$, cioè $a + b + ab \leq c$. Quindi $a + b + ab$ è l'estremo superiore di $\{a, b\}$.

Similmente si vede che ab è l'estremo superiore di $\{a, b\}$. Lasciamo questa e tutte le altre verifiche per esercizio al lettore. \square

30.5 TEOREMA. *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.*

Dimostrazione. La dimostrazione consiste nell'effettuare una sequenza di verifiche: che $(L, +)$ è gruppo abeliano, che (L, \cdot) è semigruppo commutativo, la distributività, che l'1 del reticolo è l'identità dell'anello e che ogni elemento è idempotente.

Associatività dell'addizione:

$$\begin{aligned} (a + b) + c &= [(a \wedge b') \vee (a' \wedge b)] + c \\ &= [(a \wedge b') \vee (a' \wedge b)] \wedge c' \vee [(a \wedge b') \vee (a' \wedge b)]' \wedge c \\ &= ((a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')) \vee ((a \wedge b')' \wedge (a' \wedge b)' \wedge c) \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee [(a' \vee b) \wedge (a \vee b')] \wedge c \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \\ &\quad \vee [(a' \wedge a) \vee (a' \wedge b') \vee (b \wedge a) \vee (b \wedge b')] \wedge c \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c). \end{aligned}$$

Si ottiene la stessa espressione cominciando da $a + (b + c)$.

Lo zero del reticolo è lo zero dell'anello:

$$a + 0 = (a \wedge 0') \vee (a' \wedge 0) = (a \wedge 1) \vee (a' \wedge 0) = a.$$

Ogni elemento è l'opposto di sé stesso: $a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0$.

Lasciamo le altre verifiche per esercizio al lettore. \square

Si noti che nei teoremi precedenti i reticolati hanno almeno due elementi perché ogni anello booleano ha almeno due elementi distinti 1 e 0. Al reticolo con un unico elemento corrisponderebbe l'anello banale con un unico elemento.

Le due corrispondenze dei teoremi 30.4 e 30.5 che associano ad un anello booleano una struttura di reticolo booleano e ad un reticolo booleano una struttura di anello booleano sono una l'inversa dell'altra, nel senso che se R è un anello booleano, si costruisce il reticolo (R, \leq) come nel teorema 30.4 e poi come nel teorema 30.5 si costruisce l'anello booleano del reticolo ottenuto, l'anello che si trova è proprio l'anello di partenza. Similmente se si parte da un reticolo booleano. Verifichiamo questa affermazione. Sia $(R, +, \cdot)$ un anello booleano, e consideriamo il reticolo booleano (R, \leq) ove \leq è definita da $a \leq b$ se $ab = a$. Nella dimostrazione del teorema 30.4 si è visto che $a \vee b = a + b + ab$ e similmente si vede che $a \wedge b = ab$ e $a' = 1 + a$. L'anello associato al reticolo (R, \leq) è l'anello (R, \oplus, \odot) , ove \oplus e \odot sono definite da

$$a \oplus b = (a \wedge b') \vee (a' \wedge b) \quad \text{e} \quad a \odot b = a \vee b.$$

Qui le operazioni sono state denotate con \oplus e \odot per non confonderle con le operazioni $+$ e \cdot dell'anello di partenza. Però le operazioni \oplus e \odot coincidono con quelle di partenza, perché

$$\begin{aligned} a \oplus b &= (a \wedge b') \vee (a' \wedge b) = [a \wedge (1+b)] \vee [(1+a) \wedge b] \\ &= a(1+b) + (1+a)b + a(1+b)(1+a)b \\ &= a + ab + b + ab + ab + a^2b + ab^2 + a^2b^2 = a + b, \end{aligned}$$

dato che in $(R, +, \cdot)$ ogni elemento è idempotente e la caratteristica è 2. Analogamente $a \odot b = a \wedge b = ab$. Quindi le operazioni \oplus e $+$ e le operazioni \odot e \cdot coincidono, cioè $(R, \oplus, \odot) = (R, +, \cdot)$. Similmente si procede partendo da un reticolo booleano.

30.6 ESEMPIO. 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 30.2. 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 Δ . 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

Per la dimostrazione del teorema che segue si veda l'appendice 30.1.

30.7 TEOREMA. *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 .*

Dal teorema 30.7 e dalla corrispondenza tra reticolini booleani ed anelli booleani si ottiene il seguente corollario.

30.8 COROLLARIO. *Ogni reticolo booleano è isomorfo a un sottoreticolo del reticolo $(\mathcal{P}(X), \subseteq)$ per un opportuno insieme finito X . Ogni reticolo booleano finito è isomorfo al reticolo $(\mathcal{P}(X), \subseteq)$ per un opportuno insieme finito X .*

30.9 COROLLARIO. *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 $m \geq 0$.*

Dimostrazione. Per gli anelli. Se $n = 2^m$ con $m \geq 1$ intero, sia X un insieme di cardinalità m . Allora $(\mathcal{P}(X), \Delta, \cap)$ è un anello booleano di cardinalità n . Viceversa, se R è un anello booleano finito con n elementi, per il teorema 30.7 esiste un insieme finito non vuoto X tale che R è isomorfo a $(\mathcal{P}(X), \Delta, \cap)$. In particolare $n = |R| = |\mathcal{P}(X)| = 2^{|X|}$. Quindi $n = 2^m$ con $m = |X| \geq 1$ intero.

Per i reticolini. Se $n = 2^m$ con $m \geq 0$ intero e X è un insieme di cardinalità m , allora $(\mathcal{P}(X), \subseteq)$ è un reticolo booleano di cardinalità n . Viceversa, se L è un reticolo booleano finito con n elementi, per il corollario 30.8 il reticolo L è isomorfo al reticolo

$(\mathcal{P}(X), \subseteq)$ per un opportuno insieme finito X . Sia $m = |X|$. Allora m è un intero ≥ 0 e si ha $n = |L| = |\mathcal{P}(X)| = 2^{|X|} = 2^m$. \square

30.10 COROLLARIO. Due anelli booleani finiti sono isomorfi se e solo se sono equipotenti. Due reticolati booleani finiti sono isomorfi se e solo se sono equipotenti.

Dimostrazione. Due anelli isomorfi sono certamente equipotenti. Viceversa siano R, R' due anelli booleani finiti equipotenti, diciamo entrambi di cardinalità n . Per il teorema 30.7 esiste un insieme finito non vuoto X tale che R sia isomorfo a $(\mathcal{P}(X), \Delta, \cap)$. Analogamente esiste un insieme finito non vuoto X' tale che R' sia isomorfo a $(\mathcal{P}(X'), \Delta, \cap)$. Allora $n = |R| = |\mathcal{P}(X)| = 2^{|X|}$. Analogamente $n = 2^{|X'|}$. Da $2^{|X|} = 2^{|X'|}$ segue che $|X| = |X'|$. Ma allora i due anelli $(\mathcal{P}(X), \Delta, \cap)$ e $(\mathcal{P}(X'), \Delta, \cap)$ sono isomorfi. Pertanto $R \cong \mathcal{P}(X) \cong \mathcal{P}(X') \cong R'$.

Analogamente si ragiona per i reticolati. \square

Esercizi svolti

30.1. 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). Pertanto $e \neq 0_R$, $1_R - e \neq 0_R$ ed $e(1_R - e) = e - e^2 = e - e = 0_R$. Quindi R non è un dominio d'integrità. \square

30.2. 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 il teorema 27.22(a), 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 30.1 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 30.1 R/P è un campo (isomorfo a \mathbb{Z}_2), e quindi P è un ideale massimale di R per il teorema 27.22(b). \square

Altri esercizi

30.3. Sia \mathbb{R}^X l'anello delle applicazioni di un insieme fissato non vuoto X in \mathbb{R} (esercizio 24.7). Si determinino gli elementi idempotenti in questo anello.

30.4. Sia R un anello commutativo e sia e un elemento idempotente non nullo di R . Si provi che $R_e = \{x \in R \mid xe = x\}$ è un sottoanello di R e che l'identità di R_e è e . (Quindi se $e \neq 1_R$, R_e ed R hanno identità diverse.)

Si dimostri che se R è un anello booleano, allora anche l'anello R_e è booleano.

30.5. Sia R un anello commutativo e sia e un elemento idempotente non nullo di R . Denotato con R_e l'anello dell'esercizio 30.4 e con $\varphi: R \rightarrow R_e$ l'applicazione definita da $\varphi(x) = xe$ per ogni $x \in R$, si provi che φ è un omomorfismo suriettivo di anelli il cui nucleo è l'ideale principale di R generato da $1 - e$.

30.6. Si completi la dimostrazione del teorema 30.4.

30.7. Si completi la dimostrazione del teorema 30.5.

30.8. Sia X un insieme non vuoto e sia \mathbb{Z}_2^X l'anello definito come nell'esercizio 24.7, ma con \mathbb{Z}_2 in luogo di \mathbb{R} . Si provi che \mathbb{Z}_2^X è un anello booleano e che l'anello $\mathcal{P}(X)$ delle parti di X e l'anello \mathbb{Z}_2^X sono isomorfi. [Suggerimento: ragionare come nella seconda dimostrazione della proposizione 9.7.]

30.9. Sia X un insieme infinito, sia $\mathcal{P}_f(X) = \{Y \mid Y \subseteq X, Y \text{ finito}\}$ l'insieme dei sottoinsiemi finiti di X e sia $\mathcal{P}_c(X) = \{Y \mid Y \subseteq X, X \setminus Y \text{ finito}\}$ l'insieme dei sottoinsiemi cofiniti di X , cioè dei sottoinsiemi Y di X tali che $X \setminus Y$ sia finito. Si provi che $B = \mathcal{P}_f(X) \cup \mathcal{P}_c(X)$ è sottoanello di $(\mathcal{P}(X), \Delta, \cap)$. In particolare B è un anello booleano.

30.10. (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 .

30.11. 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 sottanello di R ?
- (b) Si dimostri che E_R è chiuso per l'operazione \oplus definita, per ogni $a, b \in E_R$, da $a \oplus b = a + b - 2ab$ (e quindi \oplus è un'operazione in E_R).
- (c) Si dimostri che E_R è un sottomonoide del monoide (R, \cdot) .
- (d) Si dimostri che (E_R, \oplus, \cdot) è un anello booleano.

30.12. Si consideri $\mathbb{Z}_2[x]$, anello dei polinomi nell'indeterminata x a coefficienti nel campo \mathbb{Z}_2 . Sia $I = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid n \in \mathbb{N}, a_i \in \mathbb{Z}_2 \text{ per ogni } i = 0, 1, \dots, n, a_0 = a_1 = 0\}$.

- (a) Si dimostri che $I = \{x^2f \mid f \in \mathbb{Z}_2[x]\}$.
- (b) Si dimostri che I è un ideale di $\mathbb{Z}_2[x]$.
- (c) Si calcoli la caratteristica di $\mathbb{Z}_2[x]/I$.
- (d) Si dica se $\mathbb{Z}_2[x]/I$ è un anello booleano.

30.13. Si consideri l'anello commutativo con identità $\mathbb{Z}_2 \times \mathbb{Z}_2$ con le operazioni definite da $(a, x) + (b, y) = (a + b, x + y)$ e $(a, x)(b, y) = (ab, ay + xb)$ per ogni $(a, x), (b, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2$.

- (a) Si calcoli la caratteristica di $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- (b) Si dica se $\mathbb{Z}_2 \times \mathbb{Z}_2$ è un anello booleano.

30.14. Sia $(\mathbb{R}^{\mathbb{R}}, \leq)$ il reticolo dell'esempio 11.3 e sia

$$L = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(\mathbb{R}) \subseteq \{0, 1\}\}.$$

- (a) Si dimostri che L è un sottoreticolo di $\mathbb{R}^{\mathbb{R}}$.
- (b) Si dimostri che il reticolo L è booleano.
- (c) Sia (L, \oplus, \odot) l'anello booleano associato al reticolo booleano L . Siano $f, g: \mathbb{R} \rightarrow \mathbb{R}$ 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 $f \odot g$.

30.15. 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, \odot) l'anello booleano associato al reticolo booleano $(L, |)$. Si determinino $6 \oplus 10$ e $6 \odot 10$.

30.16. Si dia un esempio di un anello booleano avente otto elementi.

30.17. 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 $a + b = 1$.

30.18. Sia $B = \{a, b, c, d\}$ un anello booleano con quattro elementi. Si dimostri che $a + b + c + d = 0$.

- 30.19. (a) Esiste un anello commutativo con 14 elementi?
 (b) Esiste un anello booleano con 14 elementi?

30.20. Si dia un esempio, se esiste, di un reticolo booleano avente esattamente 7 elementi e di un reticolo booleano avente esattamente 8 elementi.

30.21. 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.

30.22. 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 minimi.

Appendice 30.1. Dimostrazione del teorema 30.7

In questa appendice dimostriamo il teorema 30.7.

30.11 LEMMA. Sia R un anello booleano, sia P un ideale primo di R , e siano $r, r' \in R$. Allora

- (a) $r + r' \notin P$ se e solo se $r \notin P$ e $r' \notin P$, oppure $r' \notin P$ e $r \in P$;
- (b) $rr' \notin P$ se e solo se $r \notin P$ e $r' \notin P$.

Dimostrazione. (a) Se $r, r' \in P$, allora $r + r' \in P$.

Se $r \in P$ e $r' \notin P$, allora $r + r' \notin P$, perché se fosse $r + r' \in P$, allora $r' = (r + r') - r \in P$, contraddizione. Analogamente da $r \notin P$ e $r' \in P$ segue che $r + r' \notin P$.

Infine supponiamo che $r, r' \notin P$. Dato che $(1-r)r = r - r^2 = 0 \in P$ e P è primo, si deve avere che $1-r \in P$. Analogamente $1-r' \in P$. Dato che R ha caratteristica 2 si ha $1+1=0$. Ma allora $r+r'=-(1-r)-(1-r') \in P$.

(b) Se $r \in P$ o $r' \in P$ allora $rr' \in P$ perché P è ideale. Viceversa se $rr' \in P$ allora $r \in P$ o $r' \in P$ perché P è primo. \square

30.12 TEOREMA. Siano R un anello booleano, $\text{Spec } R$ l'insieme degli ideali primi di R , e sia $(\mathcal{P}(\text{Spec } R), \Delta, \cap)$ l'anello delle parti di $\text{Spec } R$. Consideriamo l'applicazione $\varepsilon: R \rightarrow \mathcal{P}(\text{Spec } R)$ definita da $\varepsilon(r) = \{P \in \text{Spec } R \mid r \notin P\}$ per ogni $r \in R$. Allora ε è un omomorfismo iniettivo di anelli con identità. Inoltre se R è un anello booleano finito, ε è un isomorfismo.

Dimostrazione. Per verificare che ε è un omomorfismo di anelli con identità dobbiamo verificare che per ogni $r, r' \in R$ $\varepsilon(r+r') = \varepsilon(r) \Delta \varepsilon(r')$, che $\varepsilon(rr') = \varepsilon(r) \cap \varepsilon(r')$, e che $\varepsilon(1_R) = \text{Spec } R$. Quindi dobbiamo dimostrare che

$$\{P \in \text{Spec } R \mid r+r' \notin P\} = \{P \in \text{Spec } R \mid r \notin P\} \Delta \{P \in \text{Spec } R \mid r' \notin P\},$$

che

$$\{P \in \text{Spec } R \mid rr' \notin P\} = \{P \in \text{Spec } R \mid r \notin P\} \cap \{P \in \text{Spec } R \mid r' \notin P\},$$

e che

$$\{P \in \text{Spec } R \mid 1_R \notin P\} = \text{Spec } R.$$

Le prime due uguaglianze sono date rispettivamente dalla (a) e dalla (b) del lemma 30.11, la terza è data dal fatto che $1_R \notin P$ per ogni ideale proprio P di R (esercizio 25.7). Pertanto ε è un omomorfismo.

Per verificare che ε è iniettivo dobbiamo provare che $\ker \varepsilon = \{0\}$, cioè che se $r \in \ker \varepsilon$ allora $r = 0$. Sia $r \in \ker \varepsilon$. Allora $-r \in \ker \varepsilon$, ossia $\varepsilon(-r) = \emptyset$. Ma allora $\varepsilon(1-r) = \varepsilon(1) + \varepsilon(-r) = \text{Spec } R \Delta \emptyset = \text{Spec } R$. Quindi $1-r \notin P$ per ogni ideale primo P di R . Dato che ogni ideale massimale è primo (corollario 27.23) si ha in particolare che $1-r \notin M$ per ogni ideale massimale M di R . Quindi $1-r$ è invertibile (proposizione 27.25). Ma allora $r = r(1-r)(1-r)^{-1} = (r-r^2)(1-r)^{-1} = 0$.

Mostriamo che se R è finito allora ε è suriettiva. Sia $X \subseteq \text{Spec } R$ e dimostriamo che esiste $r \in R$ tale che $\varepsilon(r) = X$ per induzione su $n = |X|$. Se $X = \emptyset$, $\varepsilon(0) = \emptyset$ perché ε è un omomorfismo. Se X ha un solo elemento, $X = \{P\}$ diciamo, poniamo $R \setminus P = \{x_1, \dots, x_t\}$. Mostriamo che $\varepsilon(x_1 \dots x_t) = \{P\}$. Si deve far vedere che per ogni ideale primo Q di R si ha $x_1 \dots x_t \notin Q$ se e solo se $Q = P$. Ora se $Q = P$, applicando ripetutamente la (b) del lemma 30.11, si ha $x_1 x_2 \notin P$, e quindi $x_1 x_2 x_3 \notin P$, e così via fino a $x_1 x_2 \dots x_t \notin P$. Quindi $x_1 x_2 \dots x_t \notin P$. Se invece $Q \neq P$, allora $Q \not\subseteq P$, perché se fosse $Q \subseteq P$, allora (dato che Q è massimale per l'esercizio 30.2) si avrebbe $Q = P$, contraddizione. Dato che $Q \not\subseteq P$, esiste un elemento di Q che non appartiene a P , e quindi esiste

$i = 1, 2, \dots, t$ tale che $x_i \in Q$. Ma allora $x_1 x_2 \cdots x_t \in Q$. Questo conclude la dimostrazione nel caso in cui X ha un solo elemento.

Se infine X ha $n \geq 2$ elementi, scriviamo $X = Y \cup \{P\}$ ove $Y \subseteq X$, $|Y| = n - 1$, $P \in X$ e $Y \cap \{P\} = \emptyset$. Per l'ipotesi induttiva e per il caso $n = 1$ esistono $r_1, r_2 \in R$ tali che $\varepsilon(r_1) = Y$ e $\varepsilon(r_2) = \{P\}$, e allora $\varepsilon(r_1 + r_2) = \varepsilon(r_1) \Delta \varepsilon(r_2) = Y \Delta \{P\} = X$. Quindi ε è suriettiva. \square

Dal teorema 30.12 segue subito il teorema 30.7, perché se R è un anello booleano finito, ε è un isomorfismo di R in $(\text{Spec } R, \Delta, \cap)$, mentre se R è un anello booleano arbitrario, ε è un omomorfismo iniettivo, e quindi R è isomorfo al sottoanello $\varepsilon(R)$ dell'anello $(\text{Spec } R, \Delta, \cap)$.

§31. Algebre di Boole

Abbiamo finora incontrato tre strutture algebriche dotate di un'operazione (semigruppi, monoidi, gruppi) e una struttura algebrica dotata di due operazioni (anelli). In questo §31 mostreremo come anche i reticolati possano essere considerati una struttura algebrica dotata di due operazioni.

31.1 TEOREMA. *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:*

- (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 $x, y \in L$.

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.

Dimostrazione. La prima parte del teorema è la proposizione 11.12. Dimostriamo la seconda parte. Si osservi che $x \wedge x = x$ per ogni $x \in L$. Infatti per la proprietà di assorbimento si ha $x \vee (x \wedge x) = x$ e $x \wedge [x \vee (x \wedge x)] = x$, e quindi $x \wedge x = x \wedge [x \vee (x \wedge x)] = x$. Inoltre:

\leq è riflessiva: Se $x \in L$ si ha $x \wedge x = x$, cioè $x \leq x$.

\leq è antisimmetrica: Sia $x \leq y$ e $y \leq x$; allora $x \wedge y = x$ e $y \wedge x = y$, da cui $x = x \wedge y = y \wedge x = y$.

\leq è transitiva: Sia $x \leq y$ e $y \leq z$; allora $x \wedge y = x$ e $y \wedge z = y$, da cui $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, cioè $x \leq z$.

Per ogni $x, y \in L$, $x \wedge y$ è l'estremo inferiore di $\{x, y\}$ in (L, \leq) : Si deve verificare che $x \wedge y \leq x$, che $x \wedge y \leq y$ e che se $z \in L$, $z \leq x$ e $z \leq y$, allora $z \leq x \wedge y$. Ora $(x \wedge y) \wedge x = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y$, e quindi $x \wedge y \leq x$. Similmen-

te $x \wedge y \leq y$. Poi se $z \in L$, $z \leq x$ e $z \leq y$, allora $z \wedge x = z$ e $z \wedge y = z$ e quindi $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$, cioè $z \leq x \wedge y$.

Per ogni $x, y \in L$, $x \vee y$ è l'estremo superiore di $\{x, y\}$ in (L, \leq) : Si deve verificare che $x \leq x \vee y$, $y \leq x \vee y$, e che se $z \in L$, $x \leq z$ e $y \leq z$, allora $x \vee y \leq z$. Ora $x \wedge (x \vee y) = x$ per la proprietà di assorbimento e quindi $x \leq x \vee y$. Similmente $y \leq x \vee y$. Poi se $z \in L$, $x \leq z$ e $y \leq z$, allora $x \wedge z = x$ e $y \wedge z = y$. In particolare $x \vee z = (x \wedge z) \vee z = z$ e similmente $y \vee z = z$, da cui $(x \vee y) \wedge z = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge (x \vee (y \vee z)) = (x \vee y) \wedge ((x \vee y) \vee z) = x \vee y$, cioè $x \vee y \leq z$. Questo completa la dimostrazione. \square

Ecco quindi che avremmo potuto definire un reticolo L non come un insieme parzialmente ordinato in cui $\{x, y\}$ ha estremo superiore ed estremo inferiore per ogni $x, y \in L$, ma come un insieme dotato di due operazioni \vee e \wedge entrambe soddisfacenti alle proprietà commutativa, associativa e di assorbimento. Avremmo ottenuto essenzialmente la stessa struttura. Se avessimo proceduto in questo modo avremmo ad esempio studiato la struttura algebrica $(\mathcal{P}(X), \cup, \cap)$ invece dell'insieme parzialmente ordinato $(\mathcal{P}(X), \subseteq)$ e la struttura $(\mathbb{N}, \text{mcm}, \text{MCD})$ invece di $(\mathbb{N}, |)$. I due approcci sono del tutto equivalenti. D'ora in poi parleremo quindi indifferentemente del reticolo (L, \leq) o del reticolo (L, \vee, \wedge) , facendo uso talvolta della descrizione come insieme ordinato e talvolta di quella come insieme con due operazioni.

Si osservi che nel §11 avevamo definito i sottoreticolari di un reticolo L come i sottoinsiemi L' di L tali che $x \vee y \in L'$ e $x \wedge y \in L'$ per ogni $x, y \in L'$. Adesso dovrebbe essere chiaro il motivo di tale definizione: si erano definiti sottoreticolari di L i sottoinsiemi di L chiusi per le operazioni \vee e \wedge .

Il teorema 31.1 ha dei corollari immediati.

31.2 COROLLARIO. *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.

31.3 COROLLARIO. *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:*

- 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.

Passiamo a considerare in particolare i reticolati booleani. Ricordiamo che se A è un insieme, un'*operazione n-aria* su A è un'applicazione $\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}} \rightarrow A$. La maggior

parte delle operazioni su un insieme A che abbiamo incontrato finora (nei semigruppi, monoidi, gruppi, l'addizione e la moltiplicazione in un anello, il \vee e \wedge in un reticolo) erano tutte *operazioni binarie*, ossia applicazioni $A \times A \rightarrow A$. Siamo ora particolarmente interessati alle *operazioni unarie*, cioè alle applicazioni $A \rightarrow A$. Ecco un esempio fondamentale. Abbiamo appena visto che i reticolati (L, \leq) si possono anche pensare come insiemi dotati di due operazioni \vee e \wedge . Tra i reticolati sono particolarmente importanti i reticolati booleani, cioè i reticolati distributivi e complementati. La complementazione è un'*operazione unaria* $L \rightarrow L$ che associa ad ogni elemento $x \in L$ il suo (unico) complemento x' . Non è quindi difficile dimostrare il seguente teorema che segue subito dal corollario 31.3.

31.4 TEOREMA. 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 31.4.

Le algebre di Boole si possono quindi studiare in tre modi equivalenti, scegliendo di volta in volta quello più conveniente a seconda del problema in considerazione: come reticolati booleani (reticolati distributivi e complementati, §11), come anelli booleani (anelli

con identità in cui ogni elemento è idempotente, §30) o come algebre di Boole ($B, \vee, \wedge, '$) come abbiamo visto nel teorema 31.4.

31.5 ESEMPIO. Sia X un insieme. Come già sappiamo $(\mathcal{P}(X), \subseteq)$ 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 *sottoalgebra di Boole* di B se $0_B, 1_B \in C$ e per ogni $x, y \in C$ si ha $x \vee y, x \wedge y, x' \in C$.

31.6 LEMMA. *Siano B, C due algebre di Boole e sia $\varphi: B \rightarrow C$ un omomorfismo di reticolli. 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 reticolli tra due algebre di Boole B e C che soddisfa alle condizioni equivalenti del lemma 31.6 si dice un *omomorfismo di algebre di Boole*. Un omomorfismo di algebre di Boole che sia biettivo 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*.

31.7 LEMMA. *Siano $(B, \vee, \wedge, ')$, $(C, \vee, \wedge, ')$ due algebre di Boole, e siano $(B, +, \cdot)$, $(C, +, \cdot)$ le corrispondenti strutture di anello booleano. Sia $\varphi: B \rightarrow C$ un'applicazione. Le seguenti affermazioni sono equivalenti:*

- (a) φ è un omomorfismo di algebre di Boole;
- (b) φ è un omomorfismo di anelli con identità.

Dimostrazione. (a) \Rightarrow (b) Se φ 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 φ è un omomorfismo di anelli con identità.

(b) \Rightarrow (a) Se φ è un omomorfismo di anelli con identità, allora $\varphi(0) = 0$ e $\varphi(1) = 1$. Per dimostrare che φ è un omomorfismo di algebre di Boole è quindi sufficiente dimostrare che è un omomorfismo di reticolli, 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 $a \wedge b$ viste nella dimostrazione del teorema 30.4 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

31.8 COROLLARIO. Siano $(B, \vee, \wedge, ')$, $(C, \vee, \wedge, ')$ due algebre di Boole, siano $(B, +, \cdot)$, $(C, +, \cdot)$ le corrispondenti strutture di anello booleano, e (B, \leq) , (C, \leq) le strutture di reticolato booleano. Sia $\varphi: B \rightarrow C$ un'applicazione. Le seguenti affermazioni sono equivalenti:

- φ è un isomorfismo di algebre di Boole dell'algebra di Boole $(B, \vee, \wedge, ')$ in $(C, \vee, \wedge, ')$;
- φ è un isomorfismo di anelli con identità di $(B, +, \cdot)$ in $(C, +, \cdot)$;
- φ è un isomorfismo di insiemi parzialmente ordinati di (B, \leq) in (C, \leq) .

31.9 COROLLARIO. 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 .

31.10 COROLLARIO. Esiste un'algebra di Boole finita con n elementi se e solo se $n = 2^m$ per qualche intero $m \geq 0$.

31.11 COROLLARIO. 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, τ) è un alfabeto valutato (vedi §18); 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 §18 chiameremo variabili). Si possono quindi considerare le parole generate da (A, τ) e X . Se w_1, w_2 sono parole scriviamo $(w_1 \vee w_2)$ invece di $\vee w_1 w_2$, scriviamo $(w_1 \wedge w_2)$ invece di $\wedge w_1 w_2$, e scriviamo (w'_1) invece di $'w_1$. Le parole generate da (A, τ) e X si dicono i polinomi booleani nelle variabili x_1, x_2, \dots, x_n .

31.12 ESEMPIO. Sono polinomi booleani nelle variabili x_1, x_2, \dots, 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

$$\underbrace{B \times \cdots \times B}_{n \text{ volte}} \longrightarrow B, \quad (b_1, b_2, \dots, b_n) \longmapsto E(b_1, b_2, \dots, b_n).$$

Diremo che due polinomi booleani $E_1(x_1, x_2, \dots, x_n)$, $E_2(x_1, x_2, \dots, x_n)$ sono equivalenti, e scrivremo

$$E_1(x_1, x_2, \dots, x_n) \equiv E_2(x_1, x_2, \dots, x_n),$$

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 polino-

mi 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 quoziante $\mathcal{B}(x_1, x_2, \dots, x_n) = \mathcal{E}(x_1, x_2, \dots, x_n)/\equiv$ 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.

31.13 TEOREMA. Per ogni numero naturale n le algebre di Boole

$$\mathcal{P}(\mathcal{P}(\{x_1, \dots, x_n\})) \quad e \quad \mathcal{B}(x_1, x_2, \dots, x_n)$$

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 φ 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 formule di De Morgan (vedi esercizio 11.3) 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.

31.14 ESEMPIO. 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 formule di De Morgan) ci porta alla seguente successione di polinomi booleani tra loro equivalenti:

$$\begin{aligned} (x_1 \wedge (x_1 \vee x_2)) \vee (x'_1 \wedge x_3)' &\equiv (x_1 \wedge (x_1 \vee x_2)) \vee (x''_1 \vee x'_3) \equiv \\ &\equiv (x_1 \wedge (x_1 \vee x_2)) \vee x_1 \vee x'_3. \end{aligned}$$

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

$$\begin{aligned} x_1 &\equiv x_1 \wedge (x_2 \vee x'_2) \equiv (x_1 \wedge x_2) \vee (x_1 \wedge x'_2) \equiv \\ &\equiv (x_1 \wedge x_2 \wedge (x_3 \vee x'_3)) \vee (x_1 \wedge x'_2 \wedge (x_3 \vee x'_3)) \equiv \\ &\equiv (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x'_3) \vee (x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x'_2 \wedge x'_3), \\ x_1 \wedge x_2 &\equiv x_1 \wedge x_2 \wedge (x_3 \vee x'_3) \equiv (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x'_3), \end{aligned}$$

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

Il teorema 31.13 ha il seguente immediato corollario.

31.15 COROLLARIO. L'algebra di Boole $\mathcal{B}(x_1, x_2, \dots, x_n)$ ha 2^{2^n} elementi.

Esercizi svolti

31.1. 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

$$\begin{aligned}(E_1(x_1, x_2, \dots, x_n) \vee E_2(x_1, x_2, \dots, x_n))' &\equiv \\ &\equiv (E_1(x_1, x_2, \dots, x_n))' \wedge (E_2(x_1, x_2, \dots, x_n))'\end{aligned}$$

e

$$\begin{aligned}(E_1(x_1, x_2, \dots, x_n) \wedge E_2(x_1, x_2, \dots, x_n))' &\equiv \\ &\equiv (E_1(x_1, x_2, \dots, x_n))' \vee (E_2(x_1, x_2, \dots, x_n))'.\end{aligned}$$

Soluzione. 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 nell'esercizio 11.3 prendendo

$$a = E_1(b_1, b_2, \dots, b_n) \quad \text{e} \quad b = E_2(b_1, b_2, \dots, b_n).$$

Similmente si dimostra la seconda formula. \square

Altri esercizi

31.2. Si consideri il reticolo (\mathbb{R}, \leq) , dove \leq è l'ordinamento usuale sull'insieme \mathbb{R} dei numeri reali. Come sono definite le operazioni \vee e \wedge su \mathbb{R} ?

31.3. Si provi che se (L, \vee, \wedge) è un reticolo, anche (L, \wedge, \vee) è un reticolo (detto il *reticolo duale*) e che se $(B, \vee, \wedge,')$ è un'algebra di Boole, allora anche $(B, \wedge, \vee,')$ è un'algebra di Boole (detta *l'algebra di Boole duale*).

31.4. Si provi che se L è un reticolo limitato e distributivo, allora l'insieme degli elementi di L dotati di complemento è un sottoreticolo di L .

31.5. Sia L un reticolo. Un sottoinsieme I di L si dice un *ideale* di L se valgono le tre proprietà seguenti: (1) $I \neq \emptyset$; (2) se $x, y \in I$, allora $x \vee y \in I$; (3) se $x \in I$, $a \in L$ e $a \leq x$, allora $a \in I$.

- (a) Si dimostri che ogni ideale di L è un sottoreticolo di L .
- (b) Si dimostri che se $a \in L$, allora il sottoinsieme $(a) = \{x \mid x \in L, x \leq a\}$ di L è un ideale di L (detto *l'ideale principale generato da a*).

31.6. Si provi che se L ed L' sono reticolli limitati, $\varphi: L \rightarrow L'$ è un omomorfismo di reticolli e $\varphi(0) = 0$, allora $\varphi^{-1}(0)$ è un ideale di L .

31.7. 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 φ è un omomorfismo di reticolli del reticolo $(\mathcal{P}(\mathbb{N}), \subseteq)$ in sé stesso.

- (b) Si dica se φ è un isomorfismo di reticolati del reticolo $(\mathcal{P}(\mathbb{N}), \subseteq)$ in sé stesso.
 (c) Si dica se φ è un omomorfismo di insiemi parzialmente ordinati.
 (d) Si dica se φ è un isomorfismo di insiemi parzialmente ordinati.

31.8. Sia $(B, \vee, \wedge,')$ un'algebra di Boole, $a \in B$. Definiamo $B_a = \{x \in B \mid x \wedge a = x\}$. Su B_a consideriamo l'operazione unaria $*: B_a \rightarrow B_a$ definita da $x^* = x' \wedge a$ per ogni $x \in B_a$. Si provi che $(B_a, \vee, \wedge, *)$ è un'algebra di Boole avente 0_B come zero ed a come uno. (Qui si intende che le operazioni \vee e \wedge su B_a siano le restrizioni delle operazioni corrispondenti su B .)

31.9. Nelle notazioni dell'esercizio precedente si provi che $\varphi_a: B \rightarrow B_a$ definito da $\varphi_a(b) = b \wedge a$ per ogni $b \in B$ è un omomorfismo suriettivo di algebre di Boole.

31.10. Siano L_1, L_2, \dots, L_n reticolati. Sul prodotto cartesiano $L_1 \times L_2 \times \dots \times L_n$ si definiscano due operazioni \vee e \wedge ponendo

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

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

per ogni $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in L_1 \times L_2 \times \dots \times L_n$. Si provi che $L_1 \times L_2 \times \dots \times L_n$ è un reticolo (detto il *prodotto diretto* dei reticolati L_1, L_2, \dots, L_n). Si dia l'analogia definizione di prodotto diretto di algebre di Boole.

31.11. Consideriamo l'algebra di Boole $\{0, 1\}$ con due elementi, corrispondente all'anello di Boole \mathbb{Z}_2 . Si provi che se B è algebra di Boole finita con almeno due elementi, allora $B \cong \underbrace{\{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}}_{m \text{ volte}} \cong \{0, 1\}$, cioè B è isomorfa al prodotto diretto di m copie dell'algebra di Boole

$\{0, 1\}$, per un opportuno intero positivo m . [Suggerimento: corollari 31.10 e 31.11.]

31.12. Si consideri il sottoinsieme L di \mathbb{N} i cui elementi sono tutti i divisori positivi di 330. L'ordine $|$ su \mathbb{N} induce un ordine, che denoteremo ancora con il simbolo $|$, su L .

(a) Si determini un isomorfismo di insiemi parzialmente ordinati tra $(L, |)$ e $(\mathcal{P}(X), \subseteq)$, dove $X = \{1, 2, 3, 4\}$.

(b) Si deduca da (a) che $(L, |)$ è un reticolo booleano.

Sia $(L, \vee, \wedge,')$ l'algebra di Boole associata al reticolo booleano $(L, |)$.

(c) Si dica come sono definite le tre operazioni \vee , \wedge e $'$.

(d) Si dica se $\{1, 3, 330\}$ è una sottoalgebra di Boole di L .

(e) Si dica se $\{1, 2, 165, 330\}$ è una sottoalgebra di Boole di L .

(f) Sia $\varphi: L \rightarrow \{0, 1\}$ definita da

$$\varphi(x) = \begin{cases} 0 & \text{se } 2 \text{ non divide } x \\ 1 & \text{se } 2 \text{ divide } x. \end{cases}$$

Si dica se φ 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 $0 \leq 1$.

31.13. 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.

31.14. 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 $(\mathcal{P}(Y), \cup, \cap, ')$.

31.15. Sia L il reticolo booleano dell'esercizio 30.14, e sia $\varphi: L \rightarrow \{0, 1\}$ definita da $\varphi(f) = f(\pi)$ per ogni $f \in L$. Si dica se φ è un omomorfismo di algebre di Boole.

31.16. Sia L il reticolo booleano dell'esercizio 30.14.

- Si determinino come sono definite le operazioni \vee, \wedge e $'$ nell'algebra di Boole associata.
- Sia $\varphi: \mathbb{R} \rightarrow \mathbb{R}$ 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 Φ è un isomorfismo di algebre di Boole.
- Si costruisca un isomorfismo di algebre di Boole tra

$$L \quad \text{e} \quad (\mathcal{P}(\mathbb{R}), \cup, \cap, ').$$

31.17. 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 $(B, \vee, \wedge, ')$ è un ideale di B se e solo se I è un ideale del reticolo (B, \vee, \wedge) (vedi esercizio 31.5).

31.18. 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:

- I è un ideale dell'algebra di Boole B (vedi esercizio precedente);
- I è un ideale dell'anello B .

31.19. 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:

- se I è un ideale di B , allora $F_I = \{x' \mid x \in I\}$ è un filtro di B ;
- se F è un filtro di B , allora $I_F = \{x' \mid x \in F\}$ è un ideale di B ;
- 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;
- 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 $(\mathcal{P}(X), \cup, \cap, ')$;
- 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 .

31.20. 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?

31.21. Si determinino gli insiemi finiti A per i quali le algebre di Boole

$$\mathcal{B}(x_1, x_2, x_3) \quad \text{e} \quad \mathcal{P}(A)$$

sono isomorfe.

31.22. 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) $(x_1 \wedge x_2)' \vee x_1'$.

31.23. 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 .

Capitolo 5

QUALCHE NOZIONE DI LOGICA MATEMATICA

§32. Logica proposizionale

In questo §32 e nel seguente soffermeremo la nostra attenzione su alcune delle nozioni elementari di logica matematica da noi ripetutamente usate fino ad ora in questo libro in modo "ingenuo". La logica nasce come studio del ragionamento deduttivo; essa analizza i passaggi che permettono di dedurre un'affermazione a partire da delle ipotesi. Soffermiamoci un momento ad analizzare cosa si debba intendere per "deduzione corretta" e per "deduzione scorretta". Ecco alcuni esempi di deduzioni.

32.1 ESEMPI. (1) *Tutti gli uomini sono mortali. Socrate è un uomo. Quindi Socrate è mortale.*

(2) *Tutti i pesci sono animali. Il pesciolino rosso del mio acquario è un pesce. Quindi il pesciolino rosso del mio acquario è un animale.*

Queste sono certamente due deduzioni corrette. Si noti che entrambe hanno la stessa struttura, che è la seguente:

Tutti gli *A* sono *B*. *c* è *A*. Quindi *c* è *B*.

Ecco invece una deduzione certamente scorretta:

Ogni studente di informatica usa qualche computer. Ogni computer aiuta tutti coloro che lo usano. Quindi ogni computer aiuta qualche studente di informatica.

È facile infatti immaginare una situazione in cui tutti gli studenti usano un computer, tutti i computer sono utili, ma c'è un computer che non viene mai usato. □

Iniziamo la nostra indagine da un primo livello piuttosto grossolano, quello della cosiddetta *logica proposizionale*. Ci occuperemo pertanto di proposizioni, cioè di frasi, ma considereremo solo le cosiddette *proposizioni dichiarative*, cioè quelle che sono o vere o

false. Questo è sufficiente per quanto concerne la matematica. Per noi, quindi, una *proposizione* sarà un'espressione che è o vera o falsa, ma non contemporaneamente vera e falsa.

32.2 ESEMPI. Ecco alcuni esempi di proposizioni:

- $A \equiv$ "La mosca è un insetto";
- $B \equiv$ "L'elefante è un insetto";
- $C \equiv$ " $\sqrt{2} = 5$ ";
- $D \equiv$ "Singapore è in Europa".

Non sono invece proposizioni, nel senso da noi appena definito, le domande ("Quanti anni hai?"), le esclamazioni ("Buongiorno!"), o gli 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*. Quindi ogni proposizione ha un valore di verità. Ad esempio, il valore di verità della proposizione A degli esempi 32.2 è vero, il valore di verità delle proposizioni B , C e D è falso.

Analizziamo ora i vari modi in cui le proposizioni possono essere combinate tra loro. A partire da proposizioni molto semplici (atomiche) è possibile costruire proposizioni più complesse utilizzando i connettivi. Date due proposizioni A e B è infatti possibile formare le proposizioni

- (1) " A e B ", detta la *congiunzione* 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) "se A allora B " (o " A implica B "), detta *implicazione* e indicata con $A \rightarrow B$;
- (5) " A se e solo se B " (o anche "condizione necessaria e sufficiente affinché A è che B "), detta *doppia implicazione*, indicata con $A \leftrightarrow B$.

I simboli \wedge , \vee , \neg , \rightarrow , \leftrightarrow si dicono i *connettivi logici*. Se A , B , C , D sono le proposizioni degli esempi 32.2, 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". Si osservi che le proposizioni A , B , C , D degli esempi 32.2 non si possono scomporre ulteriormente connettendo proposizioni più semplici.

Nella logica classica, che è la logica a cui accenneremo in questo libro, si stabilisce che il valore di verità di una proposizione composta dipenda esclusivamente dai valori di verità delle proposizioni che la compongono. Ad esempio una proposizione del tipo $A \wedge B$ è vera se A e B sono vere, e questo indipendentemente da chi siano le proposizioni A e B . Più precisamente abbiamo:

- (1) $A \wedge B$ è vera se e solo se A e B sono entrambe vere;
- (2) $A \vee B$ è vera se e solo se A è vera oppure B è vera (inclusa la possibilità che A e B siano entrambe vere);

- (3) $\neg A$ è vera se e solo se A è falsa;
 (4) $A \rightarrow B$ è falsa se e solo se A è vera e B è falsa; in tutti gli altri casi $A \rightarrow B$ è vera;
 (5) $A \leftrightarrow B$ è vera se e solo se A e B hanno lo stesso valore di verità.

Ciò è descritto esplicitamente anche nella seguente *tavola di verità*, dove V sta per *vero* ed F sta per *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

32.3 ESEMPI. Continuiamo a denotare con A, B, C, D le proposizioni degli esempi 32.2. Quindi $A \wedge D \equiv$ “La mosca è un insetto e Singapore è in Europa” è una proposizione falsa, perché A è vera e D è falsa. Si osservi però un primo limite della nostra semplice modellizzazione del pensiero umano che deriva dal considerare vera la proposizione $A \wedge B$ se e solo se A e B sono entrambe vere. Nel linguaggio naturale il connettivo “e” ha spesso una connotazione temporale. Ad esempio si osservi quanto diverse sono in italiano i significati delle due espressioni “Gianni investì un pedone e accelerò” e “Gianni accelerò e investì un pedone”. Tale connotazione temporale si perde completamente con la nostra definizione del valore di verità della congiunzione $A \wedge B$.

Per illustrare un’ulteriore difficoltà legata alla nostra grossolana modellizzazione del linguaggio naturale consideriamo l’espressione “Gianni studia molto, ma non è antipatico”. In logica proposizionale il modo migliore che possiamo escogitare di decomporre tale proposizione in proposizioni atomiche è di considerarla una proposizione del tipo $A \wedge (\neg B)$, dove $A \equiv$ “Gianni studia molto” e $B \equiv$ “Gianni è antipatico”. In questo modo la congiunzione “ma” diventa però il connettivo “e”, e si viene pertanto a perdere completamente il valore avversativo del “ma”, cioè si viene a perdere la sfumatura di significato secondo la quale io mi aspettavo che Gianni, studiando molto, dovesse essere antipatico.

Tornando agli esempi 32.2, $A \vee D$ è la proposizione “La mosca è un insetto oppure Singapore è in Europa”. Questa è una proposizione vera, perché “La mosca è un insetto” è una proposizione vera, ed il fatto che “Singapore è in Europa” sia falsa non ha alcuna importanza in questo contesto. Si osservi che il valore di verità di $A \vee B$ è stata definito in senso inclusivo, cioè $A \vee B$ è vera anche quando A e B sono entrambe vere. Molto spesso, invece, nel linguaggio naturale la congiunzione “o” è adoperata in senso esclusivo (*l'aut latino*), cioè o questo è vero, o quello è vero, ma non sono entrambi veri.

Facendo sempre riferimento agli esempi 32.2 vediamo che $\neg B \equiv$ “L’elefante non è un insetto” è una proposizione vera, $A \rightarrow C \equiv$ “Se la mosca è un insetto allora $\sqrt{2} = 5$ ” è una proposizione falsa, $B \rightarrow A \equiv$ “Se l’elefante è un insetto allora la mosca è un insetto” è una proposizione vera, $B \rightarrow C \equiv$ “Se l’elefante è un insetto allora $\sqrt{2} = 5$ ” è vera, $D \rightarrow D \equiv$ “Se Singapore è in Europa allora Singapore è in Europa” è vera, e infine $B \leftrightarrow C \equiv$ “L’elefante è un insetto se e solo se $\sqrt{2} = 5$ ” è vera.

Si faccia attenzione quindi ai connettivi \rightarrow e \leftrightarrow e a come viene definito il valore di verità delle proposizioni $A \rightarrow B$ e $A \leftrightarrow B$. Il fatto che “Se l’elefante è un insetto allora $\sqrt{2} = 5$ ” e “Se $\sqrt{2} = 5$ allora la mosca è un insetto” siano per noi delle proposizioni vere può sembrare un po’ strano, innanzitutto perché nelle implicazioni $A \rightarrow B$ di cui si fa solitamente uso nel linguaggio naturale si è abituati ad una correlazione di tipo causa ed effetto tra l’antecedente A e il conseguente B (come ad esempio in “Se Singapore è in Europa allora gli abitanti di Singapore sono europei”).

Ecco infine un’ulteriore difficoltà che incontriamo nel giustificare la tavola di verità del connettivo \rightarrow . Scommettiamo con un nostro amico che se stasera Gianni va al cinema allora Andrea resta a casa. È chiaro che se Gianni va al cinema e Andrea resta a casa allora abbiamo vinto la scommessa, ed è altrettanto chiaro che se Gianni va al cinema e Andrea non resta a casa allora abbiamo perso la scommessa. Ma non è così chiaro chi vinca la scommessa se Gianni non va al cinema, perché nel linguaggio naturale non è evidente quale valore di verità dare ad $A \rightarrow B$ quando l’antecedente A non si verifica. D’altra parte $A \rightarrow B$ è una proposizione e nella logica classica abbiamo stabilito che ogni proposizione debba essere vera o falsa, qualunque siano le proposizioni A e B . Inoltre il valore di verità di $A \rightarrow B$ deve dipendere solo dal valore di verità di A e di B . Dobbiamo quindi dare un valore di verità ad ogni implicazione, anche nel caso in cui l’antecedente sia falso. □

Nello studio del ragionamento deduttivo riveste una notevole importanza il linguaggio nel quale viene fatto la deduzione, che può essere ad esempio il linguaggio naturale o il linguaggio matematico. La logica classica nacque come studio del linguaggio naturale, ma come si è visto negli esempi 32.3 la formalizzazione in tale logica di frasi e deduzioni è molto riduttiva. Come vedremo, tale formalizzazione risulta invece molto più appropriata per quanto riguarda il linguaggio matematico.

32.4 ESEMPIO. Abbiamo già detto che la logica classica considera vera un’implicazione quando l’antecedente è falso. Per giustificare tale scelta facciamo ricorso ad un esempio nel linguaggio matematico. Consideriamo la proposizione “Per ogni terna (x, y, z) di numeri interi, se x divide y oppure x divide z allora x divide yz . Questa proposizione è vera per i numeri interi (è facilmente dimostrabile a partire dalla definizione di divisibilità) ed è quindi ancora vera ogniqualvolta sostituiamo alle variabili x, y, z dei numeri interi. Considerando $x = 4$, $y = 2$ e $z = 2$ si ottiene la proposizione “Se 4 divide 2 oppure 4 divide 2 allora 4 divide 4”, mentre considerando $x = 3$, $y = 2$ e $z = 2$ si ottiene la proposizione “Se 3 divide 2 oppure 3 divide 2 allora 3 divide 4”. La prima proposizione è del tipo “falso implica vero”, mentre la seconda è del tipo “vero implica falso”, ed entrambe devono risultare vere, come istanze di una proposizione universalmente vera, cioè come casi particolari di una proposizione sempre vera. □

Sintetizzando: se A, B, C, \dots sono proposizioni, applicando ripetutamente i connettivi logici nel modo sopra descritto (ossia \neg viene posto prima di una proposizione, mentre $\wedge, \vee, \rightarrow, \leftrightarrow$ si pongono tra due proposizioni) è possibile formare *proposizioni composte* sempre più complesse. Una volta stabilito il valore di verità delle proposizioni atomiche,

utilizzando le tavole di verità possiamo stabilire univocamente il valore di verità di ogni proposizione composta costruita a partire da tali proposizioni atomiche.

Formule della logica proposizionale

Per meglio comprendere il concetto di *formula (della logica 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 *formule 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 formule polinomiali;
- se f e g sono formule polinomiali, allora $(f + g), (-f), (f \cdot g)$ sono formule polinomiali;
- sono formule polinomiali (nelle variabili x_1, x_2, \dots, x_n) solo le espressioni ottenute per mezzo di (a) e (b).

Effettueremo un procedimento simile per le proposizioni invece che per i numeri reali, ottenendo le formule della logica proposizionale invece che le formule polinomiali.

Consideriamo n simboli A_1, A_2, \dots, A_n che chiameremo *variabili proposizionali*. Le *formule* (nelle variabili A_1, A_2, \dots, A_n) sono le espressioni definite nel modo seguente:

- A_1, A_2, \dots, A_n sono formule;
- se P e Q sono formule, allora $(P \wedge Q), (P \vee Q), (\neg P), (P \rightarrow Q)$ e $(P \leftrightarrow Q)$ sono formule;
- sono formule (nelle variabili A_1, A_2, \dots, A_n) solo le espressioni ottenute per mezzo di (a) e (b).

32.5 ESEMPIO. Consideriamo le variabili proposizionali A e B . Allora $(A \rightarrow B)$ e $(\neg A)$ sono formule. Anche $((\neg A) \vee B)$ è una formula, e pertanto anche $((A \rightarrow B) \leftrightarrow ((\neg A) \vee B))$ è una formula. \square

Conviene introdurre a questo punto due convenzioni per limitare l'uso delle parentesi, il cui numero può crescere rapidamente al crescere della complessità della formula. Innanzitutto eliminiamo le parentesi più esterne. Poi, come con le formule polinomiali e in aritmetica si “eseguono prima” l’operazione di moltiplicazione \cdot e poi le operazioni di addizione $+$ e di sottrazione $-$, 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 .

32.6 ESEMPIO. 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 formula 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 formula in n variabili ha 2^n righe.

32.7 ESEMPIO. Ecco le tavole di verità delle formule

$$A \wedge B \rightarrow (A \rightarrow (A \rightarrow B)) \quad \text{e} \quad A \wedge (A \rightarrow B) \rightarrow B :$$

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	\square
V	F	F	F	V	
F	V	V	F	V	
F	F	V	F	V	

Entrambe le formule $A \wedge B \rightarrow (A \rightarrow (A \rightarrow B))$ e $A \wedge (A \rightarrow B) \rightarrow B$ dell'esempio 32.7 sono sempre vere, qualunque siano i valori di verità assegnati alle variabili A e B . Una formula 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 formule dell'esempio 32.7 sono entrambe tautologie. Anche $A \vee \neg A$ è una tautologia.

Una formula che sia sempre falsa, indipendentemente dai valori di verità assegnati alle sue variabili proposizionali, si dice una *contraddizione*. Quindi una formula P è una contraddizione se e solo se $\neg P$ è una tautologia. Ad esempio $A \wedge \neg A$ è una contraddizione.

Conseguenza logica

Diremo che una formula Q della logica proposizionale è *conseguenza logica* di una formula P se Q è vera ogniqualvolta P è vera. Scriveremo in tal caso $P \models Q$. Più in generale, se P_1, \dots, P_n sono formule, diremo che una formula Q è *conseguenza logica* di P_1, \dots, P_n , e scriveremo $P_1, \dots, P_n \models Q$ o $\{P_1, \dots, P_n\} \models Q$, se Q è vera ogniqualvolta P_1, \dots, P_n sono vere. Diremo che due formule P e Q sono *semanticamente equivalenti* se $P \models Q$ e $Q \models P$.

32.8 ESEMPIO (MODUS PONENS). Si ha $P, P \rightarrow Q \models Q$. Infatti la tavola di verità di $P \rightarrow Q$ è la seguente:

P	Q	$P \rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Esaminando la tavola vediamo che c'è un unico caso in cui P e $P \rightarrow Q$ sono entrambe vere, quello corrispondente alla prima riga. In questo caso anche Q è vera. Quindi $P, P \rightarrow Q \models Q$. \square

32.9 ESEMPIO. Mostriamo invece che P non è conseguenza logica di Q e $P \rightarrow Q$ (in simboli $Q, P \rightarrow Q \not\models P$). Guardando la tavola di verità dell'esempio 32.8 vediamo che ci sono due casi in cui Q e $P \rightarrow Q$ sono entrambe vere (quelli corrispondenti alla prima e alla terza riga). Ma nel caso che corrisponde alla terza riga P è falsa. Ecco quindi che $Q, P \rightarrow Q \not\models P$. \square

Quindi dire che P e Q sono semanticamente equivalenti vuol dire che P è vera se e solo se Q è vera, cioè che P e Q hanno le stesse tavole di verità. Pertanto:

32.10 LEMMA. *Se P e Q sono formule della logica proposizionale, le seguenti affermazioni sono equivalenti:*

- P e Q sono semanticamente 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;*
- P è falsa per una data assegnazione di valori di verità alle variabili se e solo se Q è falsa per la stessa assegnazione.*

32.11 ESEMPIO. Mostriamo che $P \rightarrow Q$ e $\neg Q \rightarrow \neg P$ sono semanticamente equivalenti. Se $P \rightarrow Q$ è vera, allora dalla tavola di verità di $P \rightarrow Q$ vediamo che Q è vera oppure P è falsa. Quindi $\neg Q$ è falsa oppure $\neg P$ è vera. In entrambi i casi $\neg Q \rightarrow \neg P$ è vera. Viceversa, se $\neg Q \rightarrow \neg P$ è vera, allora $\neg Q$ è falsa oppure $\neg P$ è vera, e quindi Q è vera oppure P è falsa. In entrambi i casi $P \rightarrow Q$ è vera. \square

Diremo che una deduzione è *corretta* quando a partire da certe premesse giungiamo a delle conclusioni in modo che ognqualvolta le premesse sono vere anche le conclusioni sono vere. Quindi diremo che un deduzione è corretta quando a partire da P_1, \dots, P_n otteniamo Q con una serie di passaggi deduttivi in modo che $P_1, \dots, P_n \models Q$.

Esercizi svolti

32.1. Si dimostri che se P e Q sono formule, allora le formule $P \rightarrow Q$, $\neg P \vee Q$, $\neg(P \wedge \neg Q)$, $\neg Q \rightarrow \neg P$ sono semanticamente equivalenti tra loro.

Soluzione. Per il lemma 32.10 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	$\neg P$	$\neg P \vee Q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	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	$\neg P$	$\neg Q$	$\neg Q \rightarrow \neg P$
V	V	F	F	V
V	F	F	V	F
F	V	V	F	V
F	F	V	V	V

Pertanto le quattro formule indicate sono tutte semanticamente equivalenti tra loro. \square

L'equivalenza semantica delle formule $P \rightarrow Q$, $\neg Q \rightarrow \neg P$ e $\neg(P \wedge \neg Q)$ appena dimostrata è 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 dimostrare che da $\neg Q$ segue $\neg P$ (*dimostrazione per contrapposizione*, o *indiretta*), oppure ragionare *per assurdo*, supponendo $P \wedge \neg Q$, e giungendo a una contraddizione (il che equivale a dimostrare $\neg(P \wedge \neg Q)$).

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.* Dimostriamolo direttamente, per contrapposizione e per assurdo.

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 $2|ab$. Come è stato dimostrato nell'esercizio 4.10, se un numero primo divide un prodotto, esso divide uno dei fattori. Quindi $2|a$ oppure $2|b$. 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

32.2. Si determini il valore di verità delle seguenti proposizioni:

- (a) Se $\sqrt{2} \neq 5$ allora \mathbb{N} è un insieme infinito.
- (b) Se \mathbb{N} è un insieme finito allora $\sqrt{2} = 5$.
- (c) Se \mathbb{N} è un insieme finito, si ha che $\sqrt{2} = 5$ e che Palermo è una città della Sicilia.

- (d) Se \mathbb{N} è un insieme finito e Palermo è una città della Sicilia, allora $\sqrt{2} = 5$.
 (e) Se \mathbb{N} è un insieme finito e Palermo non è una città della Sicilia, allora $\sqrt{2} = 5$.

32.3. La formula nelle variabili A, B, C

$$A \vee (\neg A \wedge B) \vee \neg(B \wedge \neg C) \rightarrow C$$

è una tautologia?

32.4. La formula nelle variabili A e B

$$A \wedge B \rightarrow A \vee B$$

è una tautologia?

32.5. La formula nelle variabili A, B, C

$$(A \rightarrow B \vee C) \leftrightarrow (C \rightarrow (A \wedge \neg B))$$

è una contraddizione?

32.6. Si dimostri che

$$(A \rightarrow B), (B \rightarrow C) \models (A \rightarrow C).$$

32.7. Si dimostri che le formule

$$A \vee B \rightarrow C \quad \text{e} \quad (A \rightarrow C) \wedge (B \rightarrow C)$$

nelle variabili proposizionali A, B e C sono semanticamente equivalenti.

32.8. Le formule

$$(\neg A \wedge C) \vee B \vee \neg(A \vee C) \quad \text{e} \quad (A \rightarrow B) \wedge (A \vee B \rightarrow B)$$

nelle variabili A, B, C sono semanticamente equivalenti?

32.9. Per ciascuna delle formule seguenti si determini una formula semanticamente equivalente ma "più semplice":

- (a) $A \wedge (A \rightarrow B)$;
- (b) $A \wedge (A \vee B)$;
- (c) $(A \rightarrow B) \wedge \neg B$;
- (d) $A \vee \neg A \rightarrow B$.

§33. Logica predicativa

La logica proposizionale è poco espressiva e non permette nemmeno di riconoscere se siano corrette semplici deduzioni come quelle degli esempi 32.1. Per poter parlare delle proprietà degli elementi di una struttura matematica, e per poter quindi analizzare i ragionamenti deduttivi che vengono utilizzati nel corso di una dimostrazione, introduciamo la logica predicativa. Partiamo con un esempio. Denotiamo, come al solito, con \mathbb{N}

L'insieme dei numeri naturali, con \leq l'ordinamento usuale su \mathbb{N} , e con $+$ e \cdot le operazioni di addizione e moltiplicazione su \mathbb{N} . Denotiamo poi con S l'operazione unaria di \mathbb{N} che associa ad ogni numero naturale x il suo successore $x + 1$, ossia l'applicazione $S: \mathbb{N} \rightarrow \mathbb{N}$ definita da $S(x) = x + 1$. Denotiamo infine con 0 il numero naturale zero, cioè la costante zero. Scriveremo delle formule che descrivano le proprietà degli elementi della struttura $(\mathbb{N}, \leq, +, \cdot, S, 0)$, cioè degli elementi di \mathbb{N} , dove \mathbb{N} si intende dotato della relazione \leq , delle operazioni $+$, \cdot e S , e della costante 0 . Ecco alcuni esempi delle proprietà che vogliamo scrivere:

- (a) x è diverso da 0 ;
- (b) 0 non è il successore di alcun numero naturale;
- (c) x è pari;
- (d) 0 non è pari;
- (e) x è dispari;
- (f) per ogni numero naturale x, y si ha $xy = yx$;
- (g) $x^2 > 1$;
- (h) x è un numero primo;
- (i) se x e y sono dispari, allora anche xy è dispari;
- (j) 2 è l'unico numero pari primo.

Per scrivere queste proprietà faremo uso dei simboli seguenti

- (1) le variabili individuali x, y, z, \dots ;
- (2) i connettivi logici $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$;
- (3) il simbolo di uguaglianza $=$;
- (4) i quantificatori \forall, \exists ;
- (5) i simboli ausiliari $(,)$ e $,;$;
- (6) il simbolo predicativo \leq ;
- (7) i simboli funzionali $+, \cdot, S$;
- (8) la costante 0 .

Vediamo una ad una queste otto classi di simboli. Come sempre in matematica le *variabili individuali* x, y, z, \dots sono quelle che denotano ciascuna un generico elemento, in questo caso un generico elemento di \mathbb{N} . Abbiamo già studiato in precedenza i *connettivi logici* $\wedge, \vee, \neg, \rightarrow$ e \leftrightarrow , mentre il *simbolo di uguaglianza* $=$ e i *simboli ausiliari* $(,)$ e $,;$, non hanno bisogno di spiegazione: i simboli ausiliari hanno lo stesso scopo dei segni di interpunkzione nel linguaggio naturale. Vediamo i *quantificatori* \forall (per ogni) ed \exists (esiste). Se φ è una formula, indicheremo con $\forall x \varphi$ la formula "per ogni $x \varphi$ ". Il simbolo \forall si legge quindi "per ogni" ed è detto *quantificatore universale*. Similmente indicheremo con $\exists x \varphi$ la formula "esiste x tale che φ ". Il simbolo \exists si legge "esiste" ed è detto *quantificatore esistenziale*. I *simboli predicativi* sono quelli che denotano le relazioni. I *simboli funzionali* denotano le applicazioni e le operazioni (che sono particolari applicazioni). Infine le *costanti* servono per denotare elementi particolari, nel nostro esempio il numero naturale zero.

Ecco come è possibile scrivere con queste otto classi di simboli le precedenti proprietà (a)-(j):

- (a) $\neg(x = 0)$
- (b) $\neg\exists x(0 = S(x))$
- (c) $\exists z(x = S(S(0)) \cdot z)$
- (d) $\neg(\exists y(0 = S(S(0)) \cdot y))$
- (e) $\neg\exists z(x = S(S(0)) \cdot z)$
- (f) $\forall x\forall y(x \cdot y = y \cdot x)$
- (g) $(S(0) \leq x \cdot x) \wedge \neg(x \cdot x = S(0))$
- (h) $\neg(x = S(0)) \wedge \forall y\forall z(x = y \cdot z \rightarrow y = S(0) \vee z = S(0))$
- (i) $\forall x\forall y(P(x) \wedge P(y) \rightarrow P(x \cdot y))$, dove $P(x)$ è la formula scritta in (e) e $P(y)$, $P(x \cdot y)$ si ottengono da tale formula sostituendo rispettivamente x con y e con $x \cdot y$ rispettivamente;
- (j) $\forall x(Q_1(x) \wedge Q_2(x) \leftrightarrow x = S(S(0)))$, dove $Q_1(x)$ è la formula scritta in (c) e $Q_2(x)$ è la formula scritta in (h).

Si osservi che (b), (f), (i) e (j) sono vere in \mathbb{N} , (d) è falsa in \mathbb{N} , mentre non ha senso chiedersi se (a), (c), (e), (g) ed (h) sono vere o false in \mathbb{N} , perché la verità o falsità di tali espressioni dipende da come interpretiamo x , ossia dipende dal valore che diamo alla variabile x . Ad esempio, (a) è vera se x è interpretata come 0, mentre è falsa se x è interpretata come 1.

Nel nostro esempio abbiamo introdotto i simboli \leq , $+$, \cdot , S , 0 per esprimere alcune proprietà dei numeri naturali. D'altra parte, questo stesso "linguaggio" può essere usato per esprimere proprietà dei numeri interi, o razionali, o reali e più in generale di ogni struttura matematica dotata di una relazione binaria \leq , di due operazioni binarie $+$, \cdot , di un'operazione unaria S e in cui un elemento del dominio viene chiamato 0. Ad esempio, possiamo interpretare tali simboli nel modo naturale sugli interi, ed in questa interpretazione la proprietà (b) dell'esempio precedente è falsa, perché nei numeri interi lo zero è il successore di -1 . Considerando invece la proprietà $\forall x(x \leq S(x))$ notiamo che questa è falsa se interpretiamo \leq come l'ordine usuale sugli interi e S come l'operazione unaria "predecessore" che associa ad ogni numero intero z il numero $z - 1$.

Più in generale, un *linguaggio* (del primo ordine, con identità) \mathcal{L} è costituito dai simboli seguenti:

- (1) le variabili individuali $x_1, x_2, \dots, x_n, \dots$;
- (2) i connettivi logici $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$;
- (3) il simbolo di uguaglianza $=$;
- (4) i quantificatori \forall, \exists ;
- (5) i simboli ausiliari $(,)$ e $,$;
- (6) i simboli predicativi;
- (7) i simboli funzionali;
- (8) le costanti individuali.

I simboli da (1) a (4) sono detti *simboli logici*. I simboli logici e i simboli ausiliari fanno parte di ogni linguaggio. Dipendono invece dal linguaggio in considerazione i simboli funzionali (che denotano le operazioni n -arie, ossia le applicazioni $\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}} \rightarrow A$;

abbiamo già incontrato i simboli $+$, \cdot , \circ per denotare operazioni binarie e il simbolo $'$ per denotare la complementazione, che è un'operazione unaria, nelle algebre di Boole), i simboli predicativi (che denotano le relazioni n -arie, ossia i sottoinsiemi di $\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}}$;

ad esempio abbiamo spesso usato i simboli predicativi binari \leq e \sim per denotare ordinamenti ed equivalenze) e le costanti individuali (usate per denotare particolari elementi, come 0 e 1 negli anelli o nei reticolati limitati).

33.1 ESEMPIO (IL LINGUAGGIO DEGLI INSIEMI PARZIALMENTE ORDINATI). È costituito oltre che dai simboli logici e dai simboli ausiliari, da un unico simbolo predicativo \leq . Non ha né simboli funzionali né costanti individuali. Ad esempio l'assioma a cui deve soddisfare un insieme parzialmente ordinato si può esprimere come

$$\forall x \forall y \forall z ((x \leq x) \wedge ((x \leq y) \wedge (y \leq x) \rightarrow (x = y)) \wedge ((x \leq y) \wedge (y \leq z) \rightarrow (x \leq z))). \quad \square$$

33.2 ESEMPIO (IL LINGUAGGIO DEGLI ANELLI CON IDENTITÀ). È costituito oltre che dai simboli logici e dai simboli ausiliari, da due simboli funzionali binari $+$, \cdot e da due costanti individuali 0, 1. Non ha simboli predicativi. Ad esempio un anello con identità deve soddisfare a

$$\begin{aligned} & \forall x \forall y \forall z ((x + (y + z) = (x + y) + z) \wedge (x + y = y + x) \\ & \quad \wedge (x + 0 = x) \wedge (\exists w (x + w = 0)) \wedge (x(yz) = (xy)z) \\ & \quad \wedge ((x + y)z = xz + yz) \wedge (x(y + z) = xy + xz) \wedge (x \cdot 1 = x) \wedge (1 \cdot x = x)). \quad \square \end{aligned}$$

33.3 ESEMPIO (IL LINGUAGGIO DELLE ALGEBRE DI BOOLE). È costituito, oltre che dai simboli logici e dai simboli ausiliari, da tre simboli funzionali (di cui due binari, \wedge , \vee , e uno unario, $'$) e da due costanti individuali, 0, 1. Non ha simboli predicativi. \square

I linguaggi del primo ordine sono degli "alfabeti" coi quali è possibile costruire parole e frasi. È pertanto necessario individuare quali regole di costruzione diano luogo ad espressioni "grammaticalmente corrette". Ad esempio nel linguaggio degli insiemi parzialmente ordinati l'espressione $\exists x \forall y (x \leq y)$ (\equiv "esiste x tale che per ogni y si ha $x \leq y$ ") è una formula "corretta", che è vera negli insiemi parzialmente ordinati dotati di minimo mentre non lo è in quelli privi di minimo. Invece l'espressione $xy \forall z (x \leq y)$, formata con gli stessi simboli, non è "corretta". È necessario quindi dare una "grammatica", cioè delle regole che permettano di costruire "espressioni corrette". Il metodo è il seguente.

Si dicono *termini* le espressioni definite nel modo seguente:

- (a) le variabili individuali e le costanti individuali sono termini;
- (b) se t_1, t_2, \dots, t_n sono termini ed f è un simbolo funzionale n -ario, allora

$$f(t_1, t_2, \dots, t_n)$$

è un termine;

- (c) un'espressione è un termine solo se è ottenuta in base ad (a) e (b).

I termini di un linguaggio vengono usati quindi per denotare elementi di una struttura in cui il linguaggio è interpretato. Ad esempio nella struttura \mathbb{N} in cui S è interpretato come la funzione successore il termine $S(S(0))$ denota il numero 2. Invece nella struttura \mathbb{Z} in cui S è interpretato come la funzione predecessore lo stesso termine $S(S(0))$ denota il numero -2.

Si dicono *formule* le espressioni definite nel modo seguente:

- (a) se t_1, t_2, \dots, t_n sono termini ed A è un simbolo predicativo n -ario, allora

$$A(t_1, t_2, \dots, t_n)$$

è una formula;

- (b) se t_1, t_2 sono termini, allora $t_1 = t_2$ è una formula;
 (c) se α e β sono formule, anche $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\neg \alpha)$, $(\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$ sono formule;
 (d) se α è una formula e x è una variabile individuale, anche $\forall x \alpha$ ed $\exists x \alpha$ sono formule;
 (e) un'espressione è una formula solo se è ottenuta in base ad (a), (b), (c) e (d).

Nel linguaggio degli anelli con identità dell'esempio 33.2 i termini sono espressioni ottenute a partire solo da $x_1, x_2, \dots, x_n, \dots, 0, 1, +, \cdot$. Quindi $(x_1 + x_2) \cdot x_1 + 1$ è un termine, mentre l'espressione che devono soddisfare gli anelli con identità scritta nell'esempio 33.2 è una formula.

In analogia a quanto fatto nella logica proposizionale, possiamo dare ora la nozione di conseguenza logica: una formula α è *conseguenza logica* delle formule $\alpha_1, \dots, \alpha_n$ (in simboli: $\alpha_1, \dots, \alpha_n \models \alpha$) se α è vera in ogni interpretazione che rende vere tutte le formule $\alpha_1, \dots, \alpha_n$.¹ Diremo allora che una deduzione che ottiene α a partire dalle ipotesi $\alpha_1, \dots, \alpha_n$ è corretta se $\alpha_1, \dots, \alpha_n \models \alpha$.

Se formalizziamo la deduzione dell'esempio 32.1(1) ponendo $U(x) \equiv "x \text{ è un uomo}"$, $M(x) \equiv "x \text{ è mortale}"$ ed $s \equiv \text{Socrate}$, vediamo che in tale esempio si deduceva la formula $M(s)$ a partire dalle formule $\forall x(U(x) \rightarrow M(x))$ e $U(s)$. Tale deduzione è corretta perché

$$\forall x(U(x) \rightarrow M(x)), U(s) \models M(s).$$

Allo stesso modo, riconosciamo la correttezza della deduzione svolta nell'esempio 32.1(2), che viene formalizzata esattamente nello stesso modo. L'unica differenza è che ora interpretiamo $U(x)$ come "x è un pesce", $M(x)$ come "x è un animale" ed s come "il pesciolino rosso del mio acquario".

Consideriamo invece la seguente "deduzione": *Tutti gli uomini sono mortali. Socrate è mortale. Quindi Socrate è un uomo.*

Secondo la nostra definizione tale deduzione non è corretta, anche se la conclusione "Socrate è un uomo" è vera. Infatti la sua formalizzazione porta a dedurre la formula $M(s)$ a partire dalle ipotesi $\forall x(U(x) \rightarrow M(x))$ e $M(s)$, ma si vede facilmente che $M(s)$ non è conseguenza logica di $\forall x(U(x) \rightarrow M(x))$ e $M(s)$. Si consideri ad esempio una

¹In realtà questa non è proprio la definizione formale di conseguenza logica; la definizione è tecnicamente più complessa, basandosi sul concetto di verità di una formula in una struttura che non abbiamo formalmente definito in questa nostra breve introduzione alla logica matematica.

interpretazione in cui il significato dei simboli U ed M non cambia, ma dove s non indica il filosofo Socrate bensì "il pesciolino rosso del mio acquario". In questa interpretazione, le formule $\forall x(U(x) \rightarrow M(x))$ e $M(s)$ sono vere, ma $U(s)$ è falsa. Quindi $U(s)$ non è conseguenza logica di $\forall x(U(x) \rightarrow M(x))$ e $M(s)$.

Restiamo su questo esempio. Sia $M(x) \equiv "x \text{ è mortale}"$. Allora $\forall xM(x)$ è "per ogni x , x è mortale" o meglio "ogni x è mortale" o anche "tutti gli x sono mortali". Qual è la negazione di $\forall xM(x)$? Cioè, cos'è $\neg\forall xM(x)$? È evidentemente "non tutti gli x sono mortali" che equivale a "esiste un x che non è mortale", ossia $\exists x\neg M(x)$. Più in generale: per qualunque formula φ si ha che $\neg\forall x\varphi$ equivale a $\exists x\neg\varphi$ (nel senso che sono una conseguenza logica dell'altra). Similmente avviene negando il quantificatore esistenziale: si ha che $\neg\exists x\varphi$ equivale a $\forall x\neg\varphi$. Se si scambiano il connettivo \neg con i quantificatori \forall ed \exists , i quantificatori \forall ed \exists si scambiano tra loro: $\neg\forall x\varphi$ è equivalente ad $\exists x\neg\varphi$, e $\neg\exists x\varphi$ è equivalente a $\forall x\neg\varphi$.

33.4 ESEMPIO. Si consideri la formula $\forall x_1\forall x_2(x_1 = x_2)$, che è vera in qualunque insieme di cardinalità ≤ 1 . La sua negazione è $\neg\forall x_1\forall x_2(x_1 = x_2)$ (\equiv "non si ha che per ogni x_1 e per ogni x_2 , $x_1 = x_2$ "), che equivale a $\exists x_1\neg\forall x_2(x_1 = x_2)$ (\equiv "esiste x_1 tale che non per ogni x_2 , $x_1 = x_2$ "), o anche a $\exists x_1\exists x_2\neg(x_1 = x_2)$ (\equiv "esiste x_1 ed esiste x_2 tali che $x_1 \neq x_2$ "). \square

Concludiamo qui la nostra breve introduzione alle prime nozioni di logica matematica. Abbiamo visto come si riconosce una "deduzione corretta" (grazie al concetto di conseguenza logica), ma non sappiamo ancora come costruire effettivamente una dimostrazione di una data proprietà a partire da certe ipotesi. A questo scopo l'idea è quella di isolare un certo numero di *regole elementari di inferenza*, cioè di deduzione (come ad esempio il *modus ponens* che abbiamo già incontrato nell'esempio 32.8: da P e $P \rightarrow Q$ segue Q), e di ottenere una dimostrazione di una proprietà partendo da proprietà note e usando più volte tali regole. Ad esempio per dimostrare che una data proprietà vale per i gruppi abeliani si parte dagli assiomi dei gruppi abeliani e si applicano più volte le regole elementari di inferenza. Il lettore interessato potrà approfondire questi argomenti in un qualunque libro di logica matematica.

Esercizi svolti

33.1. Sia \mathcal{L} il linguaggio del primo ordine con identità privo di simboli predicativi, di simboli funzionali e di costanti individuali. Le due formule $\forall x\exists y(x = y)$ ed $\exists y\forall x(x = y)$ sono vere o false in un insieme D con almeno due elementi? Se ne deduca che bisogna fare molta attenzione nello scambiare i quantificatori, perché questo non è lecito in generale.

Soluzione. Sia D un insieme con almeno due elementi. La formula $\forall x\exists y(x = y)$ è vera in D . È infatti sufficiente prendere per ogni elemento $x \in D$ lo stesso elemento $y = x$. Invece la formula $\exists y\forall x(x = y)$ è falsa perché D ha almeno due elementi. Quindi non è generalmente lecito scambiare i quantificatori. \square

33.2. Siano $p(x, y)$ e $q(x, y, z)$ due formule nelle variabili individuali x, y e x, y, z rispettivamente. Si neghino per esercizio le seguenti formule:

- (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 $\exists x \exists y p(x, y)$ si hanno le seguenti formule tutte equivalenti tra loro:

$$\begin{aligned} & \neg \exists x \exists y p(x, y) \\ & \forall x \neg \exists y p(x, y) \\ & \forall x \forall y \neg p(x, y). \end{aligned}$$

(b) Negando $\forall x \exists y (p(x, y) \vee \exists z q(x, y, z))$ si ha la seguente successione di formule equivalenti tra loro:

$$\begin{aligned} & \neg \forall x \exists y (p(x, y) \vee \exists z q(x, y, z)) \\ & \exists x \neg \exists y (p(x, y) \vee \exists z q(x, y, z)) \\ & \exists x \forall y \neg (p(x, y) \vee \exists z q(x, y, z)) \\ & \exists x \forall y (\neg p(x, y) \wedge \neg \exists z q(x, y, z)) \\ & \exists x \forall y (\neg p(x, y) \wedge \forall z \neg q(x, y, z)). \quad \square \end{aligned}$$

33.3. Si neghino le seguenti formule:

- (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 tutte equivalenti tra loro:

$$\begin{aligned} & \neg \exists x \forall y \forall z (p(x, y) \rightarrow q(x, z)) \\ & \forall x \exists y \exists z \neg (p(x, y) \rightarrow q(x, z)) \\ & \forall x \exists y \exists z \neg (\neg (p(x, y) \wedge \neg q(x, z))) \\ & \forall x \exists y \exists z (p(x, y) \wedge \neg q(x, z)). \end{aligned}$$

(b) Negando $\exists x \forall y (p(x, y) \rightarrow (\exists z q(x, y, z)))$ si ha la seguente successione di formule equivalenti tra loro:

$$\begin{aligned} & \neg \exists x \forall y (p(x, y) \rightarrow (\exists z q(x, y, z))) \\ & \forall x \exists y \neg (p(x, y) \rightarrow (\exists z q(x, y, z))) \\ & \forall x \exists y \neg (\neg (p(x, y) \wedge \neg (\exists z q(x, y, z)))) \\ & \forall x \exists y (p(x, y) \wedge \neg \exists z q(x, y, z)) \\ & \forall x \exists y (p(x, y) \wedge \forall z \neg q(x, y, z)). \end{aligned}$$

(c) Negando $\forall x \forall y \forall z (p(x, y) \leftrightarrow q(x, y, z))$ si ha la seguente successione di formule equivalenti tra loro:

$$\begin{aligned} & \neg \forall x \forall y \forall z (p(x, y) \leftrightarrow q(x, y, z)) \\ & \exists x \exists y \exists z \neg (p(x, y) \leftrightarrow q(x, y, z)) \\ & \exists x \exists y \exists z \neg ((p(x, y) \wedge q(x, y, z)) \vee (\neg p(x, y) \wedge \neg q(x, y, z))) \\ & \exists x \exists y \exists z (\neg (p(x, y) \wedge q(x, y, z)) \wedge \neg (\neg p(x, y) \wedge \neg q(x, y, z))) \\ & \exists x \exists y \exists z (\neg p(x, y) \vee \neg q(x, y, z)) \wedge (\neg \neg p(x, y) \vee \neg \neg q(x, y, z)) \\ & \exists x \exists y \exists z (\neg p(x, y) \vee \neg q(x, y, z)) \wedge (p(x, y) \vee q(x, y, z)). \quad \square \end{aligned}$$

Altri esercizi

33.4. Delle seguenti proposizioni si dica se sono vere o false, e si enunci una loro negazione:

- Per ogni $x \in \mathbb{Z}$ esiste $y \in \mathbb{Z}$ tale che $xy = 1$.
- Per ogni $x \in \mathbb{R}$ esiste $y \in \mathbb{R}$ tale che $x^2 = y$.
- Esiste $y \in \mathbb{R}$ tale che per ogni $x \in \mathbb{R}$ si ha $x^2 = y$.
- Per ogni $x \in \mathbb{R}$ esiste $y \in \mathbb{R}$ tale che per ogni $z \in \mathbb{R}$ si ha $x = yz$.
- 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 $xy = z^2$.
- Per ogni $x \in \mathbb{R}$ si ha che se $x \neq 0$ allora esiste $y \in \mathbb{R}$ tale che $xy = 1$.

33.5. Nel linguaggio degli anelli con identità si scriva una formula α di modo che α sia vera in un anello commutativo A con identità se e solo se A è un campo.

33.6. Chiamiamo *algebra di tipo 1* una struttura algebrica del tipo (A, f) , dove A è un insieme ed $f: A \rightarrow A$ è un'operazione unaria su A . Chiamiamo *linguaggio delle algebre di tipo 1* il linguaggio costituito, oltre che dai simboli logici e dai simboli ausiliari, da un unico simbolo funzionale'. Il linguaggio delle algebre di tipo 1 non ha quindi né simboli predicativi né costanti individuali. Si scriva una formula del linguaggio delle algebre di tipo 1 che sia vera in un'algebra (A, f) di tipo 1 se e solo se f è iniettiva ma non suriettiva.

Capitolo 6

ALGEBRA LINEARE

§34. Spazi vettoriali

34.1 DEFINIZIONE. Sia K un campo. Uno *spazio vettoriale su K* (o un *K -spazio vettoriale*) è un gruppo abeliano additivo $(V, +)$ dotato di un'ulteriore applicazione $K \times V \rightarrow V$, $(\alpha, v) \mapsto \alpha v$, detta *prodotto scalare*, per la quale sono soddisfatte le seguenti condizioni:

- (a) *associatività*: $(\alpha\beta)v = \alpha(\beta v)$ per ogni $\alpha, \beta \in K$ e ogni $v \in V$;
- (b) *distributività*: per ogni $\alpha, \beta \in K$ e ogni $v, w \in V$ si ha $\alpha(v + w) = \alpha v + \alpha w$ e $(\alpha + \beta)v = \alpha v + \beta v$;
- (c) *identità*: $1v = v$ per ogni $v \in V$. \square

Qui 1 denota l'identità del campo K . Se V è uno spazio vettoriale su K chiameremo *vettori* gli elementi di V e *scalari* gli elementi di K .

34.2 ESEMPIO. Siano K un campo ed $n \geq 1$ un intero. Sia

$$K^n = \{(\lambda_1, \lambda_2, \dots, \lambda_n) \mid \lambda_1, \lambda_2, \dots, \lambda_n \in K\}$$

l'insieme delle n -uple ad elementi in K . Definiamo una somma e un prodotto scalare ponendo

$$(\lambda_1, \lambda_2, \dots, \lambda_n) + (\mu_1, \mu_2, \dots, \mu_n) = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \dots, \lambda_n + \mu_n)$$

e

$$\alpha(\lambda_1, \lambda_2, \dots, \lambda_n) = (\alpha\lambda_1, \alpha\lambda_2, \dots, \alpha\lambda_n)$$

per ogni $(\lambda_1, \lambda_2, \dots, \lambda_n), (\mu_1, \mu_2, \dots, \mu_n) \in K^n$ e ogni $\alpha \in K$. È facile verificare che K^n è allora uno spazio vettoriale su K .

Per $n = 0$ si conviene che ci sia un'unica 0-upla a elementi in K . Se la si denota con il simbolo 0 , allora $K^0 = \{0\}$ è il gruppo abeliano banale con un solo elemento. E anzi $\{0\}$ è uno spazio vettoriale su K in cui il prodotto scalare è definito da $\alpha 0 = 0$ per ogni $\alpha \in K$. È detto lo *spazio vettoriale nullo*. \square

34.3 ESEMPIO. Sia $K[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in un campo K . Dato che $K[x]$ è un anello, sappiamo già che $K[x]$ è un gruppo abeliano rispetto all'addizione di polinomi, e anzi, essendo $K \subseteq K[x]$, sappiamo già come si fa a moltiplicare un elemento di K per uno di $K[x]$ ottenendo un elemento di $K[x]$, cioè abbiamo già definito un prodotto scalare tra un elemento $\alpha \in K$ e un elemento $f \in K[x]$. Si verifica immediatamente che gli assiomi di spazio vettoriale sono soddisfatti, e quindi l'anello $K[x]$ è anche uno spazio vettoriale su K . \square

34.4 ESEMPIO. L'esempio 34.3 può essere generalizzato al caso seguente. Supponiamo di avere un anello A , un suo sottoanello K e supponiamo che K sia un campo. Anche in questo caso A ha già una struttura di gruppo abeliano additivo e, dato che $K \subseteq A$, è possibile moltiplicare un elemento di K per uno di A (ottenendo un elemento di A). In altre parole il prodotto in A induce un prodotto scalare $K \times A \rightarrow A$. È facile verificare che sono soddisfatti gli assiomi di spazio vettoriale, e quindi A è spazio vettoriale su K . Ad esempio se prendiamo $A = \mathbb{C}$ (campo dei numeri complessi) e $K = \mathbb{R}$ (campo dei numeri reali), da $\mathbb{R} \subseteq \mathbb{C}$ segue che \mathbb{C} è spazio vettoriale su \mathbb{R} . Oppure prendendo $A = \mathbb{C}$ e $K = \mathbb{Q}$, troviamo che \mathbb{C} è spazio vettoriale sul campo \mathbb{Q} dei numeri razionali. E prendendo $A = K$ si vede che ogni campo K è spazio vettoriale su K . \square

34.5 ESEMPIO (Per chi ha già sentito parlare di vettori in fisica o in geometria). È molto probabile che lo studente abbia già incontrato nel corso di fisica o alle scuole medie superiori un'altra nozione di *vettori*, differente dalla nostra. I vettori della fisica, con i quali si descrivono ad esempio gli spostamenti, vengono in genere rappresentati da segmenti orientati nello spazio tridimensionale e sono caratterizzati da una lunghezza e da una direzione orientata. L'unica eccezione è rappresentata dal vettore nullo, rappresentato dai segmenti orientati di lunghezza nulla, per il quale la direzione non è univocamente determinata (alcuni testi dicono che la direzione di un segmento nullo non è determinata, altri dicono che non è definita, altri dicono che un segmento nullo ha tutte le direzioni). Due segmenti orientati di lunghezza non nulla rappresentano lo stesso vettore se e solo se hanno la stessa lunghezza e la stessa direzione, ossia se e solo se si ottengono l'uno dall'altro mediante una traslazione. Sia V l'insieme di tali vettori. Mediante la regola del parallelogramma è possibile definire la somma di due vettori, ossia un'addizione in V , che risulta essere associativa e commutativa. Il vettore nullo è l'elemento neutro, cioè lo zero, per questa addizione, e ogni vettore v ha un opposto avente la stessa lunghezza di v e direzione opposta a quella di v . Quindi V è un gruppo abeliano. Se α è un numero reale e v è un vettore, è possibile definire il prodotto αv nel modo seguente. Si prende un segmento orientato \overrightarrow{OP} che rappresenta v . Se $\alpha \geq 0$, si costruisce un segmento \overrightarrow{OQ} avente la stessa direzione di \overrightarrow{OP} e lunghezza $\|\overrightarrow{OQ}\| = \alpha \cdot \|\overrightarrow{OP}\|$. Se invece $\alpha < 0$, si costruisce un segmento \overrightarrow{OQ} avente direzione opposta a quella di \overrightarrow{OP} e lunghezza $\|\overrightarrow{OQ}\| = (-\alpha) \cdot \|\overrightarrow{OP}\|$. Si definisce allora come prodotto scalare αv il vettore rappresentato da \overrightarrow{OQ} . Resta così definito un prodotto scalare che conferisce a V una struttura di spazio vettoriale sul campo \mathbb{R} dei numeri reali. Quindi i vettori della fisica formano uno spazio vettoriale su \mathbb{R} nel senso da noi definito. \square

34.6 LEMMA. Sia V uno spazio vettoriale su un campo K . Si denotino con 0_V e 0_K gli zeri di V e K rispettivamente. Allora

- $\alpha 0_V = 0_V$ per ogni $\alpha \in K$;
- $0_K v = 0_V$ per ogni $v \in V$;
- $(-\alpha)v = \alpha(-v) = -(\alpha v)$ per ogni $\alpha \in K$ e ogni $v \in V$;
- per ogni $\alpha \in K$ e ogni $v \in V$ si ha $\alpha v = 0_V$ se e solo se $\alpha = 0_K$ oppure $v = 0_V$.

Dimostrazione. (a) Se $\alpha \in K$ si ha $\alpha 0_V = \alpha(0_V + 0_V) = \alpha 0_V + \alpha 0_V$. Sommando ad ambo i membri l'opposto dell'elemento $\alpha 0_V$ di V si trova che $0_V = \alpha 0_V$.

(b) Se $v \in V$ si ha $0_K v = (0_K + 0_K)v = 0_K v + 0_K v$. Sommando ad ambo i membri l'opposto dell'elemento $0_K v$ di V si trova che $0_V = 0_K v$.

(c) Per dimostrare che $(-\alpha)v = -(\alpha v)$, cioè che $(-\alpha)v$ è l'opposto di αv nel gruppo abeliano additivo V , si deve far vedere che $(-\alpha)v + (\alpha v) = 0_V$. Questo è molto facile: $(-\alpha)v + (\alpha v) = (-\alpha + \alpha)v = 0_K v = 0_V$. Analogamente si vede che $\alpha(-v) = -(\alpha v)$.

(d) (\Rightarrow) Supponiamo $\alpha v = 0_V$. Se $\alpha = 0_K$ siamo a posto. Se invece $\alpha \neq 0_K$, allora α ha un inverso α^{-1} in K perché K è un campo. Ne segue che $v = 1_K v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1}0_V = 0_V$.

(\Leftarrow) È già stato dimostrato in (a) e (b). \square

34.7 DEFINIZIONE. Se V è uno spazio vettoriale su un campo K , un sottospazio (vettoriale) W di V è un sottogruppo di $(V, +)$ tale che $\alpha w \in W$ per ogni $\alpha \in K$ e ogni $w \in W$. \square

Quindi se V è uno spazio vettoriale su K , un sottoinsieme W di V è un sottospazio vettoriale di V se e solo se $W \neq \emptyset$, $w - w' \in W$ per ogni $w, w' \in W$, e $\alpha w \in W$ per ogni $\alpha \in K, w \in W$. Per denotare che W è sottospazio di V scriveremo $W \leq V$.

34.8 ESEMPIO. Sia $K[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in un campo K . Nell'esempio 34.3 si è visto che $K[x]$ è uno spazio vettoriale su K . Siano ora $n \in \mathbb{N}$ e $K[x]_{\leq n} = \{f \in K[x] \mid \delta(f) \leq n\}$ l'insieme di tutti i polinomi appartenenti a $K[x]$ di grado $\leq n$. Certamente $K[x]_{\leq n} \neq \emptyset$, perché il polinomio nullo appartiene a $K[x]_{\leq n}$. Se f, g sono polinomi appartenenti a $K[x]_{\leq n}$ di grado $\leq n$, allora la loro differenza $f - g$ ha grado $\leq n$, e se $f \in K[x]_{\leq n}$ e $\alpha \in K$, allora $\delta(\alpha f) \leq n$. Quindi $K[x]_{\leq n}$ è un sottospazio vettoriale di $K[x]$. \square

34.9 ESEMPIO. Consideriamo i due campi $\mathbb{Q} \subseteq \mathbb{C}$. Come abbiamo visto nell'esempio 34.4 il campo \mathbb{C} è uno spazio vettoriale su \mathbb{Q} . Dato che \mathbb{R} è sottogruppo del gruppo additivo \mathbb{C} e il prodotto di un numero razionale per un numero reale è un numero reale, si ha che \mathbb{R} è sottospazio del \mathbb{Q} -spazio vettoriale \mathbb{C} . \square

34.10 ESEMPIO. Per ogni spazio vettoriale V , sono sottospazi di V il sottospazio nullo $\{0_V\}$ e il sottospazio improprio V . \square

34.11 ESEMPIO. Si verifichi per esercizio che se U e W sono sottospazi di V , allora $U + W = \{u + w \mid u \in U, w \in W\}$ e $U \cap W$ sono sottospazi di V . \square

Più in generale è facile verificare che l'intersezione di una qualunque famiglia (anche infinita) di sottospazi di uno spazio vettoriale V è un sottospazio di V . Quindi se X è un sottoinsieme di V , l'intersezione di tutti i sottospazi di V che contengono X è un sottospazio di V , ed è ovviamente il più piccolo sottospazio di V che contiene X . Lo chiameremo il *sottospazio di V generato da X* , e lo denoteremo con $\langle X \rangle$. Ad esempio $\{0_V\}$ e V sono rispettivamente il più piccolo e il più grande di tutti i sottospazi di V . Ne segue che il sottospazio $\langle \emptyset \rangle$ di V generato dall'insieme vuoto \emptyset è $\{0_V\}$ e che il sottospazio $\langle V \rangle$ di V generato da V è V . Se W è un qualunque sottospazio vettoriale di V si ha $\langle W \rangle = W$. Se V è uno spazio vettoriale su K e X è un sottoinsieme di V tale che $\langle X \rangle = V$ diremo che X genera V (o che X è un *insieme di generatori* di V). Quindi un sottoinsieme X di V genera V se e solo se l'unico sottospazio di V che contiene X è lo stesso V . È chiaro che se X genera V , anche ogni sottoinsieme Y di V che contiene X genera V .

34.12 PROPOSIZIONE. *Se V è uno spazio vettoriale su un campo K , v_1, v_2, \dots, v_m sono $m \geq 1$ vettori appartenenti a V , $X = \{v_1, v_2, \dots, v_m\}$ e $\langle X \rangle$ è il sottospazio vettoriale di V generato da X , allora*

$$\langle X \rangle = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m \mid \alpha_1, \alpha_2, \dots, \alpha_m \in K\}.$$

Dimostrazione. Sia $W = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m \mid \alpha_1, \alpha_2, \dots, \alpha_m \in K\}$. Per dimostrare che $\langle X \rangle = W$ dobbiamo fare vedere che W è il più piccolo sottospazio di V contenente X .

Vedere che W è sottospazio di V è molto facile: $W \neq \emptyset$ perché ad esempio $0_K v_1 + \cdots + 0_K v_m \in W$; se $\alpha_1 v_1 + \cdots + \alpha_m v_m, \beta_1 v_1 + \cdots + \beta_m v_m$ sono due elementi di W , anche la loro differenza appartiene a W perché $(\alpha_1 v_1 + \cdots + \alpha_m v_m) - (\beta_1 v_1 + \cdots + \beta_m v_m) = (\alpha_1 - \beta_1) v_1 + \cdots + (\alpha_m - \beta_m) v_m$; e poi se $\lambda \in K$ e $\alpha_1 v_1 + \cdots + \alpha_m v_m \in W$, anche il loro prodotto appartiene a W perché $\lambda(\alpha_1 v_1 + \cdots + \alpha_m v_m) = (\lambda \alpha_1) v_1 + \cdots + (\lambda \alpha_m) v_m$.

L'insieme W contiene X perché per ogni $i = 1, \dots, m$ si ha $v_i = 0_K v_1 + \cdots + 1_K v_i + \cdots + 0_K v_m \in W$. Quindi W è un sottospazio di V contenente X . Per mostrare che W è il più piccolo sottospazio di V contenente X resta da far vedere che se U è un qualunque sottospazio di V contenente X , allora $W \subseteq U$.

Sia U un sottospazio di V contenente X . Se $\alpha_1 v_1 + \cdots + \alpha_m v_m$ è un qualunque elemento di W ($\alpha_1, \alpha_2, \dots, \alpha_m \in K$), si ha $v_1, v_2, \dots, v_m \in U$ perché U contiene X , e quindi $\alpha_1 v_1, \dots, \alpha_m v_m \in U$ perché U è sottospazio vettoriale. Ne segue che $\alpha_1 v_1 + \cdots + \alpha_m v_m \in U$ perché U è additivamente chiuso. Quindi $W \subseteq U$. \square

34.13 DEFINIZIONE. Consideriamo $m \geq 1$ vettori v_1, v_2, \dots, v_m appartenenti ad uno spazio vettoriale V su K . Chiamiamo *combinazione lineare (a coefficienti in K)* dei vettori v_1, v_2, \dots, v_m ogni espressione del tipo $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m$ con $\alpha_1, \alpha_2, \dots, \alpha_m \in K$. \square

La proposizione 34.12 dice che il sottospazio di V generato da X consiste dei vettori che si possono scrivere come combinazione lineare degli elementi di X . In particolare se $X = \{v_1, v_2, \dots, v_m\}$ è un sottoinsieme finito non vuoto di uno spazio vettoriale V , X genera V se e solo se ogni elemento di V si può scrivere come combinazione lineare di v_1, v_2, \dots, v_m .

34.14 ESEMPIO. Siano K un campo, $n \geq 1$ un intero e $V = K^n$ il K -spazio vettoriale dell'esempio 34.2, ossia lo spazio vettoriale delle n -uple a elementi in K . Per ogni $i = 1, 2, \dots, n$ sia $e_i \in K^n$ la n -upla avente tutti gli elementi uguali a 0 eccetto quello all' i -esimo posto che è uguale a 1:

$$e_i = (0, \dots, 0, \underset{\substack{\uparrow \\ i\text{-esimo posto}}}{1}, 0, \dots, 0)$$

Ogni elemento di K^n è combinazione lineare di e_1, e_2, \dots, e_n , perché per una generica n -upla $(\lambda_1, \lambda_2, \dots, \lambda_n) \in K^n$ si ha $(\lambda_1, \lambda_2, \dots, \lambda_n) = (\lambda_1, 0, 0, \dots, 0) + (0, \lambda_2, 0, \dots, 0) + \dots + (0, 0, 0, \dots, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n$. Quindi $\{e_1, e_2, \dots, e_n\}$ è un insieme di generatori di K^n . \square

34.15 ESEMPIO. Siano \mathbb{R} il campo dei numeri reali e \mathbb{R}^3 l' \mathbb{R} -spazio vettoriale delle terne di numeri reali. Abbiamo visto nell'esempio precedente che $\{e_1, e_2, e_3\}$, dove $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$, è un insieme di generatori di \mathbb{R}^3 . Mostriamo che se $v_1 = (1, -1, 0)$, $v_2 = (1, 1, 0)$, $v_3 = (1, 0, 1)$, anche $\{v_1, v_2, v_3\}$ è un insieme di generatori di \mathbb{R}^3 . Si deve far vedere che ogni elemento di \mathbb{R}^3 si può scrivere come combinazione lineare di v_1, v_2, v_3 . Sia (a, b, c) un elemento di \mathbb{R}^3 . Si deve dimostrare che esistono $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $(a, b, c) = \alpha(1, -1, 0) + \beta(1, 1, 0) + \gamma(1, 0, 1)$. Quindi se troviamo $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $(a, b, c) = \alpha(1, -1, 0) + \beta(1, 1, 0) + \gamma(1, 0, 1) = (\alpha, -\alpha, 0) + (\beta, \beta, 0) + (\gamma, 0, \gamma) = (\alpha + \beta + \gamma, -\alpha + \beta, \gamma)$, cioè tali che $a = \alpha + \beta + \gamma$, $b = -\alpha + \beta$, $c = \gamma$, siamo a posto. In altre parole, è sufficiente far vedere che il sistema

$$(34.1) \quad \begin{cases} a = \alpha + \beta + \gamma \\ b = -\alpha + \beta \\ c = \gamma \end{cases}$$

nelle incognite α, β, γ ha soluzioni reali. Risolviamo il sistema (34.1). Dalla seconda e dalla terza equazione del sistema (34.1) si ricava $\alpha = -b + \beta$ e $\gamma = c$. Sostituendo queste espressioni di α e γ nella prima equazione di (34.1) si trova che $a = \alpha + \beta + \gamma = -b + \beta + \beta + c$, da cui $\beta = \frac{1}{2}(a + b - c)$. Quindi $(\alpha, \beta, \gamma) = (\frac{1}{2}(a - b - c), \frac{1}{2}(a + b - c), c)$ è soluzione del sistema. Dato che

$$(a, b, c) = \frac{1}{2}(a - b - c)(1, -1, 0) + \frac{1}{2}(a + b - c)(1, 1, 0) + c(1, 0, 1),$$

il vettore (a, b, c) è combinazione lineare dei vettori $v_1 = (1, -1, 0)$, $v_2 = (1, 1, 0)$, $v_3 = (1, 0, 1)$. Pertanto $\{v_1, v_2, v_3\}$ è un insieme di generatori di \mathbb{R}^3 . \square

34.16 ESEMPIO. Sia $K[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti nel campo K . Nell'esempio 34.3 abbiamo visto che $K[x]$ è uno spazio vettoriale su K . Fissiamo un numero naturale n e consideriamo gli $n+1$ polinomi $1, x, x^2, x^3, \dots, x^n$ appartenenti a $K[x]$. Se $X = \{1, x, x^2, x^3, \dots, x^n\}$, si ha $\langle X \rangle = K[x]_{\leq n}$, dove $K[x]_{\leq n}$ denota, come nell'esempio 34.8, il sottospazio vettoriale di $K[x]$ i cui elementi sono i polinomi di

grado $\leq n$. Quindi l'insieme $\{1, x, x^2, x^3, \dots, x^n\}$ genera il sottospazio vettoriale $K[x]_{\leq n}$ di $K[x]$. \square

34.17 ESEMPIO. Siano V uno spazio vettoriale su un campo K e v un vettore appartenente a V . Allora il sottospazio vettoriale di V generato dall'insieme $\{v\}$ avente v come suo unico elemento è $\langle\{v\}\rangle = \{\alpha v \mid \alpha \in K\}$. Spesso, per non appesantire la notazione, si scrive $\langle v \rangle$ per denotare lo spazio vettoriale $\langle\{v\}\rangle$. Più in generale, se $X = \{v_1, \dots, v_n\}$ è un insieme finito, si scrive spesso $\langle v_1, \dots, v_n \rangle$ in luogo di $\langle\{v_1, \dots, v_n\}\rangle$. \square

34.18 ESEMPIO. Abbiamo già osservato che per ogni spazio vettoriale V si ha $\langle\emptyset\rangle = \{0_V\}$, cioè il sottoinsieme vuoto genera il sottospazio nullo $\{0_V\}$ di V . (Quindi in particolare lo spazio vettoriale V è lo spazio vettoriale nullo avente un unico elemento se e solo se l'insieme vuoto è un insieme di generatori per V .) In vista della proposizione 34.12 si conviene quindi di poter scrivere il vettore nullo 0_V come combinazione lineare di un insieme vuoto di vettori. \square

Esercizi svolti

34.1. Siano V uno spazio vettoriale e $\mathcal{L}(V)$ l'insieme di tutti i sottospazi di V . Si ordini parzialmente $\mathcal{L}(V)$ mediante l'inclusione \subseteq . Si dimostri che se $U, W \in \mathcal{L}(V)$, allora l'estremo superiore di $\{U, W\}$ in $\mathcal{L}(V)$ è $U + W$, e l'estremo inferiore di $\{U, W\}$ in $\mathcal{L}(V)$ è $U \cap W$. Quindi $(\mathcal{L}(V), \subseteq)$ è un reticolo.

Soluzione. Siano $U, W \in \mathcal{L}(V)$. Per dimostrare che $U + W$ è l'estremo superiore di $\{U, W\}$ in $\mathcal{L}(V)$ si deve far vedere che

- $U + W \supseteq U$;
- $U + W \supseteq W$;
- se $V' \in \mathcal{L}(V)$, $V' \supseteq U$ e $V' \supseteq W$, allora $V' \supseteq U + W$.

Per dimostrare (a) si prenda un elemento $u \in U$. Dato che $0_V \in W$, si ha $u = u + 0_V \in U + W$. Questo dimostra che $U \subseteq U + W$. Per simmetria anche (b) vale. Per dimostrare (c), si prenda un $V' \in \mathcal{L}(V)$ tale che $V' \supseteq U$ e $V' \supseteq W$. Facciamo vedere che $V' \supseteq U + W$. Se $v \in U + W$, allora esistono $u \in U$ e $w \in W$ tali che $v = u + w$. Allora $u, w \in V'$, che è un sottospazio di V , e quindi $u + w \in V'$, cioè $v \in V'$.

Per dimostrare invece che $U \cap W$ è l'estremo inferiore di $\{U, W\}$ in $\mathcal{L}(V)$ si deve far vedere che

- $U \cap W \subseteq U$;
- $U \cap W \subseteq W$;
- se $V' \in \mathcal{L}(V)$, $V' \subseteq U$ e $V' \subseteq W$, allora $V' \subseteq U \cap W$.

Queste tre condizioni sono tutte tre verificate banalmente. \square

34.2. Sia V uno spazio vettoriale con un numero finito di elementi (ad esempio V potrebbe essere lo \mathbb{Z}_p -spazio vettoriale \mathbb{Z}_p^n , che ha p^n elementi, p un numero primo). Si consideri il reticolo $(\mathcal{L}(V), \subseteq)$ dei sottospazi di V (esercizio 34.1). Sia $(\mathcal{P}(V), \subseteq)$ il reticolo dell'insieme delle parti di V parzialmente ordinato dall'inclusione \subseteq . L'applicazione $\psi: \mathcal{P}(V) \rightarrow \mathcal{L}(V)$ definita da $\psi(X) = \langle X \rangle$ per ogni sottoinsieme X di V , ossia l'applicazione che associa ad ogni sottoinsieme

sieme X di V il sottospazio $\langle X \rangle$ di V generato da X , è un omomorfismo di insiemi parzialmente ordinati? È un omomorfismo di reticolli?

Soluzione. Chiedere se l'applicazione $\psi: \mathcal{P}(V) \rightarrow \mathcal{L}(V)$, $X \mapsto \langle X \rangle$, è un omomorfismo di insiemi parzialmente ordinati equivale a chiedere se sia vero che per ogni $X, Y \in \mathcal{P}(V)$, $X \subseteq Y$ implica $\langle X \rangle \subseteq \langle Y \rangle$. Questo è certamente vero.

Chiedere invece se $\psi: \mathcal{P}(V) \rightarrow \mathcal{L}(V)$ è un omomorfismo di reticolli equivale a chiedere se ψ rispetta l'estremo superiore e l'estremo inferiore nei due reticolli. L'estremo inferiore in entrambi i reticolli $(\mathcal{P}(V), \subseteq)$ e $(\mathcal{L}(V), \subseteq)$ è dato dall'intersezione, e quindi se ψ fosse un omomorfismo di reticolli si dovrebbe avere che $\psi(X \cap Y) = \psi(X) \cap \psi(Y)$ per ogni $X, Y \in \mathcal{P}(V)$, ossia $\langle X \cap Y \rangle = \langle X \rangle \cap \langle Y \rangle$ per ogni $X, Y \in \mathcal{P}(V)$. Mostriamo che invece questo non è vero in generale. Sia V uno spazio vettoriale non nullo su un campo K , siano $v \in V$, $v \neq 0$, e $\lambda \in K$, $\lambda \neq 0, 1$. Ad esempio si possono prendere un numero primo $p \geq 3$, un intero $n \geq 1$, $K = \mathbb{Z}_p$ e $V = \mathbb{Z}_p^n$, di modo che V ha certamente elementi v diversi da 0 e K ha elementi λ diversi da 0 e 1. Si ponga $X = \{v\}$ e $Y = \{\lambda v\}$. Allora $X \cap Y = \emptyset$, di modo che $\langle X \cap Y \rangle = \{0_V\}$. Invece $\lambda v \in \langle X \rangle$ e $\lambda v \in \langle Y \rangle$ (esempio 34.17), di modo che $\langle X \rangle \cap \langle Y \rangle \neq \{0_V\}$. Quindi in questo caso si ha $\langle X \cap Y \rangle \neq \langle X \rangle \cap \langle Y \rangle$, e pertanto ψ non è in generale un omomorfismo di reticolli. \square

Altri esercizi

34.3. L'insieme $U = \{(a, b, c) \mid a, b, c \in \mathbb{R}, a + b - c = 1\}$ è un sottospazio dell' \mathbb{R} -spazio vettoriale \mathbb{R}^3 ?

34.4. Siano K un campo e $M_{m \times n}(K)$ l'insieme delle matrici $m \times n$ ad elementi in K .

- (a) Si dimostri che $M_{m \times n}(K)$ è uno spazio vettoriale su K . (Qui la somma di due matrici e il prodotto tra un elemento di K e una matrice sono analoghi a quelli già definiti nel §6 per il caso di $K = \mathbb{R}$, cioè per le matrici a elementi reali. Per tali matrici si era già visto tra l'altro nel §6 che valevano gli assiomi di spazio vettoriale.)
- (b) Sia p un numero primo e supponiamo che $K = \mathbb{Z}_p$. Quanti elementi ha lo \mathbb{Z}_p -spazio vettoriale $M_{m \times n}(\mathbb{Z}_p)$?

34.5. Siano K un campo ed m, n, p tre numeri interi ≥ 1 . Siano A una matrice $m \times n$ a coefficienti nel campo K e $M_{n \times p}(K)$ l'insieme delle matrici $n \times p$ ad elementi in K . Si dimostri che $W = \{X \in M_{n \times p}(K) \mid AX = 0\}$ è un sottospazio vettoriale di $M_{n \times p}(K)$.

34.6. Si dimostri che se U, V, W sono tre sottospazi di uno spazio vettoriale dato e $U \subseteq V$, allora $U + (V \cap W) = V \cap (U + W)$.

- 34.7. (a) Qual è il sottospazio di \mathbb{R}^2 generato da $\{(1, 3), (2, 1)\}$?
- (b) Qual è il sottospazio di \mathbb{R}^2 generato da $\{(1, 3), (2, 6)\}$?

34.8. Siano K un campo e $K[x]$ lo spazio vettoriale dell'esempio 34.3. Sia $W = \{a_0 + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in K, \sum_{i=0}^n a_i = 0\}$ il sottoinsieme di $K[x]$ i cui elementi sono tutti i polinomi per i quali la somma dei coefficienti è zero. Si dimostri che W è un sottospazio vettoriale di $K[x]$.

34.9. Siano X un insieme non vuoto e K un campo. Nell'insieme

$$K^X = \{f \mid f: X \rightarrow K \text{ è un'applicazione}\}$$

si definiscano

$$(f+g)(x) = f(x) + g(x) \quad \text{e} \quad (\alpha f)(x) = \alpha \cdot f(x)$$

per ogni $f, g \in K^X$, ogni $\alpha \in K$ e ogni $x \in X$. Si provi che K^X è uno spazio vettoriale su K .

34.10. Siano X un insieme non vuoto e K un campo. Si consideri il K -spazio vettoriale K^X dell'esercizio 34.9. Per ogni $Y \subseteq X$ sia $K_Y = \{f \in K^X \mid f(y) = 0 \text{ per ogni } y \in Y\}$. Si dimostri che

- (a) K_Y è un sottospazio di K^X per ogni $Y \subseteq X$;
- (b) se $Y \subseteq Y' \subseteq X$, allora $K_Y \supseteq K_{Y'}$;
- (c) $K_\emptyset = K^X$ e $K_X = \{0\}$;
- (d) se $Y \subseteq X$ e $Y' \subseteq X$, allora $K_Y + K_{Y'} = K_{Y \cap Y'}$;
- (e) se $Y \subseteq X$ e $Y' \subseteq X$, allora $K_Y \cap K_{Y'} = K_{Y \cup Y'}$.

34.11. Come caso particolare dello spazio vettoriale K^X dell'esercizio 34.9 consideriamo il caso in cui K è il campo \mathbb{R} dei numeri reali e X è l'intervallo chiuso $[0, 1] = \{\alpha \mid \alpha \in \mathbb{R}, 0 \leq \alpha \leq 1\}$.

- (a) Si dimostri che l'insieme $C([0, 1])$ di tutte le funzioni continue $f: [0, 1] \rightarrow \mathbb{R}$ è un sottospazio vettoriale di $\mathbb{R}^{[0, 1]}$.
- (b) L'insieme di tutte le funzioni continue $f: [0, 1] \rightarrow \mathbb{R}$ il cui grafico passa per il punto $(1, 0)$ è un sottospazio vettoriale di $C([0, 1])$?
- (c) L'insieme di tutte le funzioni continue $f: [0, 1] \rightarrow \mathbb{R}$ il cui grafico passa per il punto $(1, 1)$ è un sottospazio vettoriale di $C([0, 1])$?

34.12. Come caso particolare dell'esercizio 34.10 consideriamo il caso in cui K è il campo \mathbb{Z}_5 con cinque elementi, X è un insieme $\{a, b, c\}$ di tre elementi, e $Y = \{a\}$. Quanti elementi ha il sottospazio vettoriale K_Y di K^X ?

34.13. Si dimostri che se $W_0 \subseteq W_1 \subseteq W_2 \subseteq \dots$ sono sottospazi di uno spazio vettoriale V , allora anche $W = \bigcup_{n \in \mathbb{N}} W_n$ è un sottospazio di V .

34.14. Sia $\alpha \in \mathbb{C}$ un numero complesso fissato. Siano $\mathbb{R}[x]$ lo spazio vettoriale reale (cioè sul campo \mathbb{R} dei numeri reali) dei polinomi a coefficienti reali nell'indeterminata x e

$$W = \{f \in \mathbb{R}[x] \mid x^2 + 1 \text{ divide } f \text{ nell'anello } \mathbb{R}[x] \text{ e } f(\alpha) = 0\}.$$

Si dimostri che W è un sottospazio di $\mathbb{R}[x]$.

34.15. Sia $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. Si dimostri che $\mathbb{Q}[i]$ è un sottospazio del \mathbb{Q} -spazio vettoriale \mathbb{C} dei numeri complessi.

34.16. Nell'esercizio 34.1 si è dimostrato che se V è uno spazio vettoriale su un campo K e $\mathcal{L}(V)$ è l'insieme di tutti i sottospazi di V , allora $(\mathcal{L}(V), \subseteq)$, dove \subseteq denota l'inclusione, è un reticolo. Consideriamo in particolare il caso in cui X è un insieme non vuoto e $V = K^X$ è il K -spazio vettoriale di tutte le applicazioni di X in K (esercizi 34.9 e 34.10). Come nell'esercizio 34.10 per ogni sottoinsieme Y di X sia $K_Y = \{f \in K^X \mid f(y) = 0 \text{ per ogni } y \in Y\}$. Sia $\mathcal{P}(X)^{\text{op}}$ il reticolo $\mathcal{P}(X)$ con l'ordine inverso di quello del reticolo $(\mathcal{P}(X), \subseteq)$, ossia l'insieme delle parti di X parzialmente ordinato dall'inclusione inversa \supseteq . Si dimostri che l'applicazione $\varphi: \mathcal{P}(X)^{\text{op}} \rightarrow \mathcal{L}(V)$ definita da $\varphi(Y) = K_Y$ per ogni sottoinsieme Y di X è un omomorfismo iniettivo di reticolli di $\mathcal{P}(X)^{\text{op}}$ in $(\mathcal{L}(V), \subseteq)$.

34.17. Siano K un campo, $(V, +)$ un gruppo abeliano, $\text{End}(V)$ l'anello di tutti gli endomorfismi di V come gruppo, ed $f: K \rightarrow \text{End}(V)$ un omomorfismo di anelli. Si definisca un prodotto scalare $K \times V \rightarrow V$ mediante $(\alpha, v) \mapsto f(\alpha)(v)$ per ogni $(\alpha, v) \in K \times V$. Si dimostri che $(V, +)$ con questo prodotto scalare è uno spazio vettoriale su K .

34.18. Siano $(V, +)$ un gruppo abeliano, p un numero primo, e si supponga che $pv = 0$ per ogni $v \in V$. Si definisca un prodotto scalare $\mathbb{Z}_p \times V \rightarrow V$ mediante $(\bar{n}, v) \mapsto nv$ per ogni $\bar{n} \in \mathbb{Z}_p$ e ogni $v \in V$.

- Si dimostri che questo prodotto scalare è ben definito, ossia che se $n, m \in \mathbb{Z}$ e $\bar{n} = \bar{m}$ in \mathbb{Z}_p , allora $nv = mv$ per ogni $v \in V$.
- Si dimostri che $(V, +)$ con questo prodotto scalare è uno spazio vettoriale sul campo con p elementi \mathbb{Z}_p .

34.19. Siano $(V, +)$ un gruppo abeliano, p un numero primo, e si supponga che $pv = 0$ per ogni $v \in V$. Come si è visto nell'esercizio 34.18 il gruppo V è allora in modo naturale uno spazio vettoriale sul campo \mathbb{Z}_p . Si dimostri che ogni sottogruppo del gruppo additivo V è sottospazio vettoriale di V .

34.20.

- Sia p un numero primo. Si dimostri che ogni anello di caratteristica p è uno spazio vettoriale sul campo \mathbb{Z}_p . [Suggerimento: si applichi l'esercizio 34.18.]
- Si dimostri che ogni anello booleano è uno spazio vettoriale sul campo \mathbb{Z}_2 .

§35. Spazio quoziante e applicazioni lineari

Siano V uno spazio vettoriale su un campo K e W un suo sottospazio. Dato che W è in particolare un sottogruppo del gruppo abeliano additivo V , è possibile costruire il gruppo quoziante $V/W = \{v + W \mid v \in V\}$. Definiamo su V/W un prodotto scalare ponendo per ogni $\alpha \in K$ e ogni $v \in V$

$$\alpha(v + W) = \alpha v + W.$$

Si tratta di una buona definizione, perché se $v, v' \in V$ sono tali che $v + W = v' + W$, allora $v - v' \in W$, e quindi $\alpha v - \alpha v' = \alpha(v - v') \in W$, da cui $\alpha v + W = \alpha v' + W$. È facile verificare che V/W con questo prodotto scalare risulta essere uno spazio vettoriale. Verifichiamo ad esempio l'associatività: per ogni $\alpha, \beta \in K$ e ogni $v \in V$ si ha $(\alpha\beta)(v + W) = (\alpha\beta)v + W = \alpha(\beta v) + W = \alpha(\beta v + W) = \alpha(\beta(v + W))$. Quindi anche per gli spazi vettoriali abbiamo potuto costruire una struttura quoziante: per ogni K -spazio vettoriale V e ogni suo sottospazio W abbiamo costruito uno spazio vettoriale V/W , detto lo *spazio vettoriale quoziante di V modulo W* , i cui elementi sono le classi laterali $v + W$ al variare di v in V e in cui le operazioni sono definite da

$$(v + W) + (v' + W) = (v + v') + W \quad \text{e} \quad \alpha(v + W) = \alpha v + W$$

per ogni $v + W, v' + W \in V/W, \alpha \in K$.

35.1 DEFINIZIONE. Siano V, U spazi vettoriali sullo stesso campo K . Un'applicazione lineare (o K -lineare, o trasformazione lineare, od omomorfismo di spazi vettoriali) f di V in U è un'applicazione $f: V \rightarrow U$ tale che $f(v + v') = f(v) + f(v')$ e $f(\alpha v) = \alpha f(v)$ per ogni $v, v' \in V$ e ogni $\alpha \in K$. \square

In particolare ogni applicazione lineare $f: V \rightarrow U$ è un omomorfismo di gruppi additivi, e pertanto $f(0_V) = 0_U$ e $f(-v) = -f(v)$ per ogni $v \in V$. Al solito, un isomorfismo di spazi vettoriali (o un isomorfismo lineare) è un'applicazione lineare biettiva, un endomorfismo di V è un'applicazione lineare di V in V , e un automorfismo di V è un endomorfismo biettivo di V . Due K -spazi vettoriali V ed U si dicono isomorfi se esiste un isomorfismo lineare di V in U , e se questo è il caso si scrive $V \cong U$.

35.2 ESEMPIO. Sia $f: K^n \rightarrow K$ definita da $f(\alpha_1, \alpha_2, \dots, \alpha_n) = \alpha_1 + \alpha_2 + \dots + \alpha_n$ per ogni $(\alpha_1, \alpha_2, \dots, \alpha_n) \in K^n$. È facile verificare che f è un'applicazione lineare. \square

35.3 ESEMPIO. Sia $K[x]$ lo spazio vettoriale dei polinomi in una indeterminata x a coefficienti in un campo K (esempio 34.3). Ricordiamo (vedi esercizio 28.9) che se $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in K[x]$ è un polinomio a coefficienti in K , la sua derivata è il polinomio $f' = a_1 + 2a_2x + 3a_3x^2 + \dots + na_nx^{n-1} \in K[x]$. Nell'esercizio 28.9 si è visto che $(f+g)' = f' + g'$ e $(fg)' = f'g + fg'$ per ogni $f, g \in K[x]$. In particolare se $\alpha \in K \subseteq K[x]$ si ha $\alpha' = 0$, e quindi $(\alpha g)' = \alpha'g + \alpha g' = \alpha g'$ per ogni $g \in K[x]$. Quindi l'applicazione $D: K[x] \rightarrow K[x]$ definita da $D(f) = f'$ per ogni $f \in K[x]$ è un endomorfismo del K -spazio vettoriale $K[x]$. \square

35.4 ESEMPIO. Come nell'esempio precedente, sia $K[x]$ lo spazio vettoriale dei polinomi in una indeterminata x a coefficienti in un campo K . Fissato un polinomio $h \in K[x]$, definiamo un'applicazione $M_h: K[x] \rightarrow K[x]$ ponendo $M_h(f) = hf$ per ogni $f \in K[x]$. Allora M_h è un endomorfismo del K -spazio vettoriale $K[x]$. \square

35.5 ESEMPIO. Sia K un campo e sia A una matrice $m \times n$ a coefficienti nel campo K . Invece che come m -uple scriveremo gli elementi dello spazio vettoriale K^m come matrici colonna, ossia come matrici $m \times 1$. Analogamente scriveremo gli elementi di K^n come

matrici colonna $n \times 1$. In questo modo se $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$, allora $A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, prodotto righe

per colonne della matrice $m \times n A$ per la matrice $n \times 1 \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$, è una matrice $m \times 1$, cioè

un elemento di K^m . Definiamo $f_A: K^n \rightarrow K^m$ ponendo $f_A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ per ogni

$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$. Allora f_A è un'applicazione lineare di K^n in K^m . \square

35.6 ESEMPIO. Sia \mathbb{Z}_3 il campo delle classi resto modulo 3, di modo che \mathbb{Z}_3 ha tre elementi $\bar{0}, \bar{1}, \bar{2}$. Siano \mathbb{Z}_3^3 e \mathbb{Z}_3^2 gli spazi vettoriali delle terne e delle coppie rispettivamente ad elementi in \mathbb{Z}_3 . In questo modo \mathbb{Z}_3^3 e \mathbb{Z}_3^2 sono spazi vettoriali di 27 e 9 elementi rispettivamente. Sia $\varphi: \mathbb{Z}_3^3 \rightarrow \mathbb{Z}_3^2$ l'applicazione definita da $\varphi(\alpha, \beta, \gamma) = (\bar{0}, \alpha - \bar{2}\beta)$ per ogni $(\alpha, \beta, \gamma) \in \mathbb{Z}_3^3$. È facile verificare che l'applicazione φ è lineare. \square

35.7 LEMMA. *Sia $f: V \rightarrow U$ un'applicazione lineare tra due K -spazi vettoriali V e U .*

- (a) *Se V' è un sottospazio di V , allora $f(V')$ è un sottospazio di U .*
- (b) *Se U' è un sottospazio di U , allora $f^{-1}(U')$ è un sottospazio di V .*

Dimostrazione. L'applicazione lineare $f: V \rightarrow U$ è in particolare un omomorfismo di gruppi abeliani additivi, e quindi dalla proposizione 23.5 sappiamo che $f(V')$ è un sottogruppo di U e $f^{-1}(U')$ è un sottogruppo di V per ogni sottospazio V' di V e ogni sottospazio U' di U . Per dimostrare che $f(V')$ è un sottospazio di U basta osservare che se $\alpha \in K$ e $u \in f(V')$, allora esiste $v' \in V'$ tale che $u = f(v')$, e quindi $\alpha u = \alpha f(v') = f(\alpha v') \in f(V')$. Questo conclude la dimostrazione di (a). Analogamente per provare che $f^{-1}(U')$ è un sottospazio di V è sufficiente osservare che se $\alpha \in K$ e $v \in f^{-1}(U')$, allora $f(v) \in U'$, da cui $f(\alpha v) = \alpha f(v) \in U'$, e quindi $\alpha v \in f^{-1}(U')$. Questo dimostra (b). \square

Ogni applicazione lineare $f: V \rightarrow U$ tra due K -spazi vettoriali V e U , essendo in particolare un omomorfismo di gruppi abeliani additivi, ha un nucleo $\ker f = \{v \mid v \in V, f(v) = 0_U\}$, e l'applicazione lineare $f: V \rightarrow U$ è iniettiva se e solo se $\ker f = \{0\}$. Dato che il nucleo di $f: V \rightarrow U$ è l'antiimmagine del sottospazio nullo di U , dal lemma 35.7(b) si deduce che

35.8 COROLLARIO. *Se $f: V \rightarrow U$ è un'applicazione lineare tra due K -spazi vettoriali V e U , il nucleo di f è un sottospazio vettoriale di V .*

Tralasciamo la dimostrazione del seguente teorema.

35.9 TEOREMA FONDAMENTALE DI OMOMORFISMO PER GLI SPAZI VETTORIALI. *Siano V, U spazi vettoriali sullo stesso campo K ed $f: V \rightarrow U$ un'applicazione lineare. Allora $V/\ker f$ ed $f(V)$ sono spazi vettoriali isomorfi.*

Esercizi svolti

35.1. Sia $\mathbb{Q}[x]$ il \mathbb{Q} -spazio vettoriale 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 α . Si dimostri che $\varphi_\alpha: \mathbb{Q}[x] \rightarrow \mathbb{C}$ definita da $\varphi_\alpha(f) = f(\alpha)$ per ogni polinomio $f \in \mathbb{Q}[x]$ è un'applicazione lineare tra i \mathbb{Q} -spazi vettoriali $\mathbb{Q}[x]$ e \mathbb{C} .

Soluzione. Si ha, per ogni $f, g \in \mathbb{Q}[x]$ e ogni $q \in \mathbb{Q}$,

$$\varphi_\alpha(f + g) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \varphi_\alpha(f) + \varphi_\alpha(g)$$

e

$$\varphi_\alpha(qf) = (qf)(\alpha) = q(f(\alpha)) = q\varphi_\alpha(f). \quad \square$$

35.2. Come si è visto nell'esempio 34.4, un campo K è uno spazio vettoriale sullo stesso campo K . Si dimostri che per ogni $k \in K$ l'applicazione $\varphi_k: K \rightarrow K$ definita da $\varphi_k(x) = kx$ per ogni $x \in K$ è lineare. Viceversa, si dimostri che per ogni applicazione K -lineare $\varphi: K \rightarrow K$ esiste $k \in K$ tale che $\varphi = \varphi_k$. Quindi le applicazioni K -lineari $K \rightarrow K$ sono tutte e sole le moltiplicazioni per elementi di K .

Soluzione. Sia $k \in K$. Per ogni $x, y, \alpha \in K$ si ha

$$\varphi_k(x + y) = k(x + y) = kx + ky = \varphi_k(x) + \varphi_k(y)$$

e

$$\varphi_k(\alpha x) = k(\alpha x) = \alpha(kx) = \alpha\varphi_k(x).$$

Quindi l'applicazione $\varphi_k: K \rightarrow K$ è lineare.

Viceversa, sia $\varphi: K \rightarrow K$ un'applicazione lineare. Poniamo $k = \varphi(1)$. Allora per ogni $x \in K$ si ha $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = xk = kx = \varphi_k(x)$. Questo dimostra che $\varphi = \varphi_k$. \square

Altri esercizi

35.3. Siano V uno spazio vettoriale, W un suo sottospazio, V/W lo spazio quoziante, e $\pi: V \rightarrow V/W$ la proiezione canonica, ossia l'applicazione definita da $\pi(v) = v + W$ per ogni $v \in V$. Si dimostri che l'applicazione π è lineare.

35.4. Si dica quali delle seguenti applicazioni tra spazi vettoriali su \mathbb{R} sono lineari, e tra quelle che sono applicazioni lineari si dica quali sono isomorfismi.

- (a) $f: \mathbb{R} \rightarrow \mathbb{R}$ definita da $f(x) = \cos x$ per ogni $x \in \mathbb{R}$;
- (b) $f: \mathbb{R} \rightarrow \mathbb{R}$ definita da $f(x) = -x + 1$ per ogni $x \in \mathbb{R}$;
- (c) $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ definita da $f(x, y) = 2x + y$ per ogni $(x, y) \in \mathbb{R}^2$;
- (d) $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ definita da $f(x, y) = (2x, 2x - y)$ per ogni $(x, y) \in \mathbb{R}^2$;
- (e) $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ definita da $f(x, y) = (-x, -x + y, -x + y^2)$ per ogni $(x, y) \in \mathbb{R}^2$;
- (f) $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ definita da $f(x, y) = (-x, -x + y, -x + y)$ per ogni $(x, y) \in \mathbb{R}^2$;
- (g) $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ definita da $f(x, y) = (-x, -x + y, -x + y + 1)$ per ogni $(x, y) \in \mathbb{R}^2$;
- (h) $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ definita da $f(x, y, z) = (x^3, 0, 0)$ per ogni $(x, y, z) \in \mathbb{R}^3$;
- (i) $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ definita da $f(x, y, z) = (0, y, z^2)$ per ogni $(x, y, z) \in \mathbb{R}^3$;
- (l) $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ definita da $f(x, y, z) = (x - y, x + y, x + y + z)$ per ogni $(x, y, z) \in \mathbb{R}^3$.

35.5. Sia $f: M_{m \times n}(K) \rightarrow M_{n \times m}(K)$ l'applicazione che ad ogni matrice $A \in M_{m \times n}(K)$ associa la sua matrice trasposta A^* (per la definizione di matrice trasposta si veda il §6). Si dimostri che f è un isomorfismo di spazi vettoriali su K .

35.6. Sia $f: V \rightarrow U$ un'applicazione lineare. Si dimostri che se un sottospazio W di V è generato da $\{w_1, \dots, w_m\}$, allora il sottospazio $f(W)$ di U è generato da $\{f(w_1), \dots, f(w_m)\}$. In particolare se V è generato da $\{v_1, \dots, v_n\}$, allora l'immagine $f(V)$ di f è generata da $\{f(v_1), \dots, f(v_n)\}$.

35.7. Siano $f, g: V \rightarrow U$ due applicazioni lineari. Si dimostri che se V è generato da $\{v_1, v_2, \dots, v_n\}$ e $f(v_i) = g(v_i)$ per ogni $i = 1, 2, \dots, n$, allora $f = g$.

35.8. Siano U uno spazio vettoriale e V, W due sottospazi di U . Si ponga $f(v + V \cap W) = v + W$ per ogni $v \in V$.

- (a) Si dimostri che con questa posizione si è data una buona definizione di un'applicazione $f: V/V \cap W \rightarrow V + W/W$, cioè che per ogni $v, v' \in V$ si ha che $v + V \cap W = v' + V \cap W$ implica $v + W = v' + W$.
- (b) Si dimostri che f è un isomorfismo di spazi vettoriali di $V/V \cap W$ in $V + W/W$.

35.9. Come nell'esempio 34.4 sia A un anello commutativo con identità, K un suo sottoanello, e supponiamo che K sia un campo, di modo che A è spazio vettoriale su K . Fissato un elemento $a \in A$, definiamo un'applicazione $\tau_a: A \rightarrow A$ ponendo $\tau_a(x) = ax$ per ogni $x \in A$. Allora τ_a è un endomorfismo del K -spazio vettoriale A . Se ne deduca che $\ker \tau_a = \{x \in A \mid ax = 0\}$ è un K -sottospazio di A . Dove è stata usata l'ipotesi che A sia commutativo? Era necessario che A fosse commutativo?

35.10. Si consideri l' \mathbb{R} -spazio vettoriale \mathbb{C} dei numeri complessi (esempio 34.4). Sia $f: \mathbb{C} \rightarrow \mathbb{C}$ definita da $f(z) = \bar{z}$ per ogni $z \in \mathbb{C}$. Qui \bar{z} denota il coniugato di z (esercizio 5.10). Si dimostri che f è un isomorfismo di spazi vettoriali su \mathbb{R} (cioè che è \mathbb{R} -lineare e biettiva).

35.11. Sia $f: \mathbb{Q}^3 \rightarrow \mathbb{Q}^4$ l'applicazione \mathbb{Q} -lineare definita da $f(\alpha, \beta, \gamma) = (5\alpha + 5\beta, 3\beta + 3\gamma, 5\gamma, 5\gamma)$ per ogni $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$. Si dimostri che f è iniettiva.

35.12. Sia $\varphi: K[x] \rightarrow K[x]$ definita da $\varphi(f(x)) = f(x+1)$ per ogni $f(x) \in K[x]$. Si dimostri che φ è un automorfismo del K -spazio vettoriale $K[x]$.

35.13. Si consideri lo spazio vettoriale K^X dell'esempio 34.9 nel caso particolare in cui K è il campo \mathbb{R} dei numeri reali e X è un intervallo aperto $]a, b[= \{\alpha \in \mathbb{R} \mid a < \alpha < b\}$. Qui $a < b$ sono due numeri reali fissati. Lo spazio vettoriale $\mathbb{R}^{]a, b[}$ è quindi lo spazio vettoriale di tutte le applicazioni $f:]a, b[\rightarrow \mathbb{R}$.

- (a) Si dimostri che $\mathcal{D}_1(]a, b[) = \{f \in \mathbb{R}^{]a, b[} \mid f \text{ è derivabile in }]a, b[\}$ è un sottospazio vettoriale di $\mathbb{R}^{]a, b[}$.
- (b) Si dimostri che l'applicazione $\delta: \mathcal{D}_1(]a, b[) \rightarrow \mathbb{R}^{]a, b[}$ che associa ad ogni $f \in \mathcal{D}_1(]a, b[)$ la sua derivata f' è un'applicazione lineare.
- (c) Si dimostri che $\ker \delta$ è isomorfo all' \mathbb{R} -spazio vettoriale \mathbb{R} .

35.14. Siano K un campo, $K[x]$ lo spazio vettoriale dei polinomi a coefficienti in K , $D: K[x] \rightarrow K[x]$ ed $M_x: K[x] \rightarrow K[x]$ le applicazioni lineari definite da $D(f) = f'$ (derivata formale di f , vedi esempio 35.3) e $M_x(f) = x \cdot f$ (esempio 35.4) per ogni $f \in K[x]$.

- (a) Si dimostri che D e M_x non sono omomorfismi di anelli.
- (b) Si dimostri che $DM_x - M_x D = \iota_{K[x]}$.

35.15. Si dimostri il teorema 35.9. [Suggerimento: l'isomorfismo lineare $g: V/\ker f \rightarrow f(V)$ è definito da $g(v + \ker f) = f(v)$ per ogni $v \in V$.]

§36. Dipendenza lineare e basi di uno spazio vettoriale

36.1 DEFINIZIONE. Sia V uno spazio vettoriale su un campo K e siano $v_1, v_2, \dots, v_m \in V$. I vettori v_1, v_2, \dots, v_m si dicono *linearmente indipendenti* se per ogni $\alpha_1, \alpha_2, \dots, \alpha_m \in K$ da $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0$ segue che $\alpha_i = 0$ per ogni $i = 1, 2, \dots, m$. I vettori v_1, v_2, \dots, v_m si dicono *linearmente dipendenti* se non sono linearmente indipendenti. \square

Quindi v_1, v_2, \dots, v_m sono linearmente dipendenti se e solo se esistono $\alpha_1, \alpha_2, \dots, \alpha_m \in K$ non tutti nulli tali che $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0$.

36.2 ESEMPIO. Consideriamo il K -spazio vettoriale K^n dell'esempio 34.2. Per ogni $i = 1, 2, \dots, n$ sia e_i la n -upla avente tutti gli elementi uguali a 0 eccetto quello all' i -esimo posto uguale a 1 (esempio 34.14). Mostriamo che e_1, e_2, \dots, e_n sono linearmente indipendenti. Se $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ e $\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n = 0$, cioè

$$\alpha_1(1, 0, \dots, 0) + \alpha_2(0, 1, \dots, 0) + \dots + \alpha_n(0, 0, \dots, 1) = (0, 0, \dots, 0),$$

allora

$$(\alpha_1, 0, \dots, 0) + (0, \alpha_2, \dots, 0) + \dots + (0, 0, \dots, \alpha_n) = (0, 0, \dots, 0).$$

Quindi $(\alpha_1, \alpha_2, \dots, \alpha_n) = (0, 0, \dots, 0)$, vale a dire $\alpha_i = 0$ per ogni $i = 1, 2, \dots, n$. Questo dimostra che e_1, e_2, \dots, e_n sono linearmente indipendenti. \square

36.3 ESEMPIO. Consideriamo il K -spazio vettoriale $K[x]$ nel caso particolare di $K = \mathbb{R}$ e facciamo vedere che gli elementi $1 - x, 1 + x, x^2$ di $\mathbb{R}[x]$ sono linearmente indipendenti. Siano $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $\alpha(1 - x) + \beta(1 + x) + \gamma x^2 = 0$. Allora $(\alpha + \beta) + (-\alpha + \beta)x + \gamma x^2 = 0$, ossia il polinomio $(\alpha + \beta) + (-\alpha + \beta)x + \gamma x^2$ è il polinomio nullo. Quindi tutti i suoi coefficienti devono essere nulli, vale a dire α, β e γ devono soddisfare le condizioni

$$\begin{cases} \alpha + \beta = 0 \\ -\alpha + \beta = 0 \\ \gamma = 0. \end{cases}$$

Risolvendo il sistema si trova che $\alpha = \beta = \gamma = 0$. \square

36.4 PROPOSIZIONE. Siano v_1, v_2, \dots, v_m elementi di uno spazio vettoriale V su un campo K . I vettori v_1, v_2, \dots, v_m sono linearmente dipendenti se e solo se uno di essi è combinazione lineare degli altri.

Dimostrazione. Supponiamo che i vettori v_1, v_2, \dots, v_m siano linearmente dipendenti. Allora esistono $\alpha_1, \alpha_2, \dots, \alpha_m \in K$ non tutti nulli tali che $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0$. Supponiamo ad esempio che α_i sia non nullo. Allora α_i^{-1} è invertibile nel campo K . Se $\alpha_i^{-1} \in K$ è il suo inverso, allora $v_i = \alpha_i^{-1}(\alpha_i v_i) = \alpha_i^{-1}(-\alpha_1 v_1 - \dots - \alpha_{i-1} v_{i-1} - \alpha_{i+1} v_{i+1} - \dots - \alpha_m v_m) = -\alpha_i^{-1}\alpha_1 v_1 - \dots - \alpha_i^{-1}\alpha_{i-1} v_{i-1} - \alpha_i^{-1}\alpha_{i+1} v_{i+1} - \dots - \alpha_i^{-1}\alpha_m v_m$ è una combinazione lineare di $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m$.

Viceversa supponiamo che uno dei vettori v_1, v_2, \dots, v_m sia combinazione lineare degli altri. Per semplicità di notazione supporremo che v_1 sia combinazione lineare di v_2, \dots, v_m , diciamo $v_1 = \alpha_2 v_2 + \dots + \alpha_m v_m$. Allora $-v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = 0$ è una combinazione lineare in cui il coefficiente -1 di v_1 non è nullo. Quindi i vettori v_1, v_2, \dots, v_m sono linearmente dipendenti. \square

36.5 ESEMPIO. Se gli elementi di un insieme finito $X \subseteq V$ sono linearmente indipendenti, allora anche gli elementi di un qualunque sottoinsieme non vuoto $Y \subseteq X$ sono linearmente indipendenti.

Ad esempio, supponiamo che v_1, v_2, \dots, v_m siano linearmente indipendenti. Mostriamo che se $t \leq m$, allora v_1, v_2, \dots, v_t sono linearmente indipendenti. Sia $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t = 0$ una loro combinazione lineare nulla. Allora dall'uguaglianza $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t + 0 \cdot v_{t+1} + \dots + 0 \cdot v_m = 0$ e dall'indipendenza lineare di v_1, v_2, \dots, v_m segue che $\alpha_i = 0$ per ogni $i = 1, 2, \dots, t$. Quindi v_1, v_2, \dots, v_t sono linearmente indipendenti.

Estendendo questo facile risultato anche al caso del sottoinsieme vuoto, considereremo anche l'insieme vuoto un insieme di vettori linearmente indipendenti. \square

36.6 ESEMPIO. Un unico vettore v è linearmente indipendente se e solo se $v \neq 0$. Infatti supponiamo $v \neq 0$. Se $\alpha \in K$ e $\alpha v = 0$, allora per il lemma 34.6(d) si ha che $\alpha = 0$. Dunque v è linearmente indipendente. Viceversa se $v = 0$, allora $1 \cdot v = 0$ è una combinazione lineare nulla con il coefficiente 1 non nullo. Quindi v è linearmente dipendente.

Da questo e dall'esempio 36.5 segue che se i vettori v_1, v_2, \dots, v_m sono linearmente indipendenti, allora tutti i vettori v_i devono essere $\neq 0$. \square

36.7 ESEMPIO. Due vettori v, w sono linearmente dipendenti se e solo se uno tra v e w è multiplo dell'altro, cioè esiste $\alpha \in K$ tale che $v = \alpha w$ oppure esiste $\beta \in K$ tale che $w = \beta v$. Infatti se ad esempio esiste $\alpha \in K$ tale che $v = \alpha w$, allora $v - \alpha w = 0$, e in questa combinazione lineare di v e w il coefficiente 1 di v è $\neq 0$. Quindi i vettori v, w sono linearmente dipendenti. Viceversa se v, w sono linearmente dipendenti, allora per la proposizione 36.4 uno tra v e w è combinazione lineare dell'altro, cioè o esiste $\alpha \in K$ tale che $v = \alpha w$ oppure esiste $\beta \in K$ tale che $w = \beta v$. \square

36.8 PROPOSIZIONE. Se l'insieme $\{v_0, v_1, v_2, \dots, v_m\}$ genera V e v_0 è combinazione lineare di v_1, v_2, \dots, v_m , allora anche $\{v_1, v_2, \dots, v_m\}$ genera V .

Dimostrazione. Sia $v \in V$. Dobbiamo dimostrare che v è combinazione lineare di v_1, v_2, \dots, v_m . Dato che $\{v_0, v_1, v_2, \dots, v_m\}$ genera V , si ha che v è combinazione lineare di $v_0, v_1, v_2, \dots, v_m$, cioè esistono $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_m \in K$ tali che $v = \alpha_0 v_0 + \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m$. Dato che v_0 è combinazione lineare di v_1, v_2, \dots, v_m , esistono $\beta_1, \beta_2, \dots, \beta_m \in K$ tali che $v_0 = \beta_1 v_1 + \beta_2 v_2 + \dots + \beta_m v_m$. Ma allora v è combinazione lineare di v_1, v_2, \dots, v_m perché $v = \alpha_0 v_0 + \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = \alpha_0(\beta_1 v_1 + \beta_2 v_2 + \dots + \beta_m v_m) + \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m = (\alpha_0 \beta_1 + \alpha_1) v_1 + (\alpha_0 \beta_2 + \alpha_2) v_2 + \dots + (\alpha_0 \beta_m + \alpha_m) v_m$. \square

36.9 DEFINIZIONE. Sia V uno spazio vettoriale su un campo K e sia B un sottoinsieme finito di V . Diciamo che B è una *base* di V se B è un insieme di vettori linearmente indipendenti e B genera V . \square

36.10 ESEMPIO. Consideriamo il K -spazio vettoriale K^n dell'esempio 34.2. Si è già visto che se e_i denota la n -upla avente tutti gli elementi uguali a 0 eccetto quello all' i -esimo posto uguale a 1 ($i = 1, 2, \dots, n$), allora e_1, e_2, \dots, e_n sono linearmente indipendenti (esempio 36.2) ed $\{e_1, e_2, \dots, e_n\}$ genera K^n (esempio 34.14). Quindi $\{e_1, e_2, \dots, e_n\}$ è una base di K^n , detta la *base canonica* di K^n . \square

36.11 ESEMPIO. Sia K un campo. Abbiamo già visto nell'esempio 34.16 che l'insieme $\{1, x, x^2, x^3, \dots, x^n\}$ genera il K -spazio vettoriale $K[x]_{\leq n}$ dei polinomi a coefficienti in K aventi grado $\leq n$. Infatti ogni polinomio $f = a_0 + a_1x + \dots + a_nx^n$ a coefficienti in K di grado $\leq n$ si scrive come combinazione lineare $f = a_0 \cdot 1 + a_1 \cdot x + \dots + a_n \cdot x^n$ di $1, x, x^2, x^3, \dots, x^n$. Mostriamo che $1, x, x^2, x^3, \dots, x^n$ sono linearmente indipendenti. Se $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n \in K$ e $\alpha_0 \cdot 1 + \alpha_1x + \alpha_2x^2 + \dots + \alpha_nx^n = 0$, cioè $\alpha_0 + \alpha_1x + \alpha_2x^2 + \dots + \alpha_nx^n$ è il polinomio nullo, allora $\alpha_i = 0$ per ogni $i = 0, 1, 2, \dots, n$. Quindi $1, x, x^2, x^3, \dots, x^n$ sono linearmente indipendenti, e $\{1, x, x^2, x^3, \dots, x^n\}$ è una base di $K[x]_{\leq n}$. \square

36.12 ESEMPIO. L'insieme vuoto è una base per lo spazio vettoriale nullo $V = \{0\}$. Infatti \emptyset è un insieme di vettori linearmente indipendenti (esempio 36.5) e \emptyset genera V (esempio 34.18). \square

36.13 ESEMPIO. Continuando ad usare la notazione già introdotta in alcuni esercizi precedenti, denoteremo sempre d'ora in poi con $M_{m \times n}(K)$ l'insieme delle matrici $m \times n$ ad elementi nel campo K . Nel caso particolare di $m = n$ denoteremo con $M_n(K)$ l'insieme delle matrici quadrate di ordine n ad elementi in K . Nell'esercizio 34.4 si è visto che $M_{m \times n}(K)$ è uno spazio vettoriale su K . Per ogni $i = 1, 2, \dots, m$ e ogni $j = 1, 2, \dots, n$ sia $E_{ij} \in M_{m \times n}(K)$ la matrice avente tutti gli elementi uguali a 0 eccetto quello di posto (i, j) che è uguale a 1. Mostriamo che $B = \{E_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ è una base di $M_{m \times n}(K)$.

Facciamo innanzitutto vedere che gli mn vettori E_{ij} , $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, sono linearmente indipendenti. Prendiamo mn elementi α_{ij} , $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, di K e supponiamo che

$$(36.1) \quad \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} E_{ij} = 0.$$

Dato che $\alpha_{ij} E_{ij}$ è la matrice avente tutti gli elementi uguali a 0 eccetto quello di posto (i, j) che è uguale a α_{ij} , è chiaro che la matrice scritta a sinistra nell'uguaglianza (36.1) è la matrice $m \times n$ (α_{ij}). Lo zero scritto a destra nell'uguaglianza (36.1) è lo zero dello spazio vettoriale $M_{m \times n}(K)$, ossia la matrice nulla $m \times n$. In altre parole l'uguaglianza (36.1) dice

che la matrice (α_{ij}) è la matrice nulla. Deve essere pertanto $\alpha_{ij} = 0$ per ogni $i = 1, 2, \dots, m$ e ogni $j = 1, 2, \dots, n$.

Resta da dimostrare che $B = \{E_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ genera $M_{m \times n}(K)$, ossia che ogni matrice appartenente a $M_{m \times n}(K)$ si scrive come combinazione lineare delle matrici E_{ij} . Per questo è sufficiente osservare che per una generica matrice $(a_{ij}) \in M_{m \times n}(K)$ si ha $(a_{ij}) = \sum_{i=1}^m \sum_{j=1}^n a_{ij} E_{ij}$. Quindi $B = \{E_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ è una base di $M_{m \times n}(K)$. \square

36.14 LEMMA. *Siano V uno spazio vettoriale su un campo K e X un insieme finito di generatori di V . Allora X contiene una base di V .*

Dimostrazione. Induzione sulla cardinalità $|X|$ dell'insieme di generatori. Se $|X| = 0$, allora $X = \emptyset$, e quindi come abbiamo visto nell'esempio 36.5 l'insieme X è un insieme di vettori linearmente indipendenti. Pertanto lo stesso $X = \emptyset$ è una base in questo caso.

Supponiamo $|X| = n \geq 1$. Se l'insieme finito X di generatori di V è un insieme di vettori linearmente indipendenti, allora X è già una base di V . Se invece l'insieme X di generatori è un insieme di vettori linearmente dipendenti, allora uno di essi è combinazione lineare dei rimanenti per la proposizione 36.4. Supponiamo quindi che $v_0 \in X$ sia combinazione lineare degli elementi di $X \setminus \{v_0\}$. Per la proposizione 36.8 l'insieme $X \setminus \{v_0\}$ genera V . Dato che $X \setminus \{v_0\}$ ha un elemento in meno di quanti ne ha X , applicando l'ipotesi induttiva all'insieme finito $X \setminus \{v_0\}$ di generatori di V si trova che $X \setminus \{v_0\}$ deve contenere una base di V . \square

In particolare, se V è uno spazio vettoriale, V ha un sottoinsieme finito che è una base di V se e solo se V ha un insieme finito di generatori. Infatti, se $B \subseteq V$ è un sottoinsieme finito che è una base di V , allora B è un insieme finito di generatori di V . Viceversa, se V ha un insieme finito X di generatori, allora X contiene una base B di V per il lemma 36.14.

36.15 PROPOSIZIONE. *Le seguenti affermazioni sono equivalenti per un sottoinsieme finito B di uno spazio vettoriale V :*

- B è una base di V ;*
- B è un insieme minimale di generatori di V , cioè B è un insieme di generatori di V e ogni sottoinsieme proprio di B non è un insieme di generatori di V ;*
- B è un insieme massimale di vettori linearmente indipendenti di V , cioè B è un insieme di vettori linearmente indipendenti e ogni sottoinsieme finito di V che contiene propriamente B non è un insieme di vettori linearmente indipendenti.*

Dimostrazione. (a) \Rightarrow (b) Se B è una base di V , allora B è un insieme di generatori di V . Sia Y un sottoinsieme proprio di B e sia $b \in B \setminus Y$. Se Y fosse un insieme di generatori di V , allora b sarebbe combinazione lineare degli elementi di Y , e quindi i vettori di $Y \cup \{b\}$ sarebbero linearmente dipendenti per la proposizione 36.4. Quindi i vettori di B sarebbero linearmente dipendenti, e questo contraddirebbe il fatto che B è una base.

(b) \Rightarrow (a) Supponiamo che il sottoinsieme B sia un insieme minimale di generatori di V . Per il lemma 36.14 l'insieme B contiene una base B' di V . Per la minimalità di B ogni

sottoinsieme proprio di B non è un insieme di generatori di V , e quindi non è una base. Quindi B' non può essere un sottoinsieme proprio di B , vale a dire $B' = B$. Quindi B è una base di V .

(a) \Rightarrow (c) Se B è una base di V , B è un insieme di vettori linearmente indipendenti. Sia X un sottoinsieme finito di V contenente propriamente B , e sia $v \in X \setminus B$. Allora v è combinazione lineare degli elementi di B , e quindi i vettori di $B \cup \{v\}$ sono linearmente dipendenti per la proposizione 36.4. A maggior ragione quindi i vettori di $X \supseteq B \cup \{v\}$ sono linearmente dipendenti.

(c) \Rightarrow (a) Sia $B = \{v_1, \dots, v_n\}$ un insieme massimale di vettori linearmente indipendenti di V . Dobbiamo dimostrare che B genera V , ossia che ogni vettore $v \in V$ è combinazione lineare di v_1, \dots, v_n . Sia $v \in V$. Se $v \in B$, allora certamente v è combinazione lineare di v_1, \dots, v_n . Se invece $v \notin B$, allora $\{v, v_1, \dots, v_n\}$ è un sottoinsieme finito di V che contiene propriamente B , e quindi per ipotesi i vettori v, v_1, \dots, v_n non sono linearmente indipendenti. Pertanto esiste una loro combinazione lineare $\alpha v + \alpha_1 v_1 + \dots + \alpha_n v_n = 0$ con i coefficienti $\alpha, \alpha_1, \dots, \alpha_n$ non tutti nulli. Se $\alpha = 0$, allora la combinazione lineare $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ avrebbe i coefficienti $\alpha_1, \dots, \alpha_n$ non tutti nulli, e questo mostrebbe che v_1, \dots, v_n non solo linearmente indipendenti, contraddicendo la nostra ipotesi. Quindi deve essere $\alpha \neq 0$. Ne segue che $\alpha^{-1} \in K$ e $v = -\alpha^{-1} \alpha_1 v_1 - \dots - \alpha^{-1} \alpha_n v_n$. Questo mostra che v è combinazione lineare di v_1, \dots, v_n . \square

36.16 TEOREMA DI SOSTITUZIONE. Siano V uno spazio vettoriale su un campo K , $\{v_1, \dots, v_n\}$ una base di V , e w_1, \dots, w_m vettori linearmente indipendenti di V . Allora $m \leq n$, e si può ottenere un'altra base di V sostituendo m vettori v_i con gli m vettori w_1, \dots, w_m .

Dimostrazione. Induzione su m . Il caso $m = 0$ è banale. Supponiamo che il teorema sia vero per $m - 1$. Siano $\{v_1, \dots, v_n\}$ una base di V e w_1, \dots, w_m m vettori linearmente indipendenti di V . Allora anche w_1, \dots, w_{m-1} sono vettori linearmente indipendenti, e quindi per l'ipotesi induttiva si ha che $m - 1 \leq n$ e che si può ottenere un'altra base B di V sostituendo $m - 1$ vettori v_i con gli $m - 1$ vettori w_1, \dots, w_{m-1} . Se fosse $m - 1 = n$, allora avremmo ottenuto una base di V sostituendo tutti i vettori v_i con gli $m - 1$ vettori w_1, \dots, w_{m-1} , ossia $\{w_1, \dots, w_{m-1}\}$ sarebbe una base. In particolare w_m sarebbe combinazione lineare di $\{w_1, \dots, w_{m-1}\}$, e quindi w_1, \dots, w_m sarebbero linearmente dipendenti per la proposizione 36.4, e questa è una contraddizione. Quindi $m - 1 < n$, ossia $m \leq n$. Rinumerando gli indici di $\{v_1, \dots, v_n\}$ possiamo supporre senza perdita di generalità che gli $m - 1$ vettori v_i sostituiti siano v_1, \dots, v_{m-1} , di modo che $B = \{w_1, \dots, w_{m-1}, v_m, \dots, v_n\}$ è una base. In particolare w_m è una combinazione lineare degli elementi di B , diciamo

$$(36.2) \quad w_m = \alpha_1 w_1 + \dots + \alpha_{m-1} w_{m-1} + \beta_m v_m + \dots + \beta_n v_n$$

per opportuni $\alpha_1, \dots, \alpha_{m-1}, \beta_m, \dots, \beta_n \in K$. Non può essere che $\beta_m = \beta_{m+1} = \dots = \beta_n = 0$, altrimenti da (36.2) si otterebbe l'uguaglianza

$$\alpha_1 w_1 + \dots + \alpha_{m-1} w_{m-1} - w_m = 0,$$

e questa mostrerebbe che w_1, \dots, w_m sono linearmente dipendenti, contrariamente all'ipotesi. Quindi almeno uno dei β_j è diverso da zero. Sia $i = m, m+1, \dots, n$ il più grande indice tale che $\beta_i \neq 0$, di modo che

$$(36.3) \quad w_m = \alpha_1 w_1 + \cdots + \alpha_{m-1} w_{m-1} + \beta_m v_m + \cdots + \beta_i v_i,$$

e quindi anche

$$(36.4)$$

$$v_i = -\beta_i^{-1} \alpha_1 w_1 - \cdots - \beta_i^{-1} \alpha_{m-1} w_{m-1} + \beta_i^{-1} w_m - \beta_i^{-1} \beta_m v_m - \cdots - \beta_i^{-1} \beta_{i-1} v_{i-1}.$$

Per concludere la dimostrazione basta mostrare che

$$B' = \{w_1, \dots, w_m, v_m, \dots, v_{i-1}, v_{i+1}, \dots, v_n\}$$

è una base di V . Ora $B = \{w_1, \dots, w_{m-1}, v_m, \dots, v_n\}$ è una base, e quindi genera V , e quindi a maggior ragione $B \cup \{w_m\} = \{w_1, \dots, w_{m-1}, w_m, v_m, \dots, v_n\} = B' \cup \{v_i\}$ genera V . L'uguaglianza (36.4) mostra che v_i è combinazione lineare degli elementi di B' , e pertanto per la proposizione 36.8 anche B' genera V . Mostriamo che gli elementi di B' sono linearmente indipendenti. Sia

$$\gamma_1 w_1 + \cdots + \gamma_m w_m + \delta_m v_m + \cdots + \delta_{i-1} v_{i-1} + \delta_{i+1} v_{i+1} + \cdots + \delta_n v_n = 0$$

una combinazione lineare degli elementi di B' . Sostituendo in questa uguaglianza il valore di w_m dato dalla (36.3) si ottiene

$$\begin{aligned} & \gamma_1 w_1 + \cdots + \gamma_{m-1} w_{m-1} + \gamma_m (\alpha_1 w_1 + \cdots + \alpha_{m-1} w_{m-1} + \beta_m v_m + \cdots + \beta_i v_i) \\ & \quad + \delta_m v_m + \cdots + \delta_{i-1} v_{i-1} + \delta_{i+1} v_{i+1} + \cdots + \delta_n v_n = 0, \end{aligned}$$

cioè

$$\begin{aligned} & (\gamma_1 + \gamma_m \alpha_1) w_1 + \cdots + (\gamma_{m-1} + \gamma_m \alpha_{m-1}) w_{m-1} + (\gamma_m \beta_m + \delta_m) v_m + \cdots \\ & \quad + (\gamma_m \beta_{i-1} + \delta_{i-1}) v_{i-1} + \gamma_m \beta_i v_i + \delta_{i+1} v_{i+1} + \cdots + \delta_n v_n = 0. \end{aligned}$$

Ma i vettori di B sono linearmente indipendenti, e quindi

$$\gamma_1 + \gamma_m \alpha_1 = 0, \dots, \gamma_{m-1} + \gamma_m \alpha_{m-1} = 0,$$

$$\gamma_m \beta_m + \delta_m = 0, \dots, \gamma_m \beta_{i-1} + \delta_{i-1} = 0,$$

$$\gamma_m \beta_i = 0, \quad \delta_{i+1} = 0, \dots, \delta_n = 0.$$

Dato che $\beta_i \neq 0$, da queste si ricava innanzitutto che $\gamma_m = 0$, e quindi che anche $\gamma_1, \dots, \gamma_{m-1}, \delta_m, \dots, \delta_{i-1}$ sono zero. Pertanto i vettori di B' sono linearmente indipendenti. \square

36.17 COROLLARIO. *Tutte le basi di uno spazio vettoriale V sono tra loro equipotenti.*

Dimostrazione. Siano B, B' due basi dello spazio vettoriale V e supponiamo che $|B| = n$, $|B'| = m$. Dato che B è una base di V e i vettori di B' sono linearmente indipendenti, si ha che $m \leq n$ per il teorema di sostituzione. Analogamente, sempre per il teorema di sostituzione, dato che B' è una base di V e i vettori di B sono linearmente indipendenti, si ha $n \leq m$. Quindi $n = m$. \square

Se nessun sottoinsieme finito di uno spazio vettoriale V è una base di V , diremo che V è uno spazio vettoriale di *dimensione infinita*. Se invece V ha sottoinsiemi finiti che sono basi, allora per il corollario 36.17 tutte le basi di V hanno lo stesso numero di elementi. In tal caso diremo che V ha *dimensione finita*, e denoteremo con $\dim(V)$ il numero di elementi di una sua base qualunque. Il numero $\dim(V)$ si dice la *dimensione* di V . Per quanto osservato subito dopo la dimostrazione del lemma 36.14, uno spazio vettoriale ha dimensione finita se e solo se ha un insieme finito di generatori.

36.18 ESEMPI.

- Lo spazio vettoriale K^n ha dimensione n , perché, come si è visto nell'esempio 36.10, l'insieme $\{e_1, e_2, \dots, e_n\}$ è una sua base.
- Lo spazio vettoriale $K[x]_{\leq n}$ ha dimensione $n + 1$, perché, come si è visto nell'esempio 36.11, l'insieme $\{1, x, x^2, x^3, \dots, x^n\}$ è una sua base.
- Lo spazio vettoriale $M_{m \times n}$ ha dimensione mn , perché, come si è visto nell'esempio 36.13, l'insieme $\{E_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ è una sua base.
- Nell'esempio 36.12 si è visto che l'insieme vuoto è una base per lo spazio vettoriale nullo. Ne segue che uno spazio vettoriale V ha dimensione 0 se e solo se V è lo spazio vettoriale nullo. Infatti V ha dimensione 0 se e solo se una (ogni) sua base ha cardinalità 0, ossia se e solo se l'insieme vuoto è una sua base, ossia se e solo se l'insieme vuoto genera V , vale a dire se e solo se $V = \{0_V\}$. \square

36.19 COROLLARIO (TEOREMA DEL COMPLETAMENTO DELLE BASI). *Se V è uno spazio vettoriale di dimensione finita e w_1, \dots, w_m sono vettori di V linearmente indipendenti, allora esiste una base di V che contiene w_1, \dots, w_m .*

Dimostrazione. Sia V uno spazio vettoriale di dimensione finita n , e sia $\{v_1, \dots, v_n\}$ una base di V . Per il teorema di sostituzione 36.16 si può ottenere un'altra base B di V sostituendo m vettori v_i con gli m vettori w_1, \dots, w_m . Quindi B è una base di V che contiene w_1, \dots, w_m . \square

Il corollario precedente è detto “teorema del completamento delle basi” in quanto assicura che ogni insieme di vettori linearmente indipendenti di V può essere completato ad una base di V .

36.20 PROPOSIZIONE. *Se V è uno spazio vettoriale di dimensione finita, allora ogni sotto-spazio U di V ha dimensione finita e $\dim(U) \leq \dim(V)$.*

Dimostrazione. Ragioniamo per assurdo e supponiamo che esista uno spazio vettoriale V di dimensione finita n con un sottospazio vettoriale U di dimensione infinita. Allora

nessun sottoinsieme finito di U è una base di U , ossia, per la proposizione 36.15 ogni sottoinsieme B di U costituito da vettori linearmente indipendenti non è massimale, vale a dire, per ogni sottoinsieme B di U costituito da vettori linearmente indipendenti esiste un sottoinsieme B' di U ancora costituito da vettori linearmente indipendenti e contenente B propriamente. Costruiamo una successione u_1, u_2, \dots, u_{n+1} di vettori linearmente indipendenti di U nel modo seguente. Intanto, dato che U ha dimensione infinita, sarà $U \neq \{0\}$, e quindi esiste $u_1 \in U$, $u_1 \neq 0$. In questo caso la successione u_1 è banalmente costituita da vettori linearmente indipendenti. Supponiamo ora di avere i vettori linearmente indipendenti u_1, u_2, \dots, u_i di U . Dato che U non ha insiemi di vettori linearmente indipendenti massimali, l'insieme $B = \{u_1, u_2, \dots, u_i\}$ è propriamente contenuto in un insieme B' di vettori linearmente indipendenti di U , e quindi esiste $u_{i+1} \in B' \subseteq U$ tale che $u_1, u_2, \dots, u_i, u_{i+1}$ sono linearmente indipendenti. Dopo n passi troveremo $n+1$ vettori u_1, u_2, \dots, u_{n+1} di U linearmente indipendenti. Ma l'esistenza di $n+1$ vettori linearmente indipendenti nello spazio vettoriale V di dimensione n contraddice il teorema di sostituzione 36.16. Questa contraddizione dimostra che ogni sottospazio U di uno spazio vettoriale V di dimensione finita ha dimensione finita. Inoltre $\dim(U) \leq \dim(V)$ per il teorema 36.16. \square

Esercizi svolti

36.1. Si consideri lo spazio vettoriale $\mathbb{Q}[x]_{\leq 2}$ sul campo \mathbb{Q} dei numeri razionali.

- (a) Si dimostri che $A = \{2, 1+x, 1-x^2, -2x-x^2, x^2\}$ è un insieme di generatori di $\mathbb{Q}[x]_{\leq 2}$.
(b) Si determini una base B di $\mathbb{Q}[x]_{\leq 2}$ contenuta in A .

Soluzione. (a) Si deve far vedere che ogni elemento di $\mathbb{Q}[x]_{\leq 2}$ si può esprimere come combinazione lineare degli elementi di A a coefficienti in \mathbb{Q} . Sia $q_0 + q_1x + q_2x^2$ un elemento di $\mathbb{Q}[x]_{\leq 2}$, $q_0, q_1, q_2 \in \mathbb{Q}$. Dobbiamo far vedere che esistono $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{Q}$ tali che $q_0 + q_1x + q_2x^2 = \alpha_1 \cdot 2 + \alpha_2(1+x) + \alpha_3(1-x^2) + \alpha_4(-2x-x^2) + \alpha_5x^2$. Questa uguaglianza può essere riscritta nella forma $q_0 + q_1x + q_2x^2 = (2\alpha_1 + \alpha_2 + \alpha_3) + (\alpha_2 - 2\alpha_4)x + (-\alpha_3 - \alpha_4 + \alpha_5)x^2$, e quindi equivale al sistema

$$(36.5) \quad \begin{cases} q_0 = 2\alpha_1 + \alpha_2 + \alpha_3 \\ q_1 = \alpha_2 - 2\alpha_4 \\ q_2 = -\alpha_3 - \alpha_4 + \alpha_5. \end{cases}$$

Quindi si deve far vedere che per ogni $q_0, q_1, q_2 \in \mathbb{Q}$ esistono $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \in \mathbb{Q}$ che sono soluzioni del sistema (36.5). Risolviamo il sistema (36.5) nelle incognite $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Dalla seconda equazione si ricava $\alpha_2 = q_1 + 2\alpha_4$ e dalla terza si ricava $\alpha_5 = q_2 + \alpha_3 + \alpha_4$. Sostituendo questi valori nella prima equazione del sistema (36.5) si trova $q_0 = 2\alpha_1 + (q_1 + 2\alpha_4) + \alpha_3$, da cui $\alpha_1 = \frac{1}{2}(q_0 - q_1 - 2\alpha_4 - \alpha_3)$. Le soluzioni del sistema (36.5) sono quindi tutte e sole le 5-uple

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \left(\frac{1}{2}(q_0 - q_1 - 2\alpha_4 - \alpha_3), q_1 + 2\alpha_4, \alpha_3, \alpha_4, q_2 + \alpha_3 + \alpha_4\right)$$

al variare di α_3 e α_4 in \mathbb{Q} (ci sono infinite soluzioni, una per ogni scelta della coppia (α_3, α_4)). Se vogliamo possiamo sceglierne una, ad esempio quella corrispondente ad $\alpha_3 = \alpha_4 = 0$, cioè la soluzione $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \left(\frac{1}{2}(q_0 - q_1), q_1, 0, 0, q_2\right)$. Si vede così che ogni polinomio

$q_0 + q_1x + q_2x^2$ è combinazione lineare degli elementi di A , ad esempio

$$(36.6) \quad q_0 + q_1x + q_2x^2 \\ = \frac{1}{2}(q_0 - q_1) \cdot 2 + q_1 \cdot (1+x) + 0 \cdot (1-x^2) + 0 \cdot (-2x - x^2) + q_2 \cdot x^2.$$

(b) Ogni polinomio $q_0 + q_1x + q_2x^2$ si scrive come combinazione lineare di $2, 1+x, x^2$, in quanto l'uguaglianza (36.6) dice che $q_0 + q_1x + q_2x^2 = \frac{1}{2}(q_0 - q_1) \cdot 2 + q_1(1+x) + q_2x^2$. Quindi l'insieme $\{2, 1+x, x^2\}$ genera $\mathbb{Q}[x]_{\leq 2}$. Mostriamo che $2, 1+x, x^2$ sono linearmente indipendenti. Siano $\alpha, \beta, \gamma \in \mathbb{Q}$ tali che $\alpha \cdot 2 + \beta(1+x) + \gamma x^2 = 0$. Allora $(2\alpha + \beta) + \beta x + \gamma x^2 = 0$, ossia $2\alpha + \beta = 0, \beta = 0, \gamma = 0$. Ne segue che $\alpha = \beta = \gamma = 0$. Questo dimostra che i vettori $2, 1+x, x^2$ sono linearmente indipendenti. Quindi $\{2, 1+x, x^2\}$ è una base di $\mathbb{Q}[x]_{\leq 2}$. \square

36.2. Sia \mathbb{C} il campo dei numeri complessi. Come si è visto nell'esempio 34.4, \mathbb{C} è uno spazio vettoriale sul campo \mathbb{R} dei numeri reali. Si determini una base e la dimensione dello spazio vettoriale \mathbb{C} su \mathbb{R} .

Soluzione. Mostriamo che $\{1, i\}$ è una base dell' \mathbb{R} -spazio vettoriale \mathbb{C} . Intanto $\{1, i\}$ genera \mathbb{C} , cioè ogni elemento di \mathbb{C} può essere scritto come combinazione lineare di 1 e i con coefficienti in \mathbb{R} . Infatti ogni elemento $z \in \mathbb{C}$ è del tipo $z = a + ib$, e quindi $z = a \cdot 1 + b \cdot i$ è combinazione lineare di 1 e i con i coefficienti a e b in \mathbb{R} . Inoltre i vettori 1 e i sono linearmente indipendenti, perché se $a, b \in \mathbb{R}$ e $a \cdot 1 + b \cdot i = 0$, allora $a + ib = 0$, e quindi $a = b = 0$. Questo dimostra che $\{1, i\}$ è una base di \mathbb{C} su \mathbb{R} . In particolare la dimensione dell' \mathbb{R} -spazio vettoriale \mathbb{C} è 2. \square

36.3. Si dimostri che se V è uno spazio vettoriale di dimensione finita e U è un sottospazio di V tale che $\dim(U) = \dim(V)$, allora $U = V$.

Soluzione. Sia $n = \dim(U) = \dim(V)$. Allora U ha una base $B_U = \{u_1, \dots, u_n\}$ avente n elementi. Dato che i vettori u_1, \dots, u_n di V sono linearmente indipendenti, esiste una base B_V di V che contiene B_U (teorema del completamento delle basi 36.19). Ma $n = |B_U| = |B_V|$, e quindi $B_U = B_V$. In particolare coincidono i sottospazi di V generati da B_U e da B_V , ossia $U = V$. \square

Altri esercizi

36.4. Nello spazio vettoriale \mathbb{R}^3 sul campo \mathbb{R} i vettori $(3, 1, 1), (2, 1, -1), (1, 0, 1)$ sono linearmente indipendenti?

36.5. Si dimostri che $\{(1, 0, 1), (0, -1, 0), (1, 1, 0)\}$ è una base dello spazio vettoriale \mathbb{R}^3 sul campo \mathbb{R} .

36.6. È vero che $\{(1, -1, 0), (1, 0, 1), (0, -1, -1)\}$ è una base di \mathbb{R}^3 ?

36.7. Sia $\{e_1, e_2, e_3\}$ la base canonica dello spazio vettoriale \mathbb{R}^3 sul campo \mathbb{R} . Si dimostri che anche $\{e_1, e_1 - e_2, 2e_1 - e_2 + e_3\}$ è una base di \mathbb{R}^3 .

36.8. Sia $\mathbb{Z}_3[x]$ lo \mathbb{Z}_3 -spazio vettoriale dei polinomi a coefficienti in \mathbb{Z}_3 . Si dimostri che gli elementi $\bar{1} - x, \bar{1} + x, x^2, -\bar{1} + x^2$ di questo spazio vettoriale sono linearmente dipendenti.

36.9. È vero che $\{(\bar{1}, \bar{1}, \bar{0}), (\bar{1}, -\bar{1}, \bar{1}), (\bar{0}, \bar{0}, \bar{1})\}$ è una base dello spazio vettoriale \mathbb{Z}_2^3 sul campo \mathbb{Z}_2 ?

36.10. Sia V il sottospazio di \mathbb{R}^4 generato da $\{(1, 2, 1, 2), (2, 3, 2, 3), (3, 5, 3, 5)\}$. Si determini una base di V .

36.11. Sia $B = \{E_{ij} \mid i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$ la base della spazio vettoriale $M_{m \times n}(K)$ considerata nell'esempio 36.13. Si dimostri che $E_{ij}E_{kl} = \delta_{jk}E_{il}$ per ogni $i, k = 1, 2, \dots, m$ e ogni $j, l = 1, 2, \dots, n$.

36.12. Sia $M_2(\mathbb{R})$ lo spazio vettoriale su \mathbb{R} delle matrici 2×2 ad elementi reali. Si dimostri che

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\}$$

è una base di $M_2(\mathbb{R})$.

36.13. Sia $M_2(\mathbb{R})$ lo spazio vettoriale su \mathbb{R} delle matrici 2×2 ad elementi reali. Sia W il sottospazio vettoriale di $M_2(\mathbb{R})$ generato dalle matrici

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

Si determini una base di W .

36.14. Siano $\mathbb{R}[x]$ lo spazio vettoriale su \mathbb{R} dei polinomi a coefficienti reali e $D: \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ l'applicazione \mathbb{R} -lineare definita da $D(f) = f'$ per ogni $f \in \mathbb{R}[x]$ (vedi esempio 35.3; in questo caso, in cui $K = \mathbb{R}$, la derivata formale di f coincide con la derivata che si studia nel corso di Analisi Matematica). Si determini $\ker D$ e se ne calcoli la dimensione.

36.15. Sia K un campo e, per ogni numero naturale n , sia $K[x]_{\leq n}$ lo spazio vettoriale su K dei polinomi a coefficienti in K e di grado minore o uguale a n . Sia $\varphi: K[x]_{\leq 3} \rightarrow K[x]_{\leq 3}$ l'applicazione definita da $\varphi(f) = (x^2 + x + 1)f$ per ogni $f \in K[x]_{\leq 3}$.

- (a) Si dimostri che φ è un'applicazione lineare.
- (b) Si determini $\ker \varphi$.
- (c) Si determini la dimensione di $\varphi(K[x]_{\leq 3})$.

36.16. Nell'esempio 34.4 si è visto che ogni campo K è spazio vettoriale su K . Qual è la dimensione di K come spazio vettoriale su K ? Qual è una base?

36.17. Sia $f: \mathbb{Q} \rightarrow \mathbb{Q}$ l'applicazione definita da $f(q) = \frac{1}{3}q$ per ogni $q \in \mathbb{Q}$. Si dimostri che f è un automorfismo di spazi vettoriali su \mathbb{Q} . Si dimostri che $f(W) \subseteq W$ per ogni sottospazio W di \mathbb{Q} .

§37. Somma di spazi vettoriali

Si è già visto nell'esempio 34.11 che se U, W sono due sottospazi di V , allora anche $U + W = \{u + w \mid u \in U, w \in W\}$ (detto la *somma* di U e W) e $U \cap W$ (l'*intersezione* di U e W) sono sottospazi di V . Vediamo ora come sono in relazione tra loro le dimensioni di questi sottospazi $U, W, U + W, U \cap W$ di V .

37.1 TEOREMA (FORMULA DI GRASSMANN). Sia V uno spazio vettoriale su un campo K e siano U, W due sottospazi di dimensione finita di V . Allora anche $U + W$ e $U \cap W$ hanno dimensione finita, e si ha

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W).$$

Dimostrazione. Dato che $U \cap W$ è un sottospazio dello spazio vettoriale U di dimensione finita, anche $U \cap W$ ha dimensione finita per la proposizione 36.20. Siano $n = \dim(U \cap W)$ e $\{v_1, \dots, v_n\}$ una base di $U \cap W$. Per il teorema del completamento delle basi 36.19 l'insieme $\{v_1, \dots, v_n\}$ di vettori linearmente indipendenti di U è contenuto in una base di U , e quindi esistono $u_1, \dots, u_r \in U$ tali che $\{v_1, \dots, v_n, u_1, \dots, u_r\}$ sia una base di U . Si ha pertanto che $n + r = \dim(U)$. Analogamente esistono $w_1, \dots, w_s \in W$ tali che $\{v_1, \dots, v_n, w_1, \dots, w_s\}$ sia una base di W , dove $n + s = \dim(W)$. Per concludere la dimostrazione del teorema è sufficiente provare che $B = \{v_1, \dots, v_n, u_1, \dots, u_r, w_1, \dots, w_s\}$ è una base di $U + W$, in quanto si sarà così dimostrato che $U + W$ ha dimensione finita $n + r + s = \dim(U) + \dim(W) - \dim(U \cap W)$.

Mostriamo che i vettori $v_1, \dots, v_n, u_1, \dots, u_r, w_1, \dots, w_s$ sono linearmente indipendenti. Supponiamo che

$$(37.1) \quad \alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 u_1 + \cdots + \beta_r u_r + \gamma_1 w_1 + \cdots + \gamma_s w_s = 0$$

dove $\alpha_i, \beta_j, \gamma_k \in K$ per ogni i, j, k . Allora

$$\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 u_1 + \cdots + \beta_r u_r = -\gamma_1 w_1 - \cdots - \gamma_s w_s \in U \cap W.$$

Quindi questo elemento può essere scritto come combinazione lineare degli elementi della base $\{v_1, \dots, v_n\}$ di $U \cap W$, diciamo $-\gamma_1 w_1 - \cdots - \gamma_s w_s = \delta_1 v_1 + \cdots + \delta_n v_n$ con $\delta_1, \dots, \delta_n \in K$. Ma allora $\delta_1 v_1 + \cdots + \delta_n v_n + \gamma_1 w_1 + \cdots + \gamma_s w_s = 0$, e dato che i vettori $v_1, \dots, v_n, w_1, \dots, w_s$ formano una base di W e quindi sono linearmente indipendenti, se ne ricava che $\gamma_1 = \cdots = \gamma_s = 0$. Da (37.1) si deduce quindi che $\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 u_1 + \cdots + \beta_r u_r = 0$. Dato che i vettori $v_1, \dots, v_n, u_1, \dots, u_r$ formano una base di U e quindi sono linearmente indipendenti, ne segue che $\alpha_1 = \cdots = \alpha_n = \beta_1 = \cdots = \beta_r = 0$. Pertanto i vettori di B sono linearmente indipendenti.

Proviamo che il sottospazio vettoriale $\langle B \rangle$ di V generato da $B = \{v_1, \dots, v_n, u_1, \dots, u_r, w_1, \dots, w_s\}$ è uguale a $U + W$. Dato che i v_i e gli u_j appartengono a U e che i w_k appartengono a W , si ha $B \subseteq U + W$, e quindi $\langle B \rangle \subseteq U + W$. Viceversa, per dimostrare che $U + W \subseteq \langle B \rangle$ si deve far vedere che ogni elemento $u + w$ di $U + W$ ($u \in U$ e $w \in W$) si può scrivere come combinazione lineare di $v_1, \dots, v_n, u_1, \dots, u_r, w_1, \dots, w_s$. Dato che i v_i e gli u_j formano una base di U si ha che $u = \alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 u_1 + \cdots + \beta_r u_r$ per opportuni $\alpha_i, \beta_j \in K$. Similmente, dato che i v_i e i w_k formano una base di W , si ha che $w = \alpha'_1 v_1 + \cdots + \alpha'_n v_n + \gamma_1 w_1 + \cdots + \gamma_s w_s$ per opportuni $\alpha'_i, \gamma_k \in K$. Ma allora $u + w = (\alpha_1 + \alpha'_1)v_1 + \cdots + (\alpha_n + \alpha'_n)v_n + \beta_1 u_1 + \cdots + \beta_r u_r + \gamma_1 w_1 + \cdots + \gamma_s w_s$ è la combinazione lineare voluta. Quindi $\langle B \rangle = U + W$ e B è una base di $U + W$. \square

Passiamo ora a considerare la somma diretta di spazi vettoriali. Il termine "somma diretta" ha due significati differenti, anche se essenzialmente equivalenti. In questo §37

presenteremo entrambi i significati, distinguendoli per maggior precisione. Introdurremo pertanto prima la “somma diretta esterna”, poi la “somma diretta interna”, e infine vedremo qual è la relazione tra i due concetti.

Iniziamo con la “somma diretta esterna”. Siano U, W due spazi vettoriali arbitrari sullo stesso campo K . Denotiamo con $U \oplus W$ il prodotto cartesiano degli insiemi U e W , di modo che $U \oplus W = \{(u, w) \mid u \in U, w \in W\}$. Sull'insieme $U \oplus W$ definiamo $(u, w) + (u', w') = (u + u', w + w')$ e $\alpha(u, w) = (\alpha u, \alpha w)$ per ogni $(u, w), (u', w') \in U \oplus W$. È facile verificare che con queste definizioni $U \oplus W$ risulta essere uno spazio vettoriale su K , detto la *somma diretta esterna* di U e W .

La “somma diretta interna” riguarda invece il caso in cui U e W sono sottospazi di uno stesso spazio vettoriale V . Premettiamo un lemma.

37.2 LEMMA. *Siano V uno spazio vettoriale e U, W sottospazi di V . Le seguenti condizioni sono equivalenti:*

- (a) $U + W = V$ e $U \cap W = \{0\}$.
- (b) Ogni vettore $v \in V$ si scrive in modo unico nella forma $v = u + w$ con $u \in U$ e $w \in W$.

Dimostrazione. (a) \Rightarrow (b) Da $U + W = V$ segue che ogni vettore $v \in V$ si scrive nella forma $v = u + w$ per certi $u \in U, w \in W$. Se poi si ha anche che $v = u' + w'$ con $u' \in U, w' \in W$, allora da $v = u + w = u' + w'$ segue che $u - u' = w' - w$ appartiene sia a U che a W , e quindi appartiene a $U \cap W = \{0\}$. Pertanto $u - u' = w' - w = 0$, da cui $u = u'$ e $w = w'$.

(b) \Rightarrow (a) Dato che ogni vettore $v \in V$ si scrive nella forma $v = u + w$ per opportuni $u \in U, w \in W$, si ha che $V \subseteq U + W$. Ma U e W sono contenuti entrambi nello spazio vettoriale V , e quindi $U + W \subseteq V$. Pertanto $U + W = V$. Sia $x \in U \cap W$. Allora il vettore nullo si scrive sia nella forma $0 + 0$ che nella forma $x + (-x)$, e si ha che $0, x \in U$ e $0, -x \in W$. Per l'unicità della scrittura dell'ipotesi (b) si deve avere pertanto $x = 0$. Questo dimostra che $U \cap W \subseteq \{0\}$. L'altra inclusione $U \cap W \supseteq \{0\}$ è ovvia. \square

Se V è uno spazio vettoriale e U, W sono sottospazi di V soddisfacenti le condizioni equivalenti del lemma precedente diremo che V è la *somma diretta interna* di U e W , e scriveremo anche in questo caso $V = U \oplus W$. Dalla formula di Grassmann 37.1 segue immediatamente che se V è la somma diretta interna $U \oplus W$ di U e W , allora $\dim V = \dim U + \dim W$.

Nella proposizione che segue mostreremo in che senso i due concetti di “somma diretta esterna” e di “somma diretta interna” sono essenzialmente equivalenti.

37.3 PROPOSIZIONE.

- (a) *Siano U, W due spazi vettoriali sullo stesso campo K , e sia $U \oplus W = \{(u, w) \mid u \in U, w \in W\}$ la loro somma diretta esterna. Allora $U' = \{(u, 0) \mid u \in U\}$ è un sottospazio di $U \oplus W$ isomorfo a U , $W' = \{(0, w) \mid w \in W\}$ è un sottospazio di $U \oplus W$ isomorfo a W , e $U \oplus W$ è la somma diretta interna dei suoi sottospazi U' e W' .*
- (b) *Siano V uno spazio vettoriale, U, W sottospazi di V , e supponiamo che V sia la somma*

diretta interna di U e W . Sia $U \oplus W = \{(u, w) \mid u \in U, w \in W\}$ la somma diretta esterna di U e W . Allora gli spazi vettoriali $U \oplus W$ e V sono isomorfi.

Dimostrazione. (a) Nelle notazioni della parte (a) dell'enunciato, è molto facile verificare che $U' = \{(u, 0) \mid u \in U\}$ e $W' = \{(0, w) \mid w \in W\}$ sono sottospazi di $U \oplus W$. Un isomorfismo $\varphi: U \rightarrow U'$ è definito da $\varphi(u) = (u, 0)$ per ogni $u \in U$. Analogamente un isomorfismo $\psi: W \rightarrow W'$ è definito da $\psi(w) = (0, w)$ per ogni $w \in W$. Per dimostrare che $U \oplus W$ è la somma diretta interna di U' e W' si deve far vedere che $U' + W' = U \oplus W$ e $U' \cap W' = \{0\}$. Dimostriamo che $U' + W' = U \oplus W$. Osserviamo che dato che U', W' sono sottoinsiemi dello spazio vettoriale $U \oplus W$, la somma di un elemento di U' e di un elemento di W' è un elemento di $U \oplus W$, e quindi $U' + W' \subseteq U \oplus W$. Viceversa, ogni elemento di $U \oplus W$ è del tipo (u, w) con $u \in U$, $w \in W$, e quindi $(u, w) = (u, 0) + (0, w) \in U' + W'$, cioè $U \oplus W \subseteq U' + W'$. Questo dimostra l'uguaglianza $U' + W' = U \oplus W$. L'altra uguaglianza $U' \cap W' = \{0\}$ è evidente.

(b) Supponiamo ora invece che V, U, W abbiano il significato della parte (b) dell'enunciato, di modo che U e W sono sottospazi di V e V è la somma diretta interna di U e W . Sia $U \oplus W = \{(u, w) \mid u \in U, w \in W\}$ la somma diretta esterna di U e W . Definiamo un'applicazione $\omega: U \oplus W \rightarrow V$ ponendo $\omega(u, w) = u + w$ per ogni $(u, w) \in U \oplus W$. È facile verificare che l'applicazione ω è un'applicazione lineare. Dimostriamo che è un isomorfismo di spazi vettoriali. Per mostrare che ω è iniettiva facciamo vedere che $\ker \omega = \{0_{U \oplus W}\}$. Se $(u, w) \in \ker \omega$, allora $u + w = \omega(u, w) = 0$. Quindi il vettore nullo 0 di V si scrive sia nella forma $0 = u + w$ che nella forma $0 = 0 + 0$, con $u \neq 0$ in U , e con $w \neq 0$ in W . Dato che V è la somma diretta interna di U e W , dall'unicità della scrittura di ogni elemento di V come somma di un elemento di U e uno di W , cioè dalla (b) del lemma 37.2, segue che $u = 0$ e $w = 0$. Quindi $(u, w) = (0, 0)$. Questo dimostra che $\ker \omega = \{0_{U \oplus W}\}$, e quindi ω è iniettiva. Dato che ogni vettore $v \in V$ si scrive nella forma $v = u + w$ per opportuni $u \in U$ e $w \in W$, l'applicazione $\omega: U \oplus W \rightarrow V$ è suriettiva. Quindi ω è un isomorfismo. \square

Esercizi svolti

37.1. Siano K un campo, V uno spazio vettoriale su K ed $f: V \rightarrow V$ un endomorfismo di spazi vettoriali tale che $f^2 = f$. Si dimostri che $V = \ker f \oplus f(V)$.

Soluzione. Qui $\ker f$ e $f(V)$ sono sottospazi di V , e quindi scrivendo $V = \ker f \oplus f(V)$ si intende che V è la somma diretta interna di $\ker f$ e $f(V)$. È sufficiente dimostrare quindi che valgono le due condizioni $\ker f + f(V) = V$ e $\ker f \cap f(V) = \{0\}$ (lemma 37.2(a)).

Mostriamo che $\ker f + f(V) = V$. Dato che $\ker f$ e $f(V)$ sono entrambi contenuti in V , è chiaro che $\ker f + f(V) \subseteq V$. Per far vedere che $V \subseteq \ker f + f(V)$ prendiamo un elemento $v \in V$. Si ha $v = (v - f(v)) + f(v)$. Ora $f(v - f(v)) = f(v) - f^2(v) = f(v) - f(v) = 0$, e quindi $v - f(v) \in \ker f$. Ovviamente poi $f(v) \in f(V)$. Ne segue quindi che v si può scrivere come somma dell'elemento $v - f(v)$ di $\ker f$ e dell'elemento $f(v)$ di $f(V)$. Pertanto $v \in \ker f + f(V)$. Abbiamo così dimostrato che $\ker f + f(V) = V$.

Facciamo vedere che $\ker f \cap f(V) = \{0\}$. Dato che lo zero dello spazio vettoriale V appartiene a tutti i sottospazi di V , abbiamo in particolare che 0 appartiene sia a $\ker f$ che a $f(V)$, e quindi $\ker f \cap f(V) \supseteq \{0\}$. Dimostriamo che viceversa si ha $\ker f \cap f(V) \subseteq \{0\}$. Sia $v \in \ker f \cap f(V)$.

Dato che $v \in \ker f$, si ha $f(v) = 0$. Ma $v \in f(V)$, e quindi $v = f(w)$ per qualche $w \in W$. Ne segue che $v = f(w) = f^2(w) = f(f(w)) = f(v) = 0$. Questo dimostra che $\ker f \cap f(V) \subseteq \{0\}$. \square

37.2. Si supponga che $V = U \oplus W$ sia somma diretta (interna) dei suoi due sottospazi U e W . Allora ogni elemento $v \in V$ si scrive in modo unico nella forma $v = u + w$ per opportuni $u \in U$, $w \in W$, di modo che è possibile definire un'applicazione $\pi: V \rightarrow U$ ponendo, per ogni $v \in V$ e ogni $u \in U$, $\pi(v) = u$ se e solo se esiste $w \in W$ tale che $v = u + w$.

- Si dimostri che l'applicazione π è lineare.
- Si dimostri che π è l'identità su U , ossia che $\pi(u) = u$ per ogni $u \in U$.
- Si dimostri che $\ker \pi = W$.
- Si dimostri che l'applicazione π è suriettiva.
- Applicando il teorema fondamentale di omomorfismo a π si dimostri che

$$\frac{U \oplus W}{W} \cong U.$$

Soluzione. (a) Si deve dimostrare che $\pi(v + v') = \pi(v) + \pi(v')$ e $\pi(\lambda v) = \lambda \pi(v)$ per ogni $v, v' \in V, \lambda \in K$. Se $v, v' \in V$, allora $v = u + w$ e $v' = u' + w'$ per opportuni $u, u' \in U$, $w, w' \in W$, e si ha $\pi(v) = u$ e $\pi(v') = u'$. Ma allora $v + v' = u + u' + w + w'$, con $u + u' \in U$ e $w + w' \in W$, e pertanto $\pi(v + v') = u + u'$. Quindi $\pi(v + v') = \pi(v) + \pi(v')$. Analogamente si vede che $\pi(\lambda v) = \lambda \pi(v)$.

- Sia $u \in U$. Dato che si può scrivere $u = u + 0$ (e qui $u \in U$ e $0 \in W$), ne segue che $\pi(u) = u$.
- Sia $w \in W$. Dato che si può scrivere $w = 0 + w$ (e qui $0 \in U$ e $w \in W$), ne segue che $\pi(w) = 0$. Questo dimostra che $W \subseteq \ker \pi$. Mostriamo che viceversa si ha $\ker \pi \subseteq W$. Sia $v \in \ker \pi$. Allora $\pi(v) = 0$, ossia, scrivendo v nella forma $v = u + w$ con $u \in U$ e $w \in W$, si ha $u = 0$. Quindi $v = u + w = 0 + w = w \in W$.
- Sia $u \in U$. Si è visto in (b) che $\pi(u) = u$. In particolare π è suriettiva.
- Per il teorema fondamentale di omomorfismo per gli spazi vettoriali 35.9 applicato all'applicazione lineare $\pi: V \rightarrow U$ si ha $V/\ker \pi \cong \pi(V)$. Ma $V = U \oplus W$, $\ker \pi = W$ per (c), e $\pi(V) = U$ per (d). Quindi $U \oplus W/W \cong U$. \square .

Altri esercizi

37.3. Siano $V = \{(\alpha, \beta, 0) \mid \alpha, \beta \in \mathbb{R}\}$ e W il sottospazio vettoriale di \mathbb{R}^3 generato dal vettore $(1, 2, 3)$. Si dimostri che $\mathbb{R}^3 = V \oplus W$.

37.4. Siano V uno spazio vettoriale e U, W sottospazi di V . Si dimostri che le seguenti condizioni sono equivalenti:

- $U \cap W = \{0\}$.
- ogni vettore $v \in U + W$ si scrive in modo unico nella forma $v = u + w$ con $u \in U$ e $w \in W$. Se valgono queste condizioni equivalenti, allora $U + W$ è la somma diretta interna dei suoi sottospazi U e W , cioè $U + W = U \oplus W$.

37.5. Sia $f: V \rightarrow U$ un'applicazione lineare tra due K -spazi vettoriali V e U .

- Si dimostri che se V' è sottospazio di V , allora $f^{-1}(f(V')) = V' + \ker f$.
- Si dimostri che se U' è sottospazio di U , allora $f(f^{-1}(U')) = U' \cap f(V)$.

37.6. Si consideri lo spazio vettoriale \mathbb{Z}_3^3 su \mathbb{Z}_3 .

(a) Quanti elementi ha \mathbb{Z}_3^3 ?

Siano V, W i sottospazi di dimensione 1 di \mathbb{Z}_3^3 generati da $\{(\bar{0}, \bar{1}, \bar{2})\}$, $\{(\bar{1}, \bar{2}, \bar{0})\}$ rispettivamente.

(b) L'elemento $(\bar{2}, \bar{0}, \bar{1})$ di \mathbb{Z}_3^3 appartiene a $V + W$?

(c) Che dimensione ha $V \cap W$?

37.7. Si dimostri che se V è uno spazio vettoriale di dimensione finita e W è un sottospazio di V , allora esiste un sottospazio U di V tale che $V = W \oplus U$.

37.8. Sia V uno spazio vettoriale su un campo K , siano A, B sottoinsiemi di V , e siano $\langle A \rangle, \langle B \rangle, \langle A \cup B \rangle$ i sottospazi di V generati da $A, B, A \cup B$ rispettivamente. È vero o falso che $\langle A \rangle + \langle B \rangle = \langle A \cup B \rangle$?

37.9. Siano W, W', U tre sottospazi di uno spazio vettoriale V , e si supponga che $V = W \oplus U = W' \oplus U$. Si dimostri che W e W' sono isomorfi.

37.10. Il lemma 37.2 si può generalizzare dal caso di due sottospazi U, W al caso di $n \geq 2$ sottospazi U_1, U_2, \dots, U_n di V . Si dimostri che se V è uno spazio vettoriale e U_1, U_2, \dots, U_n sono sottospazi di V , allora le seguenti condizioni sono equivalenti:

(a) $U_1 + U_2 + \dots + U_n = V$ e $U_i \cap (U_1 + \dots + U_{i-1} + U_{i+1} + \dots + U_n) = \{0\}$ per ogni $i = 1, 2, \dots, n$.

(b) ogni vettore $v \in V$ si scrive in modo unico nella forma $v = u_1 + u_2 + \dots + u_n$ con $u_1 \in U_1, u_2 \in U_2, \dots, u_n \in U_n$.

In tal caso si dice che V è *somma diretta (interna)* dei suoi sottospazi U_1, U_2, \dots, U_n , e si scrive $V = U_1 \oplus U_2 \oplus \dots \oplus U_n$.

37.11. Siano K un campo ed n, m interi positivi. Si denoti con U il sottospazio di K^{n+m} i cui elementi sono le $(n+m)$ -uple (a_1, \dots, a_{n+m}) con

$$a_{n+1} = \dots = a_{n+m} = 0$$

e W il sottospazio di K^{n+m} i cui elementi sono le $(n+m)$ -uple (a_1, \dots, a_{n+m}) con

$$a_1 = \dots = a_n = 0.$$

Si dimostri che $U \cong K^n$, $W \cong K^m$ e che K^{n+m} è la somma diretta interna di U e W .

37.12. Siano V uno spazio vettoriale sul campo \mathbb{R} ed $f: V \rightarrow V$ un endomorfismo di spazi vettoriali tale che $f^2 = \iota_V$.

(a) Si dimostri che f è un automorfismo di V .

(b) Siano $W = \{w \in V \mid f(w) = w\}$ e $U = \{u \in V \mid f(u) = -u\}$. Si dimostri che W e U sono sottospazi di V .

(c) Si dimostri che $V = W \oplus U$. [Suggerimento: per ogni $v \in V$ si consideri la decomposizione $v = (v + f(v))/2 + (v - f(v))/2$.]

§38. Estensione per linearità

38.1 TEOREMA. Siano V, W spazi vettoriali sullo stesso campo K , $\{v_1, v_2, \dots, v_n\}$ una base di V e (w_1, w_2, \dots, w_n) una n -upla di vettori di W . Allora esiste un'unica applicazione

lineare $f: V \rightarrow W$ tale che $f(v_i) = w_i$ per ogni $i = 1, 2, \dots, n$.

Dimostrazione. *Esistenza.* Mostriamo che esiste un'applicazione lineare $f: V \rightarrow W$ tale che $f(v_i) = w_i$ per ogni $i = 1, 2, \dots, n$. Dato un qualunque $v \in V$, v si può scrivere in modo unico nella forma $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ per certi $\alpha_1, \dots, \alpha_n \in K$. Si definisca l'applicazione $f: V \rightarrow W$ ponendo $f(v) = \alpha_1 w_1 + \dots + \alpha_n w_n$. Si ha certamente $f(v_i) = w_i$ per ogni $i = 1, 2, \dots, n$. Per mostrare che f è un'applicazione lineare si prendano due vettori arbitrari $v, v' \in V$. Allora si ha $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ e $v' = \alpha'_1 v_1 + \dots + \alpha'_n v_n$ per certi $\alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_n \in K$, da cui $v + v' = (\alpha_1 + \alpha'_1)v_1 + \dots + (\alpha_n + \alpha'_n)v_n$, e quindi

$$\begin{aligned} f(v + v') &= (\alpha_1 + \alpha'_1)w_1 + \dots + (\alpha_n + \alpha'_n)w_n \\ &= \alpha_1 w_1 + \dots + \alpha_n w_n + \alpha'_1 w_1 + \dots + \alpha'_n w_n = f(v) + f(v'). \end{aligned}$$

Similmente $f(\alpha v) = \alpha f(v)$ per ogni $\alpha \in K, v \in V$.

Unicità. Sia $f': V \rightarrow W$ un'altra applicazione lineare con la proprietà richiesta, ossia un'applicazione lineare tale che $f'(v_i) = w_i$ per ogni $i = 1, 2, \dots, n$. Dato un qualunque $v \in V$ si ha $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ per certi $\alpha_1, \dots, \alpha_n \in K$, e quindi $f'(v) = f'(\alpha_1 v_1 + \dots + \alpha_n v_n) = f'(\alpha_1 v_1) + \dots + f'(\alpha_n v_n) = \alpha_1 f'(v_1) + \dots + \alpha_n f'(v_n) = \alpha_1 w_1 + \dots + \alpha_n w_n = f(v)$. Per l'arbitrarietà di $v \in V$ si ha quindi $f' = f$. \square

Nel teorema 38.1 si è visto che se $\varphi: \{v_1, v_2, \dots, v_n\} \rightarrow W$ è una qualunque applicazione e $\{v_1, v_2, \dots, v_n\}$ è una base di V , esiste un'unica applicazione $f: V \rightarrow W$ che è lineare ed estende φ . Si dice in questo caso che l'applicazione f è definita *estendendo per linearità* l'applicazione φ .

38.2 ESEMPIO. Siano $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$, $e'_1 = (1, 0)$, $e'_2 = (0, 1)$, di modo che $\{e_1, e_2, e_3\}$ ed $\{e'_1, e'_2\}$ sono le basi canoniche di \mathbb{R}^3 ed \mathbb{R}^2 rispettivamente. Per il teorema precedente esiste un'unica applicazione lineare $f: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ tale che $f(e_1) = e'_1 + e'_2$, $f(e_2) = e'_1$ e $f(e_3) = e'_1 - 2e'_2$. L'immagine $f(\alpha, \beta, \gamma)$ del generico vettore $(\alpha, \beta, \gamma) \in \mathbb{R}^3$ è $f(\alpha, \beta, \gamma) = f(\alpha e_1 + \beta e_2 + \gamma e_3) = \alpha f(e_1) + \beta f(e_2) + \gamma f(e_3) = \alpha(e'_1 + e'_2) + \beta e'_1 + \gamma(e'_1 - 2e'_2) = (\alpha + \beta + \gamma)e'_1 + (\alpha - 2\gamma)e'_2$. \square

38.3 LEMMA. Siano V, W spazi vettoriali sullo stesso campo K , $\{v_1, v_2, \dots, v_n\}$ una base di V , ed $f: V \rightarrow W$ un'applicazione lineare. Allora f è un isomorfismo se e solo se $\{f(v_1), f(v_2), \dots, f(v_n)\}$ è una base di W .

Dimostrazione. Supponiamo che $f: V \rightarrow W$ sia un isomorfismo. Mostriamo che i vettori $f(v_1), f(v_2), \dots, f(v_n)$ sono linearmente indipendenti. Se $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ e $\alpha_1 f(v_1) + \dots + \alpha_n f(v_n) = 0$, allora $f(\alpha_1 v_1 + \dots + \alpha_n v_n) = f(\alpha_1 v_1) + \dots + f(\alpha_n v_n) = \alpha_1 f(v_1) + \dots + \alpha_n f(v_n) = 0 = f(0)$. Dato che f è iniettiva, ne segue che $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Ma $\{v_1, v_2, \dots, v_n\}$ è una base di V , e quindi i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti. Da questo si ottiene che $\alpha_i = 0$ per ogni $i = 1, 2, \dots, n$, e pertanto i vettori $f(v_1), f(v_2), \dots, f(v_n)$ sono linearmente indipendenti. Mostriamo che

$\{f(v_1), f(v_2), \dots, f(v_n)\}$ genera W . Dobbiamo fare vedere che ogni vettore di W si può scrivere come combinazione lineare dei vettori $f(v_1), f(v_2), \dots, f(v_n)$. Sia w un vettore di W . Dato che f è suriettiva, $w = f(v)$ per qualche $v \in V$. Il vettore v si può scrivere come combinazione lineare di v_1, v_2, \dots, v_n perché questi vettori formano una base di V . Quindi $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ per opportuni $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. Ne segue che $w = f(v) = f(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 f(v_1) + \dots + \alpha_n f(v_n)$ è combinazione lineare di $f(v_1), f(v_2), \dots, f(v_n)$. Pertanto $\{f(v_1), f(v_2), \dots, f(v_n)\}$ è una base di W .

Viceversa supponiamo che $f: V \rightarrow W$ sia un'applicazione lineare, $\{v_1, v_2, \dots, v_n\}$ sia una base di V , e $\{f(v_1), f(v_2), \dots, f(v_n)\}$ sia una base di W . Vogliamo dimostrare che f è un isomorfismo. Per far vedere che f è iniettiva mostriamo che $\ker f = \{0\}$. Se $v \in \ker f$, allora v si scrive come combinazione lineare dei vettori v_1, v_2, \dots, v_n , diciamo $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ per opportuni $\alpha_1, \alpha_2, \dots, \alpha_m \in K$. Allora $0 = f(v) = f(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 f(v_1) + \dots + \alpha_n f(v_n)$. Dato che $f(v_1), f(v_2), \dots, f(v_n)$ sono linearmente indipendenti, si deve avere pertanto che $\alpha_i = 0$ per ogni $i = 1, 2, \dots, n$. Quindi $v = 0$. Questo dimostra che $\ker f = \{0\}$, cioè che f è iniettiva.

Mostriamo che f è suriettiva. Per l'esercizio 35.6, dato che V è generato da $\{v_1, \dots, v_n\}$, l'immagine $f(V)$ di f è generata da $\{f(v_1), \dots, f(v_n)\}$. Quindi $f(V)$ è generata da una base di W . Ma una base di W genera tutto W , vale a dire $f(V) = W$, ossia f è suriettiva. \square

38.4 TEOREMA. *Se W è uno spazio vettoriale di dimensione n su un campo K , allora $W \cong K^n$.*

Dimostrazione. Siano $\{e_1, e_2, \dots, e_n\}$ la base canonica di K^n e $\{w_1, w_2, \dots, w_n\}$ una base di W . Per il teorema 38.1 esiste un'unica applicazione lineare $f: K^n \rightarrow W$ tale che $f(e_i) = w_i$ per ogni $i = 1, 2, \dots, n$. Per il lemma 38.3 l'applicazione lineare f è un isomorfismo. \square

Se ne deduce, come corollario, che due spazi vettoriali V, W sullo stesso campo K sono isomorfi se e solo se hanno la stessa dimensione.

38.5 PROPOSIZIONE. *Sia $f: V \rightarrow U$ un'applicazione lineare e si supponga che V abbia dimensione finita. Allora anche il sottospazio $f(V)$ di U ha dimensione finita, e si ha $\dim(V) = \dim(\ker f) + \dim(f(V))$.*

Dimostrazione. Sia V di dimensione finita ed $f: V \rightarrow U$ un'applicazione lineare. Osserviamo innanzitutto che il sottospazio $\ker f$ di V ha dimensione finita per la proposizione 36.20. Sia quindi $\{v_1, \dots, v_k\}$ una base di $\ker f$. I vettori v_1, \dots, v_k di V sono linearmente indipendenti, e quindi per il teorema del completamento delle basi 36.19 l'insieme $\{v_1, \dots, v_k\}$ è contenuto in una base $B = \{v_1, \dots, v_k, w_1, \dots, w_h\}$ di V . Per dimostrare la proposizione è quindi sufficiente dimostrare che l'insieme $C = \{f(w_1), \dots, f(w_h)\}$ ha h elementi ed è una base di $f(V)$.

Mostriamo intanto che i vettori $f(w_1), \dots, f(w_h)$ sono linearmente indipendenti. Sia $\alpha_1 f(w_1) + \dots + \alpha_h f(w_h) = 0$ una combinazione lineare ($\alpha_1, \dots, \alpha_h \in K$). Allora

$f(\alpha_1 w_1 + \cdots + \alpha_h w_h) = f(\alpha_1 w_1) + \cdots + f(\alpha_h w_h) = \alpha_1 f(w_1) + \cdots + \alpha_h f(w_h) = 0$, e quindi $\alpha_1 w_1 + \cdots + \alpha_h w_h \in \ker f$. Quindi $\alpha_1 w_1 + \cdots + \alpha_h w_h$ deve essere una combinazione lineare degli elementi v_1, \dots, v_k della base di $\ker f$, diciamo $\alpha_1 w_1 + \cdots + \alpha_h w_h = \beta_1 v_1 + \cdots + \beta_k v_k$ per certi $\beta_1, \dots, \beta_k \in K$. Ma allora $-\beta_1 v_1 - \cdots - \beta_k v_k + \alpha_1 w_1 + \cdots + \alpha_h w_h = 0$, ed essendo i vettori della base B di V linearmente indipendenti, se ne ricava che $-\beta_1 = \cdots = -\beta_k = \alpha_1 = \cdots = \alpha_h = 0$. Quindi i vettori $f(w_1), \dots, f(w_h)$ sono linearmente indipendenti. In particolare C ha h elementi.

Mostriamo ora che il sottospazio vettoriale $\langle C \rangle$ di U generato da $C = \{f(w_1), \dots, f(w_h)\}$ è uguale a $f(V)$. Dato che i w_i appartengono a V , si ha che $C \subseteq f(V)$, e pertanto $\langle C \rangle \subseteq f(V)$. Per dimostrare che viceversa si ha $f(V) \subseteq \langle C \rangle$, si deve far vedere che ogni elemento di $f(V)$ si scrive come combinazione lineare degli elementi di C . Ora un elemento di $f(V)$ è del tipo $f(v)$ con $v \in V$. Dato che B è una base di V si ha $v = \alpha_1 v_1 + \cdots + \alpha_k v_k + \beta_1 w_1 + \cdots + \beta_h w_h$ per opportuni $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_h \in K$. Ma allora $f(v) = f(\alpha_1 v_1 + \cdots + \alpha_k v_k + \beta_1 w_1 + \cdots + \beta_h w_h) = \alpha_1 f(v_1) + \cdots + \alpha_k f(v_k) + \beta_1 f(w_1) + \cdots + \beta_h f(w_h) = \beta_1 f(w_1) + \cdots + \beta_h f(w_h)$ perché i v_i appartengono al nucleo di f . Pertanto $f(v)$ è combinazione lineare degli elementi di C . Questo dimostra che $f(V) \subseteq \langle C \rangle$, e quindi C è una base di $f(V)$. \square

38.6 COROLLARIO. Siano V uno spazio vettoriale di dimensione finita su un campo K , W un suo sottospazio, e V/W lo spazio quoziante. Allora V/W ha dimensione finita, e si ha $\dim(V/W) = \dim(V) - \dim(W)$.

Dimostrazione. Si applichi la proposizione 38.5 alla proiezione canonica $\pi: V \rightarrow V/W$ osservando che $\ker \pi = W$ e $\pi(V) = V/W$ perché π è suriettiva. \square

38.7 COROLLARIO. Sia $f: V \rightarrow V$ un endomorfismo di uno spazio vettoriale V di dimensione finita. Allora f è un automorfismo se e solo se f è iniettivo, se e solo se f è suriettivo.

Dimostrazione. È sufficiente dimostrare che l'endomorfismo f è iniettivo se e solo se è suriettivo. Se f è iniettivo, allora $\ker f = \{0\}$, e quindi $\dim(\ker f) = 0$. Dalla proposizione 38.5 segue che $\dim(V) = \dim(f(V))$, e quindi $V = f(V)$ (esercizio 36.3). Questo dimostra che f è anche suriettivo.

Se invece supponiamo che l'endomorfismo f di V sia suriettivo, allora $f(V) = V$, e quindi $\dim(V) = \dim(f(V))$. Dalla proposizione 38.5 segue che $\dim(\ker f) = 0$, e quindi $\ker f = \{0\}$. Pertanto f è anche iniettivo. \square

Gli endomorfismi di uno spazio vettoriale V di dimensione finita che non sono automorfismi (equivalentemente, non sono iniettivi o non sono suriettivi) si dicono anche *singolari*. Gli altri si dicono *nonsingolari*.

Esercizi svolti

38.1. Nello spazio vettoriale reale \mathbb{R}^3 si considerino i tre vettori $v_1 = (1, 2, -1)$, $v_2 = (3, 1, 2)$, $v_3 = (0, -5, 5)$.

(a) Si calcoli la dimensione del sottospazio vettoriale W generato da $\{v_1, v_2, v_3\}$.

- (b) Si determinino tutte le applicazioni lineari $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ tali che $f(v_1) = 0$, $f(v_2) = v_1$, $f(v_3) = v_1$.
(c) Si determinino tutte le applicazioni lineari $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ tali che $f(v_1) = 0$, $f(v_2) = v_1$, $f(v_3) = -v_2$.

Soluzione. (a) Vediamo se i tre vettori v_1, v_2, v_3 sono linearmente indipendenti (perché se così fosse W avrebbe dimensione 3). Siano $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$. Si ha $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$ se e solo se $\lambda_1(1, 2, -1) + \lambda_2(3, 1, 2) + \lambda_3(0, -5, 5) = (0, 0, 0)$, ossia se e solo se $(\lambda_1 + 3\lambda_2, 2\lambda_1 + \lambda_2 - 5\lambda_3, -\lambda_1 + 2\lambda_2 + 5\lambda_3) = (0, 0, 0)$, vale a dire se e solo se $(\lambda_1, \lambda_2, \lambda_3)$ è una soluzione del sistema

$$(38.1) \quad \begin{cases} \lambda_1 + 3\lambda_2 = 0 \\ 2\lambda_1 + \lambda_2 - 5\lambda_3 = 0 \\ -\lambda_1 + 2\lambda_2 + 5\lambda_3 = 0. \end{cases}$$

Risolviamo questo sistema. Dalla prima equazione si ricava $\lambda_1 = -3\lambda_2$. Sostituendo questa espressione di λ_1 nelle altre due equazioni si trova

$$\begin{cases} -5\lambda_2 - 5\lambda_3 = 0 \\ 5\lambda_2 + 5\lambda_3 = 0. \end{cases}$$

Queste due equazioni si ottengono l'una dall'altra cambiando il segno, e quindi le soluzioni del sistema (38.1) sono tutte e sole le $(\lambda_1, \lambda_2, \lambda_3) = (-3\lambda_2, \lambda_2, -\lambda_2)$ al variare di λ_2 in \mathbb{R} . Ad esempio $(-3, 1, -1)$ è una soluzione del sistema (38.1), e quindi $-3v_1 + v_2 - v_3 = 0$. I tre vettori v_1, v_2, v_3 non sono pertanto linearmente indipendenti, e anzi da $-3v_1 + v_2 - v_3 = 0$ si vede che $v_3 = -3v_1 + v_2$ appartiene allo spazio vettoriale generato da $\{v_1, v_2\}$. Quindi lo spazio vettoriale W generato da $\{v_1, v_2, v_3\}$ coincide con lo spazio vettoriale generato da $\{v_1, v_2\}$.

Vediamo se i due vettori v_1, v_2 sono linearmente indipendenti (perché se così è, lo spazio vettoriale W da loro generato ha dimensione 2). Siano $\lambda_1, \lambda_2 \in \mathbb{R}$. Si ha $\lambda_1 v_1 + \lambda_2 v_2 = 0$ se e solo se $\lambda_1 v_1 + \lambda_2 v_2 + 0v_3 = 0$, ossia se e solo se $(\lambda_1, \lambda_2, 0)$ è una soluzione del sistema (38.1). Per quanto si è visto nel paragrafo precedente questo accade se e solo se $(\lambda_1, \lambda_2, 0) = (-3\lambda_2, \lambda_2, -\lambda_2)$ per qualche $\lambda_2 \in \mathbb{R}$, ossia se e solo se $(\lambda_1, \lambda_2, 0) = (0, 0, 0)$. Quindi i vettori v_1, v_2 sono linearmente indipendenti, e pertanto lo spazio vettoriale W da loro generato ha dimensione 2.

(b) e (c). Si osservi innanzitutto che per risolvere le parti (b) e (c) non si può applicare direttamente il teorema 38.1, in quanto $\{v_1, v_2, v_3\}$ non è una base di \mathbb{R}^3 . Mostriamo che se invece prendiamo ad esempio $v = (0, 0, 1)$, allora $\{v_1, v_2, v\}$ è una base di \mathbb{R}^3 . Basta far vedere che v_1, v_2, v sono linearmente indipendenti. Ma se $\mu_1, \mu_2, \mu_3 \in \mathbb{R}$ sono tali che $\mu_1 v_1 + \mu_2 v_2 + \mu_3 v = 0$, cioè $\mu_1(1, 2, -1) + \mu_2(3, 1, 2) + \mu_3(0, 0, 1) = (0, 0, 0)$, allora $(\mu_1 + 3\mu_2, 2\mu_1 + \mu_2, -\mu_1 + 2\mu_2 + \mu_3) = (0, 0, 0)$, e quindi (μ_1, μ_2, μ_3) deve essere una soluzione del sistema

$$\begin{cases} \mu_1 + 3\mu_2 = 0 \\ 2\mu_1 + \mu_2 = 0 \\ -\mu_1 + 2\mu_2 + \mu_3 = 0. \end{cases}$$

Risolvendo questo sistema si trova $\mu_1 = \mu_2 = \mu_3 = 0$. Questo dimostra che $\{v_1, v_2, v\}$ è una base di \mathbb{R}^3 . Dal teorema 38.1 abbiamo quindi che per ogni $w \in \mathbb{R}^3$ c'è esattamente una applicazione lineare $f_w: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ tale che $f_w(v_1) = 0$, $f_w(v_2) = v_1$, $f_w(v) = w$. Vediamo dove deve mandare v_3 una tale applicazione f_w . Si è visto nella parte (a) che $v_3 = -3v_1 + v_2$. Quindi per ogni applicazione lineare f_w si deve avere $f_w(v_3) = f_w(-3v_1 + v_2) = -3f_w(v_1) + f_w(v_2) = -3 \cdot 0 + v_1 = v_1$.

Quindi ogni applicazione f_w che mandi v_1 in 0 e v_2 in v_1 deve necessariamente mandare v_3 in v_1 . Ecco quindi che la soluzione di (b) è “sono tutte le applicazioni lineari f_w al variare di w in \mathbb{R}^3 ”, mentre la soluzione di (c) è “non ce n’è nessuna”. \square

38.2. Siano v, w due elementi non nulli di uno spazio vettoriale V di dimensione finita. Si dimostri che esiste un isomorfismo di spazi vettoriali $f: V \rightarrow V$ tale che $f(v) = w$.

Soluzione. Supponiamo che V abbia dimensione n . Si osservi che $\{v\}$ è un insieme di vettori linearmente indipendenti di V perché $v \neq 0$. Quindi per il teorema del completamento delle basi (corollario 36.19), esiste una base di V del tipo $\{v, v_2, v_3, \dots, v_n\}$. Analogamente esiste una base di V del tipo $\{w, w_2, w_3, \dots, w_n\}$. Per il teorema 38.1 esiste un’unica applicazione lineare $f: V \rightarrow V$ tale che $f(v) = w$ e $f(v_i) = w_i$ per ogni $i = 2, 3, \dots, n$. Per il lemma 38.3 l’applicazione f è un isomorfismo di spazi vettoriali. \square

38.3. Siano A un dominio d’integrità, K un campo, e si supponga che K sia un sottoanello di A , di modo che A è spazio vettoriale su K (esempio 34.4). Si dimostri che se la dimensione del K -spazio vettoriale A è finita, allora A è un campo.

Soluzione. Supponiamo che A e K soddisfino alle ipotesi. Per dimostrare che A è un campo dobbiamo far vedere che ogni elemento non nullo di A è invertibile in A . Sia $a \in A$, $a \neq 0$; si consideri l’applicazione $\tau_a: A \rightarrow A$ definita da $\tau_a(x) = ax$ per ogni $x \in A$. È facile verificare che τ_a è un endomorfismo del K -spazio vettoriale A . Mostriamo che τ_a è iniettivo: se $x \in \ker \tau_a$, allora $\tau_a(x) = 0$, cioè $ax = 0$. Dato che A è un dominio di integrità ed $a \neq 0$, ne segue che $x = 0$. Abbiamo così dimostrato che $\ker \tau_a = \{0\}$, cioè che $\tau_a: A \rightarrow A$ è iniettivo. Ma A ha dimensione finita, e quindi $\tau_a: A \rightarrow A$ è un automorfismo per il corollario 38.7. In particolare esiste $b \in A$ tale che $\tau_a(b) = 1_A$, ove 1_A denota l’identità di A . Questo vuol dire che $ab = 1_A$, ed essendo A commutativo, si ha anche che $ba = 1_A$. Quindi a è invertibile e $b \in A$ è il suo inverso. \square

Altri esercizi

38.4. Siano K un campo, a un elemento di K , n un numero intero positivo e $K[x]_{\leq n}$ lo spazio vettoriale dei polinomi di grado $\leq n$ a coefficienti in K . Si consideri l’applicazione $\varphi_a: K[x]_{\leq n} \rightarrow K$ definita da $\varphi_a(f(x)) = f(a)$ per ogni $f(x) \in K[x]_{\leq n}$.

- Si dimostri che l’applicazione φ è lineare.
- Si determini l’immagine di φ .
- Si determini la dimensione del nucleo di φ .
- Si determini il nucleo di φ .
- Si determini una base del nucleo di φ .

38.5. Siano $\{e_1, e_2, e_3\}$ la base canonica di \mathbb{C}^3 ed $f: \mathbb{C}^3 \rightarrow \mathbb{C}^2$ l’unica applicazione \mathbb{C} -lineare tale che $f(e_1) = (5, 0)$, $f(e_2) = (5, 3)$, $f(e_3) = (0, 3)$. Si dimostri che f è suriettiva.

38.6. Sia $\{e_1, e_2, e_3\}$ la base canonica di \mathbb{R}^3 , e sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}[x]$ l’applicazione lineare tale che

$$f(e_1) = 1 + x, \quad f(e_2) = 1 + x^2, \quad f(e_3) = 1 - x + x^3.$$

Si determini $f(1, -1, 3)$.

38.7. Si dimostri che $\{(0, 0, 1), (0, 1, 2), (1, -1, 1)\}$ è una base di \mathbb{R}^3 . Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}[x]$ l’applicazione lineare tale che $f(0, 0, 1) = 1 + x$, $f(0, 1, 2) = 1 + x^2$, $f(1, -1, 1) = 1 - x + x^3$. Si determini $f(1, -1, 3)$.

38.8. Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}[x]$ un'applicazione lineare tale che $f(0,0,1) = 1+x$, $f(0,1,2) = 1+x^2$. Si determini $f(0,2,2)$.

38.9. Siano $M_2(\mathbb{R})$ lo spazio vettoriale reale delle matrici quadrate di ordine 2 ad elementi in \mathbb{R} ed $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ la base canonica di $M_2(\mathbb{R})$ (vedi esempio 36.13). Sia $f: M_2(\mathbb{R}) \rightarrow M_2(\mathbb{R})$ l'applicazione lineare tale che $f(E_{11}) = E_{12}$, $f(E_{12}) = E_{21}$, $f(E_{21}) = E_{11} - E_{22}$, $f(E_{22}) = \begin{pmatrix} 1 & -1 \\ 2 & -2 \end{pmatrix}$. Si calcoli $\dim \ker f$. L'applicazione f è iniettiva?

38.10. Siano V, W spazi vettoriali sullo stesso campo K , $\{v_1, v_2, \dots, v_n\}$ una base di V , ed $f: V \rightarrow W$ un'applicazione lineare. Si dimostri che f è iniettiva se e solo se i vettori $f(v_1), f(v_2), \dots, f(v_n)$ di W sono linearmente indipendenti.

38.11. Siano V, W spazi vettoriali sullo stesso campo K , $\{v_1, v_2, \dots, v_n\}$ una base di V , ed $f: V \rightarrow W$ un'applicazione lineare. Si dimostri che f è suriettiva se e solo se l'insieme $\{f(v_1), f(v_2), \dots, f(v_n)\}$ genera W . [Suggerimento: esercizio 35.6.]

38.12. Siano V uno spazio vettoriale di dimensione n su un campo K , f una permutazione di $\{1, 2, \dots, n\}$ e $\{v_1, v_2, \dots, v_n\}$ una base di V . Si dimostri che esiste un unico automorfismo φ di V tale che $\varphi(v_i) = v_{f(i)}$ per ogni $i = 1, 2, \dots, n$.

38.13. Siano $m \leq n$ due interi non negativi. Si calcoli

$$\dim \left(\frac{K[x]_{\leq n}}{K[x]_{\leq m}} \right).$$

38.14. Sia W il sottospazio dello spazio vettoriale \mathbb{R}^4 sul campo \mathbb{R} definito da

$$W = \{(a, b, c, d) \mid a, b, c, d \in \mathbb{R}, a + b = 0, a - b + c = 0\}.$$

- (a) Si determini una base di W .
- (b) Si determini una base di \mathbb{R}^4 / W .

38.15. Siano V uno spazio vettoriale di dimensione finita su un campo K e v un vettore non nullo di V .

- (a) Si dimostri che esiste un'applicazione K -lineare $f: V \rightarrow K$ tale che $f(v) \neq 0$. [Suggerimento: si faccia uso del teorema di completamento delle basi.]
- (b) Si dimostri che se U è un sottospazio di V e $v \notin U$, allora esiste un'applicazione lineare $f: V \rightarrow K$ tale che $f(v) \neq 0$ e $f(u) = 0$ per ogni $u \in U$.
- (c) Nel caso particolare in cui $V = K^3$ e $v = (0, 1, 1)$, si dia un esempio di un'applicazione lineare $f: V \rightarrow K$ tale che $f(v) \neq 0$.

38.16. Sia $\{w_1, w_2, \dots, w_n\}$ una base di uno spazio vettoriale W su un campo K . Si definisca un isomorfismo $g: W \rightarrow K^n$.

§39. Matrice associata a un'applicazione lineare

Siano V, W spazi vettoriali di dimensione finita su uno stesso campo K e sia $f: V \rightarrow W$ un'applicazione lineare. Siano $\{v_1, v_2, \dots, v_n\}$ una base di V e $\{w_1, w_2, \dots, w_m\}$ una base

di W . Per ogni $j = 1, 2, \dots, n$ l'elemento $f(v_j)$ appartiene a W , e quindi è combinazione lineare degli elementi della base $\{w_1, w_2, \dots, w_m\}$ di W , ossia esistono degli $a_{ij} \in K$, univocamente determinati, tali che

$$f(v_j) = \sum_{i=1}^m a_{ij} w_i.$$

La matrice

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

si dice la *matrice associata all'applicazione lineare* $f: V \rightarrow W$ rispetto alle basi $\{v_1, v_2, \dots, v_n\}$ di V e $\{w_1, w_2, \dots, w_m\}$ di W . Nel caso degli endomorfismi $f: V \rightarrow V$ supporremo in generale che $v_i = w_i$ per ogni $i = 1, 2, \dots, n = m$ (a meno che non sia detto esplicitamente il contrario).

Si noti che nella matrice A la prima colonna è costituita dai coefficienti dell'espressione di $f(v_1)$ come combinazione lineare di w_1, w_2, \dots, w_m , la seconda colonna è costituita dai coefficienti dell'espressione di $f(v_2)$ come combinazione lineare di w_1, w_2, \dots, w_m , e così via. La matrice A è una matrice $m \times n$ (qui m è la dimensione del codominio W di f , ed n è la dimensione del dominio V).

Se $v = \sum_{j=1}^n \alpha_j v_j$ è un generico elemento di V , allora si ha che

$$\begin{aligned} f(v) &= f\left(\sum_{j=1}^n \alpha_j v_j\right) = \sum_{j=1}^n \alpha_j f(v_j) = \sum_{j=1}^n \alpha_j \sum_{i=1}^m a_{ij} w_i \\ &= \sum_{i=1}^m \sum_{j=1}^n \alpha_j a_{ij} w_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \alpha_j \right) w_i. \end{aligned}$$

Osserviamo che se C_v è la matrice colonna

$$C_v = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

allora $\sum_{j=1}^n a_{ij} \alpha_j$ è l'elemento di posto $(i, 1)$ nella matrice AC_v . Quindi se $C_v = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ è

la matrice colonna i cui elementi sono i coefficienti dell'espressione di v come combinazione lineare di v_1, v_2, \dots, v_n , allora la matrice colonna AC_v ha come elementi i coefficienti dell'e-

spressione di $f(v)$ come combinazione lineare di w_1, w_2, \dots, w_m . In altre parole, f manda

il vettore i cui coefficienti sono $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ nel vettore i cui coefficienti sono $A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$.

39.1 ESEMPIO. Sia $\mathbb{R}[x]_{\leq 2}$ lo spazio vettoriale dei polinomi di grado ≤ 2 a coefficienti reali. Fissiamo come base di $\mathbb{R}[x]_{\leq 2}$ la base canonica $\{1, x, x^2\}$. Sia $f: \mathbb{R}[x]_{\leq 2} \rightarrow \mathbb{R}[x]_{\leq 2}$ l'applicazione definita da $f(a + bx + cx^2) = a + (a+b)x + (b+c)x^2$ per ogni $a + bx + cx^2 \in \mathbb{R}[x]_{\leq 2}$. È facile dimostrare che l'applicazione f è lineare. Scriviamone la matrice associata. Si ha

$$\begin{aligned} f(1) &= 1 + x \\ f(x) &= x + x^2 \\ f(x^2) &= x^2. \end{aligned}$$

I coefficienti di $f(1)$ sono quindi 1, 1, 0, i coefficienti di $f(x)$ sono 0, 1, 1, e i coefficienti di $f(x^2)$ sono 0, 0, 1. Pertanto la matrice associata ad f è la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}. \quad \square$$

39.2 ESEMPIO. Se $\iota_V: V \rightarrow V$ è l'applicazione identica di V e $\{v_1, v_2, \dots, v_n\}$ è una base di V , si ha

$$\begin{aligned} \iota_V(v_1) &= v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n \\ \iota_V(v_2) &= v_2 = 0 \cdot v_1 + 1 \cdot v_2 + \cdots + 0 \cdot v_n \\ &\vdots \\ \iota_V(v_n) &= v_n = 0 \cdot v_1 + 0 \cdot v_2 + \cdots + 1 \cdot v_n. \end{aligned}$$

Quindi la matrice associata all'applicazione identica $\iota_V: V \rightarrow V$ è la matrice identica di ordine n . \square

Si osservi che quando si scrive la matrice A associata ad un'applicazione lineare $f: V \rightarrow W$ è sempre importante che sia ben chiaro rispetto a quali basi $\{v_1, v_2, \dots, v_n\}$ di V e $\{w_1, w_2, \dots, w_m\}$ di W si calcola la matrice. Non solo, anche l'ordine in cui si scrivono gli elementi delle due basi è importante, in quanto cambiandolo cambia la matrice A , come verrà mostrato nell'esempio che segue. In tale esempio considereremo come applicazione lineare $f: V \rightarrow W$ l'applicazione identica $\iota_V: V \rightarrow V$. Nell'esercizio precedente abbiamo fatto vedere che se si fissa la stessa base $\{v_1, v_2, \dots, v_n\}$ sia sul dominio di ι_V che sul codominio, allora la matrice associata a ι_V è la matrice identica. Vediamo cosa succede invece prendendo basi differenti di V sul dominio e sul codominio di ι_V .

39.3 ESEMPIO. Sia V uno spazio vettoriale di dimensione 3 sul campo \mathbb{R} dei numeri reali. Sia $\{v_1, v_2, v_3\}$ una sua base. Dimostriamo che:

(a) anche $\{v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3\}$ è una base di V .

Sia $W = V$ e $\iota_V : V \rightarrow W$ l'applicazione identica. Si determini la matrice associata all'applicazione lineare $\iota_V : V \rightarrow W$

(b) rispetto alle basi $\{v_1, v_2, v_3\}$ di V e $\{v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3\}$ di W ;

(c) rispetto alle basi $\{v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3\}$ di V e $\{v_1, v_2, v_3\}$ di W ;

(d) rispetto alle basi $\{v_1, v_2, v_3\}$ di V e $\{v_2, v_1, v_3\}$ di W . \square

Dimostrazione. (a) Mostriamo che i vettori $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$ sono linearmente indipendenti. Siano $\alpha, \beta, \gamma \in \mathbb{R}$ e supponiamo che $\alpha(v_1 + v_2) + \beta(v_1 + v_2 + v_3) + \gamma(v_1 + 2v_2 + v_3) = 0$. Allora $(\alpha + \beta + \gamma)v_1 + (\alpha + \beta + 2\gamma)v_2 + (\beta + \gamma)v_3 = 0$. Dato che v_1, v_2, v_3 sono linearmente indipendenti, deve essere quindi

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha + \beta + 2\gamma = 0 \\ \beta + \gamma = 0. \end{cases}$$

Risolviamo questo sistema. Dall'ultima equazione si ricava che $\beta = -\gamma$, e sostituendo questa espressione di β nelle prime due equazioni si trova che

$$\begin{cases} \alpha = 0 \\ \alpha + \gamma = 0. \end{cases}$$

Da $\alpha = 0$ segue che $\gamma = 0$, e quindi anche che $\beta = 0$. Questo dimostra che $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$ sono linearmente indipendenti.

I tre vettori linearmente indipendenti $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$ sono contenuti in una base B di V per il teorema del completamento delle basi 36.19. Ma V ha dimensione 3, quindi B ha tre elementi, e pertanto $B = \{v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3\}$. Questo dimostra (a).

(b) Si ha $\iota_V(v_1) = v_1$. Scriviamo v_1 come combinazione lineare di $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$. Si devono determinare $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $v_1 = \alpha(v_1 + v_2) + \beta(v_1 + v_2 + v_3) + \gamma(v_1 + 2v_2 + v_3)$. Questa uguaglianza equivale a $\alpha(v_1 + v_2) + \beta(v_1 + v_2 + v_3) + \gamma(v_1 + 2v_2 + v_3) - v_1 = 0$, che equivale a sua volta a $(\alpha + \beta + \gamma - 1)v_1 + (\alpha + \beta + 2\gamma)v_2 + (\beta + \gamma)v_3 = 0$. Dato che v_1, v_2, v_3 sono linearmente indipendenti, questo accade se e solo se α, β, γ soddisfano il sistema

$$\begin{cases} \alpha + \beta + \gamma - 1 = 0 \\ \alpha + \beta + 2\gamma = 0 \\ \beta + \gamma = 0. \end{cases}$$

Risolvendo il sistema si trova $\alpha = 1, \beta = 1, \gamma = -1$. Quindi $v_1 = (v_1 + v_2) + (v_1 + v_2 + v_3) - (v_1 + 2v_2 + v_3)$, e pertanto i coefficienti di $\iota_V(v_1) = v_1$ rispetto alla base

$\{v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3\}$ sono $1, 1, -1$. Quindi nella prima colonna della matrice cercata si avranno $1, 1, -1$.

Similmente per la seconda colonna. Si ha $\iota_V(v_2) = v_2$. Scriviamo v_2 come combinazione lineare di $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$. Si devono determinare $\alpha, \beta, \gamma \in \mathbb{R}$ tali che $v_2 = \alpha(v_1 + v_2) + \beta(v_1 + v_2 + v_3) + \gamma(v_1 + 2v_2 + v_3)$. Si vede facilmente che questa uguaglianza equivale al sistema

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha + \beta + 2\gamma - 1 = 0 \\ \beta + \gamma = 0. \end{cases}$$

Risolvendo il sistema si trova $\alpha = 0, \beta = -1, \gamma = 1$. Quindi $\iota_V(v_2) = v_2 = -(v_1 + v_2 + v_3) + (v_1 + 2v_2 + v_3)$. Quindi nella seconda colonna della matrice cercata si avrà $0, -1, 1$.

Per la terza colonna: Si scriva v_3 come combinazione lineare di $v_1 + v_2, v_1 + v_2 + v_3, v_1 + 2v_2 + v_3$. Si trova che $\iota_V(v_3) = v_3 = -(v_1 + v_2) + (v_1 + v_2 + v_3)$, e quindi nella terza colonna della matrice si deve avere $-1, 1, 0$. La matrice cercata è quindi

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

(c) Vediamo cosa si deve scrivere nella prima colonna della matrice 3×3 cercata. Il primo vettore della base del dominio è $v_1 + v_2$. Si ha $\iota_V(v_1 + v_2) = v_1 + v_2 = 1 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3$. Quindi nella prima colonna si devono scrivere $1, 1, 0$. Procedendo in modo analogo per le altre due colonne si trova che la matrice cercata è la

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

(d) Si ha $\iota_V(v_1) = v_1 = 0 \cdot v_2 + 1 \cdot v_1 + 0 \cdot v_3$. Quindi nella prima colonna si devono scrivere $0, 1, 0$. E così via. La matrice cercata è

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad \square$$

39.4 ESEMPIO. Mostriamo che *ogni matrice $m \times n$ a elementi in un campo K è la matrice di un'opportuna applicazione lineare di uno spazio vettoriale di dimensione n su K in uno di dimensione m* . (Per un'altra dimostrazione, lievemente differente da questa, si veda la dimostrazione della suriettività nella proposizione 39.8.) Sia

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

una matrice $m \times n$ ad elementi in K . Come nell'esempio 35.5 si scrivano gli elementi di K^n e di K^m come matrici colonne e si consideri l'applicazione lineare $f_A: K^n \rightarrow K^m$ definita da $f_A(X) = AX$ per ogni $X \in K^n$. Facciamo vedere che la matrice associata ad f_A rispetto alle basi canoniche di K^n e di K^m è proprio la matrice A .

Siano $\{e_1, \dots, e_n\}$ ed $\{e'_1, \dots, e'_m\}$ le basi canoniche di K^n e di K^m rispettivamente. Allora

$$\begin{aligned} f_A(e_1) = Ae_1 &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} \\ &= a_{11}e'_1 + a_{21}e'_2 + \dots + a_{m1}e'_m \end{aligned}$$

ha come coefficienti $a_{11}, a_{21}, \dots, a_{m1}$. Quindi la matrice associata ad f_A ha nella prima colonna $a_{11}, a_{21}, \dots, a_{m1}$, proprio come A . E così via per tutte le altre colonne. Ad esempio per l'ultima si ha che

$$\begin{aligned} f_A(e_n) = Ae_n &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} \\ &= a_{1n}e'_1 + a_{2n}e'_2 + \dots + a_{mn}e'_m \end{aligned}$$

ha come coefficienti $a_{1n}, a_{2n}, \dots, a_{mn}$, e quindi la matrice associata ad f_A ha nell'ultima colonna $a_{1n}, a_{2n}, \dots, a_{mn}$, come A . Pertanto la matrice associata ad f_A è uguale ad A . \square

39.5 PROPOSIZIONE. Siano V, W, U spazi vettoriali di dimensione finita sullo stesso campo K e siano $f: V \rightarrow W$ e $g: W \rightarrow U$ due applicazioni lineari. Siano $\{v_1, v_2, \dots, v_n\}$ una base di V , $\{w_1, w_2, \dots, w_m\}$ una base di W , e $\{u_1, u_2, \dots, u_p\}$ una base di U . Se A, B sono le matrici associate alle applicazioni lineari f, g rispetto alle basi date, allora BA è la matrice associata all'applicazione gf .

Dimostrazione. Per definizione A e B sono matrici $m \times n$ e $p \times m$ rispettivamente, e si ha $A = (a_{jk})_{j,k}$ e $B = (b_{ij})_{i,j}$, dove $f(v_k) = \sum_{j=1}^m a_{jk}w_j$ e $g(w_j) = \sum_{i=1}^p b_{ij}u_i$ per ogni j, k . Mostriamo che la matrice associata all'applicazione lineare composta gf è la matrice prodotto righe per colonne BA . La matrice BA ha nel posto (i, k) l'elemento $\sum_{j=1}^m b_{ij}a_{jk}$ per ogni i e ogni k . Quindi è sufficiente verificare che $gf(v_k) = \sum_{i=1}^p (\sum_{j=1}^m b_{ij}a_{jk})u_i$. Un facile calcolo mostra che

$$\begin{aligned} gf(v_k) &= g\left(\sum_{j=1}^m a_{jk}w_j\right) = \sum_{j=1}^m a_{jk}g(w_j) = \sum_{j=1}^m a_{jk} \sum_{i=1}^p b_{ij}u_i \\ &= \sum_{i=1}^p \left(\sum_{j=1}^m a_{jk}b_{ij} \right) u_i = \sum_{i=1}^p \left(\sum_{j=1}^m b_{ij}a_{jk} \right) u_i. \quad \square \end{aligned}$$

Denotiamo con $M_n(K)$ l'anello delle matrici $n \times n$ ad elementi in un campo K . Una matrice $n \times n A$ ad elementi in K si dice una *matrice invertibile* se è un elemento invertibile dell'anello $M_n(K)$, ossia se esiste $B \in M_n(K)$ tale che $AB = I$ e $BA = I$, ove con I abbiamo indicato la matrice identica di ordine n . Se A è invertibile, la matrice B tale che $AB = BA = I$ è unica, si denota con A^{-1} e si chiama la *matrice inversa* di A .

Supponiamo ora che V, W siano spazi vettoriali di dimensione finita e che $f: V \rightarrow W$ sia un isomorfismo di spazi vettoriali. Siano poi $\{v_1, v_2, \dots, v_n\}$ una base di V , $\{w_1, w_2, \dots, w_n\}$ una base di W , e $f^{-1}: W \rightarrow V$ l'inverso di f . Se A, B sono le matrici associate a f, f^{-1} rispettivamente, allora $ff^{-1} = \iota_W$ e $f^{-1}f = \iota_V$, e pertanto $AB = I$ e $BA = I$, dove con I abbiamo denotato la matrice identica $n \times n$. Quindi A è una matrice invertibile e $B = A^{-1}$. Abbiamo così dimostrato il seguente corollario:

39.6 COROLLARIO. *Se A è la matrice associata ad un isomorfismo f , allora la matrice A è invertibile e la sua matrice inversa A^{-1} è la matrice associata ad f^{-1} .*

Nell'anello $M_n(K)$ un elemento, cioè una matrice $n \times n$, è invertibile a sinistra se e solo se è invertibile a destra, come dimostrato nel seguente corollario.

39.7 COROLLARIO. *Siano $A, B \in M_n(K)$. Allora $AB = I$ se e solo se $BA = I$.*

Dimostrazione. Per simmetria basta dimostrare che se $AB = I$, allora $BA = I$. Siano A, B due matrici $n \times n$ tali che $AB = I$. Allora $f_A, f_B: K^n \rightarrow K^n$ sono due applicazioni lineari tali che $f_A \circ f_B = \iota_{K^n}$ (esempio 39.4). Per la proposizione 3.2 l'applicazione lineare f_A è suriettiva. Per il corollario 38.7 l'applicazione f_A è un automorfismo di K^n . Ma allora A è invertibile in $M_n(K)$ (corollario 39.6), e quindi il suo inverso a destra B è anche un inverso a sinistra, cioè $BA = I$. \square

Siano ora V, W due spazi vettoriali arbitrari (eventualmente di dimensione infinita) sullo stesso campo K . Denotiamo con $\text{Hom}_K(V, W)$ l'insieme di tutte le applicazioni lineari di V in W . Sull'insieme $\text{Hom}_K(V, W)$ definiamo

$$(f + g)(v) = f(v) + g(v) \quad \text{e} \quad (\alpha f)(v) = \alpha(f(v))$$

per ogni $f, g \in \text{Hom}_K(V, W)$, $\alpha \in K$, $v \in V$. Rispetto a queste operazioni si verifica che anche $\text{Hom}_K(V, W)$ risulta essere uno spazio vettoriale su K . Lo zero di questo spazio vettoriale è l'applicazione lineare nulla $V \rightarrow W$ che associa ad ogni vettore $v \in V$ lo zero 0_W di W . Se $f \in \text{Hom}_K(V, W)$, il suo opposto nello spazio vettoriale $\text{Hom}_K(V, W)$ è l'applicazione lineare $-f: V \rightarrow W$ definita da $(-f)(v) = -(f(v))$ per ogni $v \in V$.

Nel caso in cui V e W sono spazi vettoriali entrambi di dimensione finita sullo stesso campo K , fissiamo una base $\{v_1, v_2, \dots, v_n\}$ di V e una base $\{w_1, w_2, \dots, w_m\}$ di W . Per ogni applicazione lineare $f \in \text{Hom}_K(V, W)$ denotiamo con A_f la matrice associata ad $f: V \rightarrow W$ rispetto alle basi $\{v_1, v_2, \dots, v_n\}$ di V e $\{w_1, w_2, \dots, w_m\}$ di W .

39.8 PROPOSIZIONE. *L'applicazione $\mu: \text{Hom}_K(V, W) \rightarrow M_{m \times n}(K)$ che ad ogni applica-*

zione lineare $f \in \text{Hom}_K(V, W)$ fa corrispondere la matrice A_f associata ad f è un isomorfismo di spazi vettoriali.

Dimostrazione. Per dimostrare che l'applicazione μ è lineare si deve far vedere che $A_{f+g} = A_f + A_g$ e $A_{\alpha f} = \alpha A_f$ per ogni $f, g \in \text{Hom}_K(V, W)$ e ogni $\alpha \in K$. Mostriamo la prima. Fissiamo $f, g \in \text{Hom}_K(V, W)$. Per provare che $A_{f+g} = A_f + A_g$ basta far vedere che le matrici A_{f+g} e $A_f + A_g$ hanno lo stesso elemento di posto (i, j) per ogni $i = 1, 2, \dots, m$ e ogni $j = 1, 2, \dots, n$. Ora gli elementi a_{ij} della matrice A_f sono caratterizzati dalla condizione $f(v_j) = \sum_{i=1}^m a_{ij} w_i$. Analogamente gli elementi b_{ij} della matrice A_g sono caratterizzati dalla condizione $g(v_j) = \sum_{i=1}^m b_{ij} w_i$, e gli elementi c_{ij} della matrice A_{f+g} sono caratterizzati da $(f+g)(v_j) = \sum_{i=1}^m c_{ij} w_i$. Quindi $\sum_{i=1}^m c_{ij} w_i = (f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i = \sum_{i=1}^m (a_{ij} + b_{ij}) w_i$. Dalla indipendenza lineare dei w_j segue che $c_{ij} = a_{ij} + b_{ij}$ per ogni i e ogni j . Quindi $A_{f+g} = A_f + A_g$. Analogamente si vede che $A_{\alpha f} = \alpha A_f$.

Mostriamo che μ è iniettiva. Sia $f \in \ker \mu$. Allora $A_f = 0$, ossia la matrice A_f ha tutti gli elementi nulli. Per come è definita la matrice $A_f = (a_{ij})$ associata ad f , questo vuol dire che $f(v_j) = \sum_{i=1}^m a_{ij} w_i = 0$ per ogni j . Se v è un vettore di V , esistono $a_1, a_2, \dots, a_n \in K$ tali che $v = \sum_{j=1}^n a_j v_j$, e quindi $f(v) = f(\sum_{j=1}^n a_j v_j) = \sum_{j=1}^n a_j f(v_j) = 0$. Questo dimostra che f è l'applicazione nulla $V \rightarrow W$, e pertanto μ è iniettiva.

Mostriamo che μ è suriettiva. Sia $A \in M_{m \times n}(K)$, $A = (a_{ij})$. Applichiamo il teorema 38.1 alla base $\{v_1, v_2, \dots, v_n\}$ di V e alla n -upla

$$\left(\sum_{i=1}^m a_{i1} w_i, \sum_{i=1}^m a_{i2} w_i, \dots, \sum_{i=1}^m a_{in} w_i \right)$$

di elementi di W . Esiste allora un'unica applicazione lineare $f: V \rightarrow W$ tale che $f(v_j) = \sum_{i=1}^m a_{ij} w_i$ per ogni $j = 1, 2, \dots, n$. Questo vuol dire che la matrice A_f associata ad f è proprio la matrice $A = (a_{ij})$, cioè che $\mu(f) = A$. \square

In particolare, l'applicazione $\mu: \text{Hom}_K(K^n, K^m) \rightarrow M_{m \times n}(K)$ che ad ogni applicazione lineare $f: K^n \rightarrow K^m$ fa corrispondere la matrice A_f associata ad f rispetto alle basi canoniche di K^n e K^m è un isomorfismo. L'isomorfismo inverso $\mu^{-1}: M_{m \times n}(K) \rightarrow \text{Hom}_K(K^n, K^m)$ associa ad ogni matrice $A \in M_{m \times n}(K)$ l'applicazione f_A dell'esempio 39.4. Quindi tutte le applicazioni lineari di K^n in K^m sono del tipo f_A per qualche $A \in M_{m \times n}(K)$.

Dato che $\dim(M_{m \times n}(K)) = mn$ si ha che

39.9 COROLLARIO. *Se V e W hanno dimensione finita, allora*

$$\dim(\text{Hom}_K(V, W)) = \dim(V) \cdot \dim(W).$$

Se V è uno spazio vettoriale su K , lo spazio vettoriale $\text{Hom}_K(V, K)$ si dice lo spazio vettoriale *duale* di V . Per il corollario 39.9 se V ha dimensione finita n anche il suo duale $\text{Hom}_K(V, K)$ ha dimensione n .

Se A è una matrice $m \times n$ ad elementi in un campo K , denotiamo con A_1, \dots, A_n le colonne di A , di modo che $A = (A_1 \dots A_n)$. Le colonne A_1, \dots, A_n di A possono essere viste come matrici colonna $m \times 1$. Se scriviamo, come abbiamo già fatto, gli elementi dello spazio vettoriale K^m come matrici colonna, ecco che le colonne A_1, A_2, \dots, A_n di A sono n elementi di K^m , e quindi generano un sottospazio $\langle A_1, A_2, \dots, A_n \rangle$ di K^m . Chiamiamo *rango* (o *caratteristica*) di A la dimensione $\dim(\langle A_1, A_2, \dots, A_n \rangle)$ di questo sottospazio.

In generale, se V è un qualunque spazio vettoriale e v_1, \dots, v_n sono vettori di V , possiamo costruire il sottospazio vettoriale $W = \langle v_1, \dots, v_n \rangle$ di V generato da $\{v_1, \dots, v_n\}$. L'insieme di generatori $\{v_1, \dots, v_n\}$ di W deve contenere un insieme minimale di generatori di W , cioè (proposizione 36.15) una base B di W . La dimensione di W , cioè la cardinalità della base B di $W = \langle v_1, \dots, v_n \rangle$, è quindi il massimo numero di vettori tra v_1, \dots, v_n che sono linearmente indipendenti. Applicando questa osservazione allo spazio vettoriale K^m e alle colonne A_1, \dots, A_n di una matrice $m \times n$ A , si vede quindi che *il rango di A è il massimo numero di colonne di A linearmente indipendenti*.

Per il calcolo del rango di una matrice A si procede quindi come segue. Si verifica se le colonne di A sono linearmente indipendenti. Se sono linearmente indipendenti, il rango di A è uguale al numero di colonne di A . Se non sono linearmente indipendenti, una delle colonne è combinazione lineare dalle altre. Si cancella quella colonna. Le colonne rimanenti sono linearmente indipendenti? Se la risposta è sì, il loro numero è il rango della matrice A , altrimenti una delle colonne rimaste è combinazione lineare dalle altre. Si cancella anche quella colonna, ..., e così via. Alla fine del procedimento si resta con un insieme di colonne linearmente indipendenti, il cui numero è proprio il rango di A .

39.10 ESEMPIO.

Calcoliamo il rango della matrice ad elementi reali

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

Le tre colonne

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$

di A sono elementi di \mathbb{R}^2 , che ha dimensione 2, e quindi le tre colonne non possono essere certamente linearmente indipendenti. Cerchiamo tre numeri reali α, β, γ non tutti nulli tali che

$$(39.1) \quad . \quad \alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \gamma \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Si ha

$$\alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \gamma \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} \alpha \\ -\alpha \end{pmatrix} + \begin{pmatrix} 2\beta \\ 3\beta \end{pmatrix} + \begin{pmatrix} 3\gamma \\ -2\gamma \end{pmatrix} = \begin{pmatrix} \alpha + 2\beta + 3\gamma \\ -\alpha + 3\beta - 2\gamma \end{pmatrix},$$

e quindi l'uguaglianza (39.1) equivale al sistema

$$\begin{cases} \alpha + 2\beta + 3\gamma = 0 \\ -\alpha + 3\beta - 2\gamma = 0. \end{cases}$$

Dalla seconda equazione si ricava $\alpha = 3\beta - 2\gamma$, e questa sostituita nella prima dà $(3\beta - 2\gamma) + 2\beta + 3\gamma = 0$, da cui $\gamma = -5\beta$. Le soluzioni del sistema sono quindi le terne $(\alpha, \beta, \gamma) = (13\beta, \beta, -5\beta)$ al variare di β in \mathbb{R} . Una soluzione con α, β, γ non tutti nulli è quindi ad esempio $(\alpha, \beta, \gamma) = (13, 1, -5)$. Abbiamo così trovato che

$$13 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} - 5 \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Una delle colonne è quindi combinazione lineare delle altre, ad esempio

$$\begin{pmatrix} 2 \\ 3 \end{pmatrix} = -13 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + 5 \begin{pmatrix} 3 \\ -2 \end{pmatrix}.$$

Cancelliamo quindi la colonna

$$\begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

e vediamo se le colonne

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$

sono linearmente indipendenti. Siano $\alpha, \beta \in \mathbb{R}$ tali che

$$\alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \beta \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Allora

$$\begin{pmatrix} \alpha + 3\beta \\ -\alpha - 2\beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

da cui

$$\begin{cases} \alpha + 3\beta = 0 \\ -\alpha - 2\beta = 0. \end{cases}$$

Risolviamo questo sistema. Dalla seconda equazione si ricava $\alpha = -2\beta$, che sostituita nella prima dà $\beta = 0$. Se ne ricava che anche $\alpha = 0$. Questo dimostra che le colonne

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$

sono linearmente indipendenti. Quindi il rango di A è 2. \square

Ovviamente il rango r di una matrice A $m \times n$ è $\leq \min\{m, n\}$: si ha $r \leq m$ in quanto il rango r è la dimensione del sottospazio di K^m generato dalle colonne di A , e quindi la dimensione di questo sottospazio deve essere \leq alla dimensione di K^m , che è m ; si ha $r \leq n$ in quanto il rango r è la dimensione del sottospazio generato dalle n colonne di A , e quindi la dimensione di questo sottospazio può essere al più n .

Se $f: V \rightarrow W$ è un'applicazione lineare chiamiamo *rango* (o *caratteristica*) di f la dimensione $\dim(f(V))$ dell'immagine di f .

Mostriamo che queste due definizioni, quella di rango di un'applicazione lineare e quella di rango di una matrice, sono in accordo tra loro.

39.11 PROPOSIZIONE. *Siano V, W spazi vettoriali di dimensione finita su uno stesso campo K e sia $f: V \rightarrow W$ un'applicazione lineare. Fissate una base di V e una base di W , sia A la matrice associata ad f rispetto a queste basi. Allora il rango dell'applicazione lineare f è uguale al rango della matrice A .*

Dimostrazione. Supponiamo che $A = (a_{ij})$ sia la matrice associata ad f rispetto alla base $\{v_1, v_2, \dots, v_n\}$ di V e alla base $\{w_1, w_2, \dots, w_m\}$ di W , di modo che $f(v_j) = \sum_{i=1}^m a_{ij} w_i$ per ogni $j = 1, 2, \dots, n$. Scriviamo gli elementi di K^m come matrici colonne $m \times 1$ e consideriamo la base canonica $\{e_1, e_2, \dots, e_m\}$ di K^m , dove

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad e_m = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Per il teorema 38.1 esiste un'unica applicazione lineare $\Phi: K^m \rightarrow W$ tale che $\Phi(e_i) = w_i$ per ogni $i = 1, 2, \dots, m$, e questa Φ è un isomorfismo per il lemma 38.3. Se A_1, \dots, A_n sono le colonne di A , per ogni $j = 1, \dots, n$ si ha $A_j = \sum_{i=1}^m a_{ij} e_i$, e quindi $\Phi(A_j) = \Phi(\sum_{i=1}^m a_{ij} e_i) = \sum_{i=1}^m a_{ij} \Phi(e_i) = \sum_{i=1}^m a_{ij} w_i = f(v_j)$. Quindi $\Phi: K^m \rightarrow W$ induce un isomorfismo tra il sottospazio $\langle A_1, \dots, A_n \rangle$ di K^m generato da $\{A_1, \dots, A_n\}$ e il sottospazio $\langle f(v_1), \dots, f(v_n) \rangle$ di W generato da $\{f(v_1), \dots, f(v_n)\}$. In particolare

$$\dim(\langle A_1, \dots, A_n \rangle) = \dim(\langle f(v_1), \dots, f(v_n) \rangle).$$

Per dimostrare che il rango $\dim(\langle A_1, \dots, A_n \rangle)$ della matrice A è uguale al rango $\dim(f(V))$ dell'applicazione lineare f basta quindi dimostrare che $\langle f(v_1), \dots, f(v_n) \rangle = f(V)$, ossia che l'immagine $f(V)$ di f è generata da $\{f(v_1), \dots, f(v_n)\}$. Questo è stato già visto nell'esercizio 35.6. \square

39.12 PROPOSIZIONE. *Sia A una matrice quadrata di ordine n a coefficienti in un campo K . La matrice A è invertibile se e solo se A ha rango n .*

Dimostrazione. Siano $M_n(K)$ l'anello delle matrici quadrate di ordine n ad elementi in K e $A \in M_n(K)$. Sia $f_A: K^n \rightarrow K^n$ l'applicazione lineare definita da $f_A(X) = AX$ per ogni $X \in K^n$, di modo che A è la matrice associata ad f_A (esempio 39.4), e in particolare il rango di f_A è uguale al rango di A (proposizione 39.11).

Se A è invertibile in $M_n(K)$ e $A^{-1} \in M_n(K)$ è la sua inversa, allora l'applicazione lineare $f_A: K^n \rightarrow K^n$ è suriettiva, perché per ogni $Y \in K^n$ si ha $f_A(A^{-1}Y) = A(A^{-1}Y) = (AA^{-1})Y = Y$. Quindi il rango di A , che è uguale al rango di f_A , cioè alla dimensione di $f_A(K^n) = K^n$, è n .

Viceversa se A ha rango n , allora f_A ha rango n , cioè il sottospazio $f_A(K^n)$ di K^n ha dimensione n . Quindi f_A è suriettiva. Per il corollario 38.7 l'applicazione lineare $f_A: K^n \rightarrow K^n$ è un isomorfismo. Ma allora A , che è la matrice associata ad f_A , è invertibile per il corollario 39.6. \square

Esercizi svolti

39.1. Siano V, W due spazi vettoriali della stessa dimensione sullo stesso campo K , $f: V \rightarrow W$ un'applicazione lineare, e A la matrice associata a f rispetto a una base di V e a una base di W . Si dimostri che se A è invertibile, allora f è un isomorfismo. Questo dimostra l'inverso del corollario 39.6.

Soluzione. Supponiamo che la matrice A associata ad $f: V \rightarrow W$, rispetto ad una base di V e a una base di W , sia invertibile e sia A^{-1} la matrice inversa. Per la proposizione 39.8 c'è un'unica applicazione lineare $g: W \rightarrow V$ la cui matrice associata, sempre rispetto alle stesse basi di V e W , è A^{-1} . Per la proposizione 39.5 la matrice associata all'applicazione fg è $AA^{-1} = I$, e quindi fg è l'applicazione identica di W . Analogamente la matrice associata a gf è $A^{-1}A = I$, e quindi gf è l'applicazione identica di V . Pertanto f è una biiezione e $g = f^{-1}$. \square

39.2. Si dimostri che se U, V, W sono tre spazi vettoriali sullo stesso campo K , allora $\text{Hom}_K(U \oplus V, W) \cong \text{Hom}_K(U, W) \oplus \text{Hom}_K(V, W)$.

Soluzione. Siano $\varepsilon_U: U \rightarrow U \oplus V$ l'applicazione definita da $\varepsilon_U(u) = (u, 0)$ per ogni $u \in U$ e $\varepsilon_V: V \rightarrow U \oplus V$ l'applicazione definita da $\varepsilon_V(v) = (0, v)$ per ogni $v \in V$. Faremo vedere che l'applicazione $\Phi: \text{Hom}_K(U \oplus V, W) \rightarrow \text{Hom}_K(U, W) \oplus \text{Hom}_K(V, W)$ definita da $\Phi(f) = (f \circ \varepsilon_U, f \circ \varepsilon_V)$ per ogni $f \in \text{Hom}_K(U \oplus V, W)$ è un isomorfismo di spazi vettoriali su K .

Mostriamo che l'applicazione Φ è lineare. Si deve far vedere che $\Phi(f + g) = \Phi(f) + \Phi(g)$ e $\Phi(\lambda f) = \lambda \Phi(f)$ per ogni $f, g \in \text{Hom}_K(U \oplus V, W)$ e ogni $\lambda \in K$. Ora $\Phi(f + g) = \Phi(f) + \Phi(g)$ equivale a $((f + g) \circ \varepsilon_U, (f + g) \circ \varepsilon_V) = (f \circ \varepsilon_U, f \circ \varepsilon_V) + (g \circ \varepsilon_U, g \circ \varepsilon_V)$, che a sua volta equivale alle due uguaglianze $(f + g) \circ \varepsilon_U = (f \circ \varepsilon_U) + (g \circ \varepsilon_U)$ e $(f + g) \circ \varepsilon_V = (f \circ \varepsilon_V) + (g \circ \varepsilon_V)$. Per dimostrare che le due applicazioni $(f + g) \circ \varepsilon_U$ e $(f \circ \varepsilon_U) + (g \circ \varepsilon_U)$ di U in W sono uguali si deve far vedere che $((f + g) \circ \varepsilon_U)(u) = ((f \circ \varepsilon_U) + (g \circ \varepsilon_U))(u)$ per ogni $u \in U$. E questo è vero in quanto $((f + g) \circ \varepsilon_U)(u) = (f + g)(\varepsilon_U(u)) = (f + g)(u, 0) = f(u, 0) + g(u, 0) = f(\varepsilon_U(u)) + g(\varepsilon_U(u)) = ((f \circ \varepsilon_U) + (g \circ \varepsilon_U))(u)$. In modo del tutto simile si prova che $(f + g) \circ \varepsilon_V = (f \circ \varepsilon_V) + (g \circ \varepsilon_V)$. Questo dimostra che $\Phi(f + g) = \Phi(f) + \Phi(g)$. Analogamente si vede che $\Phi(\lambda f) = \lambda \Phi(f)$ per ogni $f \in \text{Hom}_K(U \oplus V, W)$ e ogni $\lambda \in K$.

Mostriamo che Φ è iniettiva. Sia f un elemento del nucleo di Φ , cioè un'applicazione $f \in \text{Hom}_K(U \oplus V, W)$ tale che $\Phi(f) = 0$. Allora $\Phi(f) = (f \circ \varepsilon_U, f \circ \varepsilon_V) = 0$ per ogni $u \in U$ e $v \in V$, ossia $f \circ \varepsilon_U = 0$ e $f \circ \varepsilon_V = 0$. Allora $f(u, 0) = 0$ per ogni $u \in U$ e $f(0, v) = 0$ per ogni $v \in V$. Ma allora per ogni $(u, v) \in U \oplus V$ si ha $f(u, v) = f(u, 0) + f(0, v) = 0$, vale a dire f è l'applicazione nulla, ossia lo zero di $\text{Hom}_K(U \oplus V, W)$. Si è così dimostrato che Φ è iniettiva.

Mostriamo che Φ è suriettiva. Fissiamo un elemento di $\text{Hom}_K(U, W) \oplus \text{Hom}_K(V, W)$, che dovrà quindi essere del tipo (h, ℓ) con $h \in \text{Hom}_K(U, W)$ ed $\ell \in \text{Hom}_K(V, W)$. Definiamo un'applicazione $f: U \oplus V \rightarrow W$ ponendo $f(u, v) = h(u) + \ell(v)$ per ogni $(u, v) \in U \oplus V$. Si osservi che f è lineare, in quanto $f((u, v) + (u', v')) = f(u + u', v + v') = h(u + u') + \ell(v + v') =$

$h(u) + h(u') + \ell(v) + \ell(v') = h(u) + \ell(v) + h(u') + \ell(v') = f(u, v) + f(u', v')$, e similmente $f(\lambda(u, v)) = \lambda f(u, v)$. Quindi $f \in \text{Hom}_K(U \oplus V, W)$. Mostriamo che $\Phi(f) = (h, \ell)$, cioè che $(f \circ \varepsilon_U, f \circ \varepsilon_V) = (h, \ell)$. Per ogni $u \in U$ si ha $(f \circ \varepsilon_U)(u) = f(u, 0) = h(u) + \ell(0) = h(u)$, e quindi $f \circ \varepsilon_U = h$. Analogamente $f \circ \varepsilon_V = \ell$. Pertanto $\Phi(f) = (f \circ \varepsilon_U, f \circ \varepsilon_V) = (h, \ell)$. Questo dimostra che Φ è suriettiva. \square

39.3. Si calcoli la matrice inversa della matrice

$$A = \begin{pmatrix} 0 & i & 1 \\ 0 & 1 & 1 \\ i & 0 & -i \end{pmatrix}$$

ad elementi nel campo \mathbb{C} .

Soluzione. Per il corollario 39.7 è sufficiente determinare gli elementi $\beta_{ij} \in \mathbb{C}$, $i, j = 1, 2, 3$, tali che $AB = I$, dove $B = (\beta_{ij})$ e I denota la matrice identica 3×3 . Ora l'uguaglianza $AB = I$ equivale a

$$\begin{pmatrix} 0 & i & 1 \\ 0 & 1 & 1 \\ i & 0 & -i \end{pmatrix} \begin{pmatrix} \beta_{11} & \beta_{12} & \beta_{13} \\ \beta_{21} & \beta_{22} & \beta_{23} \\ \beta_{31} & \beta_{32} & \beta_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ossia a

$$\begin{pmatrix} i\beta_{21} + \beta_{31} & i\beta_{22} + \beta_{32} & i\beta_{23} + \beta_{33} \\ \beta_{21} + \beta_{31} & \beta_{22} + \beta_{32} & \beta_{23} + \beta_{33} \\ i\beta_{11} - i\beta_{31} & i\beta_{12} - i\beta_{32} & i\beta_{13} - i\beta_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Quindi si ha $AB = I$ se e solo se le β_{ij} sono soluzioni del sistema di nove equazioni lineari nelle nove incognite β_{ij}

$$\left\{ \begin{array}{l} i\beta_{21} + \beta_{31} = 1 \\ i\beta_{22} + \beta_{32} = 0 \\ i\beta_{23} + \beta_{33} = 0 \\ \beta_{21} + \beta_{31} = 0 \\ \beta_{22} + \beta_{32} = 1 \\ \beta_{23} + \beta_{33} = 0 \\ i\beta_{11} - i\beta_{31} = 0 \\ i\beta_{12} - i\beta_{32} = 0 \\ i\beta_{13} - i\beta_{33} = 1. \end{array} \right.$$

*

Risolvendo questo sistema si trova che la sua soluzione è

$$\begin{aligned} \beta_{11} &= \frac{1}{2} + \frac{i}{2}, & \beta_{12} &= \frac{1}{2} - \frac{i}{2}, & \beta_{13} &= -i, \\ \beta_{21} &= -\frac{1}{2} - \frac{i}{2}, & \beta_{22} &= \frac{1}{2} + \frac{i}{2}, & \beta_{23} &= 0, \\ \beta_{31} &= \frac{1}{2} + \frac{i}{2}, & \beta_{32} &= \frac{1}{2} - \frac{i}{2}, & \beta_{33} &= 0. \end{aligned}$$

Quindi la matrice

$$B = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} & -i \\ -\frac{1}{2} - \frac{i}{2} & \frac{1}{2} + \frac{i}{2} & 0 \\ \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} & 0 \end{pmatrix}$$

è la matrice inversa cercata. \square

Altri esercizi

39.4. Si scrivano le matrici associate alle seguenti applicazioni lineari rispetto alle basi canoniche:

- La prima proiezione canonica $\pi_1: \mathbb{R}^2 \rightarrow \mathbb{R}$ definita da $\pi_1(\alpha, \beta) = \alpha$ per ogni $(\alpha, \beta) \in \mathbb{R}^2$.
- L'applicazione \mathbb{Q} -lineare $f: \mathbb{Q}^3 \rightarrow \mathbb{Q}^4$ definita da $f(\alpha, \beta, \gamma) = (5\alpha + 5\beta, 3\beta + 3\gamma, 5\gamma, 5\gamma)$ per ogni $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$.
- L'applicazione \mathbb{C} -lineare $f: \mathbb{C}^n \rightarrow \mathbb{C}^n$ definita da $f(v) = iv$ per ogni $v \in \mathbb{C}^n$.
- L'applicazione \mathbb{R} -lineare $f: \mathbb{C} \rightarrow \mathbb{C}$ definita da $f(z) = iz$ per ogni $z \in \mathbb{C}$. (Qual è la base canonica di \mathbb{C} come spazio vettoriale su \mathbb{R} ?)
- L'applicazione K -lineare $f: K^n \rightarrow K^n$ definita da $f(v) = -v$ per ogni $v \in K^n$. Qui K è un campo arbitrario.
- L'unica applicazione \mathbb{Z}_3 -lineare $f: \mathbb{Z}_3^3 \rightarrow \mathbb{Z}_3^3$ tale che $f(e_1) = e_1$, $f(e_2) = e_1 + e_2$, $f(e_3) = e_1 + \bar{2}e_2 + e_3$.

39.5. Siano $f: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^3$ e $g: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^2$ le applicazioni \mathbb{Z}_2 -lineari definite da $f(a, b) = (a+b, 0, a)$ e $g(a, b, c) = (a+b+c, a+b)$ rispettivamente per ogni $a, b, c \in \mathbb{Z}_2$.

- Senza eseguire alcuna moltiplicazione tra matrici, si calcolino le matrici A, B, C, D associate ad $f, g, f \circ g, g \circ f$ rispetto alle basi canoniche di \mathbb{Z}_2^2 e \mathbb{Z}_2^3 .
- Si verifichi che $C = AB$ e $D = BA$.

39.6. (a) Si dimostri che $B = \{(1, 0, 0), (1, 1, 0), (1, 1, -1)\}$ è una base di \mathbb{R}^3 .

- Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare definita da $f(a, b, c) = (a, 0, b+c)$ per ogni $a, b, c \in \mathbb{R}$. Si determini la matrice associata ad f rispetto alla base B .

39.7. Sia $\{e_1, e_2, e_3\}$ la base canonica di \mathbb{R}^3 .

- Sia $B = \{e_1, e_1 + e_2, 2e_1 - e_2 - e_3\}$. Si dimostri che B è una base di \mathbb{R}^3 .
- Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'unica applicazione lineare tale che

$$f(e_1) = e_1, \quad f(e_2) = e_1 + e_2, \quad f(e_3) = e_1 - 2e_2.$$

Si determini la matrice associata ad f rispetto alla base B .

39.8. Sia V uno spazio vettoriale su un campo K e sia $B = \{v_1, v_2, v_3\}$ una base di V . Siano a un elemento di K ed f l'endomorfismo di V la cui matrice associata rispetto alla base B è

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 1 \end{pmatrix}.$$

- Si determini una base del nucleo di f .

(b) Si determini una base dell'immagine di f .

39.9. Siano $v_1 = (1, -1, 0)$, $v_2 = (2, -1, 1)$, $v_3 = (0, 1, -2)$.

(a) Si dimostri che $\{v_1, v_2, v_3\}$ è una base di \mathbb{R}^3 .

(b) Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare la cui matrice associata rispetto alla base $\{v_1, v_2, v_3\}$ è

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

Si determini $f(v_1 - v_2 - v_3)$.

(c) Si determini $f^2(v_1 + v_2 + v_3)$.

39.10. Siano V uno spazio vettoriale di dimensione n , U e W due suoi sottospazi vettoriali di dimensione p e q rispettivamente, e si supponga che $V = U \oplus W$.

(a) Si dimostri che rispetto a una base opportuna di V la matrice dell'applicazione lineare $\varepsilon: V \rightarrow V$ definita da $\varepsilon(u + w) = u$ per ogni $u \in U$, $w \in W$, è

$$A = \begin{pmatrix} 1 & & & & & 0 \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & 0 & \\ & & & & & 0 \\ 0 & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

(qui si intende che ci siano p uno e q zero sulla diagonale e che tutti gli elementi fuori della diagonale siano zero.)

(b) Si dimostri che A è idempotente, ossia che $A^2 = A$.

39.11. Si dimostri che se U, V, W sono tre spazi vettoriali sullo stesso campo K , allora $\text{Hom}_K(U, V \oplus W) \cong \text{Hom}_K(U, V) \oplus \text{Hom}_K(U, W)$. [Suggerimento: Siano $\pi_V: V \oplus W \rightarrow V$ e $\pi_W: V \oplus W \rightarrow W$ le applicazioni lineari definite da $\pi_V(v, w) = v$ e $\pi_W(v, w) = w$ per ogni $(v, w) \in V \oplus W$. Si dimostri che l'applicazione $\Phi: \text{Hom}_K(U, V \oplus W) \rightarrow \text{Hom}_K(U, V) \oplus \text{Hom}_K(U, W)$ definita da $\Phi(f) = (\pi_V \circ f, \pi_W \circ f)$ per ogni $f \in \text{Hom}_K(U, V \oplus W)$ è un isomorfismo.]

39.12. Si calcoli la matrice inversa della matrice

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

a elementi reali.

39.13. Sia V uno spazio vettoriale di dimensione finita n su un campo K . È facile vedere che $\text{End}_K(V) = \text{Hom}_K(V, V)$ è un anello (qui la moltiplicazione è la composizione di applicazioni),

detto l'*anello degli endomorfismi di V*. Fissiamo una base $\{v_1, v_2, \dots, v_n\}$ di V . Per ogni applicazione lineare $f \in \text{End}_K(V)$ denotiamo con A_f la matrice associata ad $f: V \rightarrow V$ (rispetto alla base $\{v_1, v_2, \dots, v_n\}$). Sia $\mu: \text{End}_K(V) \rightarrow M_n(K)$ l'applicazione che ad ogni applicazione lineare $f \in \text{End}_K(V)$ fa corrispondere la matrice A_f . Si dimostri che μ è un isomorfismo di anelli.

39.14. Si calcoli il rango della matrice a elementi razionali

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 9 \\ 2 & -2 & 0 \end{pmatrix}.$$

39.15. Si calcoli il rango della matrice a elementi complessi

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

39.16. Si calcoli il rango della matrice

$$\begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \frac{1}{2} & \frac{4}{4} & \frac{1}{1} \\ \frac{3}{3} & \frac{1}{1} & \frac{4}{4} \end{pmatrix}$$

a elementi nel campo \mathbb{Z}_5 .

39.17. Si calcoli il rango della matrice

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{0} & \bar{0} \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

a elementi nel campo \mathbb{Z}_2 .

39.18. Sia A la matrice a elementi razionali

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

(a) Si determini il rango di A .

Sia $f: \mathbb{Q}^2 \rightarrow \mathbb{Q}^3$ l'applicazione definita da $f(a, b) = (a \ b)A$ per ogni $(a, b) \in \mathbb{Q}^2$.

(b) Si determini il rango di f .

(c) Si determini il nucleo $\ker f$ di f .

(d) Si determini una base di $\ker f$.

(e) Si determini una base dell'immagine di f .

39.19. Per ogni numero reale λ si determini la dimensione del sottospazio dello spazio vettoriale reale \mathbb{R}^3 generato dai vettori $(\lambda, \lambda, \lambda), (1, \lambda, \lambda), (\lambda, 2 - \lambda, \lambda)$.

39.20. Siano V, W due spazi vettoriali su uno stesso campo K , e siano $\{v_1, v_2, v_3\}, \{w_1, w_2, w_3\}$ basi di V, W rispettivamente. Siano $A = \langle v_1, v_2 \rangle, B = \langle w_1, w_2 \rangle$ i sottospazi vettoriali generati da $\{v_1, v_2\}, \{w_1, w_2\}$ rispettivamente.

- (a) Si dimostri che se $f: V \rightarrow W$ è un'applicazione lineare, si ha $f(A) \subseteq B$ se e solo se la matrice di f rispetto alle basi date di V e W è del tipo

$$\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{pmatrix}$$

per opportuni $a, b, c, d, e, f, g \in K$.

- (b) Si dimostri che $U = \{f \in \text{Hom}_K(V, W) \mid f(A) \subseteq B\}$ è un sottospazio dello spazio vettoriale $\text{Hom}_K(V, W)$.
(c) Si calcoli la dimensione dello spazio vettoriale U .

§40. Cambi di base

40.1 LEMMA. Siano $\{v_1, \dots, v_n\}$ e $\{v'_1, \dots, v'_n\}$ due basi di uno spazio vettoriale V su un campo K . Per ogni $i, j, h, k = 1, \dots, n$ siano $p_{hj}, \tilde{p}_{ik} \in K$ tali che $v'_j = \sum_{h=1}^n p_{hj} v_h$ e $v_k = \sum_{i=1}^n \tilde{p}_{ik} v'_i$, e siano P, \tilde{P} le matrici $P = (p_{hj})_{h,j}$ e $\tilde{P} = (\tilde{p}_{ik})_{i,k}$. Allora $P\tilde{P} = I$ e $\tilde{P}P = I$, cioè $\tilde{P} = P^{-1}$.

Si osservi che la matrice P ha come colonna j -esima i coefficienti di v'_j espresso come combinazione lineare di v_1, \dots, v_n , e la matrice \tilde{P} ha come colonna k -esima i coefficienti di v_k espresso come combinazione lineare di v'_1, \dots, v'_n .

Dimostrazione. Per ogni $k = 1, \dots, n$ si ha

$$v_k = \sum_{i=1}^n \tilde{p}_{ik} v'_i = \sum_{i=1}^n \tilde{p}_{ik} \sum_{h=1}^n p_{hi} v_h = \sum_{h=1}^n \left(\sum_{i=1}^n \tilde{p}_{ik} p_{hi} \right) v_h = \sum_{h=1}^n \left(\sum_{i=1}^n p_{hi} \tilde{p}_{ik} \right) v_h,$$

e quindi per l'unicità della scrittura di ogni elemento di V come combinazione lineare di elementi della base $\{v_1, \dots, v_n\}$ si ottiene che $\sum_{i=1}^n p_{hi} \tilde{p}_{ik} = \delta_{hk}$ per ogni $h, k = 1, 2, \dots, n$. Ne segue che $P\tilde{P} = I$. Analogamente $\tilde{P}P = I$. Quindi le matrici P e \tilde{P} sono una l'inversa dell'altra. \square

Siano ora $f: V \rightarrow W$ un'applicazione lineare e $B(V) = \{v_1, v_2, \dots, v_n\}$, $B(W) = \{w_1, w_2, \dots, w_m\}$ basi di V, W rispettivamente. Rispetto a queste basi, ad f è associata una matrice $m \times n A = (a_{ij})_{i,j}$. Fissiamo ora altre due basi $B'(V) = \{v'_1, v'_2, \dots, v'_n\}$, $B'(W) = \{w'_1, w'_2, \dots, w'_m\}$ di V e W . Rispetto a queste nuove basi ad f è associata un'altra matrice $m \times n A' = (a'_{ij})_{i,j}$. Cerchiamo la relazione tra A e A' . Siano $v'_j = \sum_{h=1}^n p_{hj} v_h$ e $w'_k = \sum_{\ell=1}^m q_{\ell k} w_{\ell}$ le formule del cambio di base. Poniamo $P = (p_{hj})_{h,j}$ e $Q = (q_{\ell k})_{\ell,k}$, di modo che se $Q^{-1} = (\tilde{q}_{ik})_{i,k}$ si ha $w_k = \sum_{i=1}^m \tilde{q}_{ik} w'_i$ per il lemma 40.1. Per come è definita A si ha $f(v_h) = \sum_{k=1}^m a_{kh} w_k$, e per come è definita A' si ha

$$f(v'_j) = \sum_{i=1}^m a'_{ij} w'_i.$$

D'altra parte

$$\begin{aligned} f(v'_j) &= f\left(\sum_{h=1}^n p_{hj} v_h\right) = \sum_{h=1}^n p_{hj} f(v_h) = \sum_{h=1}^n p_{hj} \sum_{k=1}^m a_{kh} w_k = \sum_{h=1}^n p_{hj} \sum_{k=1}^m a_{kh} \sum_{i=1}^m \tilde{q}_{ik} w'_i \\ &= \sum_{i=1}^m \left(\sum_{h=1}^n p_{hj} \sum_{k=1}^m a_{kh} \tilde{q}_{ik} \right) w'_i = \sum_{i=1}^m \left(\sum_{k=1}^m \sum_{h=1}^n \tilde{q}_{ik} a_{kh} p_{hj} \right) w'_i, \end{aligned}$$

e quindi dall'unicità della scrittura di ogni elemento di W come combinazione lineare di elementi della base $\{w'_1, \dots, w'_m\}$ ricaviamo che

$$a'_{ij} = \sum_{k=1}^m \sum_{h=1}^n \tilde{q}_{ik} a_{kh} p_{hj}$$

per ogni i e ogni j , ossia $A' = Q^{-1}AP$.

Abbiamo così dimostrato che:

40.2 PROPOSIZIONE. Sia V uno spazio vettoriale su un campo K , siano $B(V) = \{v_1, v_2, \dots, v_n\}$ e $B'(V) = \{v'_1, v'_2, \dots, v'_n\}$ due basi di V e sia P la matrice quadrata di ordine n la cui colonna j -esima è data dai coefficienti dell'espressione di v'_j come combinazione lineare di v_1, v_2, \dots, v_n per ogni $j = 1, 2, \dots, n$. Sia poi W un altro spazio vettoriale sullo stesso campo K , siano $B(W) = \{w_1, w_2, \dots, w_m\}$ e $B'(W) = \{w'_1, w'_2, \dots, w'_m\}$ due basi di W , e sia Q la matrice quadrata di ordine m la cui colonna k -esima è data dai coefficienti dell'espressione di w'_k come combinazione lineare di w_1, w_2, \dots, w_m per ogni $k = 1, 2, \dots, m$. Siano A e A' le matrici associate ad un'applicazione lineare di V in W rispetto alle basi $B(V), B(W)$ e $B'(V), B'(W)$ rispettivamente. Allora $A' = Q^{-1}AP$.

Nel caso particolare di un endomorfismo $f: V \rightarrow V$, supponendo di fissare la stessa base sia sul dominio che sul codominio di f , il risultato precedente diventa:

40.3 COROLLARIO. Sia V uno spazio vettoriale su un campo K , siano $B(V) = \{v_1, v_2, \dots, v_n\}$ e $B'(V) = \{v'_1, v'_2, \dots, v'_n\}$ due basi di V e sia P la matrice quadrata di ordine n la cui colonna j -esima è data dai coefficienti dell'espressione di v'_j come combinazione lineare di v_1, v_2, \dots, v_n per ogni $j = 1, 2, \dots, n$. Siano A e A' le matrici associate ad un endomorfismo f di V rispetto alle basi $B(V)$ e $B'(V)$ rispettivamente. Allora $A' = P^{-1}AP$.

Due matrici $A, A' \in M_n(K)$ si dicono simili se esiste una matrice invertibile $P \in M_n(K)$ tale che $A' = P^{-1}AP$. Due matrici quadrate di ordine n sono simili se e solo se rappresentano lo stesso endomorfismo f di uno spazio vettoriale V di dimensione n rispetto a due basi di V .

Esercizi svolti

40.1. Sia $A = (a_{ij})$ una matrice quadrata di ordine n a elementi in un campo K . Chiamiamo traccia di A l'elemento $\text{tr}(A) = \sum_{i=1}^n a_{ii}$ di K , cioè la somma degli elementi sulla diagonale di A .

- (a) Si dimostri che l'applicazione $\text{tr}: M_n(K) \rightarrow K$, $A \mapsto \text{tr}(A)$, è K -lineare e che la traccia della matrice identica $I \in M_n(K)$ è n .
- (b) Si dimostri che se A, B sono matrici quadrate di ordine n ad elementi in K , allora $\text{tr}(AB) = \text{tr}(BA)$.
- (c) Si dimostri che se P è una matrice invertibile, allora $\text{tr}(P^{-1}AP) = \text{tr}(A)$.
- (d) Si deduca da (c) che è possibile definire la *traccia* di un endomorfismo di un qualunque spazio vettoriale di dimensione finita.

Soluzione. (a) Se $A = (a_{ij})$ e $B = (b_{ij})$ sono elementi di $M_n(K)$, allora $\text{tr}(A+B) = \text{tr}(a_{ij} + b_{ij}) = \sum_{i=1}^n (a_{ii} + b_{ii}) = \sum_{i=1}^n a_{ii} + \sum_{i=1}^n b_{ii} = \text{tr}(A) + \text{tr}(B)$. Inoltre per ogni $\lambda \in K$ si ha $\text{tr}(\lambda A) = \text{tr}(\lambda a_{ij}) = \sum_{i=1}^n \lambda a_{ii} = \lambda \sum_{i=1}^n a_{ii} = \lambda \text{tr}(A)$. È poi ovvio che $\text{tr}(I) = n$.

(b) La matrice AB ha nel posto (i, i) l'elemento $\sum_{k=1}^n a_{ik}b_{ki}$. Quindi la traccia della matrice AB è $\text{tr}(AB) = \sum_{i=1}^n \sum_{k=1}^n a_{ik}b_{ki}$. Analogamente la matrice BA ha nel posto (k, k) l'elemento $\sum_{i=1}^n b_{ki}a_{ik}$, e quindi la sua traccia è $\text{tr}(BA) = \sum_{k=1}^n \sum_{i=1}^n b_{ki}a_{ik}$. Ma allora per la commutatività della moltiplicazione di K si ha che

$$\text{tr}(AB) = \sum_{i,k} a_{ik}b_{ki} = \sum_{i,k} b_{ki}a_{ik} = \text{tr}(BA).$$

(c) Si ha $\text{tr}(P^{-1}AP) = \text{tr}(P^{-1}(AP)) = \text{tr}((AP)P^{-1})$ per quanto visto in (b), da cui $\text{tr}(P^{-1}AP) = \text{tr}(APP^{-1}) = \text{tr}(AI) = \text{tr}(A)$.

(d) In (c) si è visto che due matrici simili hanno la stessa traccia. Quindi se $f: V \rightarrow V$ è un endomorfismo di uno spazio vettoriale V di dimensione finita n , fissiamo una base $\{v_1, \dots, v_n\}$ di V e denotiamo con A la matrice associata ad f rispetto alla base $\{v_1, \dots, v_n\}$, allora possiamo definire la traccia di f come la traccia della matrice A . Tale traccia non dipende infatti dalla scelta della base $\{v_1, \dots, v_n\}$ di V , in quanto se fissiamo un'altra base $\{v'_1, \dots, v'_n\}$ di V e denotiamo con A' la matrice associata ad f rispetto alla base $\{v'_1, \dots, v'_n\}$, allora $A' = P^{-1}AP$ per un'opportuna matrice invertibile P (corollario 40.3), e quindi $\text{tr}(A') = \text{tr}(A)$ per quanto visto in (c). \square

Altri esercizi

40.2. Sia $\{v_1, v_2, v_3, v_4\}$ una base di uno spazio vettoriale reale di dimensione 4. Sia f l'endomorfismo di V la cui matrice associata rispetto alla base $\{v_1, v_2, v_3, v_4\}$ è

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

- (a) Si determini $\ker f$.
- (b) Si determini una base di $\ker f$.
- (c) Si determini una base dell'immagine di f .
- (d) Si completi la base di $\ker f$ trovata in (b) ad una base di V e si scriva la matrice associata ad f in questa nuova base.

40.3. Sia $f: \mathbb{Q}^2 \rightarrow \mathbb{Q}^3$ l'applicazione lineare la cui matrice associata rispetto alle basi canoniche di \mathbb{Q}^2 e \mathbb{Q}^3 è

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

- (a) Si dimostri che $B' = \{(1, -1), (2, 1)\}$ è una base di \mathbb{Q}^2 .
 (b) Si scriva la matrice A' associata ad f rispetto alla base B' di \mathbb{Q}^2 e alla base canonica di \mathbb{Q}^3 .

40.4. Sia $B = \{v_1, v_2, v_3\}$ una base di uno spazio vettoriale V e sia

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix}$$

la matrice associata a un endomorfismo f di V rispetto alla base B . Siano $v'_1 = -v_1 + v_3$, $v'_2 = 2v_2$ e $v'_3 = v_2 + v_3$, e $B' = \{v'_1, v'_2, v'_3\}$.

- (a) Si dimostri che B' è una base di V .
 (b) Si scriva la matrice associata ad f rispetto alla base B' .

40.5. In \mathbb{R}^3 i vettori $v_1 = (1, 1, 0)$, $v_2 = (1, 0, 0)$, $v_3 = (0, 0, 2)$ formano una base, e quindi esiste un unico endomorfismo di spazi vettoriali $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ che manda v_1, v_2, v_3 in $(-2, 0, 0)$, $(0, 3, 0)$, $(-2, 0, 0)$ rispettivamente.

- (a) Si scriva la matrice di f rispetto alla base $\{v_1, v_2, v_3\}$.
 (b) Si scriva la matrice di f rispetto alla base canonica di \mathbb{R}^3 .

40.6. Sia $\{e_1, e_2\}$ la base canonica dello spazio vettoriale reale \mathbb{R}^2 . Siano $v_1 = e_1 + e_2$ e $v_2 = e_1 - 2e_2$.

- (a) Si dimostri che $\{v_1, v_2\}$ è una base di \mathbb{R}^2 .

Sia $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ l'unica applicazione lineare tale che $f(v_1) = v_1 + v_2$, $f(v_2) = v_2$.

- (b) Si scriva la matrice A associata ad f rispetto alla base $\{v_1, v_2\}$.
 (c) Si verifichi che se $\alpha, \beta \in \mathbb{R}$, allora i coefficienti del vettore $f(\alpha v_1 + \beta v_2)$ scritto come combinazione lineare di v_1 e v_2 sono proprio gli elementi della matrice colonna $A \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.
 (d) Si scriva la matrice B associata ad f rispetto alla base $\{e_1, e_2\}$.
 (e) Si verifichi che se $\alpha, \beta \in \mathbb{R}$, allora i coefficienti del vettore $f(\alpha e_1 + \beta e_2)$ scritto come combinazione lineare di e_1 ed e_2 sono proprio gli elementi della matrice colonna $B \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

40.7. Siano U e V i due sottospazi di dimensione 1 di \mathbb{R}^2 generati rispettivamente da $(1, 1)$ e da $(1, -1)$.

- (a) Si dimostri che $\mathbb{R}^2 = U \oplus V$.
 (b) Sia f l'endomorfismo di \mathbb{R}^2 tale che $f(u) = 0$ per ogni $u \in U$ e $f(v) = v$ per ogni $v \in V$. Si determini $f(a, b)$ per ogni $(a, b) \in \mathbb{R}^2$.
 (c) Si scriva la matrice di f rispetto alla base canonica di \mathbb{R}^2 .
 (d) Si determini una base $\{v_1, v_2\}$ di \mathbb{R}^2 rispetto alla quale la matrice di f è $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

40.8. Si dimostri che le matrici

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

sono simili determinando una matrice invertibile P tale che $P^{-1}AP = B$.

40.9. Le matrici ad elementi reali

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 5 & -1 & 0 \end{pmatrix}$$

sono simili? [Suggerimento: Si deve vedere se esiste una matrice 3×3 invertibile P tale che $A = P^{-1}BP$. Si trovino quindi le matrici

$$P = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

tali che $PA = BP$ risolvendo il sistema $PA = BP$ di nove equazioni lineari nelle nove incognite $a, b, c, d, e, f, g, h, i$. Tra tutte le P trovate si veda se ne esiste una di rango 3.]

40.10. Le matrici ad elementi reali

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

sono simili?

40.11. Si dimostri che due matrici simili hanno lo stesso rango.

§41. Sistemi di equazioni lineari

Consideriamo un sistema di m equazioni lineari in n incognite

$$(41.1) \quad \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{array} \right.$$

ove supponiamo che gli a_{ij} e i b_i siano elementi di un campo K . Ponendo

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

il sistema (41.1) si riscrive nella forma $AX = B$. La matrice $m \times n$ A si dice la matrice *incompleta* del sistema. La matrice $m \times (n+1)$

$$A' = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix},$$

ottenuta aggiungendo ad A come $(n+1)$ -esima colonna la colonna B dei *termini noti*, si dice la matrice *completa* del sistema (41.1). Sia K^n lo spazio vettoriale delle matrici colonna $n \times 1$. Si chiama *soluzione* del sistema ogni

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \in K^n$$

tale che $AC = B$.

Abbiamo già considerato (esempio 35.5) l'applicazione lineare $f_A: K^n \rightarrow K^m$ definita ponendo $f_A(C) = AC$ per ogni $C \in K^n$. Denotando, come abbiamo fatto nel paragrafo precedente, con A la matrice incompleta del sistema (41.1) e con B la colonna dei termini noti, di modo che il sistema (41.1) si scrive semplicemente nella forma $AX = B$, si ha che $C \in K^n$ è una soluzione del sistema se e solo se $f_A(C) = B$. Ne segue, in particolare, che il sistema (41.1) ha soluzioni se e solo se B appartiene all'immagine dell'applicazione lineare f_A . Si osservi poi che se C è una soluzione del sistema, allora per ogni $H \in \ker f_A$ anche $C + H$ è una soluzione del sistema. Infatti $f_A(C + H) = f_A(C) + f_A(H) = B + 0 = 0$.

Il teorema che segue riguarda il caso $m = n$, ossia i sistemi di n equazioni lineari in n incognite.

41.1 TEOREMA DI CRAMER. *Un sistema di n equazioni lineari in n incognite*

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{array} \right.$$

ha un'unica soluzione se e solo se la sua matrice incompleta $A = (a_{ij})$ ha rango n , cioè è invertibile. In tal caso, l'unica soluzione del sistema è $C = A^{-1}B$.

Dimostrazione. Sappiamo già che la matrice A ha rango n se e solo se è invertibile (proposizione 39.12).

Se il sistema ha un'unica soluzione, allora $\ker f_A = \{0\}$, in quanto la somma di una soluzione e di un elemento di $\ker f_A$ è ancora una soluzione. Quindi $f_A: K^n \rightarrow K^n$ è iniettiva, e dunque suriettiva (corollario 38.7). Ne segue che la dimensione dell'immagine di f_A , ossia il rango di f_A , è n . Per la proposizione 39.11 il rango della matrice associata ad f_A è n . Ma come abbiamo visto nell'esempio 39.4 la matrice associata ad f_A è proprio la matrice A .

Viceversa, supponiamo che la matrice A sia invertibile. Denotiamo con A^{-1} la matrice inversa di A e con I la matrice identica $n \times n$. Allora $A^{-1}B$ è una soluzione del sistema, in quanto $A(A^{-1}B) = (AA^{-1})B = IB = B$. Inoltre questa è l'unica soluzione del sistema, in quanto se C è una qualsiasi soluzione si deve avere $AC = B$, da cui

$C = IC = (A^{-1}A)C = A^{-1}(AC) = A^{-1}B$. Questo dimostra che la soluzione del sistema è unica e questa unica soluzione è $C = A^{-1}B$. \square

Un sistema di m equazioni lineari in n incognite del tipo

$$(41.2) \quad \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0. \end{array} \right.$$

si dice un sistema *omogeneo*. Se A è la sua matrice incompleta, il sistema si può quindi scrivere nella forma $AX = 0$. Se $f_A: K^n \rightarrow K^m$ è l'applicazione lineare definita da $f_A(C) = AC$ per ogni $C \in K^n$, si ha che C è soluzione del sistema, ossia $AC = 0$, se e solo se $C \in \ker f_A$. Quindi, per un sistema omogeneo di m equazioni lineari in n incognite $AX = 0$, l'insieme delle soluzioni coincide con $\ker f_A$, ed è quindi un sottospazio vettoriale di K^n .

Torniamo al caso più generale di un sistema non necessariamente omogeneo di m equazioni lineari in n incognite. Dato un tale sistema $AX = B$, il suo *sistema omogeneo associato* è il sistema di m equazioni lineari in n incognite $AX = 0$.

41.2 TEOREMA DI ROUCHÉ-CAPELLI. *Il sistema di m equazioni lineari in n incognite $AX = B$ ha almeno una soluzione se e solo se la sua matrice incompleta A e la sua matrice completa A' hanno lo stesso rango. In tal caso, sia C_0 una soluzione del sistema $AX = B$, sia W il sottospazio vettoriale di K^n i cui elementi sono le soluzioni del sistema omogeneo associato $AX = 0$, e sia r il rango di A . Allora le soluzioni del sistema $AX = B$ sono tutte e sole del tipo $C_0 + H$ con $H \in W$, e W è uno spazio vettoriale di dimensione $n - r$.*

Dimostrazione. Supponiamo che il sistema $AX = B$ abbia una soluzione $C \in K^n$, di modo che $AC = B$. Se

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \in K^n$$

e denotiamo con A_1, \dots, A_n le colonne di A , allora $A_1c_1 + \cdots + A_nc_n = B$. Quindi B è combinazione lineare di A_1, \dots, A_n nello spazio vettoriale K^n . Ne segue che B appartiene al sottospazio vettoriale di K^n generato da $\{A_1, \dots, A_n\}$, e quindi il sottospazio generato da $\{A_1, \dots, A_n\}$ è uguale al sottospazio generato da $\{A_1, \dots, A_n, B\}$. Quindi questi due sottospazi hanno la stessa dimensione, ossia il rango della matrice incompleta A è uguale al rango della matrice completa A' .

Viceversa, supponiamo che il rango della matrice incompleta A sia uguale al rango della matrice completa A' . Allora, denotando con A_1, \dots, A_n le colonne di A , si ha che il sottospazio di K^n generato da $\{A_1, \dots, A_n\}$ e il sottospazio generato da $\{A_1, \dots, A_n, B\}$ hanno la stessa dimensione. Dato che questi due sottospazi sono uno contenuto nell'altro,

ne segue che i due sottospazi coincidono (esercizio 36.3). Quindi B appartiene al sottospazio di K^n generato da $\{A_1, \dots, A_n\}$, ossia è combinazione lineare di A_1, \dots, A_n . Siano $c_1, \dots, c_n \in K$ tali che $A_1c_1 + \dots + A_nc_n = B$. Posto

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \in K^n,$$

si ha quindi $AC = B$. Questo dimostra che C è una soluzione del sistema $AX = B$.

Siano ora C_0 una soluzione del sistema $AX = B$, W il sottospazio vettoriale di K^n i cui elementi sono le soluzioni del sistema omogeneo associato $AX = 0$, ed r il rango di A . Se C è una soluzione del sistema $AX = B$, si ha allora $AC = B$ e $AC_0 = B$, da cui $AC = AC_0$, e quindi $A(C - C_0) = 0$. Ne segue che $C - C_0$ è una soluzione del sistema $AX = 0$, ossia $C - C_0 = H$ per qualche $H \in W$, da cui $C = C_0 + H$. Viceversa, per ogni $H \in W$ si ha $AH = 0$, e quindi $A(C_0 + H) = AC_0 + AH = B + 0 = B$. Questo dimostra che ogni $C_0 + H$ è una soluzione del sistema $AX = B$.

Resta solo da dimostrare che $\dim(W) = n - r$. Sia $f_A : K^n \rightarrow K^m$ l'applicazione lineare definita da $f_A(C) = AC$ per ogni $C \in K^n$. Allora $W = \ker f_A$, e quindi per la proposizione 38.5 si ha $\dim(K^n) = \dim(\ker f_A) + \dim(f_A(K^n))$. Ma $\dim(K^n) = n$, $\dim(\ker f_A) = \dim(W)$, e $\dim(f_A(K^n))$ è il rango di f_A , ossia il rango r di A (proposizione 39.11). Pertanto $\dim(W) = n - r$. \square

Esercizi svolti

A partire dal prossimo esercizio scriveremo gli elementi di \mathbb{Z}_n senza la sbarra sopra ogniqualvolta non ci sarà pericolo di confusione. Pertanto scriveremo a intendendo $\bar{a} = a + n\mathbb{Z}$.

41.1. Si consideri il sistema in \mathbb{Z}_3

$$\begin{cases} x + 2y = 1 \\ 2x - 2y = 2. \end{cases}$$

- (a) Si scrivano la matrice incompleta A e la matrice completa A' del sistema.
- (b) Si determinino quali e quante sono le soluzioni del sistema in \mathbb{Z}_3 .

Soluzione. (a) Si ha

$$A = \begin{pmatrix} 1 & 2 \\ 2 & -2 \end{pmatrix} \quad \text{e} \quad A' = \begin{pmatrix} 1 & 2 & 1 \\ 2 & -2 & 2 \end{pmatrix}.$$

- (b) Dalla prima equazione si ricava $x = 1 - 2y$, e sostituendo questa espressione di x nella seconda equazione del sistema si ottiene $2(1 - 2y) - 2y = 2$, cioè $-6y = 0$. Dato che $6 = 0$ in \mathbb{Z}_3 , si ha $-6y = 0$ per ogni valore di y in \mathbb{Z}_3 . Le soluzioni del sistema sono quindi tutte le coppie $(x, y) \in \mathbb{Z}_3^2$ con $y \in \mathbb{Z}_3$ arbitrario e $x = 1 - 2y$. Quindi le soluzioni del sistema sono 3:

$$(1, 0), \quad (-1, 1) = (2, 1) \quad \text{e} \quad (-3, 2) = (0, 2). \quad \square$$

41.2. Si consideri il seguente sistema di tre equazioni lineari in tre incognite a coefficienti in \mathbb{Z}_5 :

$$(41.3) \quad \begin{cases} x + \lambda y = 4 \\ x + 3y = -1 \\ (\lambda + 1)x + 3y + \lambda z = 2. \end{cases}$$

Si determini per quali valori del parametro $\lambda \in \mathbb{Z}_5$ il rango della matrice incompleta o della matrice completa del sistema è uguale a 3. Si determini facendo uso dei teoremi di Cramer e di Rouché-Capelli quante soluzioni ha il sistema al variare del parametro λ in \mathbb{Z}_5 .

Soluzione. Le matrici incompleta e completa del sistema sono rispettivamente

$$A = \begin{pmatrix} 1 & \lambda & 0 \\ 1 & 3 & 0 \\ \lambda + 1 & 3 & \lambda \end{pmatrix} \quad \text{e} \quad A' = \begin{pmatrix} 1 & \lambda & 0 & 4 \\ 1 & 3 & 0 & -1 \\ \lambda + 1 & 3 & \lambda & 2 \end{pmatrix}.$$

Calcoliamo il rango della matrice incompleta A , ossia la dimensione dello spazio vettoriale generato dalle sue colonne

$$(41.4) \quad \begin{pmatrix} 1 \\ 1 \\ \lambda + 1 \end{pmatrix}, \quad \begin{pmatrix} \lambda \\ 3 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix}.$$

Vediamo quando queste tre matrici colonna sono linearmente indipendenti. Supponiamo che $\alpha, \beta, \gamma \in \mathbb{Z}_5$ siano tali che

$$\alpha \begin{pmatrix} 1 \\ 1 \\ \lambda + 1 \end{pmatrix} + \beta \begin{pmatrix} \lambda \\ 3 \\ 3 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Allora

$$\begin{pmatrix} \alpha + \beta\lambda \\ \alpha + 3\beta \\ \alpha(\lambda + 1) + 3\beta + \gamma\lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

e quindi α, β, γ soddisfano le equazioni

$$\begin{cases} \alpha + \beta\lambda = 0 \\ \alpha + 3\beta = 0 \\ \alpha(\lambda + 1) + 3\beta + \gamma\lambda = 0. \end{cases}$$

Dalla seconda equazione si ricava che $\alpha = -3\beta$, e sostituendo questa espressione nelle altre due equazioni si ricava

$$\begin{cases} -3\beta + \beta\lambda = 0 \\ -3\beta(\lambda + 1) + 3\beta + \gamma\lambda = 0, \end{cases} \quad \text{ossia} \quad \begin{cases} (\lambda - 3)\beta = 0 \\ -3\lambda\beta + \gamma\lambda = 0. \end{cases}$$

Ora se $\lambda - 3 \neq 0$, ossia se $\lambda \neq 3$, dalla prima equazione di questo sistema di due equazioni lineari si ricava che $\beta = 0$, e quindi $\alpha = 0$, e dalla seconda equazione si ha $\gamma\lambda = 0$. Pertanto se $\lambda \neq 3$ e $\lambda \neq 0$, si può concludere che $\alpha = \beta = \gamma = 0$, e quindi i tre vettori (41.4) sono linearmente

indipendenti in questo caso. Ne segue che lo spazio vettoriale che essi generano è tutto \mathbb{Z}_5^3 , e quindi il rango della matrice incompleta A è 3. Per il teorema di Cramer il sistema dato (41.3) ha un'unica soluzione in questo caso di $\lambda \neq 3$ e $\lambda \neq 0$. Anche il rango della matrice completa A' deve essere necessariamente 3 in questo caso.

Per $\lambda = 0$, i tre vettori (41.4) sono linearmente dipendenti in quanto l'ultimo è il vettore nullo. Quindi in questo caso il rango della matrice incompleta A è minore di 3. Mostriamo invece che il rango della matrice completa

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

è 3, ossia che lo spazio vettoriale generato dalle colonne di A' è tutto \mathbb{Z}_5^3 . È sufficiente dimostrare che le tre colonne

$$(41.5) \quad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 4 \\ -1 \\ 2 \end{pmatrix}$$

sono linearmente indipendenti. Siano $\alpha, \beta, \gamma \in \mathbb{Z}_5$ tali che

$$\alpha \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix} + \gamma \begin{pmatrix} 4 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Allora

$$\begin{pmatrix} \alpha + 4\gamma \\ \alpha + 3\beta - \gamma \\ \alpha + 3\beta + 2\gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Ne segue che α, β, γ soddisfano il sistema

$$(41.6) \quad \begin{cases} \alpha + 4\gamma = 0 \\ \alpha + 3\beta - \gamma = 0 \\ \alpha + 3\beta + 2\gamma = 0. \end{cases}$$

Sottraendo la seconda equazione dalla terza si ricava $3\gamma = 0$, da cui $\gamma = 0$, e quindi dalla prima equazione del sistema (41.6) si ha $\alpha = 0$, e sostituendo nella seconda equazione del sistema (41.6) si ottiene che anche $\beta = 0$. Quindi i tre vettori colonna (41.5) sono linearmente indipendenti, ossia generano tutto \mathbb{Z}_5^3 , e pertanto il rango della matrice incompleta A' è 3. Dal teorema di Rouché-Capelli si deduce quindi che per $\lambda = 0$ il sistema (41.3) non ha soluzioni.

Resta da esaminare il caso $\lambda = 3$. In questo caso la matrice incompleta del sistema è la

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

Lasciamo al lettore la verifica del fatto che le tre colonne di questa matrice sono linearmente dipendenti in quanto si ha, ad esempio,

$$-3 \begin{pmatrix} 1 \\ 1 \\ 4 \end{pmatrix} + \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix} + 3 \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Quindi ad esempio la terza colonna è combinazione lineare delle prime due, e pertanto lo spazio vettoriale generato dalle colonne della matrice incompleta coincide con lo spazio vettoriale generato dalle prime due colonne. Dato che queste due colonne non sono proporzionali, esse sono linearmente indipendenti. Quindi il rango della matrice incompleta è 2. Anche la quarta colonna della matrice completa

$$\begin{pmatrix} 1 & 3 & 0 & 4 \\ 1 & 3 & 0 & -1 \\ 4 & 3 & 3 & 2 \end{pmatrix}$$

è somma delle prime due (si ricordi che stiamo lavorando in \mathbb{Z}_5) e quindi anche la matrice completa ha rango 2. Per il teorema di Rouché-Capelli il sistema dato ha quindi tante soluzioni quanti sono gli elementi di uno spazio vettoriale di dimensione $3 - 2 = 1$ sul campo \mathbb{Z}_5 . Se ne conclude che il sistema ha 5 soluzioni nel caso $\lambda = 3$.

Ricapitolando: il rango della matrice incompleta è uguale a 3 per $\lambda \neq 0$ e $\lambda \neq 3$ (ossia per λ uguale a 1, 2 o 4); il rango della matrice completa è uguale a 3 per $\lambda \neq 3$ (ossia per λ uguale a 0, 1, 2 o 4); il sistema ha un'unica soluzione per $\lambda \neq 0$ e $\lambda \neq 3$ (ossia per λ uguale a 1, 2 o 4), non ha soluzioni per $\lambda = 0$, ha cinque soluzioni per $\lambda = 3$. \square

Il lettore avrà notato quanto macchinosa sia stata la soluzione dell'esercizio precedente. Questa macchinosità è dovuta al fatto che è stato necessario calcolare il rango di varie matrici. Nel seguito impareremo delle tecniche più efficienti per calcolare il rango. Questo renderà molto più rapido verificare con il teorema di Rouché-Capelli se un sistema di equazioni lineari ha soluzioni e calcolare quante ne ha.

Altri esercizi

41.3. Per ciascuno dei seguenti sistemi di tre equazioni lineari in tre incognite in un campo K

- (a) si scrivano la matrice incompleta A del sistema e la colonna B dei termini noti;
- (b) si calcoli il rango di A ;
- (c) si dica se il sistema ha un'unica soluzione;
- (d) se la risposta a (c) è affermativa si calcolino l'inversa A^{-1} di A e il prodotto $A^{-1}B$;
- (e) si verifichi che $A^{-1}B$ è soluzione del sistema.

$$(1) \quad K = \mathbb{R}, \quad \begin{cases} x + y = 0 \\ x - 2y + 2z = 5 \\ x - y = 1; \end{cases}$$

$$(2) \quad K = \mathbb{C}, \quad \begin{cases} x + y = 0 \\ x - 2y + 2z = 5 \\ -x + 5y - 4z = 10; \end{cases}$$

$$(3) \quad K = \mathbb{Z}_7, \quad \begin{cases} x + y + z = 0 \\ 4x + z = 1 \\ y + 2z = -2; \end{cases}$$

$$(4) \quad K = \mathbb{Z}_5, \quad \begin{cases} x + y + z = 0 \\ 4x + z = 1 \\ y + 2z = -2. \end{cases}$$

41.4. Per ogni valore del parametro reale a , si determini quante soluzioni reali ha il sistema

$$\begin{cases} 2x + ay + 3z = 2a \\ -ax + y + z = 6 \\ 4x - y + z = -10. \end{cases}$$

41.5. Si considerino i quattro sistemi nei campi \mathbb{R} , \mathbb{C} , \mathbb{Z}_7 , \mathbb{Z}_5 rispettivamente studiati nell'esercizio 41.3. Svolgendo quegli esercizi si sarà visto che il rango della loro matrice incompleta A è 3, 2, 3, 2 rispettivamente. Per ciascuno dei quattro sistemi:

- (a) si scriva il sistema omogeneo associato;
- (b) si calcoli il rango della matrice completa del sistema dato;
- (c) si dica se il sistema dato ha almeno una soluzione;
- (d) se la risposta a (c) è affermativa, si determini una soluzione del sistema dato;
- (e) si dica quante sono le soluzioni del sistema.

41.6. (a) Sia $K = \mathbb{R}$ il campo dei numeri reali. Per ogni valore del parametro $\lambda \in K$ si determini quante soluzioni ha in K il sistema

$$\begin{cases} \lambda x + 2y - 2z = \lambda \\ x - 4y + \lambda z = 3 \\ 5x + y + z = 1. \end{cases}$$

(b) Si risolva lo stesso esercizio con $K = \mathbb{Z}_{11}$, il campo con 11 elementi.

§42. Determinante

Impareremo ora ad associare ad ogni matrice quadrata A ad elementi in un campo K un elemento di K detto il *determinante* di A . Lo denoteremo con $\det A$. Prima di definirlo in modo rigoroso, cosa che seguirà dal teorema 42.5, vediamo uno dei metodi per calcolarlo in pratica. Si tratta di un metodo che permette di ridurre il calcolo del determinante di una qualunque matrice quadrata di ordine n al calcolo del determinante di matrici quadrate di ordine $n - 1$.

Per le matrici quadrate di ordine 1 poniamo intanto $\det(a) = a$ per ogni matrice (a) . Sia ora $A = (a_{ij})$ una qualunque matrice quadrata di ordine $n \geq 2$. Per ogni $i, j = 1, 2, \dots, n$ denotiamo con A_{ij} la matrice ottenuta da A cancellando la i -esima riga e la j -esima colonna. Quindi A_{ij} è una matrice quadrata di ordine $n - 1$. Fissiamo una qualunque riga di A , diciamo la i -esima. Il determinante di A sarà l'elemento di K definito da

$$(42.1) \quad \det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}.$$

Vi è naturalmente da verificare che il determinante $\det A$ così definito non dipende dalla scelta della riga fissata e questo verrà visto solo nel teorema 42.5. Per il momento facciamo alcuni esempi per prendere un po' di confidenza con lo scalare $\det A$ appena definito.

Per quanto riguarda le matrici quadrate di ordine 1 non c'è ovviamente nessun problema. Vediamo cos'è il determinante di una generica matrice quadrata di ordine 2

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Fissiamo la prima riga. Allora

$$\begin{aligned} \det A &= \sum_{j=1}^2 (-1)^{1+j} a_{1j} \det A_{1j} = a_{11} \det A_{11} - a_{12} \det A_{12} \\ &= a_{11} \det(a_{22}) - a_{12} \det(a_{21}) = a_{11}a_{22} - a_{12}a_{21}. \end{aligned}$$

Abbiamo così imparato a calcolare il determinante di una qualunque matrice 2×2 . Vediamo il determinante di una matrice 3×3

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Fissiamo anche in questo caso la prima riga. Si ha

$$\begin{aligned} \det A &= \sum_{j=1}^3 (-1)^{1+j} a_{1j} \det A_{1j} = a_{11} \det A_{11} - a_{12} \det A_{12} + a_{13} \det A_{13} \\ &= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}) \\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}. \end{aligned}$$

Come ultimo esempio calcoliamo il determinante di una particolare matrice quadrata di ordine 4 a elementi reali:

$$A = \begin{pmatrix} -1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 5 & 0 & 1 & 1 \\ 4 & 1 & 0 & 1 \end{pmatrix}.$$

Fissiamo questa volta la seconda riga. Si trova che

$$\begin{aligned} \det A &= \sum_{j=1}^4 (-1)^{2+j} a_{2j} \det A_{2j} = -a_{21} \det A_{21} + a_{22} \det A_{22} - a_{23} \det A_{23} + a_{24} \det A_{24} \\ &= -2 \det A_{21} + 0 \cdot \det A_{22} - 0 \cdot \det A_{23} + 0 \cdot \det A_{24} = -2 \det \begin{pmatrix} 0 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Sviluppando rispetto alla terza riga, cioè fissando la terza riga, si vede che

$$\det A = -2 \left(\det \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} + \det \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} \right) = -2((2 \cdot 1 - 1 \cdot 1) + (0 \cdot 1 - 2 \cdot 0)) = -2.$$

Il determinante di una matrice A si denota $\det A$ oppure scrivendo la matrice A tra due sbarre verticali invece che tra due parentesi. Per esempio avremmo potuto scrivere

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}, \quad \text{e} \quad \begin{vmatrix} -1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 5 & 0 & 1 & 1 \\ 4 & 1 & 0 & 1 \end{vmatrix} = -2.$$

Siano K un campo ed $n \geq 1$ un intero. Denotiamo gli elementi di K^n come matrici colonna $n \times 1$. Per ogni matrice quadrata $A \in M_n(K)$ denotiamo con A_1, \dots, A_n le colonne di A , di modo che $A_i \in K^n$ per ogni $i = 1, 2, \dots, n$. Possiamo quindi scrivere $A = (A_1 \dots A_n)$.

42.1 DEFINIZIONE. Siano K un campo ed $n \geq 1$ un numero intero. Un'applicazione $f: M_n(K) \rightarrow K$ si dice un'applicazione *multilineare alternante* se soddisfa le seguenti due condizioni:

- (a) (multilinearità) per ogni $j = 1, 2, \dots, n$ e per ogni $A_1, \dots, A_{j-1}, A_{j+1}, \dots, A_n \in K^n$ l'applicazione $K^n \rightarrow K$ definita da

$$X \mapsto f(A_1 \dots A_{j-1} X A_{j+1} \dots A_n)$$

per ogni $X \in K^n$ è lineare;

- (b) (alternanza) per ogni matrice $A \in M_n(K)$ tale che $A_j = A_k$ per qualche $j, k = 1, 2, \dots, n$, $j \neq k$, si ha $f(A) = 0$. \square

42.2 ESEMPIO. Sia $f: M_2(\mathbb{R}) \rightarrow \mathbb{R}$ l'applicazione definita da $f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2bc - 2ad$ per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. Mostriamo che f è multilineare alternante.

Fissiamo $a, c \in \mathbb{R}$ e facciamo vedere che l'applicazione $f_2: \mathbb{R}^2 \rightarrow \mathbb{R}$ definita da $f_2 \begin{pmatrix} b \\ d \end{pmatrix} = f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2bc - 2ad$ per ogni $\begin{pmatrix} b \\ d \end{pmatrix} \in \mathbb{R}^2$ è lineare. Se $\begin{pmatrix} b \\ d \end{pmatrix}, \begin{pmatrix} b' \\ d' \end{pmatrix} \in \mathbb{R}^2$, allora

$$\begin{aligned} f_2 \left(\begin{pmatrix} b \\ d \end{pmatrix} + \begin{pmatrix} b' \\ d' \end{pmatrix} \right) &= f_2 \begin{pmatrix} b+b' \\ d+d' \end{pmatrix} = 2(b+b')c - 2a(d+d') \\ &= (2bc - 2ad) + (2b'c - 2ad') = f_2 \begin{pmatrix} b \\ d \end{pmatrix} + f_2 \begin{pmatrix} b' \\ d' \end{pmatrix}. \end{aligned}$$

Se poi $\lambda \in \mathbb{R}$ si ha anche

$$f_2 \left(\lambda \begin{pmatrix} b \\ d \end{pmatrix} \right) = f_2 \begin{pmatrix} \lambda b \\ \lambda d \end{pmatrix} = 2(\lambda b)c - 2a(\lambda d) = \lambda(2bc - 2ad) = \lambda f_2 \begin{pmatrix} b \\ d \end{pmatrix}.$$

Quindi $f_2: \mathbb{R}^2 \rightarrow \mathbb{R}$ è lineare, ossia f è lineare sulla seconda colonna.

Similmente si dimostra che, fissando $b, d \in \mathbb{R}$, l'applicazione $f_1: \mathbb{R}^2 \rightarrow \mathbb{R}$ definita da $f_1 \begin{pmatrix} a \\ c \end{pmatrix} = f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2bc - 2ad$ per ogni $\begin{pmatrix} a \\ c \end{pmatrix} \in \mathbb{R}^2$ è lineare, ossia f è lineare anche sulla prima colonna. Quindi f è multilinearare.

È anche alternante, perché per ogni $a, c \in \mathbb{R}$ si ha $f \begin{pmatrix} a & a \\ c & c \end{pmatrix} = 2ac - 2ac = 0$. \square

42.3 ESEMPIO. L'applicazione nulla $f: M_n(K) \rightarrow K$ definita da $f(A) = 0$ per ogni $A \in M_n(K)$ è multilinearare alternante. \square

42.4 LEMMA. Sia $f: M_n(K) \rightarrow K$ una qualunque applicazione multilinearare alternante. Allora valgono le seguenti proprietà:

(1) Per ogni $A_1, \dots, A_n \in K^n$ e ogni $j \neq k$ si ha

$$f(A_1 \dots A_j \dots A_k \dots A_n) = -f(A_1 \dots A_k \dots A_j \dots A_n),$$

cioè scambiando due colonne in una matrice la f cambia di segno.

(2) Per ogni $A_1, A_2, \dots, A_n \in K^n$ e ogni permutazione σ di $\{1, 2, \dots, n\}$ si ha

$$f(A_{\sigma(1)} A_{\sigma(2)} \dots A_{\sigma(n)}) = \text{sgn}(\sigma) f(A_1 A_2 \dots A_n).$$

(3) Se $I \in M_n(K)$ denota la matrice identità, per ogni $A = (a_{ij}) \in M_n(K)$ si ha

$$f(A) = f(I) \cdot \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Dimostrazione. (1) Per la matrice

$$B = (A_1 \dots A_j + A_k \dots A_k \dots A_n),$$

avente le colonne j -esima e k -esima entrambe uguali a $A_j + A_k$, si ha $f(B) = 0$ a causa dell'alternanza. Ma per la multilinearità si deve avere anche

$$\begin{aligned} f(B) &= f(A_1 \dots A_j \dots A_j \dots A_n) + f(A_1 \dots A_j \dots A_k \dots A_n) \\ &\quad + f(A_1 \dots A_k \dots A_j \dots A_n) + f(A_1 \dots A_k \dots A_k \dots A_n) \\ &= f(A_1 \dots A_j \dots A_k \dots A_n) + f(A_1 \dots A_k \dots A_j \dots A_n). \end{aligned}$$

Quindi $f(A_1 \dots A_j \dots A_k \dots A_n) = -f(A_1 \dots A_k \dots A_j \dots A_n)$.

(2) Ogni permutazione di $\{1, 2, \dots, n\}$ è prodotto di un numero finito di trasposizioni, e se una permutazione σ è prodotto di r trasposizioni si ha $\text{sgn}(\sigma) = (-1)^r$. Quindi $(A_{\sigma(1)} A_{\sigma(2)} \dots A_{\sigma(n)})$ si ottiene da $(A_1 A_2 \dots A_n)$ trasponendo, cioè scambiando, successivamente r coppie di colonne. Per la (1) scambiando due colonne di una matrice, la f cambia di segno. Da questo segue immediatamente la proprietà (2).

(3) Sia I la matrice identità $n \times n$, ossia l'identità dell'anello $M_n(K)$, e siano I_1, I_2, \dots, I_n le colonne di I . Allora per ogni matrice $A = (a_{ij}) \in M_n(K)$, la j -esima colonna A_j di A è

$A = a_{1j}I_1 + a_{2j}I_2 + \cdots + a_{nj}I_n = \sum_{\ell=1}^n a_{\ell j}I_\ell$, e quindi

$$f(A) = f(A_1 \dots A_n) = f\left(\sum_{\ell_1=1}^n a_{\ell_1 1} I_{\ell_1} \dots \sum_{\ell_n=1}^n a_{\ell_n n} I_{\ell_n}\right).$$

Dalla multilinearità si ricava quindi che

$$(42.2) \quad f(A) = \sum_{\ell_1=1}^n \dots \sum_{\ell_n=1}^n f(a_{\ell_1 1} I_{\ell_1} \dots a_{\ell_n n} I_{\ell_n}) = \sum_{\ell_1=1}^n \dots \sum_{\ell_n=1}^n a_{\ell_1 1} \dots a_{\ell_n n} f(I_{\ell_1} \dots I_{\ell_n}).$$

In questa somma tutti gli addendi in cui compare una matrice con due colonne I_ℓ uguali sono nulli per l'alternanza della f . Quindi nella somma (42.2) sono eventualmente non nulli solo gli addendi in cui ℓ_1, \dots, ℓ_n sono tutti distinti tra loro, ossia sono una permutazione di $\{1, 2, \dots, n\}$, vale a dire gli addendi in cui ℓ_1, \dots, ℓ_n sono uguali rispettivamente a $\sigma(1), \dots, \sigma(n)$ per qualche permutazione $\sigma \in S_n$. Pertanto l'equazione (42.2) si può riscrivere nella forma

$$f(A) = \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} f(I_{\sigma(1)} \dots I_{\sigma(n)}).$$

Per la proprietà (2) si ha quindi

$$f(A) = \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} \operatorname{sgn}(\sigma) f(I_1 \dots I_n) = f(I) \cdot \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n}. \quad \square$$

42.5 TEOREMA. *Sia K un campo. Per ogni intero $n \geq 1$ esiste un'unica applicazione multilineare alternante $\det: M_n(K) \rightarrow K$ tale che $\det I_n = 1$, dove I_n denota l'identità dell'anello $M_n(K)$.*

Per tale applicazione \det , detta determinante, si ha

$$(42.3) \quad \det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n}$$

per ogni matrice $A = (a_{ij}) \in M_n(K)$, e, se $n \geq 2$,

$$(42.4) \quad \det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}$$

per ogni $i = 1, 2, \dots, n$, dove A_{ij} denota la matrice ottenuta da A cancellando la i -esima riga e la j -esima colonna.

Dimostrazione. Se esiste un'applicazione multilineare alternante $\det: M_n(K) \rightarrow K$ tale che $\det I_n = 1$, allora tale applicazione è unica. Infatti per il lemma 42.4(3) e per il fatto che $\det I_n = 1$, si deve avere

$$\det A = \det I_n \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n}.$$

Questo dimostra che se una tale funzione det esiste, essa è necessariamente unica e deve soddisfare l'uguaglianza (42.3).

Restano da dimostrare l'esistenza dell'applicazione \det e le uguaglianze (42.4). La dimostrazione dell'esistenza è per induzione su $n \geq 1$. Il caso $n = 1$ è banale, dato che l'applicazione $\det: M_1(K) \rightarrow K$ definita da $\det(a) = a$ per ogni $(a) \in M_1(K) \rightarrow K$ è chiaramente multilineare (è lineare), alternante (in modo banale) e manda (1) in 1. Supponiamo quindi che l'asserto valga per l'intero $n - 1$, cioè che esista un'applicazione multilineare alternante $\det: M_{n-1}(K) \rightarrow K$ che manda la matrice identica $(n-1) \times (n-1)$ in 1. Per ogni indice $i = 1, 2, \dots, n$ sia $f_i: M_n(K) \rightarrow K$ l'applicazione definita da $f_i(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}$, ossia il determinante calcolato sviluppando la i -esima riga. Per concludere la dimostrazione del teorema è sufficiente dimostrare che le applicazioni f_i sono multilineari alternanti e mandano I_n in 1. Infatti, in vista dell'unicità già dimostrata, questo proverà sia il passo induttivo che le uguaglianze (42.4).

Multilinearità. Siano $j = 1, 2, \dots, n$ e $A_1, \dots, A_{j-1}, A_{j+1}, \dots, A_n \in K^n$. Si deve dimostrare che l'applicazione $K^n \rightarrow K$, definita da

$$X \mapsto f_i(A_1 \dots A_{j-1} X A_{j+1} \dots A_n)$$

per ogni $X \in K^n$, è lineare, cioè che

$$\begin{aligned} f_i(A_1 \dots A_{j-1} X + Y A_{j+1} \dots A_n) \\ = f_i(A_1 \dots A_{j-1} X A_{j+1} \dots A_n) + f_i(A_1 \dots A_{j-1} Y A_{j+1} \dots A_n) \end{aligned}$$

e

$$f_i(A_1 \dots A_{j-1} \lambda X A_{j+1} \dots A_n) = \lambda f_i(A_1 \dots A_{j-1} X A_{j+1} \dots A_n)$$

per ogni $X, Y \in K^n$ e ogni $\lambda \in K$. Siano $A = (A_1 \dots A_{j-1} X + Y A_{j+1} \dots A_n)$, $B = (A_1 \dots A_{j-1} X A_{j+1} \dots A_n)$ e $C = (A_1 \dots A_{j-1} Y A_{j+1} \dots A_n)$. Per definizione $f_i(A) = \sum_{k=1}^n (-1)^{i+k} a_{ik} \det A_{ik}$. Per ogni $k \neq j$ le matrici A_{ik} , B_{ik} e C_{ik} hanno tutti gli elementi uguali salvo quelli della colonna precedentemente indicata da k , e in questa colonna gli elementi di A_{ik} sono la somma dei corrispondenti elementi di B_{ik} e di C_{ik} . Quindi per l'ipotesi induttiva $\det A_{ik} = \det B_{ik} + \det C_{ik}$. Per $k = j$ si ha $A_{ij} = B_{ij} + C_{ij}$ e $a_{ij} = b_{ij} + c_{ij}$. Pertanto

$$\begin{aligned} f_i(A) &= (-1)^{i+j} a_{ij} \det A_{ij} + \sum_{k \neq j} (-1)^{i+k} a_{ik} \det A_{ik} \\ &= (-1)^{i+j} (b_{ij} + c_{ij}) \det A_{ij} + \sum_{k \neq j} (-1)^{i+k} a_{ik} (\det B_{ik} + \det C_{ik}) = f_i(B) + f_i(C). \end{aligned}$$

Analogamente sia $D = (A_1 \dots A_{j-1} \lambda X A_{j+1} \dots A_n)$. Si ha

$$f_i(D) = \sum_{k=1}^n (-1)^{i+k} d_{ik} \det D_{ik}.$$

Per ogni $k \neq j$ le matrici B_{ik} e D_{ik} hanno tutti gli elementi uguali salvo quelli della colonna precedentemente indicata da k , e in questa colonna gli elementi di D_{ik} sono il prodotto dello scalare λ per i corrispondenti elementi di B_{ik} . Quindi per l'ipotesi induttiva $\det D_{ik} = \lambda \det B_{ik}$. Per $k = j$ si ha $D_{ij} = B_{ij}$ e $d_{ij} = \lambda b_{ij}$. Quindi $f_i(D) = \lambda f_i(B)$.

Alternanza. Sia A una matrice $n \times n$ tale che $A_j = A_k$ per qualche $j, k = 1, 2, \dots, n$, $j < k$. Si deve dimostrare che $f_i(A) = 0$.

Si ha

$$f_i(A) = \sum_{t=1}^n (-1)^{i+t} a_{it} \det A_{it} = (-1)^{i+j} a_{ij} \det A_{ij} + (-1)^{i+k} a_{ik} \det A_{ik}$$

perché A_{it} ha due colonne uguali per ogni t diverso da j e da k . Ora $A_j = A_k$ implica che $a_{ij} = a_{ik}$. Inoltre se per ogni $\ell = 1, 2, \dots, n$ si denota con A'_ℓ la colonna A_ℓ a cui è stata tolta la i -esima riga, di modo che $A'_j = A'_k$ e quindi

$$\begin{aligned} A_{ij} &= (A'_1 \dots A'_{j-1} A'_{j+1} \dots A'_{k-1} A'_k A'_{k+1} \dots A'_n) \\ A_{ik} &= (A'_1 \dots A'_{j-1} A'_k A'_{j+1} \dots A'_{k-1} A'_{k+1} \dots A'_n), \end{aligned}$$

si vede che A_{ik} si ottiene da A_{ij} permutando ciclicamente le $k - j$ colonne $A'_{j+1}, A'_{j+2}, \dots, A'_{k-1}, A'_k$. Se σ è un ciclo di lunghezza $k - j$, si ha, nella notazione del §21, $\lambda(\sigma) = k - j - 1$, e quindi $\operatorname{sgn}(\sigma) = (-1)^{k-j-1}$. Per il lemma 42.4(2) si ha quindi $\det A_{ik} = \operatorname{sgn}(\sigma) \det A_{ij} = (-1)^{k-j-1} \det A_{ij}$. Pertanto

$$\begin{aligned} f_i(A) &= (-1)^{i+j} a_{ij} \det A_{ij} + (-1)^{i+k} a_{ik} (-1)^{k-j-1} \det A_{ij} \\ &= (-1)^{i+j} a_{ij} \det A_{ij} + (-1)^{i+2k-j-1} a_{ij} \det A_{ij} \\ &= (-1)^{i+j} a_{ij} \det A_{ij} - (-1)^{i+j} a_{ij} \det A_{ij} = 0. \end{aligned}$$

f_i manda I_n in 1. Si ha $f_i(I_n) = \sum_{t=1}^n (-1)^{i+t} \delta_{it} \det I_{it} = (-1)^{i+i} \det I_{ii}$. Ma I_{ii} è la matrice identica $(n-1) \times (n-1)$, e quindi $f_i(I_n) = 1$. \square

Dal lemma 42.4(3) e dall'equazione (42.3) si deduce immediatamente che:

42.6 COROLLARIO. Se $f: M_n(K) \rightarrow K$ è un'applicazione multilineare alternante, allora $f(A) = f(I) \det A$ per ogni matrice $A \in M_n(K)$.

Ricordiamo dal §6 che la *trasposta* di una matrice $m \times n$ $A = (a_{ij})$ è la matrice $n \times m$ A^* il cui elemento di posto (i, j) è a_{ji} , cioè è la matrice che si ottiene da A scambiando le righe con le colonne.

42.7 PROPOSIZIONE. Se A^* è la matrice trasposta di una matrice $A \in M_n(K)$, allora $\det A^* = \det A$.

Dimostrazione. Se $A = (a_{ij})$, per la matrice trasposta A^* si ha $A^* = (a'_{ij})$, dove $a'_{ij} = a_{ji}$. Quindi

$$(42.5) \quad \det A^* = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a'_{\sigma(1),1} \cdots a'_{\sigma(n),n} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Ora si osservi che al variare di σ in S_n si ha che anche σ^{-1} varia in S_n . Quindi scrivendo σ^{-1} al posto di σ nell'uguaglianza (42.5) si trova che

$$\det A^* = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) \prod_{k=1}^n a_{k,\sigma^{-1}(k)}.$$

Ma $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$ per ogni $\sigma \in S_n$. Inoltre per ogni $\sigma \in S_n$, mediante la sostituzione $k = \sigma(j)$ si osserva che k varia nell'insieme $\{1, 2, \dots, n\}$ se e solo se j varia nell'insieme $\{1, 2, \dots, n\}$. Quindi

$$\prod_{k=1}^n a_{k,\sigma^{-1}(k)} = \prod_{j=1}^n a_{\sigma(j),\sigma^{-1}(\sigma(j))} = \prod_{j=1}^n a_{\sigma(j),j}.$$

Pertanto

$$\det A^* = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^n a_{\sigma(j),j} = \det A. \quad \square$$

Nella proposizione che segue abbiamo raccolto gran parte delle proprietà del determinante viste finora.

42.8 PROPOSIZIONE.

- (1) Scambiando due colonne di una matrice il determinante cambia di segno.
- (2) Se una matrice ha due colonne uguali, il suo determinante è zero.
- (3) Se tre matrici A, B, C hanno tutti gli elementi uguali eccetto in una colonna, nella quale gli elementi di A sono la somma degli elementi corrispondenti di B e di C , allora $\det A = \det B + \det C$.
- (4) Se in una matrice A si moltiplicano tutti gli elementi di una colonna per uno stesso scalare λ , allora il determinante della matrice così ottenuta è $\lambda \det A$.
- (5) Cambiando di segno tutti gli elementi di una colonna, il determinante cambia di segno.
- (6) Se una matrice ha una colonna tutta di zeri, il suo determinante è zero.

Valgono inoltre le proprietà analoghe alle (1)-(6) che si ottengono sostituendo la parola "colonna" con la parola "riga".

Dimostrazione. La (1) è stata dimostrata nel lemma 42.4(1). La (2) è data dal fatto che per il determinante vale l'alternanza. La (3) e la (4) dicono esattamente che il determinante è multilineare. Dato che una qualunque applicazione lineare manda l'opposto nell'opposto e lo zero nello zero, (5) e (6) seguono dalla multilinearità del determinante. Infine le proprietà per le righe seguono dalle proprietà delle colonne usando la proposizione 42.7. \square

Sempre dalla proposizione 42.7 si ottiene che il determinante si può calcolare anche sviluppandolo rispetto a una colonna, cioè che

$$(42.6) \quad \det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij}.$$

42.9 ESEMPIO. Calcoliamo il determinante della matrice

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

Sviluppando il determinante rispetto alla seconda riga si trova che

$$\begin{vmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{vmatrix} = - \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -(-1) = 1.$$

Ma avremmo potuto calcolarlo rispetto alla prima colonna, trovando

$$\begin{vmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 0 & 1 \end{vmatrix} = 1,$$

oppure rispetto alla seconda colonna, trovando

$$\begin{vmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{vmatrix} = - \begin{vmatrix} 0 & 1 \\ 1 & -1 \end{vmatrix} = -(-1) = 1. \quad \square$$

Esercizi svolti

42.1. Si calcoli il determinante della matrice

$$\begin{pmatrix} 1 & -1 & 5 & 6 \\ 0 & 1 & 7 & 2 \\ 0 & 0 & -1 & 0 \\ 0 & 3 & 8 & 4 \end{pmatrix}.$$

Soluzione. Sviluppando il determinante rispetto alla prima colonna si trova che

$$\begin{vmatrix} 1 & -1 & 5 & 6 \\ 0 & 1 & 7 & 2 \\ 0 & 0 & -1 & 0 \\ 0 & 3 & 8 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 7 & 2 \\ 0 & -1 & 0 \\ 3 & 8 & 4 \end{vmatrix}.$$

Sviluppando questo rispetto alla seconda riga si trova che il determinante della matrice data è uguale a

$$-(\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix}) = -(4 - 6) = 2. \quad \square$$

Altri esercizi

42.2. Si calcoli il determinante delle matrici

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 2 & 0 & -2 & 2 \\ 3 & 1 & -1 & 0 \\ -1 & -3 & -2 & 0 \end{pmatrix}.$$

42.3. Si dimostri che se

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

è una *matrice triangolare superiore* (cioè una matrice in cui tutti gli elementi sotto la diagonale sono nulli), allora il determinante di A è il prodotto degli elementi sulla diagonale, ossia

$$\det A = a_{11}a_{22}a_{33}\cdots a_{nn}.$$

42.4. (a) Si dimostri che se in una matrice A una colonna è combinazione lineare delle altre, allora $\det A = 0$.

(b) Nella matrice

$$A = \begin{pmatrix} 1 & 0 & 1 & 2 & 3 \\ 2 & 1 & 1 & 4 & 5 \\ 3 & 0 & 3 & 6 & 7 \\ 4 & 1 & 3 & 8 & 9 \\ 5 & 2 & 3 & 10 & 10 \end{pmatrix}$$

la terza colonna è la differenza delle prime due. Si calcoli $\det A$.

42.5. Si calcolino i determinanti delle matrici

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

$$D = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 1 & -1 & 0 & 1 & -1 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 2 & 0 \\ 4 & 0 & 3 & 4 & 0 \\ 5 & -1 & 0 & 1 & -1 \end{pmatrix}, \quad F = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 3 & -1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 2 & 0 \\ 4 & 0 & 3 & 4 & 0 \\ 6 & -1 & 0 & 1 & -1 \end{pmatrix}.$$

[*Suggerimento:* per fare il minor numero di conti possibile, si osservino attentamente le matrici.]

42.6. Senza effettuare nessun calcolo, ma semplicemente osservando le matrici, si verifichi che $\det C = \det A + \det B$, $\det D = 2 \det A$, $\det E = -\det A$, e $\det F = 0$, dove

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 1 & -2 & 3 & -4 \\ -5 & -6 & -7 & 8 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 1 & 3 & 1 \\ 5 & 6 & 7 & 8 \\ 1 & -2 & 3 & -4 \\ -5 & -6 & -7 & 8 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 3 & 6 & 5 \\ 5 & 6 & 7 & 8 \\ 1 & -2 & 3 & -4 \\ -5 & -6 & -7 & 8 \end{pmatrix},$$

$$D = \begin{pmatrix} 2 & 4 & 6 & 8 \\ 5 & 6 & 7 & 8 \\ 1 & -2 & 3 & -4 \\ -5 & -6 & -7 & 8 \end{pmatrix}, \quad E = \begin{pmatrix} -1 & -2 & -3 & -4 \\ 5 & 6 & 7 & 8 \\ 1 & -2 & 3 & -4 \\ -5 & -6 & -7 & 8 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 0 & 0 & 0 & 0 \\ -5 & -6 & -7 & 8 \end{pmatrix}.$$

42.7. Al variare del parametro $\lambda \in \mathbb{Z}_5$ si calcoli il determinante della matrice $A(\lambda) = \begin{pmatrix} 1 & 1 \\ 2 & 2\lambda \end{pmatrix}$ a elementi in \mathbb{Z}_5 . Per quali valori di λ si ha $\det A(\lambda) = 0$?

42.8. Si dimostri che

$$\begin{vmatrix} a & a & a \\ a & b & b \\ a & b & c \end{vmatrix} = a(a-b)(b-c).$$

42.9. Siano α, β, γ tre numeri reali. Si dimostri che

$$\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix} = (\beta - \alpha)(\gamma - \alpha)(\gamma - \beta).$$

42.10.

(a) Si calcolino i determinanti delle tre matrici

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & -1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 5 & 2 & 3 & 4 & 1 \\ 4 & -1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & -1 & 0 \\ 2 & 0 & 0 & 0 & 0 \end{pmatrix}, C = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 2 & 3 & 4 & -1 & 0 \\ 1 & 2 & 3 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \end{pmatrix}.$$

- (b) La matrice B è ottenuta da A scambiando la prima e l'ultima colonna. Si verifichi quindi che per le soluzioni trovate in (a) si ha $\det B = -\det A$.
- (c) Se $A = (A_1 \dots A_5)$, cioè A_1, \dots, A_5 denotano le cinque colonne di A , allora $C = (A_3 \ A_4 \ A_5 \ A_2 \ A_1)$. Si determini $\operatorname{sgn}(\sigma)$ dove σ è la permutazione di $\{1, 2, 3, 4, 5\}$ tale che $C = (A_{\sigma(1)} \ A_{\sigma(2)} \ \dots \ A_{\sigma(5)})$, e si verifichi che per le soluzioni trovate in (a) si ha $\det C = \operatorname{sgn}(\sigma) \det A$.

42.11. Siano K un campo ed $f: M_4(K) \rightarrow K$ un'applicazione multilineare alternante. Si dimostrì che per ogni $A_1, A_2, A_3, A_4 \in K^4$ si ha:

- (a) $f(A_2 \ A_3 \ A_4 \ A_1) = -f(A_1 \ A_2 \ A_3 \ A_4)$;
 (b) $f(A_1 \ A_3 \ A_4 \ A_2) = f(A_1 \ A_2 \ A_3 \ A_4)$.

42.12. Sia $f: M_2(\mathbb{Z}_5) \rightarrow \mathbb{Z}_5$ l'applicazione definita da $f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 3bc + 2ad$ per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_5)$. Si dimostri che f è multilineare alternante.

42.13. Sia $f: M_2(\mathbb{Z}_7) \rightarrow \mathbb{Z}_7$ l'applicazione definita da $f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 3bc + 2ad$ per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_7)$. Si dimostri che f non è multilineare alternante.

42.14. Per l'applicazione multilineare alternante dell'esercizio 42.12 si verifichi direttamente che si ha $f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = f \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix}$ per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_5)$, come asserito nel corollario 42.6.

§43. Altre proprietà del determinante

43.1 TEOREMA DI BINET. Se $A, B \in M_n(K)$, allora $\det(AB) = \det A \cdot \det B$.

Dimostrazione. Fissiamo una matrice $A \in M_n(K)$ e definiamo un'applicazione

$$f: M_n(K) \longrightarrow K$$

ponendo $f(X) = \det(AX)$ per ogni $X \in M_n(K)$. Si vede facilmente che f è un'applicazione multilineare alternante, e quindi per il corollario 42.6 si deve avere che $f(X) = f(I) \det X$ per ogni matrice $X \in M_n(K)$. In particolare $\det(AB) = f(B) = f(I) \det B = \det(AI) \det B = \det A \cdot \det B$. \square

43.2 PROPOSIZIONE. Se $A = (a_{ij})$ è una qualunque matrice quadrata di ordine n e B è la matrice quadrata di ordine n il cui elemento di posto (i, j) è $(-1)^{i+j} \det A_{ji}$ per ogni $i, j = 1, 2, \dots, n$, allora

$$AB = \det A \cdot I_n \quad e \quad BA = \det A \cdot I_n.$$

Dimostrazione. Sia $B = (b_{ij})$ la matrice $n \times n$ il cui elemento di posto (i, j) è $b_{ij} = (-1)^{i+j} \det A_{ji}$ per ogni $i, j = 1, 2, \dots, n$. Calcoliamo l'elemento c_{ij} di posto (i, j) nella matrice prodotto AB . Se $i = j$ si ha

$$c_{ii} = \sum_{k=1}^n a_{ik} b_{ki} = \sum_{k=1}^n a_{ik} (-1)^{k+i} \det A_{ik} = \sum_{k=1}^n (-1)^{i+k} a_{ik} \det A_{ik} = \det A$$

per l'uguaglianza (42.4). Supponiamo invece $i \neq j$. Sia A' la matrice ottenuta da A sostituendo la j -esima riga con la i -esima, cioè $A' = (a'_{\ell k})$, dove $a'_{\ell k} = a_{\ell k}$ per $\ell \neq j$, e $a'_{jk} = a_{ik}$. Dato che A' ha due righe uguali, si deve avere $\det A' = 0$ per la proposizione 42.8. D'altra parte sviluppando $\det A'$ rispetto alla j -esima riga, cioè applicando l'uguaglianza (42.4) alla matrice A' , si trova che

$$0 = \det A' = \sum_{k=1}^n (-1)^{j+k} a'_{jk} \det A'_{jk} = \sum_{k=1}^n (-1)^{j+k} a_{ik} \det A_{jk},$$

e quindi

$$c_{ij}^* = \sum_{k=1}^n a_{ik} b_{kj} = \sum_{k=1}^n a_{ik} (-1)^{k+j} \det A_{jk} = \sum_{k=1}^n (-1)^{j+k} a_{ik} \det A_{jk} = 0.$$

Pertanto $AB = \det A \cdot I_n$.

L'uguaglianza $BA = \det A \cdot I_n$ si dimostra analogamente usando le colonne invece che le righe, cioè con l'uguaglianza (42.6) invece che con la (42.4). \square

43.3 PROPOSIZIONE. Sia K un campo. Una matrice $A \in M_n(K)$ è invertibile se e solo se $\det A \neq 0$. In tal caso $A^{-1} \in M_n(K)$ è la matrice il cui elemento di posto (i, j) è $(\det A)^{-1} (-1)^{i+j} \det A_{ji}$ per ogni $i, j = 1, 2, \dots, n$.

Dimostrazione. Se la matrice $A \in M_n(K)$ è invertibile, cioè se esiste $A^{-1} \in M_n(K)$ tale che $AA^{-1} = I$, allora $1 = \det I = \det(AA^{-1}) = \det(A)\det(A^{-1})$ per il teorema di Binet, e quindi $\det A \neq 0$.

Supponiamo viceversa che $A \in M_n(K)$ sia una matrice con determinante diverso da zero. Denotiamo con $B = (b_{ij})$ la matrice $n \times n$ il cui elemento b_{ij} di posto (i, j) è $b_{ij} = (-1)^{i+j} \det A_{ji}$ per ogni $i, j = 1, 2, \dots, n$. Allora $(\det A)^{-1}B$, cioè la matrice ottenuta da B dividendo tutti gli elementi per $\det A$, è la matrice inversa A^{-1} di A . \square

Per calcolare l'inversa di una matrice A conviene procedere secondo i seguenti passi:

- (1) calcolare la matrice il cui elemento di posto (i, j) è $\det A_{ij}$ per ogni i, j ;
- (2) "cambiare i segni", cioè calcolare la matrice il cui elemento di posto (i, j) è

$$(-1)^{i+j} \det A_{ij};$$

- (3) trasporre;

- (4) dividere tutti gli elementi della matrice per $\det A$.

43.4 ESEMPIO. Calcoliamo l'inversa della matrice ad elementi reali

$$A = \begin{pmatrix} 1 & -1 & 5 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Osserviamo intanto che si ha $\det A = -2$, e quindi la matrice è invertibile. Cerchiamo la matrice il cui elemento di posto (i, j) è $\det A_{ij}$ per ogni i, j . Si ha

$$\det A_{11} = \begin{vmatrix} 2 & 0 \\ 0 & -1 \end{vmatrix} = -2, \quad \det A_{12} = \begin{vmatrix} 0 & 0 \\ 0 & -1 \end{vmatrix} = 0, \quad \text{ecc.}$$

In definitiva si trova che la matrice cercata è la matrice

$$(\det A_{ij})_{i,j} = \begin{pmatrix} -2 & 0 & 0 \\ 1 & -1 & 0 \\ -10 & 0 & 2 \end{pmatrix}.$$

Cambiando i segni degli elementi di posto (i, j) per i quali $(-1)^{i+j} = -1$ si trova che

$$((-1)^{i+j} \det A_{ij})_{i,j} = \begin{pmatrix} -2 & 0 & 0 \\ -1 & -1 & 0 \\ -10 & 0 & 2 \end{pmatrix}.$$

Trasponendo questa matrice si trova la matrice

$$\begin{pmatrix} -2 & -1 & -10 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Dividendo tutto per $\det A = -2$ si trova infine che

$$A^{-1} = \begin{pmatrix} 1 & 1/2 & 5 \\ 0 & 1/2 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \quad \square$$

43.5 TEOREMA (REGOLA DI CRAMER). *Un sistema di n equazioni lineari in n incognite*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

ha un'unica soluzione se e solo se $\det A \neq 0$, dove $A = (a_{ij})$ è la matrice incompleta del sistema. In tal caso l'unica soluzione (c_1, c_2, \dots, c_n) del sistema è data da $c_i = (\det A)^{-1} \det A'_i$, dove A'_i è la matrice $n \times n$ ottenuta da A sostituendo la i -esima colonna con la colonna dei termini noti del sistema.

Dimostrazione. Sappiamo già che il sistema ha un'unica soluzione se e solo se la sua matrice incompleta A è invertibile (teorema 41.1), e quindi se e solo se $\det A \neq 0$ (proposizione 43.3).

Supponiamo quindi che $\det A \neq 0$ e che $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ sia l'unica soluzione del

sistema. Sia A_i la i -esima colonna di A per ogni $i = 1, \dots, n$ e B la colonna dei termini noti, di modo che

$$A = (A_1 \ \dots \ A_n) \quad \text{e} \quad A'_i = (A_1 \ \dots \ A_{i-1} \ B \ A_{i+1} \ \dots \ A_n).$$

L'uguaglianza $AC = B$ si può riscrivere nella forma $A_1c_1 + \cdots + A_nc_n = B$, e quindi

$$\det A'_i = \det(A_1 \ \dots \ A_{i-1} \ A_1c_1 + \cdots + A_nc_n \ A_{i+1} \ \dots \ A_n)$$

$$= \sum_{k=1}^n \det(A_1 \ \dots \ A_{i-1} \ A_k \ A_{i+1} \ \dots \ A_n) \cdot c_k$$

per la multilinearità del determinante. Ora per $k = 1, \dots, i-1, i+1, \dots, n$ si ha $\det(A_1 \ \dots \ A_{i-1} \ A_k \ A_{i+1} \ \dots \ A_n) = 0$ per l'alternanza, e per $k = i$ si ha

$$\det(A_1 \ \dots \ A_{i-1} \ A_k \ A_{i+1} \ \dots \ A_n) = \det A.$$

Pertanto $\det A'_i = \det A \cdot c_i$. \square

Passiamo ad una altro argomento: il calcolo del rango di una matrice. A pagina 340 abbiamo visto un primo metodo per calcolare il rango di una matrice $m \times n$ data A . Il

metodo è il seguente. Si verifica se le colonne di A sono linearmente indipendenti. Se sono linearmente indipendenti, il rango di A è uguale al numero n di colonne di A . Se non sono linearmente indipendenti, si cancellano una ad una le colonne che dipendono dalle rimanenti, fino a restare con un insieme di colonne linearmente indipendenti che genera il sottospazio vettoriale di K^m generato dalle colonne di A . La cardinalità di questo insieme di colonne linearmente indipendenti è il rango di A .

Vediamo un secondo metodo. Un minore di una matrice $m \times n A$ è il determinante di una qualunque matrice quadrata ottenuta da A cancellando alcune righe e alcune colonne. L'ordine di un minore di A è l'ordine della matrice quadrata di cui il minore è il determinante. Quindi se A è una matrice $m \times n$, un minore di ordine t è il determinante di una matrice che si ottiene da A cancellando $m - t$ righe e $n - t$ colonne. Ovviamente deve essere $t \leq \min\{m, n\}$.

43.6 LEMMA. *Siano s un intero positivo e A una matrice di rango r . Allora A ha un minore non nullo di ordine s se e solo se $s \leq r$.*

Dimostrazione. Sia A una matrice $m \times n$ di rango r e sia $s \leq r$. Allora $A = (A_1 \dots A_n)$ ha s colonne linearmente indipendenti. Supponiamo che A_{j_1}, \dots, A_{j_s} siano s colonne linearmente indipendenti di A , dove $1 \leq j_1 < j_2 < \dots < j_s \leq n$. Ora le colonne di A sono elementi di K^m , che è uno spazio vettoriale di dimensione m avente come base la base canonica $\{e_1, \dots, e_m\}$ (qui, come abbiamo già fatto ripetutamente, pensiamo gli elementi di K^m come matrici colonna, ossia come matrici $m \times 1$). Per il teorema di sostituzione 36.16 si può ottenere un'altra base di K^m sostituendo s vettori e_i con gli s vettori A_{j_1}, \dots, A_{j_s} . Quindi per opportuni $i_1 < \dots < i_{m-s}$ si ha una base $\{A_{j_1}, \dots, A_{j_s}, e_{i_1}, \dots, e_{i_{m-s}}\}$ di K^m . Per il lemma 40.1 la matrice del cambio di base $P = (A_{j_1} \dots A_{j_s}, e_{i_1} \dots e_{i_{m-s}})$ è invertibile, e quindi $\det P \neq 0$ per la proposizione 43.3. Ma il determinante di P differisce al più per il segno dal determinante della matrice quadrata di ordine s ottenuto dalla matrice $(A_{j_1} \dots A_{j_s})$ cancellando le righe i_1 -esima, i_2 -esima, ..., i_{m-s} -esima. Quindi la matrice A ha un minore non nullo di ordine s .

Viceversa, supponiamo che $A = (A_1 \dots A_n)$ abbia un minore non nullo di ordine s . Supponiamo che un minore non nullo si ottenga, ad esempio, cancellando le righe i_1 -esima, i_2 -esima, ..., i_{m-s} -esima, e corrispondente alle colonne $A_{j_1}, A_{j_2}, \dots, A_{j_s}$, dove $i_1 < i_2 < \dots < i_{m-s}$ e $j_1 < j_2 < \dots < j_s$. Allora è non nullo il determinante della matrice $P = (A_{j_1} \dots A_{j_s}, e_{i_1} \dots e_{i_{m-s}})$. La matrice P è invertibile (proposizione 43.3), e quindi l'endomorfismo $f_P: K^m \rightarrow K^m$ definito da $f_P(U) = PU$ per ogni $U \in K^m$, dove K^m viene visto come l'insieme delle matrici colonna $m \times 1$, è un isomorfismo. In particolare i vettori $A_{j_1}, \dots, A_{j_s}, e_{i_1}, \dots, e_{i_{m-s}}$, immagini dei vettori della base e_1, \dots, e_m mediante l'isomorfismo f_P , formano una base di K^m . Ne segue che i vettori A_{j_1}, \dots, A_{j_s} sono linearmente indipendenti, e quindi A ha rango $\geq s$. \square

Dal lemma 43.6 si ottiene immediatamente la seguente proposizione.

43.7 PROPOSIZIONE. *Il rango di una matrice è il massimo intero s tale che la matrice abbia minori non nulli di ordine s .*

Tale proposizione fornisce immediatamente un ulteriore criterio (algoritmico) per calcolare il rango di una matrice: basta trovare il massimo intero s tale che la matrice abbia minori non nulli di ordine s .

Concludiamo questo §43 con un ulteriore corollario.

43.8 COROLLARIO. *Una matrice e la sua matrice trasposta hanno lo stesso rango. Quindi il rango di una matrice A è il massimo numero di righe linearmente indipendenti di A .*

Dimostrazione. Per la proposizione 42.7 una matrice e la sua matrice trasposta hanno gli stessi minori di ordine s per ogni intero positivo s . Il corollario segue pertanto immediatamente dalla proposizione 43.7. \square

Esercizi svolti

43.1. Siano V, W due spazi vettoriali sullo stesso campo K ed $f: V \rightarrow W$ un'applicazione lineare. Sia A la matrice associata ad f rispetto a una base di V e a una base di W . Si dimostri che f è un isomorfismo se e solo se $\det A \neq 0$.

Soluzione. Per il corollario 39.6 e l'esercizio 39.1 un'applicazione lineare $f: V \rightarrow W$ è un isomorfismo se e solo se la sua matrice associata A è invertibile. Ma A è invertibile se e solo se $\det A \neq 0$ (proposizione 43.3). \square

43.2. Sia $\{v_1, v_2, \dots, v_n\}$ una base di uno spazio vettoriale V su un campo K . Sia $A = (a_{ij})$ una matrice quadrata di ordine n ad elementi in K . Si dimostri che

$$\left\{ \sum_{i=1}^n a_{i1} v_i, \sum_{i=1}^n a_{i2} v_i, \dots, \sum_{i=1}^n a_{in} v_i \right\}$$

è una base di V se e solo se $\det A \neq 0$.

Soluzione. Sia $f: V \rightarrow V$ l'unica applicazione lineare tale che $f(v_j) = \sum_{i=1}^n a_{ij} v_i$ per ogni $j = 1, 2, \dots, n$. Per il lemma 38.3 l'insieme

$$\left\{ \sum_{i=1}^n a_{i1} v_i, \sum_{i=1}^n a_{i2} v_i, \dots, \sum_{i=1}^n a_{in} v_i \right\}$$

è una base di V se e solo se f è un isomorfismo. Per l'esercizio 43.1 l'applicazione lineare f è un isomorfismo se e solo se la sua matrice associata ha determinante $\neq 0$. Ma la matrice associata ad f rispetto alla base $\{v_1, v_2, \dots, v_n\}$ è proprio A . \square

Altri esercizi

43.3. Si dimostri che se A è una matrice quadrata di ordine n , allora $\det(-A) = (-1)^n \det A$.

43.4. Si dimostri che se A è una matrice quadrata di ordine n ad elementi reali e $A^* = -A$, allora o n è pari oppure $\det A = 0$.

43.5. Sia K un campo. Si dimostri che

$$\left\{ \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nn} \end{pmatrix} \right\} \text{ è una base di } K^n \text{ se e solo se } \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \neq 0.$$

43.6. Si calcoli il rango delle seguenti matrici ad elementi reali:

$$(a) \begin{pmatrix} 1 & 10 & 11 & 15 \\ 1 & 10 & 11 & 16 \end{pmatrix}; \quad (b) \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}; \quad (c) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 1 \\ -1 & 2 & 0 & 0 \end{pmatrix}; \quad (d) \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

43.7. Si dimostri che se A è una matrice invertibile, allora $\det(A^{-1}) = (\det A)^{-1}$.

43.8. Si dimostri che il sistema

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n \end{cases}$$

ha un'unica soluzione se e solo se il sistema

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \dots + a_{n1}x_n = b_1 \\ a_{12}x_1 + a_{22}x_2 + \dots + a_{n2}x_n = b_2 \\ \vdots \\ a_{1n}x_1 + a_{2n}x_2 + \dots + a_{nn}x_n = b_n \end{cases}$$

ha un'unica soluzione.

43.9. Per ogni $\lambda \in \mathbb{R}$ si consideri il sistema

$$\begin{cases} \lambda x + 2y + z = 0 \\ x + \lambda y + \lambda z = 0 \\ x + z = 1. \end{cases}$$

Per quali $\lambda \in \mathbb{R}$ il sistema ha soluzioni? Per quali $\lambda \in \mathbb{R}$ il sistema ha un'unica soluzione?

43.10. Con la regola di Cramer si determini per quali a, b, c, d, e, f il sistema

$$\begin{cases} ax + by + c = 0 \\ dx + ey + f = 0 \end{cases}$$

ha un'unica soluzione e si determini tale soluzione.

43.11. Con la regola di Cramer si determini se il sistema

$$\begin{cases} -x + 2y + z = 0 \\ x - y - z = 1 \\ x + z = 1. \end{cases}$$

ha un'unica soluzione e, in caso affermativo, si determini tale soluzione.

43.12. Sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}^4$ l'applicazione lineare tale che $f(1, 0, 0) = (1, 2, -1, 0)$, $f(0, 1, 0) = (-1, -2, 0, 5)$, $f(0, 0, 1) = (-1, -2, -1, 10)$. Si determini la dimensione di $\ker f$.

43.13. Siano K un campo, $n \geq 2$ un numero intero pari, $\{e_1, \dots, e_n\}$ la base canonica di K^n ed $f: K^n \rightarrow K^n$ l'applicazione lineare tale che $f(e_i) = \sum_{j=1}^i (-1)^j e_j$ per ogni $i = 1, 2, \dots, n$.

- (a) Si scriva la matrice A associata ad f rispetto alla base canonica $\{e_1, \dots, e_n\}$.
- (b) Si dimostri che $\det A = (-1)^{\frac{n}{2}}$.
- (c) Si dimostri che f è un automorfismo di K^n .

43.14. Si dica per quali valori di $\lambda \in \mathbb{Z}_5$ esiste ed è unico l'endomorfismo $\varphi_\lambda: \mathbb{Z}_5^3 \rightarrow \mathbb{Z}_5^3$ tale che

$$\begin{aligned} \varphi_\lambda(\lambda, 1, 0) &= (\lambda, 1, 0), \\ \varphi_\lambda(1, \lambda, 0) &= (0, 1, 0), \\ \varphi_\lambda(0, 0, 1) &= (0, 0, 1). \end{aligned}$$

Tra i $\lambda \in \mathbb{Z}_5$ per i quali l'endomorfismo φ_λ di \mathbb{Z}_5^3 esiste ed è unico, quali sono quelli per i quali φ_λ è un isomorfismo di spazi vettoriali?

43.15. Si calcolino le inverse delle matrici ad elementi reali

$$\begin{pmatrix} 2 & 1 & 0 \\ 3 & 4 & -1 \\ 5 & 6 & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix}.$$

43.16. Si calcoli l'inversa della matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. (Ovviamente l'inversa esiste se e solo se il determinante della matrice è $\neq 0$.)

43.17. Si risolva con la regola di Cramer il sistema

$$\begin{cases} x - 2y = 0 \\ x + y + z = 1 \\ 3y - z = 0. \end{cases}$$

43.18. Sia $K[x]$ l'anello dei polinomi in una indeterminata x a coefficienti in un campo K .

- (a) Dimostrare che ogni matrice $n \times n$ i cui elementi sono tutti polinomi appartenenti a $K[x]$ di grado ≤ 1 ha come determinante un polinomio di grado $\leq n$.
- (b) Dimostrare che ogni matrice $n \times n$ i cui elementi sono tutti polinomi appartenenti a $K[x]$ di grado ≤ 1 e con una riga tutta di elementi di K ha come determinante un polinomio di grado $\leq n-1$.

[In questo esercizio, a differenza di quanto abbiamo fatto fino ad ora, non stiamo considerando matrici ad elementi in un campo, ma matrici ad elementi nel dominio di integrità $K[x]$. Si potrebbe dimostrare che gran parte della teoria svolta fino ad ora si generalizza anche al caso della matrici ad elementi in un dominio di integrità R . Anche per queste matrici è possibile definire il determinante, che è un elemento di R , calcolarlo sviluppandolo rispetto a una riga o a una colonna, ecc.]

§44. Autovalori, autovettori

44.1 DEFINIZIONE. Siano K un campo, V uno spazio vettoriale su K , ed $f: V \rightarrow V$ un endomorfismo dello spazio vettoriale V . Un sottospazio vettoriale W di V si dice *invariante per f* se $f(W) \subseteq W$. \square

Ad esempio è facile dimostrare che se f è un qualunque endomorfismo di V , allora il sottospazio nullo $\{0\}$, il sottospazio improprio V , l'immagine $f(V)$ e il nucleo $\ker f$ sono sottospazi invarianti di V . È anche molto facile vedere che se f è la moltiplicazione per una costante, cioè è l'applicazione $f_\lambda: V \rightarrow V$ definita da $f_\lambda(x) = \lambda x$ per ogni $x \in V$ (qui λ è un elemento fissato di K), allora ogni sottospazio di V è invariante per f .

44.2 ESEMPIO. Siano K un campo, V uno spazio vettoriale su K , ed $f: V \rightarrow V$ un endomorfismo dello spazio vettoriale V . Siano v un elemento non nullo di V e W il sottospazio di dimensione 1 di V generato da v . Si dimostri per esercizio che W è invariante per f se e solo se esiste $\lambda \in K$ tale che $f(v) = \lambda v$. \square

Dato un endomorfismo f di V ci domandiamo se esistono vettori $v \in V$ ed elementi $\lambda \in K$ tali che $f(v) = \lambda v$. Cerchiamo cioè le soluzioni dell'equazione $f(v) = \lambda v$. Qui f è un endomorfismo fissato di V , mentre λ e v , elementi di K e V rispettivamente, sono le nostre "quantità da determinare". Si osservi intanto che $v = 0$ e $\lambda = \text{"elemento arbitrario di } K\text{"}$ sono sempre una soluzione dell'equazione in questione, in quanto $f(0) = \lambda 0$ per ogni $\lambda \in K$. Queste "soluzioni banali" sono quindi poco interessanti e vengono trascurati nella definizione che segue.

44.3 DEFINIZIONE. Siano V uno spazio vettoriale sul campo K ed f un endomorfismo di V . Siano $v \in V$, $v \neq 0$, e $\lambda \in K$. Se $f(v) = \lambda v$ diremo che λ è un *autovalore* di f (relativo all'autovettore v) e che v è un *autovettore* di f (relativo all'autovalore λ). \square

Questa terminologia si trasporta facilmente dagli endomorfismi alle matrici quadrate. Siano K un campo, $n \geq 1$ un intero e A una matrice $n \times n$. Ad A è associato l'endomorfismo $f_A: K^n \rightarrow K^n$ dello spazio vettoriale $K^n = M_{n \times 1}(K)$ definito da $f_A(v) = Av$ per ogni $v \in K^n$. Un sottospazio vettoriale W di K^n si dice *invariante per A* se $Aw \in W$ per ogni $w \in W$.

Equivalentemente un sottospazio W di K^n è invariante per A se e solo se $f_A(W) \subseteq W$. Chiameremo autovalori (autovettori) di A gli autovalori (autovettori) di f_A . Quindi:

44.4 DEFINIZIONE. Siano K un campo e A una matrice $n \times n$ ad elementi in K . Siano $v \in K^n$, $v \neq 0$, e $\lambda \in K$. Se $Av = \lambda v$ diremo che λ è un *autovalore* di A (relativo all'autovettore v) e che v è un *autovettore* di A (relativo all'autovalore λ). \square

44.5 ESEMPIO. Sia A una matrice $n \times n$ ad elementi in K . Si dimostri per esercizio che se λ e μ sono due autovalori di A relativi allo stesso autovettore, allora $\lambda = \mu$. \square

Fissiamo ora una matrice quadrata A di ordine n , un vettore non nullo $v \in K^n$ e un elemento $\lambda \in K$. Se I_n è la matrice identica $n \times n$, si ha $Av = \lambda v$ se e solo se $Av = (\lambda I_n)v$, cioè se e solo se $(A - \lambda I_n)v = 0$, vale a dire se e solo se v è una soluzione non nulla del sistema $(A - \lambda I_n)v = 0$. Se questo accade si dovrà avere in particolare $\det(A - \lambda I_n) = 0$. Viceversa, se $\det(A - \lambda I_n) = 0$, il sistema $(A - \lambda I_n)v = 0$ ha una soluzione $v \neq 0$. Abbiamo così dimostrato che

44.6 PROPOSIZIONE. *Sia A una matrice quadrata di ordine n ad elementi in un campo K e sia $\lambda \in K$. Allora λ è un autovalore di A se e solo se $\det(A - \lambda I_n) = 0$.*

Sia ora $K[x]$ l'anello dei polinomi in un'indeterminata x a coefficienti in K . Se $A = (a_{ij})$ è una matrice quadrata di ordine n , possiamo considerare la matrice $A - xI_n$, che è una matrice ad elementi in $K[x]$. Si osservi che si ha

$$A - xI_n = \begin{pmatrix} a_{11} - x & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} - x & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} - x & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} - x \end{pmatrix}.$$

Di questa matrice $A - xI_n$ ad elementi in $K[x]$ possiamo calcolare il determinante, che è ancora un elemento di $K[x]$. (In realtà la teoria che abbiamo sviluppato fino ad ora a proposito dei determinanti riguardava matrici e determinanti di matrici ad elementi in un campo K , mentre ora ci troviamo di fronte ad una matrice ad elementi in $K[x]$, che non è un campo ma solamente un dominio di integrità. Sarebbe interessante, e non particolarmente difficile, vedere quali delle proprietà vere per le matrici ad elementi in un campo restano vere per le matrici ad elementi in un dominio di integrità, ma non lo faremo qui. Ci limitiamo a dire che data una matrice ad elementi in $K[x]$ possiamo definire e calcolare il suo determinante con le stesse "formule" e gli stessi algoritmi usati nel caso di matrici ad elementi in un campo.)

Abbiamo così un polinomio $\det(A - xI_n) \in K[x]$, detto il *polinomio caratteristico* di A . Lo denoteremo con $p_A(x)$. La proposizione 44.6 dice che gli autovalori di A sono esattamente le radici del polinomio caratteristico $p_A(x)$ di A .

44.7 ESEMPIO. Sia $K = \mathbb{Z}_5$ l'anello delle classi resto modulo 5. Il polinomio caratteristico

della matrice

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

è

$$\begin{aligned} p_A(x) &= \det \begin{pmatrix} -x & 1 & 2 \\ 1 & -1-x & 2 \\ 0 & 0 & 3-x \end{pmatrix} = (3-x) \det \begin{pmatrix} -x & 1 \\ 1 & -1-x \end{pmatrix} \\ &= (3-x)(x(1+x)-1) = (3-x)(x^2+x-1). \end{aligned}$$

Quindi $p_A(x) = 0$ se e solo se $x = 3$ oppure $x^2 + x - 1 = 0$. Ora $x^2 + x - 1 = x^2 + 6x + 9 = (x+3)^2$. Ecco quindi che 3 e -3 , radici del polinomio caratteristico, sono gli autovalori di A .

Cerchiamo gli autovettori relativi all'autovalore 3. Sia $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}_5^3$. Si ha $Av = 3v$ se e solo se $(A - 3I_3)v = 0$, cioè se e solo se

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

Questo equivale a dire che (x_1, x_2, x_3) è soluzione del sistema

$$\begin{cases} -3x_1 + x_2 + 2x_3 = 0 \\ x_1 - 4x_2 + 2x_3 = 0. \end{cases}$$

Ricavando x_1 dalla seconda equazione e sostituendo nella prima si ha

$$\begin{cases} x_1 = 4x_2 - 2x_3 \\ -x_2 + 3x_3 = 0, \end{cases} \quad \text{da cui} \quad \begin{cases} x_2 = 3x_3 \\ x_1 = 12x_3 - 2x_3 = 0, \end{cases} \quad \text{cioè} \quad v = \begin{pmatrix} 0 \\ 3\alpha \\ \alpha \end{pmatrix}, \quad \alpha \in \mathbb{Z}_5.$$

Ecco quindi che gli autovettori di A relativi all'autovalore 3 sono i vettori del tipo $v = \begin{pmatrix} 0 \\ 3\alpha \\ \alpha \end{pmatrix}$ con $\alpha \in \mathbb{Z}_5$, $\alpha \neq 0$.

Cerchiamo gli autovettori relativi all'autovalore -3 . Sia $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}_5^3$. Si ha $Av = -3v$ se e solo se $(A + 3I_3)v = 0$, cioè se e solo se

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0,$$

vale a dire se e solo se (x_1, x_2, x_3) è soluzione del sistema

$$\begin{cases} 3x_1 + x_2 + 2x_3 = 0 \\ x_1 + 2x_2 + 2x_3 = 0 \\ x_3 = 0. \end{cases}$$

Da qui si ha, successivamente,

$$\begin{array}{l} \begin{cases} 3x_1 + x_2 = 0 \\ x_1 + 2x_2 = 0 \\ x_3 = 0, \end{cases} \quad \begin{cases} 3x_1 + x_2 = 0 \\ x_1 = 3x_2 \\ x_3 = 0, \end{cases} \quad \begin{cases} 9x_2 + x_2 = 0 \\ x_1 = 3x_2 \\ x_3 = 0. \end{cases} \end{array}$$

La prima equazione nell'ultimo sistema è un'identità. Le soluzioni sono quindi le terne $v = \begin{pmatrix} 3\alpha \\ \alpha \\ 0 \end{pmatrix}$ con $\alpha \in \mathbb{Z}_5$. Pertanto gli autovettori di A relativi all'autovalore -3 sono i vettori del tipo $v = \begin{pmatrix} 3\alpha \\ \alpha \\ 0 \end{pmatrix}$ con $\alpha \in \mathbb{Z}_5, \alpha \neq 0$. \square

44.8 PROPOSIZIONE. Siano $A = (a_{ij})$ una matrice $n \times n$ ad elementi in un campo K e $p_A(x)$ il suo polinomio caratteristico. Allora:

- (a) $p_A(x)$ è un polinomio a coefficienti in K di grado n .
- (b) Il coefficiente direttivo di $p_A(x)$, cioè il coefficiente di x^n , è $(-1)^n$.
- (c) Il coefficiente di x^{n-1} è $(-1)^{n-1} \operatorname{tr}(A)$.
- (d) Il termine noto di $p_A(x)$, cioè il coefficiente di x^0 , è $\det A$.

Dimostrazione. (d) Il termine noto di $p_A(x)$ è

$$p_A(0) = \det(A - 0I_n) = \det A.$$

Dimostriamo (a), (b) e (c) per induzione su $n \geq 1$. Il caso $n = 1$ è molto facile, perché per $n = 1$ si ha $A = (a)$, $p_A(x) = \det(A - xI_1) = a - x$ e si vede subito che (a), (b) e (c) valgono. Supponiamo quindi $n > 1$ e calcoliamo $p_A(x) = \det(A - xI_n)$. Sviluppando il determinante rispetto alla prima riga si ha

$$\det(A - x\overset{\circ}{I}_n) = (a_{11} - x)p_{A'}(x) - a_{12}\det A''_{12} + a_{13}\det A''_{13} + \cdots + (-1)^{1+n}a_{1n}\det A''_{1n},$$

dove A' è la matrice $(n-1) \times (n-1)$ che si ottiene da A cancellando la prima riga e la prima colonna, e A''_{1j} la matrice che si ottiene da $A - xI_n$ cancellando la prima riga e la j -esima colonna per ogni $j = 2, 3, \dots, n$. Ogni A''_{1j} , $j = 2, 3, \dots, n$, è una matrice $(n-1) \times (n-1)$ con una riga tutta di elementi di K , e quindi per l'esercizio 43.18(b) ogni $\det A''_{1j}$ è un polinomio di grado $\leq n-2$. Per l'ipotesi induttiva $p_{A'}(x)$ è un polinomio di grado $n-1$, quindi $(a_{11} - x)p_{A'}(x)$ è un polinomio di grado n . Ne segue che $p_A(x)$, somma del polinomio $(a_{11} - x)p_{A'}(x)$ di grado n e di polinomi di grado $\leq n-2$, è

un polinomio di grado n , che il coefficiente direttivo di $p_A(x)$ è il prodotto del coefficiente direttivo del polinomio $p_{A'}(x)$ per il coefficiente direttivo di $a_{11} - x$, e che il coefficiente di x^{n-1} nel polinomio $p_A(x)$ è

$$a_{11} \cdot (\text{coefficiente di } x^{n-1} \text{ in } p_{A'}(x)) + (-1) \cdot (\text{coefficiente di } x^{n-2} \text{ in } p_{A'}(x)).$$

Per l'ipotesi induttiva tale coefficiente è quindi

$$a_{11} \cdot (-1)^{n-1} + (-1) \cdot (-1)^{n-2} \operatorname{tr}(A') = (-1)^{n-1} \sum_{i=1}^n a_{ii} = (-1)^{n-1} \operatorname{tr}(A).$$

Infine il coefficiente direttivo di $p_A(x)$, prodotto del coefficiente direttivo del polinomio $p_{A'}(x)$ per il coefficiente direttivo di $a_{11} - x$, è $(-1)^{n-1} \cdot (-1) = (-1)^n$. \square

44.9 PROPOSIZIONE. *Siano K un campo, V uno spazio vettoriale su K ed f un endomorfismo di V . Siano $v_1, v_2, \dots, v_n \in V$ autovettori di f relativi ad autovalori $\lambda_1, \lambda_2, \dots, \lambda_n$ rispettivamente. Se $\lambda_1, \lambda_2, \dots, \lambda_n$ sono a due a due distinti, allora v_1, v_2, \dots, v_n sono linearmente indipendenti.*

Dimostrazione. Induzione su $n \geq 1$. Nel caso $n = 1$ non c'è nulla da dimostrare: dato che v_1 è un autovettore, si ha $v_1 \neq 0$, e quindi v_1 è linearmente indipendente.

Supponiamo $n > 1$. Siano $v_1, v_2, \dots, v_n \in V$ autovettori di f relativi agli autovalori $\lambda_1, \lambda_2, \dots, \lambda_n$ rispettivamente, dove $\lambda_1, \lambda_2, \dots, \lambda_n$ sono a due a due distinti. Per l'ipotesi induttiva v_1, v_2, \dots, v_{n-1} sono linearmente indipendenti. Sia $\sum_{i=1}^n \alpha_i v_i = 0_V$ una combinazione lineare nulla. Allora

$$0_V = f\left(\sum_{i=1}^n \alpha_i v_i\right) = \sum_{i=1}^n \alpha_i f(v_i) = \sum_{i=1}^n \alpha_i \lambda_i v_i$$

e

$$0_V = \lambda_n \cdot 0_V = \lambda_n \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n \alpha_i \lambda_n v_i.$$

Sottraendo membro a membro si ottiene $0_V = \sum_{i=1}^{n-1} \alpha_i (\lambda_i - \lambda_n) v_i$. Dall'ipotesi induttiva si deduce che $\alpha_i (\lambda_i - \lambda_n) = 0$ per ogni $i = 1, 2, \dots, n-1$. Dato che i λ_i sono a due a due distinti, si ha $\lambda_i - \lambda_n \neq 0$ per ogni $i = 1, 2, \dots, n-1$, e quindi $\alpha_i = 0$ per ogni $i = 1, 2, \dots, n-1$. Ne segue che $\alpha_n v_n = 0$. Ma v_n è un autovettore, quindi $v_n \neq 0$, da cui anche $\alpha_n = 0$. \square

Una matrice quadrata $A = (a_{ij})$ si dice una matrice *diagonale* se $a_{ij} = 0$ per ogni $i \neq j$. Una matrice quadrata A si dice *diagonalizzabile* se è simile ad una matrice diagonale, ossia se esiste una matrice invertibile P tale che $P^{-1}AP$ sia diagonale.

44.10 COROLLARIO. *Sia V uno spazio vettoriale di dimensione finita n e sia f un endomorfismo di V . Allora*

(a) *f ha al più n autovalori distinti.*

(b) Se f ha esattamente n autovalori distinti, allora V ha una base composta tutta di autovettori di f , e rispetto a tale base la matrice di f è una matrice diagonale.

Dimostrazione. (a) Gli autovalori di f sono gli zeri del polinomio caratteristico. Dato che il polinomio caratteristico ha grado n , esso può avere al più n zeri distinti.

(b) Se f ha esattamente n autovalori distinti $\lambda_1, \lambda_2, \dots, \lambda_n$, fissiamo per ogni $i = 1, 2, \dots, n$ un autovettore v_i relativo all'autovalore λ_i . Per la proposizione 44.9 i vettori dell'insieme $B = \{v_1, v_2, \dots, v_n\}$ sono linearmente indipendenti. Dato che V ha dimensione n , B è una base di V . Si ha $f(v_i) = \lambda_i v_i$ per ogni i , e quindi la matrice di f rispetto a questa base B è

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \lambda_n \end{pmatrix}. \quad \square$$

44.11 COROLLARIO. Se una matrice quadrata A di ordine n ha n autovalori distinti, allora A è diagonalizzabile.

Dimostrazione. Sia A una matrice quadrata di ordine n ad elementi in un campo K con n autovalori distinti. Consideriamo l'applicazione lineare $f_A: K^n \rightarrow K^n$, $v \mapsto Av$. Allora f_A ha n autovalori distinti. Per il corollario precedente K^n ha una base B composta tutta di autovettori di f_A , e rispetto a tale base B la matrice di f_A è una matrice diagonale D . Dato che la matrice associata ad f_A rispetto alla base canonica di K^n è A e la matrice associata ad f_A rispetto alla base B è D , ne segue che A e D sono simili. Quindi A è diagonalizzabile. \square

44.12 COROLLARIO. Sia V uno spazio vettoriale su un campo K e sia f un endomorfismo di V . Se ogni vettore non nullo $v \in V$ è un autovettore di V , allora esiste $\lambda \in K$ tale che $f(v) = \lambda v$ per ogni $v \in V$.

Dimostrazione. Per ogni vettore non nullo $v \in V$ sia $\lambda_v \in K$ tale che $f(v) = \lambda_v v$. Basta dimostrare che fissati $v, w \in V$, $v, w \neq 0$, si ha $\lambda_v = \lambda_w$. Se $v + w = 0$, allora $\lambda_v v = f(v) = f(-w) = -f(w) = -\lambda_w w = \lambda_v v$, da cui $\lambda_v = \lambda_w$. Supponiamo $v + w \neq 0$. Si ha $\lambda_v v + \lambda_w w = f(v) + f(w) = f(v+w) = \lambda_{v+w}(v+w)$. Da $\lambda_v v + \lambda_w w = \lambda_{v+w}(v+w)$ segue che $(\lambda_v - \lambda_{v+w})v + (\lambda_w - \lambda_{v+w})w = 0$. Se per assurdo fosse $\lambda_v \neq \lambda_w$, allora per la proposizione 44.9 i vettori v e w sarebbero linearmente indipendenti, e quindi si avrebbe $\lambda_v - \lambda_{v+w} = 0$ e $\lambda_w - \lambda_{v+w} = 0$. Quindi $\lambda_v = \lambda_{v+w} = \lambda_w$, assurdo. Pertanto deve essere $\lambda_v = \lambda_w$. \square

44.13 TEOREMA DI HAMILTON-CAYLEY. Se A è una matrice quadrata ad elementi in un campo K e $p_A(x)$ è il suo polinomio caratteristico, allora $p_A(A) = 0$.

Dimostrazione. Per ogni $i, j = 1, 2, \dots, n$ sia A'_{ij} la matrice che si ottiene da $A - xI_n$ can-

cellando la i -esima riga e la j -esima colonna, e sia B la matrice quadrata di ordine n il cui elemento di posto (i, j) è $(-1)^{i+j} \det A'_{ji}$ per ogni i, j . Per la proposizione 43.2 si ha quindi

$$(44.1) \quad (A - xI_n)B = p_A(x) \cdot I_n.$$

Ogni A'_{ji} è una matrice $(n-1) \times (n-1)$ i cui elementi sono tutti polinomi appartenenti a $K[x]$ di grado ≤ 1 , e quindi per l'esercizio 43.18(a) ogni $\det A'_{ji}$ è un polinomio di grado $\leq n-1$. Quindi la matrice B si può scrivere nella forma $B = B_0 + B_1x + \cdots + B_{n-2}x^{n-2} + B_{n-1}x^{n-1}$ per opportune matrici $B_i \in M_n(K)$, ossia B si può vedere come un polinomio nella indeterminata x a coefficienti in $M_n(K)$. D'altro canto $p_A(x)$ è un polinomio di grado n a coefficienti in K , e quindi si può scrivere nella forma $p_A(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$. Pertanto l'uguaglianza (44.1) diventa

$$\begin{aligned} (A - xI_n)(B_0 + B_1x + \cdots + B_{n-2}x^{n-2} + B_{n-1}x^{n-1}) \\ = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n) \cdot I_n. \end{aligned}$$

Confrontando in questa uguaglianza i coefficienti di x^i si vede che, per $i = 0$, $AB_0 = a_0I_n$, $AB_i - B_{i-1} = a_iI_n$ per ogni $i = 1, 2, \dots, n-1$, e infine $-B_{n-1} = a_nI_n$. Ma allora

$$\begin{aligned} p_A(A) &= I_n a_0 + \sum_{i=1}^{n-1} A^i a_i + A^n a_n = AB_0 + \sum_{i=1}^{n-1} A^i (AB_i - B_{i-1}) + A^n (-B_{n-1}) \\ &= AB_0 + \sum_{i=1}^{n-1} A^{i+1} B_i - \sum_{i=1}^{n-1} A^i B_{i-1} + A^n (-B_{n-1}) = \sum_{i=0}^{n-1} A^{i+1} B_i - \sum_{i=1}^n A^i B_{i-1}. \end{aligned}$$

Dato che per ogni $i = 1, 2, \dots, n$ l' i -esimo addendo $A^i B_{i-1}$ nell'ultima somma coincide con l'addendo $A^i B_{i-1}$ indicato da $i-1$ nella somma precedente, si ricava quindi che $p_A(A) = 0$. \square

44.14 ESEMPIO. Siano K il campo dei numeri reali ed $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$. Il polinomio

caratteristico di A è $p_A(x) = \det(A - xI_3) = (1-x)^3$. Il teorema di Hamilton-Cayley dice che se calcolo il valore di questo polinomio $p_A(x)$ nell'anello delle matrici $M_3(K)$ sostituendo A al posto di x si ottiene 0. Calcolare il valore di $p_A(x) = (1-x)^3$ nell'anello $M_3(K)$ vuol dire che come 1 e 0 si devono intendere l'1 e lo 0 dell'anello $M_3(K)$, ossia la matrice identica I_3 e la matrice nulla 3×3 . Si ha infatti

$$p_A(A) = (I_3 - A)^3 = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & -1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \quad \square$$

Esercizi svolti

44.1. Siano K un campo, V uno spazio vettoriale su K ed f un endomorfismo di V .

- (a) Si dimostri che se $\lambda \in K$, allora $V_\lambda = \{v \in V \mid f(v) = \lambda v\}$ è un sottospazio vettoriale di V . Si osservi che se λ non è un autovalore di f , allora $V_\lambda = \{0\}$. Se invece λ è un autovalore di f , allora V_λ è l'insieme degli autovettori di f relativi all'autovalore λ più il vettore nullo, e quindi in particolare $V_\lambda \neq \{0\}$. In tal caso V_λ si dice l'*autospazio* di f relativo all'autovalore λ .
- (b) Si dimostri che se $\lambda, \mu \in K$ e $\lambda \neq \mu$, allora $V_\lambda \cap V_\mu = \{0\}$.

Soluzione. (a) Si ha $f(0_V) = 0_V = \lambda 0_V$, e quindi $0_V \in V_\lambda$. In particolare $V_\lambda \neq \emptyset$. Se $v, w \in V_\lambda$, allora $f(v - w) = f(v) - f(w) = \lambda v - \lambda w = \lambda(v - w)$, e pertanto $v - w \in V_\lambda$. Se poi $\alpha \in K$ e $v \in V_\lambda$, allora $f(\alpha v) = \alpha f(v) = \alpha(\lambda v) = \lambda(\alpha v)$, e quindi $\alpha v \in V_\lambda$. Questo dimostra che V_λ è un sottospazio vettoriale di V .

(b) Certamente $V_\lambda \cap V_\mu \supseteq \{0\}$. Viceversa sia $v \in V_\lambda \cap V_\mu$. Allora $f(v) = \lambda v$ e $f(v) = \mu v$, e quindi $(\lambda - \mu)v = \lambda v - \mu v = f(v) - f(v) = 0$. Da $\lambda \neq \mu$ segue che $\lambda - \mu \neq 0$, e pertanto $v = 0$ per il lemma 34.6(d). Questo dimostra che $V_\lambda \cap V_\mu \subseteq \{0\}$. \square

44.2. Siano K un campo, V uno spazio vettoriale su K ed f un endomorfismo di V . Siano $\lambda_1, \lambda_2, \dots, \lambda_n$ autovalori distinti di f , e per ogni $i = 1, 2, \dots, n$ sia $V_i = \{v \in V \mid f(v) = \lambda_i v\}$ l'autospazio di f relativo all'autovalore λ_i (esercizio precedente). Si dimostri che la somma $V_1 + \dots + V_n$ è diretta, ossia che $V_1 + \dots + V_n = V_1 \oplus \dots \oplus V_n$.

Soluzione. Per l'esercizio 37.10 dire che la somma $V_1 + \dots + V_n$ è diretta equivale a dire che $V_i \cap (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_n) = \{0\}$ per ogni $i = 1, 2, \dots, n$. Certamente $V_i \cap (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_n) \supseteq \{0\}$. Viceversa, per dimostrare che $V_i \cap (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_n) \subseteq \{0\}$ ragioniamo per assurdo e supponiamo che esista un $v_i \in V_i \cap (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_n)$, $v_i \neq 0$. Allora $v_i \in V_i$ e $v_i = v_1 + \dots + v_{i-1} + v_{i+1} + \dots + v_n$ per opportuni $v_j \in V_j$. In particolare i v_j sono o 0 oppure sono autovalori relativi all'autovalore λ_j . Considerando la combinazione lineare $v_1 + \dots + v_{i-1} - v_i + v_{i+1} + \dots + v_n = 0$, per la proposizione 44.9 si ha che $v_1 = \dots = v_{i-1} = v_i = v_{i+1} = \dots = v_n = 0$, contraddizione. \square

44.3. Siano V uno spazio vettoriale di dimensione finita su un campo K ed f un endomorfismo di V . Si dimostri che 0 è autovalore di f se e solo se f non è un automorfismo.

Soluzione. Si ha che 0 è un autovalore di f se e solo se esiste $v \in V$, $v \neq 0$, tale che $f(v) = 0 \cdot v$, cioè se e solo se esiste $v \in V$, $v \neq 0$ tale che $f(v) = 0$. Questo equivale a dire che $\ker f \neq \{0\}$, ossia che f non è iniettiva. Ma per il corollario 38.7, l'applicazione lineare f non è iniettiva se e solo se non è un automorfismo. \square

44.4. Siano $V \neq \{0\}$ uno spazio vettoriale di dimensione finita su un campo K ed f un endomorfismo di V tale che $f^m = 0$ per qualche $m \geq 1$.

- (a) Si dimostri che 0 è un autovalore di f .
 (b) Si dimostri che 0 è l'unico autovalore di f .

Soluzione. (a) Per l'esercizio 44.3, 0 è autovalore di f se e solo se f non è un automorfismo. Quindi basta far vedere che f non è un automorfismo. Ma se f fosse un automorfismo, allora f^t sarebbe un automorfismo per ogni $t \geq 1$. Ma dato che $f^m = 0$ per un opportuno $m \geq 1$, se ne dedurrebbe che 0 è un automorfismo di V , e quindi che $V = \{0\}$, contraddizione. Questa contraddizione dimostra che f non è un automorfismo.

(b) Sia $\lambda \in K$ un arbitrario autovalore di f . Allora esiste $v \in V$, $v \neq 0$, tale che $f(v) = \lambda v$. Ne segue facilmente per induzione che $f^i(v) = \lambda^i v$ per ogni $i \geq 1$, in quanto $f^{i+1}(v) = f(f^i(v)) = f(\lambda^i v) = \lambda^i f(v) = \lambda^i \lambda v = \lambda^{i+1} v$. In particolare $0 = f^m(v) = \lambda^m v$. Dato che $v \neq 0$, si deve

avere che $\lambda^m = 0$, e quindi, essendo K un dominio di integrità, si deve avere $\lambda = 0$. Abbiamo così dimostrato che 0 è l'unico autovalore di f . \square

Altri esercizi

44.5. Sia $K = \mathbb{Q}$, il campo dei numeri razionali. Determinare autovettori e autovalori della matrice

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

44.6. Sia $K = \mathbb{C}$, il campo dei numeri complessi. Determinare autovettori e autovalori della matrice

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & -1 & 0 \\ 2 & -1 & 1 \end{pmatrix}.$$

44.7. Per ogni $\lambda \in \mathbb{Z}_3$ si consideri la matrice

$$A(\lambda) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \lambda - 1 & \lambda^2 + \lambda - 1 & 0 & 0 \\ (\lambda - 1)^2 & (\lambda - 1)^3 & \lambda & 0 \\ \lambda & \lambda - 1 & \lambda - 2 & \lambda \end{pmatrix}.$$

- (a) Si calcoli, al variare di $\lambda \in \mathbb{Z}_3$, il rango della matrice $A(\lambda)$.
- (b) Si calcoli, al variare di $\lambda \in \mathbb{Z}_3$, il polinomio caratteristico della matrice $A(\lambda)$.
- (c) Si calcolino, al variare di $\lambda \in \mathbb{Z}_3$, gli autovalori della matrice $A(\lambda)$.

44.8. Si dimostri che se A e B sono due matrici simili, allora A e B hanno la stessa traccia, lo stesso determinante, lo stesso polinomio caratteristico e gli stessi autovalori.

44.9. Supponiamo che A sia una matrice quadrata diagonalizzabile, di modo che esiste una matrice

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

simile ad A . Si determinino la traccia, il determinante, e gli autovalori di A .

44.10. Siano V uno spazio vettoriale di dimensione finita su un campo K ed $f: V \rightarrow V$ un'applicazione lineare. Siano A e B le matrici associate ad f rispetto a due basi distinte di V .

- (a) Si dimostri che se A è una matrice scalare, cioè del tipo λI con $\lambda \in K$, allora $A = B$.
- (b) Si deduca da (a) che se A è una matrice scalare, allora l'unica matrice simile ad A è A stessa.
- (c) Si determinino gli autovalori e gli autovettori della seguente matrice a coefficienti in \mathbb{R} :

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

(d) Si dimostri che C non è diagonalizzabile.

44.11. Si dica se la matrice $A = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$ è diagonalizzabile.

44.12. Si dimostri che le matrici a elementi reali

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

sono simili trovando prima gli autovalori di B e poi ragionando come nella dimostrazione del corollario 44.10(b).

44.13. Si consideri la matrice

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

(a) Si provi che A è diagonalizzabile in \mathbb{C} .

(b) Si provi che A non è diagonalizzabile in \mathbb{R} .

44.14. Si consideri la matrice

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

ad elementi reali e sia $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare la cui matrice associata rispetto alla base canonica $\{e_1, e_2, e_3\}$ di \mathbb{R}^3 è A .

(a) Calcolare gli autovalori e gli autovettori di A .

(b) Per ogni autovalore λ di A si calcoli la dimensione dell'autospazio V_λ relativo a λ (vedi esercizio 44.1).

(c) Si dimostri che se $\lambda_1, \lambda_2, \dots, \lambda_n$ sono gli autovalori di A , allora $\mathbb{R}^3 = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_n}$.

(d) Si dimostri che la matrice A è diagonalizzabile e si determini una base $B = \{v_1, v_2, v_3\}$ di \mathbb{R}^3 tutta costituita di autovettori.

(e) Si scriva la matrice associata ad f rispetto alla base B .

(f) Per ogni intero $n \geq 0$ si scriva la matrice associata ad $f^n: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ rispetto alla base B .

44.15. Siano V uno spazio vettoriale ed f un automorfismo di V . Si dimostri che se λ è un autovalore di f , allora λ^{-1} è un autovalore di f^{-1} .

44.16. Si dimostri che una matrice quadrata a elementi in un campo e la sua matrice trasposta hanno lo stesso polinomio caratteristico e gli stessi autovalori. Hanno anche gli stessi autovettori?

44.17. Siano A, B matrici quadrate ad elementi in un campo K e sia $f(x) \in K[x]$ un polinomio. Si dimostri che se A e B sono simili, allora $f(A)$ e $f(B)$ sono simili.

44.18. Si dimostri che se A è una matrice invertibile $n \times n$ ad elementi in un campo K , allora esiste un polinomio $f \in K[x]$ di grado $\leq n-1$ tale che $A^{-1} = f(A)$. [Suggerimento: usare il teorema di Hamilton-Cayley.]

Capitolo 7

ESTENSIONI DI CAMPI

§45. Estensioni di campi

In questo §45 i simboli K ed F denotano campi e K è sottocampo (cioè sottoanello che è anche campo) di F . Diremo in tal caso che F è *estensione* di K . Ad esempio \mathbb{C} è estensione di \mathbb{R} ed \mathbb{R} è estensione di \mathbb{Q} .

Sia F un'estensione di K , e sia $\alpha \in F$. Si noti che se R_λ è un sottoanello di F per ogni $\lambda \in \Lambda$, allora $\bigcap_{\lambda \in \Lambda} R_\lambda$ è un sottoanello di F . In particolare l'intersezione di tutti i sottoanelli di F che contengono $K \cup \{\alpha\}$ è un sottoanello di F , ed è il più piccolo sottoanello di F che contiene $K \cup \{\alpha\}$. Lo chiameremo il sottoanello di F generato da $K \cup \{\alpha\}$, e lo denoteremo con $K[\alpha]$.

45.1 LEMMA. *Se K ed F sono campi, F è un'estensione di K ed $\alpha \in F$, allora*

$$K[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_t\alpha^t \mid t \in \mathbb{N}, a_0, a_1, \dots, a_t \in K\}.$$

Dimostrazione. Sia $R = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_t\alpha^t \mid t \in \mathbb{N}, a_0, a_1, \dots, a_t \in K\}$. Si deve dimostrare che $R = K[\alpha]$, cioè che R è il più piccolo sottoanello di F che contiene $K \cup \{\alpha\}$. Si deve pertanto far vedere che: (i) R è sottoanello di F ; (ii) $R \supseteq K \cup \{\alpha\}$; (iii) se S è sottoanello di F che contiene $K \cup \{\alpha\}$, allora $S \supseteq R$. La (i) e la (ii) sono di verifica immediata. Per dimostrare la (iii) fissiamo un sottoanello S di F che contiene $K \cup \{\alpha\}$, e prendiamo un elemento $r \in R$. Allora si ha $r = a_0 + a_1\alpha + \cdots + a_t\alpha^t$ per opportuni $a_i \in K$. Dato che $K \cup \{\alpha\} \subseteq S$, ne segue che a_0, a_1, \dots, a_t e α appartengono a S , ed essendo S un anello si ha che $r = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_t\alpha^t \in S$. Questo dimostra che $S \supseteq R$. \square

Sia sempre F un'estensione di K e $\alpha \in F$. Per il teorema 26.1 (proprietà universale dell'anello dei polinomi) esiste un unico omomorfismo d'anelli $\varphi_\alpha: K[x] \rightarrow F$ tale che $\varphi_\alpha(a) = a$ per ogni $a \in K$ e $\varphi_\alpha(x) = \alpha$. L'omomorfismo φ_α è definito da $\varphi_\alpha(f) = f(\alpha)$ per ogni $f \in K[x]$. L'immagine di φ_α è proprio il sottoanello $K[\alpha]$ di F , e il suo nucleo $\ker \varphi_\alpha = \{f \in K[x] \mid f(\alpha) = 0\}$ è l'insieme dei polinomi di $K[x]$ che hanno α come radice.

Manteniamo la stessa notazione, ossia F è un'estensione di K e $\alpha \in F$. Posso presentarsi due casi:

(1) Non esiste alcun polinomio $f \in K[x]$, $f \neq 0$, tale che $f(\alpha) = 0$. In tal caso si dice che $\alpha \in F$ è *trascendente* su K . Equivalentemente α è trascendente su K se e solo se per ogni $n \in \mathbb{N}$ e per ogni $a_0, a_1, \dots, a_n \in K$, se $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$, allora $a_0 = a_1 = \dots = a_n = 0$. Già sappiamo che F è K -spazio vettoriale (esempio 34.4). L'elemento $\alpha \in F$ è trascendente su K se e solo se gli elementi $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^n$ del K -spazio vettoriale F sono linearmente indipendenti per ogni $n \in \mathbb{N}$.

(2) Esiste almeno un polinomio $f \in K[x]$, $f \neq 0$, tale che $f(\alpha) = 0$. In tal caso si dice che $\alpha \in F$ è *algebrico* su K . Equivalentemente α è algebrico su K se e solo se esistono $n \in \mathbb{N}$ e $a_0, a_1, \dots, a_n \in K$ non tutti nulli tali che $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$.

Studiamo separatamente i due casi.

Caso trascendente. Se α è trascendente su K , il polinomio nullo è l'unico polinomio $f \in K[x]$ tale che $f(\alpha) = 0$. Equivalentemente $\ker \varphi_\alpha = \{0\}$, cioè l'omomorfismo $\varphi_\alpha: K[x] \rightarrow F$ è iniettivo. Dato che $K[\alpha]$ è l'immagine di φ_α se ne deduce che gli anelli $K[x]$ e $K[\alpha]$ sono isomorfi. Ad esempio i numeri reali $\pi = 3,14\dots$ ed $e = 2,71\dots$ sono trascendenti su \mathbb{Q} . Quindi non esistono numeri razionali non tutti nulli q_0, q_1, \dots, q_n tali che $q_0 + q_1\pi + q_2\pi^2 + \dots + q_n\pi^n = 0$ e similmente per e . Le dimostrazioni della trascendenza di π ed e su \mathbb{Q} , due successi della matematica del XIX secolo, sono dovute rispettivamente a Lindemann (1822) e a Hermite (1873).

Caso algebrico. Diamo alcuni esempi. I numeri reali $\sqrt{2}$ e $\sqrt[3]{2}$ sono algebrici su \mathbb{Q} perché sono rispettivamente radici dei polinomi $x^2 - 2$ e $x^3 - 2 \in \mathbb{Q}[x]$. Il numero complesso i è algebrico su \mathbb{R} perché è radice di $x^2 + 1 \in \mathbb{R}[x]$. Naturalmente π ed e sono algebrici su \mathbb{R} perché sono radici di $x - \pi$ e $x - e \in \mathbb{R}[x]$.

45.2 TEOREMA. Siano K un campo, F un'estensione di K , $\alpha \in F$ un elemento algebrico su K . Sia $f \in K[x]$ un polinomio monico di grado minimo tra i polinomi per i quali $f(\alpha) = 0$; sia n tale grado minimo. Allora

- (a) f è unico;
- (b) f è irriducibile in $K[x]$;
- (c) $K[\alpha]$ è un campo isomorfo a $K[x]/(f)$;
- (d) se $g \in K[x]$ si ha $g(\alpha) = 0$ se e solo se $f \mid g$ in $K[x]$;
- (e) $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ è una base del K -spazio vettoriale $K[\alpha]$.

Dimostrazione. Supponiamo che f_1 e f_2 siano entrambi polinomi monici di grado minimo tra i polinomi per i quali $f(\alpha) = 0$. In altre parole f_1 e f_2 sono due polinomi monici con $f_1(\alpha) = f_2(\alpha) = 0$, $n = \delta(f_1) = \delta(f_2)$, e $g(\alpha) \neq 0$ per ogni polinomio monico g di grado $< n$. Supponiamo per assurdo $f_1 \neq f_2$. Allora $f_1 - f_2$ è un polinomio non nullo di grado $< n$ e $(f_1 - f_2)(\alpha) = 0$. Moltiplicando $f_1 - f_2$ per l'inverso del suo coefficiente direttivo si ottiene un polinomio monico g di grado $\delta(g) = \delta(f_1 - f_2) < n$ tale che $g(\alpha) = 0$. Ciò contraddice la minimalità di n . Questo dimostra (a), cioè che il polinomio f con le proprietà richieste è unico.

Se f fosse riducibile in $K[x]$, allora $f = gh$ con $g, h \in K[x]$, g, h monici di grado $< n$. Allora $0 = f(\alpha) = g(\alpha)h(\alpha)$. Dato che F è un dominio di integrità, si deve avere allora o $g(\alpha) = 0$ oppure $h(\alpha) = 0$. In entrambi i casi si contraddice la minimalità di n . Questo dimostra (b).

Consideriamo ora l'omomorfismo $\varphi_\alpha: K[x] \rightarrow F$ definito da $\varphi_\alpha(g) = g(\alpha)$ per ogni $g \in K[x]$. L'immagine di φ_α è $K[\alpha]$, il suo nucleo è $\ker \varphi_\alpha = \{g \in K[x] \mid g(\alpha) = 0\}$. Dato che α è algebrico su K , $\ker \varphi_\alpha \neq \{0\}$. Per il teorema 28.3 l'ideale $\ker \varphi_\alpha$ è principale, cioè $\ker \varphi_\alpha = (h)$ per un opportuno $h \in K[x]$, $h \neq 0$. Quindi $\{g \in K[x] \mid g(\alpha) = 0\} = \{h\ell \mid \ell \in K[x]\}$ e pertanto in questo ideale l'unico polinomio monico f di grado minimo è $f = ha_n^{-1}$ dove a_n è il coefficiente direttivo di h . In particolare f è associato ad h , e quindi $\ker \varphi_\alpha = (f)$. Quindi $K[x]/(f) = K[x]/\ker \varphi_\alpha \cong \varphi_\alpha(K[x]) = K[\alpha]$. In (b) si è visto che $f \in K[x]$ è irriducibile. Ma allora (f) è massimale (proposizione 28.9), e quindi $K[x]/(f)$ è un campo (teorema 27.22(b)). Si è così provata l'affermazione (c).

Poi $\{g \in K[x] \mid g(\alpha) = 0\} = \ker \varphi_\alpha = (f) = \{g \in K[x] \mid f \mid g \text{ in } K[x]\}$, e quindi (d) vale.

Mostriamo che $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ genera $K[\alpha]$. Sia β un elemento di $K[\alpha]$. Allora $\beta = g(\alpha)$ per qualche $g \in K[x]$. Dividendo g per f si ha $g = qf + r$ con $q, r \in K[x]$ ed r di grado $< n$. Quindi $\beta = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha)$, vale a dire β si scrive nella forma $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$. Questo dimostra che $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ genera il K -spazio vettoriale $K[\alpha]$. Mostriamo che $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ sono linearmente indipendenti su K . Supponiamo per assurdo che $a_0 \cdot 1 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} = 0$ sia una combinazione lineare con gli $a_i \in K$ non tutti nulli. Posto $g = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in K[x]$ si ha che $g(\alpha) = 0$, e quindi $f \mid g$ in $K[x]$ per la (d). Ma f ha grado n e g ha grado $< n$, e pertanto da $f \mid g$ segue che $g = 0$, ossia $a_0 = a_1 = \dots = a_{n-1} = 0$. Questo mostra che $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ sono linearmente indipendenti su K , e conclude la dimostrazione di (e). \square

Se K è un campo e α è un elemento algebrico su K , il polinomio del teorema 45.2, cioè il polinomio monico $f \in K[x]$ di grado minimo tra i polinomi per i quali $f(\alpha) = 0$, si dice il *polinomio minimo di α su K* e il grado di f si dice il *grado di α su K* . Per il teorema 45.2 il polinomio minimo di α su K è polinomio monico irriducibile che divide tutti i polinomi di cui α è radice.

45.3 TEOREMA. *Sia K un campo, sia $f \in K[x]$ un polinomio irriducibile e sia $K' = K[x]/(f)$. Allora K' è un campo, l'applicazione $\varepsilon: K \rightarrow K'$ definita da $\varepsilon(a) = a + (f)$ per ogni $a \in K$ è un omomorfismo iniettivo di anelli, e identificando gli elementi di K con le loro immagini secondo ε , cioè considerando K' estensione di K tramite ε , l'elemento $x + (f)$ di K' è una radice del polinomio $f \in K[x]$.*

Dimostrazione. Dato che f è un elemento irriducibile di $K[x]$, l'ideale (f) è massimale (proposizione 28.9) e quindi $K' = K[x]/(f)$ è un campo.

L'applicazione $\varepsilon: K \rightarrow K'$, $\varepsilon(a) = a + (f)$ per ogni $a \in K$, è ovviamente un omomorfismo di anelli. Inoltre $\ker \varepsilon \trianglelefteq K$, e quindi, essendo K un campo, $\ker \varepsilon = \{0\}$ oppure $\ker \varepsilon = K$ (lemma 27.21). Se fosse $\ker \varepsilon = K$, allora $1 + (f) = \varepsilon(1) = 0 + (f)$ e quindi

$1 \in (f)$, da cui $1 = fg$ per un $g \in K[x]$ opportuno, vale a dire f sarebbe invertibile in $K[x]$, assurdo perché f è irriducibile. Pertanto $\ker \varepsilon = \{0\}$, cioè ε è iniettivo.

Abbiamo così dimostrato che $\varepsilon: K \rightarrow K'$ è un omomorfismo iniettivo, e quindi $\varepsilon(K)$ è un sottoanello di K' isomorfo a K . Possiamo quindi identificare ogni elemento $a \in K$ con il corrispondente elemento $\varepsilon(a) = a + (f) \in K' = K[x]/(f)$. Con tale identificazione ogni elemento di K è un elemento di K' , e K' è un'estensione di K .

Mostriamo che $x + (f) \in K'$ è una radice di $f \in K[x]$. Se

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

$a_i \in K$, allora

$$\begin{aligned} f(x + (f)) &= a_0 + a_1(x + (f)) + a_2(x + (f))^2 + \cdots + a_n(x + (f))^n \\ &= (a_0 + (f)) + (a_1 + (f))(x + (f)) + (a_2 + (f))(x^2 + (f)) + \cdots \\ &\quad + (a_n + (f))(x^n + (f)) \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + (f) = f + (f) = (f) = 0_{K'}. \end{aligned}$$

Quindi $x + (f)$ è radice di f . \square

Esercizi svolti

- 45.1. (a) L'anello $\mathbb{Q}[x]/(2x^2 - 3x - 1)$ è un campo? Qual è l'inverso di $1 + 2x + (2x^2 - 3x - 1)$?
 (b) L'anello $\mathbb{Z}_7/(2x^2 - 3x - 1)$ è un campo? Qual è l'inverso di $1 + 2x + (2x^2 - 3x - 1)$?

Soluzione. (a) L'anello $\mathbb{Q}[x]/(2x^2 - 3x - 1)$ è un campo se e solo se l'ideale $(2x^2 - 3x - 1)$ di $\mathbb{Q}[x]$ è massimale (teorema 27.22), e quindi se e solo se l'elemento $2x^2 - 3x - 1$ di $\mathbb{Q}[x]$ è irriducibile. Supponiamo che $2x^2 - 3x - 1$ non sia irriducibile in $\mathbb{Q}[x]$, ossia che si possa scrivere $2x^2 - 3x - 1 = fg$ con $f, g \in \mathbb{Q}[x]$, f, g entrambi non invertibili. Allora f e g devono avere entrambi grado ≥ 1 , e dato che $2x^2 - 3x - 1$ ha grado 2, f e g devono avere entrambi grado 1. Dato che i polinomi di grado 1 hanno sempre una radice, f e g hanno una radice in \mathbb{Q} , e quindi $2x^2 - 3x - 1$ ha una radice in \mathbb{Q} . Le due radici di $2x^2 - 3x - 1$ sono

$$\frac{-3 \pm \sqrt{9+8}}{2} = \frac{-3 \pm \sqrt{17}}{2},$$

e se una di queste due stesse in \mathbb{Q} , allora $\sqrt{17} \in \mathbb{Q}$. Quindi $\sqrt{17} = a/b$, con $a, b \in \mathbb{Z}$, $a, b \neq 0$, a e b primi tra loro, da cui $17b^2 = a^2$. Dato che 17 è primo, da $17|a^2$ seguirebbe $17|a$, e quindi $a = 17a'$, da cui $17b^2 = 17^2a'^2$, ossia $b^2 = 17a'^2$. Ma allora $17|b$, contraddizione, perché a e b erano primi tra loro. Questa contraddizione mostra che $\sqrt{17} \notin \mathbb{Q}$, e quindi $2x^2 - 3x - 1$ non ha radici in \mathbb{Q} , e pertanto è irriducibile in $\mathbb{Q}[x]$. Quindi $\mathbb{Q}[x]/(2x^2 - 3x - 1)$ è un campo.

Cerchiamo l'inverso di $1 + 2x + (2x^2 - 3x - 1)$. Si osservi innanzitutto che gli elementi di $\mathbb{Q}[x]/(2x^2 - 3x - 1)$ sono tutti e soli del tipo $f + (2x^2 - 3x - 1)$ con $f \in \mathbb{Q}[x]$. Ma se $f \in \mathbb{Q}[x]$ e si divide f per $2x^2 - 3x - 1$, si vede che esistono $q, r \in \mathbb{Q}[x]$ tali che $f = (2x^2 - 3x - 1)q + r$ e $\delta(r) < 2$. Ma allora $f + (2x^2 - 3x - 1) = r + (2x^2 - 3x - 1)$. Ecco quindi che gli elementi di $\mathbb{Q}[x]$ sono tutti e soli del tipo $r + (2x^2 - 3x - 1)$ con $r \in \mathbb{Q}[x]$ e $\delta(r) < 2$, ossia del tipo $a + bx + (2x^2 - 3x - 1)$ con $a, b \in \mathbb{Q}$. Siamo ora pronti a determinare l'inverso di $1 + 2x + (2x^2 - 3x - 1)$. Dobbiamo trovare $a, b \in \mathbb{Q}$ tali che

$$[1 + 2x + (2x^2 - 3x - 1)][a + bx + (2x^2 - 3x - 1)] = 1 + (2x^2 - 3x - 1).$$

Ora

$$[1 + 2x + (2x^2 - 3x - 1)][a + bx + (2x^2 - 3x - 1)] = a + (2a + b)x + 2bx^2 + (2x^2 - 3x - 1),$$

e questo è uguale a $1 + (2x^2 - 3x - 1)$ se e solo se $2x^2 - 3x - 1$ divide la differenza $a + (2a + b)x + 2bx^2 - 1$ in $\mathbb{Q}[x]$. Dato che entrambi questi polinomi hanno grado 2, si trova che $2x^2 - 3x - 1$ divide $(a - 1) + (2a + b)x + 2bx^2$ in $\mathbb{Q}[x]$ se e solo se esiste $c \in \mathbb{Q}$ tale che $(a - 1) + (2a + b)x + 2bx^2 = c(2x^2 - 3x - 1)$, ossia se e solo se

$$\begin{cases} a - 1 = -c \\ 2a + b = -3c \\ 2b = 2c. \end{cases}$$

Risolvendo questo sistema si trova la soluzione $a = 2$, $b = -1$, $c = -1$. Quindi $2 - x + (2x^2 - 3x - 1)$ è l'inverso di $1 + 2x + (2x^2 - 3x - 1)$ in $\mathbb{Q}[x]$. Verifichiamolo direttamente. Si ha

$$\begin{aligned} [1 + 2x + (2x^2 - 3x - 1)][2 - x + (2x^2 - 3x - 1)] &= (1 + 2x)(2 - x) + (2x^2 - 3x - 1) \\ &= 2 + 3x - 2x^2 + (2x^2 - 3x - 1) \\ &= 2 + 3x - 2x^2 + 2x^2 - 3x - 1 + (2x^2 - 3x - 1) \\ &= 1 + (2x^2 - 3x - 1). \end{aligned}$$

(b) Si ragioni come nella parte (a) sostituendo \mathbb{Z}_7 a \mathbb{Q} . Si trova che $\mathbb{Z}_7[x]/(2x^2 - 3x - 1)$ è un campo se e solo se l'elemento $2x^2 - 3x - 1$ di $\mathbb{Z}_7[x]$ è irriducibile. Come in (a), supponendo che $2x^2 - 3x - 1$ non sia irriducibile in $\mathbb{Z}_7[x]$ si trova che 17 è un quadrato in \mathbb{Z}_7 . Ora i 7 elementi di \mathbb{Z}_7 sono $0, \pm 1, \pm 2, \pm 3$, e questi hanno come quadrati $0, 1, 4, 9 = 2$ rispettivamente. Ma $17 = 3$ non è nessuno di questi. Quindi 17 non è un quadrato in \mathbb{Z}_7 , e pertanto $2x^2 - 3x - 1$ non ha radici in \mathbb{Z}_7 . Si conclude che $2x^2 - 3x - 1$ è irriducibile in $\mathbb{Z}_7[x]$ e pertanto $\mathbb{Z}_7[x]/(2x^2 - 3x - 1)$ è un campo.

In modo del tutto analogo a quello visto in (a), si trova poi che l'inverso di $1 + 2x + (2x^2 - 3x - 1) \in \mathbb{Z}_7[x]/(2x^2 - 3x - 1)$ è $2 - x + (2x^2 - 3x - 1)$. \square

45.2. Si trovi il polinomio minimo su \mathbb{Q} del numero complesso $\sqrt{2} + i\sqrt{3}$.

Soluzione. Sia $\alpha = \sqrt{2} + i\sqrt{3}$. Allora $\alpha - \sqrt{2} = i\sqrt{3}$, da cui $(\alpha - \sqrt{2})^2 = -3$, ossia $\alpha^2 - 2\sqrt{2}\alpha + 2 = -3$. Ma allora $\alpha^2 + 5 = 2\sqrt{2}\alpha$, ed elevando al quadrato si trova $\alpha^4 + 10\alpha^2 + 25 = 8\alpha^2$. Quindi $\alpha = \sqrt{2} + i\sqrt{3}$ è radice del polinomio $x^4 + 2x^2 + 25$. Mostriamo che questo polinomio monico appartenente a $\mathbb{Q}[x]$ è proprio il polinomio minimo di α su \mathbb{Q} . A tal fine è sufficiente dimostrare che $x^4 + 2x^2 + 25 = fg$ e $\delta(f), \delta(g) \geq 1$. Da $x^4 + 2x^2 + 25 = fg$ e $\delta(f), \delta(g) \geq 1$ segue che o uno dei due fattori f e g ha grado 1, oppure $\delta(f) = \delta(g) = 2$. Distinguiamo questi due casi.

Supponiamo intanto che uno dei due polinomi $f, g \in \mathbb{Q}[x]$ abbia grado 1. Dato che i polinomi di grado 1 appartenenti a $\mathbb{Q}[x]$ hanno sempre una radice in \mathbb{Q} , ne segue che $x^4 + 2x^2 + 25$ ha una radice in \mathbb{Q} . Risolvendo l'equazione $x^4 + 2x^2 + 25 = 0$ si trova

$$x^2 = \frac{-2 \pm \sqrt{4 - 100}}{2} = -1 \pm i2\sqrt{6},$$

e quindi le quattro radici di $x^4 + 2x^2 + 25$ sono $\pm\sqrt{-1 \pm i2\sqrt{6}}$. Se una di queste fosse razionale, allora anche il suo quadrato $-1 \pm i2\sqrt{6}$ sarebbe razionale, mentre questo non è nemmeno un numero reale. Quindi $x^4 + 2x^2 + 25$ non ha radici in \mathbb{Q} , e quindi non può avere fattori in $\mathbb{Q}[x]$ di grado 1.

Supponiamo ora che $\delta(f) = \delta(g) = 2$. Senza perdita di generalità possiamo supporre anche che f e g siano entrambi monici, ossia $f = x^2 + ax + b$ e $g = x^2 + cx + d$ con $a, b, c, d \in \mathbb{Q}$. L'ugualianza $x^4 + 2x^2 + 25 = fg$ si scrive allora nella forma $x^4 + 2x^2 + 25 = (x^2 + ax + b)(x^2 + cx + d)$, ossia $x^4 + 2x^2 + 25 = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (ad+bc)x + bd$, e questo equivale al sistema

$$(45.1) \quad \begin{cases} a+c=0 \\ b+ac+d=2 \\ ad+bc=0 \\ bd=25. \end{cases}$$

Risolviamolo. Dalla prima equazione si ricava $c = -a$, e questa, sostituita nella terza, dà $ad - ab = 0$, cioè $a(d - b) = 0$. Si può avere quindi $a = 0$ oppure $d - b = 0$. Se $a = 0$, allora $c = 0$ e il sistema (45.1) diventa

$$(45.2) \quad \begin{cases} b+d=2 \\ bd=25. \end{cases}$$

In questo caso b e d devono essere le due radici dell'equazione $x^2 - 2x + 25 = 0$. Dato che questa equazione ha discriminante < 0 , non ha soluzioni reali, e quindi non esistono $b, d \in \mathbb{Q}$ che sono soluzioni del sistema (45.2). Deve quindi essere $d - b = 0$, ossia $d = b$. Dall'ultima equazione del sistema (45.1) si ricava quindi che o $d = b = 5$ oppure $d = b = -5$. Se $d = b = 5$, la seconda equazione di (45.1) diventa $5 - a^2 + 5 = 2$, da cui $a^2 = 8$, che non ha soluzioni razionali. Se $d = b = -5$, la seconda equazione di (45.1) diventa $-5 - a^2 - 5 = 2$, da cui $a^2 = -12$, che pure non ha soluzioni razionali.

Abbiamo così dimostrato che il sistema (45.1) non ha soluzioni razionali, e quindi $x^4 + 2x^2 + 25$ non si può scrivere come prodotto di due polinomi $f, g \in \mathbb{Q}[x]$ di grado ≥ 1 . Pertanto $x^4 + 2x^2 + 25 \in \mathbb{Q}[x]$ è irriducibile, e quindi è il polinomio minimo di $\sqrt{2} + i\sqrt{3}$ su \mathbb{Q} . \square

Altri esercizi

45.3. Si provi che se F è un'estensione del campo K e $\alpha \in F$ è trascendente su K , allora $K[\alpha]$ non è un campo.

45.4. Siano $F_1 \subseteq F_2 \subseteq F_3$ campi e sia $\alpha \in F_3$. Si provi che:

- (a) se α è algebrico su F_1 , allora α è algebrico su F_2 ;
- (b) se α è trascendente su F_2 , allora α è trascendente su F_1 ;
- (c) può accadere che α sia contemporaneamente trascendente su F_1 e algebrico su F_2 . [Suggerimento: $\alpha = \pi$.]

45.5. Si dica quali dei seguenti anelli sono campi: $\mathbb{Z}_2[x]/(x^2 + 1)$, $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$, $\mathbb{Z}_2[x]/(x^2 + x + 1)$, $\mathbb{Z}_2[x]/(x^4 + x + 1)$.

45.6. L'anello $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ è un campo? Se $a, b \in \mathbb{Q}$ e $a + b\sqrt{2} \neq 0$, come si scrive l'inverso di $a + b\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$ nella forma $c + d\sqrt{2}$, $c, d \in \mathbb{Q}$?

45.7. Si trovino i polinomi minimi e i gradi su \mathbb{Q} dei numeri reali $\sqrt[3]{2}$, $1 + \sqrt{3}$, $3 - \sqrt{2}$, $\sqrt{2} + \sqrt{3}$ e dei numeri complessi i e $(-1 + i\sqrt{3})/2$.

45.8. Se $\alpha \in K$, quali sono il polinomio minimo e il grado di α su K ?

45.9. Sia K un campo, $f \in K[x]$ un polinomio monico irriducibile, F un'estensione di K , e $\alpha \in F$ una radice di f . Si provi che f è un polinomio minimo di α su K .

45.10. Abbiamo visto che se K è un campo, α è un elemento algebrico su K ed f è polinomio minimo di α su K , allora $K[\alpha] \cong K[x]/(f)$ (teorema 45.2). Abbiamo visto anche che gli elementi di $K[\alpha]$ si scrivono in modo unico nella forma $g(\alpha)$ ove $g \in K[x]$ è un polinomio di grado $\leq n-1$. Ora se $g_1(\alpha), g_2(\alpha) \in K[\alpha]$ e g_1, g_2 hanno grado $\leq n-1$, si ha $g_1(\alpha) + g_2(\alpha) = (g_1 + g_2)(\alpha)$ e $g_1 + g_2 \in K[x]$ ha grado $\leq n-1$. Invece $g_1 g_2$ non è detto che abbia grado $\leq n-1$. Si provi che $g_1(\alpha)g_2(\alpha) = r(\alpha)$ ove r è il resto della divisione di g_1g_2 per f (e quindi r ha grado $\leq n-1$).

45.11. L'esercizio 45.10 e i teoremi 45.2 e 45.3 ci spiegano come fare "in pratica" a costruire estensioni che contengono radici di polinomi irriducibili. Ad esempio: partiamo dal campo \mathbb{R} e costruiamo un'estensione di \mathbb{R} contenente una radice del polinomio $x^2 + 1 \in \mathbb{R}[x]$. Dopo aver verificato che $x^2 + 1$ è un elemento irriducibile di $\mathbb{R}[x]$, fissiamo un simbolo α e consideriamo l'insieme $F = \{a + b\alpha \mid a, b \in \mathbb{R}\}$ di tutte le espressioni formali $a + b\alpha$ (queste sono espressioni formali, perché non ha significato moltiplicare un simbolo α per un numero reale b). Si noti che ci fermiamo al grado 1 perché il polinomio $x^2 + 1$ ha grado 2. Se il polinomio avesse avuto grado n , avremmo dovuto considerare l'insieme di tutte le espressioni formali $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$. A questo punto si definiscono un'addizione e una moltiplicazione in F ponendo $(a + b\alpha) + (a' + b'\alpha) = (a + a') + (b + b')\alpha$ e $(a + b\alpha)(a' + b'\alpha) = \text{"resto della divisione di } (a + b\alpha)(a' + b'\alpha) \text{ per } x^2 + 1 \text{ calcolato in } \alpha"$ (si provi che il risultato è $(aa' - bb') + (ab' + ba')\alpha$). Allora F è un campo, estensione di \mathbb{R} , isomorfo a $\mathbb{R}[x]/(x^2 + 1)$, e $\alpha \in F$ è una radice di $x^2 + 1$. (Naturalmente questo è ciò che i matematici incominciarono a fare nel XVI secolo usando il simbolo i invece del simbolo α .) Si ripeta questa costruzione per il campo $\mathbb{Q}[\alpha]$, ove α è una radice di $x^3 - 2$ (in genere si usa il simbolo $\sqrt[3]{2}$ in luogo di α) e per $\mathbb{Z}_3[i]$, ove i è una radice di $x^2 + 1 \in \mathbb{Z}_3[x]$.

45.12. Sia $f = \sum_{i=0}^n a_i x^i$ il polinomio minimo di un elemento algebrico α su K , ove $\alpha \notin K$. Per il teorema 45.2, $\alpha^{-1} \in K[\alpha]$ (perché $K[\alpha]$ è un campo) e α^{-1} si scrive in modo unico nella forma $\sum_{j=0}^{n-1} b_j \alpha^j$ per opportuni $b_0, b_1, \dots, b_{n-1} \in K$. Calcolare b_0, b_1, \dots, b_{n-1} .

45.13. Sia $f = ax^2 + bx + c$, ove $a, b, c \in \mathbb{R}$ e $b^2 - 4ac < 0$. Si provi che $f \in \mathbb{R}[x]$ è irriducibile e che $\mathbb{R}[x]/(f) \cong \mathbb{C}$. [Suggerimento: per dimostrare che f è irriducibile, si faccia vedere che un polinomio $f \in K[x]$ riducibile in $K[x]$ e di grado ≤ 3 ha una radice in K ; per dimostrare che $\mathbb{R}[x]/(f) \cong \mathbb{C}$, costruire con la proprietà universale dell'anello dei polinomi un omomorfismo di anelli $\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$ tale che $\varphi(x) = (-b + i\sqrt{4ac - b^2})/2a$ e applicare il teorema fondamentale di omomorfismo.]

45.14. Si provi che $\mathbb{Q}[(-1 + i\sqrt{3})/2] \cong \mathbb{Q}[x]/(x^2 + x + 1)$.

45.15. Si provi che se $K \subseteq F$ è un'estensione di campi, allora $G(F|K) = \{\varphi: F \rightarrow F \mid \varphi$ è un automorfismo di anelli, $\varphi(k) = k$ per ogni $k \in K\}$ è un gruppo rispetto alla composizione di applicazioni. ($G(F|K)$ è detto il *gruppo di Galois di F su K* .)

§46. Campi algebricamente chiusi e campi finiti

Abbiamo dimostrato che se K è un campo ed $f \in K[x]$ è un polinomio irriducibile allora esiste un'estensione K' di K contenente una radice di f (teorema 45.3). Se $\alpha \in K'$ è una radice di f , allora $(x - \alpha) | f$ in $K'[x]$ e quindi $f = (x - \alpha)g$ per qualche $g \in K'[x]$. In realtà sarebbe possibile dimostrare il seguente teorema.

46.1 TEOREMA. *Sia K un campo e sia $f \in K[x]$ un polinomio di grado $n \geq 1$. Allora esiste un campo F con le seguenti proprietà:*

- (a) *F è un'estensione di K ;*
- (b) *esistono $k \in K$ e $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ tali che $f = k(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ in $F[x]$;*
- (c) *se F' è un campo, $K \subseteq F' \subseteq F$ e $\alpha_1, \alpha_2, \dots, \alpha_n \in F'$, allora $F = F'$.*

Inoltre se F_1 è un altro campo con le proprietà (a), (b), (c), allora $F \cong F_1$.

Il teorema dice che dati K ed $f \in K[x]$, esiste un più piccolo campo contenente K e tutte le radici di f , e che tale campo è unico a meno di isomorfismi. Un campo F con le proprietà del teorema 46.1 si dice un *campo di riducibilità completa di f su K* .

Ma è possibile dimostrare ancora di più.

46.2 TEOREMA. *Sia K un campo. Allora esiste un campo \overline{K} con le seguenti proprietà:*

- (a) *\overline{K} è un'estensione di K ;*
- (b) *per ogni $f \in K[x]$ di grado $n \geq 1$ esistono $k \in K$ e $\alpha_1, \alpha_2, \dots, \alpha_n \in \overline{K}$ tali che $f = k(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$;*
- (c) *ogni elemento di \overline{K} è algebrico su K .*

Inoltre se \overline{K}_1 è un altro campo con le proprietà (a), (b), (c), allora $\overline{K} \cong \overline{K}_1$.

Il campo \overline{K} con le proprietà del teorema 46.2 si dice una *chiusura algebrica* di K . Un campo K si dice *algebricamente chiuso* se $K = \overline{K}$, ossia se K coincide con la propria chiusura algebrica. Quindi un campo K è algebricamente chiuso se e solo se ogni polinomio di $K[x]$ ha tutte le radici in K . Ad esempio \mathbb{Q} non è algebricamente chiuso, perché $x^2 - 2 \in \mathbb{Q}[x]$ non ha radici in \mathbb{Q} ; anche \mathbb{R} non è algebricamente chiuso, perché $x^2 + 1 \in \mathbb{R}[x]$ non ha radici in \mathbb{R} .

46.3 TEOREMA FONDAMENTALE DELL'ALGEBRA. *Il campo dei numeri complessi \mathbb{C} è algebricamente chiuso.*

Anche di questo teorema omettiamo la dimostrazione. Abbandoniamo ora lo studio di questi problemi e occupiamoci invece dei campi finiti, ossia dei campi con un numero finito di elementi. (Si osservi che i campi finiti coincidono con i domini d'integrità finiti, corollario 27.2.)

46.4 LEMMA. *Sia F un campo con t elementi. Allora $x^t = x$ per ogni $x \in F$.*

Dimostrazione. Se $x = 0$ si ha certamente $x^t = x$. Supponiamo quindi $x \neq 0$. Allora l'app-

plicazione $\varphi: F^* \rightarrow F^*$ definita da $\varphi(a) = ax$ per ogni $a \in F^*$ è iniettiva, perché da $\varphi(a) = \varphi(b)$ segue che $ax = bx$, e quindi $(a - b)x = 0$ da cui $a = b$ perché $x \neq 0$. Quindi φ è una biiezione. Ne segue che il prodotto p dei $t - 1$ elementi non nulli di F si può scrivere sia come $\prod_{a \in F^*} a$ che come $\prod_{a \in F^*} (ax)$. Ma allora $p = \prod_{a \in F^*} (ax) = x^{t-1} \prod_{a \in F^*} a = x^{t-1} p$, da cui, essendo $p \neq 0$, $x^{t-1} = 1$. Ma allora $x^t = x$. \square

46.5 TEOREMA. *Sia F un campo finito. Allora la caratteristica di F è un numero primo p ed F ha p^n elementi per un opportuno intero positivo n .*

Dimostrazione. Ogni campo ha caratteristica 0 o un numero primo o zero (corollario 27.18). Ma un campo di caratteristica zero contiene un sottoanello isomorfo a \mathbb{Z} (proposizione 27.17) e quindi è infinito. Pertanto un campo finito F ha come caratteristica un numero primo p , e quindi contiene un sottocampo P isomorfo a \mathbb{Z}_p (proposizione 27.17). In particolare F è spazio vettoriale su P , ed essendo finito è certamente di dimensione finita n , diciamo. Ma allora $F \cong P^n$ come spazio vettoriale su P , e quindi $|F| = |P^n| = |P|^n = p^n$. \square

46.6 TEOREMA. *Per ogni numero primo p e intero positivo n esiste un campo con p^n elementi, unico a meno di isomorfismi (ossia se F ed F' sono due campi entrambi con p^n elementi, allora $F \cong F'$). Inoltre un campo ha p^n elementi se e solo se è un campo di riducibilità completa del polinomio $x^{p^n} - x$ su \mathbb{Z}_p .*

Dimostrazione. Mostriamo che un campo ha p^n elementi se e solo se è campo di riducibilità completa di $x^{p^n} - x$ su \mathbb{Z}_p .

Sia F un campo di riducibilità completa di $x^{p^n} - x$ su \mathbb{Z}_p . Sia $K = \{a \in F \mid a^{p^n} = a\}$ il sottoinsieme di F di tutte le radici di $x^{p^n} - x$. Mostriamo che il sottoinsieme K è un sottocampo di F . Si osservi che $0 \in K$ e $1 \in K$. Se $a, b \in K$, allora $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ perché, come abbiamo visto nell'esercizio 27.16(e), l'applicazione $a \mapsto a^{p^n}$ è un omomorfismo di anelli $K \rightarrow K$, e quindi $(-a)^{p^n} = -a^{p^n} = -a$, $(ab)^{p^n} = a^{p^n}b^{p^n}$, e se $a \neq 0$ allora $(a^{-1})^{p^n} = (a^{p^n})^{-1}$. Quindi K è un sottocampo di F . Ma F , campo di riducibilità completa di $x^{p^n} - x$ su \mathbb{Z}_p , è il più piccolo campo che contiene \mathbb{Z}_p e K , e quindi $F = K$.

Si osservi ora che la derivata formale del polinomio $x^{p^n} - x$ è -1 (esercizi 28.9 e 28.10). Dato che la derivata non ha radici, il polinomio non ha radici multiple. Quindi le radici di $x^{p^n} - x$ sono tutte p^n distinte. In particolare $F = K$ ha esattamente p^n elementi. Abbiamo così dimostrato che ogni campo di riducibilità completa di $x^{p^n} - x$ su \mathbb{Z}_p è un campo con p^n elementi.

Viceversa sia F' un campo con p^n elementi. Abbiamo già osservato che F' contiene \mathbb{Z}_p a meno di isomorfismi. Inoltre per il lemma 46.4 gli elementi di F' sono esattamente le p^n radici distinte di $x^{p^n} - x$. Quindi F' è il più piccolo campo che contiene le radici di $x^{p^n} - x$ e \mathbb{Z}_p , cioè F' è campo di riducibilità completa di $x^{p^n} - x$ su \mathbb{Z}_p .

Abbiamo così dimostrato la seconda asserzione dell'enunciato. Ma dato che il campo di riducibilità completa esiste ed è unico a meno di isomorfismi (teorema 46.1), anche il campo con p^n elementi esiste ed è unico a meno di isomorfismi; ciò prova la prima asserzione dell'enunciato. \square

radice di $x^2 + x + \bar{1} \in \mathbb{Z}_2[x]$, la tabella moltiplicativa di un campo di 4 elementi è

	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Ripetere l'esercizio con un campo di 8 elementi e uno di 9.

46.12 (PICCOLO TEOREMA DI FERMAT). Si provi che se $a \in \mathbb{Z}$ e p è un numero primo, allora $a^p \equiv a \pmod{p}$. [Suggerimento: applicare il lemma 46.4 a \mathbb{Z}_p .]

Capitolo 8

ANCORA ESERCIZI. SOLUZIONI

§47. Alcuni esercizi più difficili

2.28. 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 φ è iniettiva?
- (b) L'applicazione φ è suriettiva?

2.29. 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 φ è iniettiva?
- (b) L'applicazione φ è suriettiva?

2.30. 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 φ è iniettiva?
- (b) L'applicazione φ è suriettiva?

2.31. Sia $\varphi: \mathbb{Z} \rightarrow \mathbb{R}$ l'applicazione definita da $\varphi(x) = x^4$ per ogni $x \in \mathbb{Z}$.

- (a) L'applicazione φ 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 $\alpha \in \mathbb{R}$?

2.32. 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 .

2.33. 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 $f(X) \setminus f(Y) = f(X \setminus Y)$.

2.34. 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 $f(X \setminus Y) = f(X) \setminus f(Y)$.

3.21. 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 φ è iniettiva.
- (b) Si dimostri che φ è suriettiva.
- (c) Si dica come è definita l'applicazione inversa φ^{-1} di φ .

3.22. 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 $b \in B$.

3.23. 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 φ è iniettiva.
- (b) Si dimostri che

$$\varphi(B^C) = \{g \in B^A \mid \text{per ogni } a, a' \in A, \text{ se } f(a) = f(a') \text{ allora } g(a) = g(a')\}.$$

5.20. 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 $z = -1$. Se n è pari, nessuno dei suoi vertici è sull'asse reale.

7.22. 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 $a \in \mathbb{R}^*$.

- (a) Si dimostri che $\psi^{-1}(y) \subseteq \{y, y^{-1}\}$ per ogni $y \in \mathbb{R}$, $y \neq 0$.
- (b) Si dimostri che $|\psi^{-1}(y)| \leq 2$ per ogni $y \in \mathbb{R}$.

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

7.23. Siano A un insieme, \sim una relazione di equivalenza su A , A/\sim l'insieme quoziante 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

$$\pi^{-1}(\pi(B)) = B.$$

7.24. Sia A un insieme non vuoto e sia \mathbb{N}^A l'insieme di tutte le applicazioni di A nell'insieme \mathbb{N} dei numeri naturali. In \mathbb{N}^A si definisca una relazione \sim ponendo, per ogni $f, g \in \mathbb{N}^A$, $f \sim g$ 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 \mathbb{N}^A .
 (b) Si dimostri che la relazione \sim su \mathbb{N}^A è la relazione banale (cioè $f \sim g$ per ogni $f, g \in \mathbb{N}^A$) 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 $\varphi: \mathbb{N} \rightarrow \mathbb{N}^A/\sim$ definita da $\varphi(n) = [f_n]_\sim$ per ogni $n \in \mathbb{N}$ è iniettiva.

7.25. 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.

7.26. 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 biiezioni, una inversa dell'altra. [Suggerimento: per dimostrare che f e g sono due biiezioni, una inversa dell'altra, è sufficiente dimostrare che $g \circ f = \iota_{\mathcal{E}}$ e $f \circ g = \iota_{\mathcal{P}}$.]

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

- (a) Si dimostri che \sim_f è la relazione banale ω 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 $x \in \mathbb{Z}$.
 (b) Si dimostri che se \sim_f è la relazione di uguaglianza $=$, allora l'insieme A è infinito, cioè ha infiniti elementi distinti.

10.27. 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 $\mathbb{P} = \{2n \mid n \in \mathbb{N}\}$? Se esiste lo si calcoli.

10.28. Siano A un insieme e ϱ una relazione riflessiva e transitiva su A . Si definisca una relazione σ su A ponendo, per ogni $a, b \in A$, $a \sigma b$ se $a \varrho b$ e $b \varrho a$.

- (a) Si provi che σ è un'equivalenza su A .
 (b) Sull'insieme quoziente A/σ si definisca una relazione τ ponendo, per ogni $[a]_\sigma, [b]_\sigma \in A/\sigma$, $[a]_\sigma \tau [b]_\sigma$ se $a \varrho b$. Si provi che la relazione τ su A/σ è ben definita.
 (c) Si provi che τ è un ordinamento parziale su A/σ .

17.14. 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 sottomonoide 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 φ è un omomorfismo di monoidi. Qui, come al solito, si intende che l'operazione sul monoide $(A/\sim)^{(A/\sim)}$ è la composizione di applicazioni.

20.20. Siano 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 (\overline{W}, \circ) il monoide libero sull'insieme quoziente A/\sim e $\overline{\varphi}: A/\sim \rightarrow \overline{W}$ l'applicazione canonica di A/\sim in \overline{W} . Si consideri l'applicazione composta $f = \overline{\varphi} \circ \pi: A \rightarrow \overline{W}$. 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 $f = \overline{\varphi} \circ \pi: A \rightarrow \overline{W}$ esiste un unico omomorfismo di monoidi $\widehat{f}: W \rightarrow \overline{W}$ che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\sim \\ \varphi \downarrow & & \downarrow \overline{\varphi} \\ W & \xrightarrow{\widehat{f}} & \overline{W} \end{array}$$

cioè tale che $\widehat{f} \circ \varphi = \overline{\varphi} \circ \pi$. Si dimostri che l'omomorfismo \widehat{f} è suriettivo.

- (d) Si dimostri che l'equivalenza \equiv e l'equivalenza $\sim_{\widehat{f}}$ associata all'applicazione \widehat{f} coincidono.
 (e) Si dimostri che i monoidi W/\equiv e \overline{W} sono isomorfi.

27.34. Siano R ed S anelli con identità ed $f: R \rightarrow S$ un omomorfismo di anelli con identità, cioè un omomorfismo d'annehi tale che $f(1_R) = 1_S$.

- (a) Si dimostri che se S ha caratteristica zero, allora anche l'anello R ha caratteristica zero.
 (b) Si dimostri che se P_R e P_S sono il sottoanello fondamentale di R e di S rispettivamente, allora $f(P_R) = P_S$.
 (c) Si dimostri che se R ha caratteristica $n > 0$, allora la caratteristica di S è un divisore di n .

36.18. Sia $\{v_1, v_2, \dots, v_n\}$ una base di uno spazio vettoriale V di dimensione ≥ 2 su un campo K . È vero o falso che anche $\{v_1 + v_2, v_2 + v_3, \dots, v_{n-1} + v_n, v_n + v_1\}$ è una base di V ?

43.19. Sia $V = \mathbb{R}^{\mathbb{R}}$ l'insieme di tutte le applicazioni $\mathbb{R} \rightarrow \mathbb{R}$. L'insieme V è uno spazio vettoriale sul campo \mathbb{R} dei numeri reali rispetto alle operazioni definite da $(f+g)(x) = f(x) + g(x)$ e $(\lambda f)(x) = \lambda(f(x))$ per ogni $x \in \mathbb{R}$, ogni $f, g \in V$ e ogni $\lambda \in \mathbb{R}$. Sia W il sottospazio vettoriale di V generato dalle quattro applicazioni $f_i: \mathbb{R} \rightarrow \mathbb{R}$, $i = 1, 2, 3, 4$, definite da $f_1(x) = e^x$, $f_2(x) = e^{-x}$, $f_3(x) = \sin x$, $f_4(x) = \cos x$ per ogni $x \in \mathbb{R}$.

- (a) Si verifichi che $B = \{f_1, f_2, f_3, f_4\}$ è una base di W .
 (b) Sia $d: W \rightarrow W$ l'applicazione lineare che associa ad ogni $f \in W$ la derivata prima f' di f .
 Si scriva la matrice di d rispetto alla base B .
 (c) L'applicazione d è iniettiva? suriettiva? biiettiva?

§48. 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 $x \in \{\emptyset\}$, allora $x = \emptyset$, mentre $\emptyset \notin A$, perché gli elementi di A sono 0, 1, 2. La (e) è falsa: gli elementi di A sono 0, 1, 2, e l'insieme $\{\emptyset\}$ non è nessuno di questi. La (f) è falsa: gli elementi di A sono 0, 1, 2, e \emptyset non è nessuno di questi. La (g) è vera, in quanto $\emptyset \subseteq A$ per ogni insieme A .

1.20. 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 $A \cup B \subseteq (A \setminus B) \cup B$.

1.24. Soluzione di (c):

$$\begin{aligned} (A \Delta B) \Delta C &= [(A \Delta B) \setminus C] \cup [C \setminus (A \Delta B)] \\ &= [(A \setminus B) \cup (B \setminus A) \setminus C] \cup [C \setminus ((A \cup B) \setminus (A \cap B))] \\ &= [(A \setminus B) \setminus C] \cup [(B \setminus A) \setminus C] \cup [C \setminus (A \cup B)] \cup (C \cap A \cap B) \\ &\quad \text{per la (i) e la (ii) di (b)} \\ &= [A \setminus (B \cup C)] \cup [B \setminus (A \cup C)] \cup [C \setminus (A \cup B)] \cup [A \cap B \cap C] \\ &\quad \text{per la (iii) di (b).} \end{aligned}$$

Similmente

$$\begin{aligned} A \Delta (B \Delta C) &= [A \setminus (B \Delta C)] \cup [(B \Delta C) \setminus A] \\ &= [A \setminus ((B \cup C) \setminus (B \cap C))] \cup [(B \setminus C) \cup (C \setminus B)] \setminus A \\ &= [A \setminus (B \cup C)] \cup [A \cap B \cap C] \cup [(B \setminus C) \setminus A] \cup [(C \setminus B) \setminus A] \end{aligned}$$

per la (ii) e la (i) di (b)
 $= [A \setminus (B \cup C)] \cup [A \cap B \cap C] \cup [B \setminus (A \cup C)] \cup [C \setminus (A \cup B)]$
 per la (iii) di (b).

Soluzione di (e):

$$\begin{aligned} A \cap (B \Delta C) &= A \cap [(B \setminus C) \cup (C \setminus B)] = [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)] \\ &= [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)] \quad \text{per (d)} \\ &= (A \cap B) \Delta (A \cap C). \quad \square \end{aligned}$$

1.29. Si osservi che 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 $\bigcap_{i \in \mathbb{Z}} A_i = \emptyset$.

2.5. Sono 24.

2.6. Quella in (b) lo è, quelle in (a) e (c) non lo sono.

2.7. Quella in (b) lo è, quelle in (a) e (c) non lo sono.

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 $\varphi^{-1}(\varphi(A')) = \varphi^{-1}(\varphi(\{1\})) = \varphi^{-1}(\{\varphi(1)\}) = \varphi^{-1}(\{1\}) = \{1, 2\} = A \supset A'$.

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 $b = \varphi(a) \in \varphi(\varphi^{-1}(B'))$.

2.19. Innanzi tutto si osservi che π_A è un'applicazione, perché associa ad ogni elemento (a, b) di $A \times B$ l'unico elemento a di A . Mostriamo che π_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 π_A è suriettiva. La dimostrazione per π_B è analoga (e usa il fatto che $A \neq \emptyset$).

2.22. Si considerino le applicazioni degli esempi 2.8 e 2.7.

2.28. (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 φ 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 φ è iniettiva.

(b) L'applicazione φ 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.

2.29. È suriettiva, ma non iniettiva.

2.30. (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 φ 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 φ è strettamente crescente, cioè se $z, z' \in \mathbb{Z}$ e $z < z'$, allora $\varphi(z) < \varphi(z')$. Quindi φ 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.

2.31. (b) Esistono infinite soluzioni S, T possibili. Ad esempio siano $S = \{2\}$ e $T = \{3\}$. In questo caso si ha che $S \neq T$ e $\varphi^{-1}(S) = \varphi^{-1}(T) = \emptyset$.

2.32. (a) Supponiamo che f sia iniettiva, e fissiamo un sottoinsieme X di A . Sia $y \in f(A \setminus X)$. 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 dimostriamo 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.

2.33. (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 $b \in f(X) \setminus f(Y)$.

2.34. (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 ipotesi si ha $f(X) \cap f(Y) = \emptyset$. Ma $f(X) = \{f(x)\}$ e $f(Y) = \{f(y)\}$, e pertanto $\{f(x)\} \cap \{f(y)\} = \emptyset$. 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 $x \in X$ e $x \notin Y$. 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 dimostriamo che f è iniettiva. Siano $a, b \in A$ tali che $f(a) = f(b)$. Allora $f(\{a\} \setminus \{b\}) = f(\{a\}) \setminus f(\{b\}) = \{f(a)\} \setminus \{f(b)\} = \emptyset$. Da $f(\{a\} \setminus \{b\}) = \emptyset$ segue che $\{a\} \setminus \{b\} = \emptyset$. Pertanto $a = b$ ed f è iniettiva.

3.6. Calcoliamo l'applicazione composta $\psi \circ \varphi: \mathbb{R} \rightarrow \mathbb{Z}$. Per ogni $x \in \mathbb{R}$ si ha $\varphi(x) = 1/(1+x^2)$, 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 φ non è iniettiva perché $\varphi(1) = \varphi(-1)$; l'applicazione ψ non è iniettiva perché $\psi(1) = \psi(2) = 1$; l'applicazione $\psi \circ \varphi$ non è iniettiva, perché $(\psi \circ \varphi)(0) = (\psi \circ \varphi)(1) = 1$. L'applicazione φ non è suriettiva perché ad esempio non esiste nessun $x \in \mathbb{R}$ tale che $\varphi(x) = 0$; l'applicazione ψ non è suriettiva perché non esiste nessun $x \in \mathbb{R}$ tale che $\psi(x) = 2$; infine l'applicazione $\psi \circ \varphi$ non è suriettiva perché non esiste nessun $x \in \mathbb{R}$ tale che $(\psi \circ \varphi)(x) = 0$.

3.9. 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 $\psi_1 \circ \varphi = \iota_A$. Dato che $\psi_1 \circ \varphi = \iota_A$ è iniettiva, anche φ è iniettiva per la proposizione 3.2(a). Ma allora φ è sia iniettiva che suriettiva, dunque biiettiva, assurdo.

Essendo invece φ suriettiva, per l'esercizio 3.4 esiste un'applicazione ψ_2 tale che $\varphi \circ \psi_2 = \iota_B$.

3.13. (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 φ è iniettiva e ψ 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 φ e ψ forniscono un esempio che risponde sia al quesito (b) che al quesito (c).

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 φ manda i numeri naturali pari nei numeri interi non negativi, e i numeri naturali dispari nei numeri interi negativi (vedi figura 48.1). L'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 ≥ 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 φ è definita per ogni $z \in \mathbb{Z}$ da

$$\varphi^{-1}(z) = \begin{cases} 2z & \text{se } z \geq 0, \\ -2z - 1 & \text{se } z < 0. \end{cases} \quad \square$$

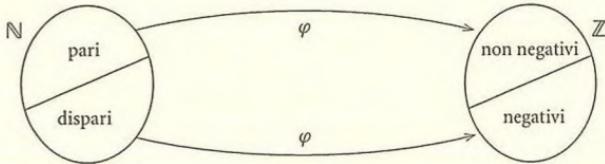


FIGURA 48.1.

3.22. (\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 $B \cup C = A$, $B \cap C = \emptyset$. 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 $f \circ f = f$.

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 $f(a') = c$, 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 $g = \varphi(h) \in \varphi(B^C)$.

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 , c in prodotto di primi. Allora $p_1 p_2 \cdots p_r p'_1 p'_2 \cdots p'_s$ e $p''_1 p''_2 \cdots p''_t p$ 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.

4.11. Supponiamo $\sqrt{n} \in \mathbb{Q}$ e dimostriamo 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 $\sqrt{n} = a/b$ con a e b interi 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 $\sqrt{n} = a/b$ si ottiene che $n = a^2/b^2$, 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 non ci sia nessun numero primo che divide b , cioè si deve avere $b = 1$. Si conclude così che $\sqrt{n} = a/b = a/1 \in \mathbb{Z}$.

4.12. Si ha che $a \mid 0$, $0 \mid 0$, e per ogni $c \in \mathbb{Z}$, se $a \mid c$ e $0 \mid c$, allora $0 \mid c$. Questo dimostra che 0 è un mcm di a e 0. Per mostrare che 0 è l'unico mcm di a e 0, prendiamo un altro mcm m di a e 0. Allora $0 \mid m$, ossia $m = 0 \cdot m'$ per qualche $m' \in \mathbb{Z}$, e quindi $m = 0$.

4.22. Per $n = 5$ si ha $n^2 = 25$ e $11n - 30 = 25$. 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 .

4.30. 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 $h, c_1, c_2, \dots, c_h, \ell, d_1, d_2, \dots, d_\ell \in \mathbb{N}$ tali che $n = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_h \cdot h! = d_1 \cdot 1! + d_2 \cdot 2! + d_3 \cdot 3! + \cdots + d_\ell \cdot \ell!$, $c_i \leq i$ per ogni $i = 1, 2, \dots, h$ e $d_j \leq j$ per ogni $j = 1, 2, \dots, \ell$. 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 $d_\ell \neq 0$ e che $h \leq \ell$.

Se $h < \ell$, allora $n = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_h \cdot h! \leq 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + h \cdot h! = (h+1)! - 1$ (esercizio 4.4), e $n = d_1 \cdot 1! + d_2 \cdot 2! + d_3 \cdot 3! + \cdots + d_\ell \cdot \ell! \geq d_\ell \cdot \ell! \geq \ell! \geq (h+1)!$ perché $\ell \geq h+1$. Questa è una contraddizione.

Deve quindi essere $h = \ell$. Ma allora $n - h! = c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + (c_h - 1) \cdot h! = d_1 \cdot 1! + d_2 \cdot 2! + d_3 \cdot 3! + \cdots + (d_\ell - 1) \cdot \ell!$ 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 .

4.31. Si ha

$$1234 = 12 \cdot 102 + 10$$

$$102 = 12 \cdot 8 + 6$$

$$8 = 12 \cdot 0 + 8.$$

Quindi la soluzione è 86A.

4.32. Si ha $5 = 2 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$, $1 = 2 \cdot 0 + 1$. Quindi la risposta è 101.

4.33. 1111100.

4.37. $\alpha = 1/(b - 1)$.4.38. $1/7 = 0.\overline{142857}$.

4.39. Sia $\alpha = 1,\overline{234}$. Allora $1000\alpha = 1234,\overline{34}$ e $10\alpha = 12,\overline{34}$, da cui, sottraendo membro a membro, $990\alpha = 1234 - 12 = 1222$. Pertanto $\alpha = 1222/990 = 611/495$.

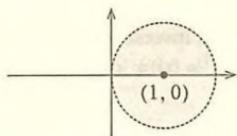
4.40. No, non è periodico.

4.41. Un numero m può essere scritto con $\leq N$ cifre in base b se e solo se $m = \sum_{i=0}^{N-1} a_i b^i$ per opportuni a_0, \dots, a_{N-1} compresi tra 0 e $b - 1$, cioè se e solo se $m \leq \sum_{i=0}^{N-1} (b-1)b^i$, ossia se e solo se $m < b^N$. Quindi per scrivere i numeri $< n$ sono necessarie N cifre, dove N è il più piccolo intero con $n \leq b^N$, ossia tale che $\log_b n \leq N$. La risposta è pertanto $\log_b n$ se $\log_b n$ è un intero, e $\lfloor \log_b n \rfloor + 1$ se $\log_b n$ non è un intero.

4.42. (a) $b = 7$; (b) qualunque b con $7 \leq b \leq 10$; (c) $b = 5$.

5.2. Se $z, z' \in \mathbb{C}$ e $zz' = 0$, allora $|z| \cdot |z'| = |zz'| = |0| = 0$ per la proposizione 5.6. Quindi $|z|$ e $|z'|$ sono due numeri reali il cui prodotto è nullo, e quindi uno dei due è nullo. Ne segue che o $z = 0$ oppure $z' = 0$.

5.5. Se $z = x + iy$ ($x, y \in \mathbb{R}$), allora $|z - 1| = |x + iy - 1| = \sqrt{(x-1)^2 + y^2}$, e quindi $|z - 1| < 1$ se e solo se $\sqrt{(x-1)^2 + y^2} < 1$, cioè se e solo se il punto P di coordinate (x, y) e il punto di coordinate $(1, 0)$ distano meno di 1, ossia se e solo se il punto P di coordinate (x, y) è interno alla circonferenza di centro $(1, 0)$ e raggio 1. Pertanto l'insieme di numeri complessi dato è rappresentato nel piano di Argand-Gauss dall'insieme dei punti interni alla circonferenza di centro $(1, 0)$ e raggio 1.



5.8. (a) Da $z = a + ib$ segue che $iz = i(a + ib) = -b + ia$. Quindi iz è rappresentato dal punto di coordinate $(-b, a)$.

$$(b) iz = \left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}\right) \varrho (\cos \varphi + i \sin \varphi) = \varrho \left(\cos \left(\frac{\pi}{2} + \varphi\right) + i \sin \left(\frac{\pi}{2} + \varphi\right)\right).$$

5.20. 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 dell'equazione $z^n = 1$, si ricava che l'equazione $z^n = -1$ ha esattamente 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 $z = -1$. Se invece n è pari, per nessun numero reale z si ha $z^n < 0$.

$$6.5. AB = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad BA = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}.$$

6.13. 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 $\sum_{k=1}^n b_{ik}^*a_{kj}^* = \sum_{k=1}^n b_{ki}a_{jk} = \sum_{k=1}^n a_{jk}b_{ki}$.

7.7. No, ad esempio $1 \notin 1$.

7.8. Le tre condizioni affinché ω sia un'equivalenza (riflessività, simmetria e transitività) sono soddisfatte, in quanto

- ▷ per ogni $a \in A$ si ha $(a, a) \in A \times A = \omega$, e quindi ω è riflessiva;
- ▷ per ogni $a, b \in A$ si ha $b \omega a$, e quindi ω è simmetrica;
- ▷ per ogni $a, b, c \in A$ si ha $a \omega c$, e quindi ω è transitiva.

Si ha poi $[a]_\omega = A$ per ogni $a \in A$, e quindi $A/\omega = \{A\}$.

7.10. *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 $f \sim h$.

7.12. Il codominio di π è $A/\sim = \{[a]_\sim \mid a \in A\}$. Pertanto un qualunque elemento del codominio di π è del tipo $[a]_\sim$ per qualche $a \in A$, cioè è del tipo $\pi(a)$ per qualche $a \in A$. Questo ci dice proprio che $\pi: A \rightarrow A/\sim$ è suriettiva.

7.13. La \sim_{ι_A} è la relazione di uguaglianza = su A .

7.19. La relazione di equivalenza \sim_F è definita, per ogni $n, m \in \mathbb{N}$, da $n \sim_F m$ se e solo se $|n| = |m|$.

7.21. Si osservi innanzitutto che gli elementi $f^{-1}(X)$ di \mathcal{G} sono sottoinsiemi non vuoti di A . In particolare, vale la (a) della definizione di partizione. Per dimostrare la (b), prendiamo un elemento $a \in A$. Allora $f(a) \in B$, e quindi esiste $X \in \mathcal{F}$ tale che $f(a) \in X$. Ne segue che $a \in f^{-1}(X)$;

in particolare $f^{-1}(X) \neq \emptyset$. Quindi $f^{-1}(X)$ è un elemento di \mathcal{G} , e a appartiene a questo elemento di \mathcal{G} . Per la (c) si considerino due elementi $f^{-1}(X) \neq f^{-1}(Y)$ di \mathcal{G} . Qui $X, Y \in \mathcal{F}$, $f^{-1}(X) \neq \emptyset$ e $f^{-1}(Y) \neq \emptyset$. Se fosse $X = Y$ si avrebbe $f^{-1}(X) = f^{-1}(Y)$, contraddizione. Quindi $X \neq Y$, e pertanto (\mathcal{F} è una partizione) $X \cap Y = \emptyset$. Mostriamo che $f^{-1}(X) \cap f^{-1}(Y) = \emptyset$. Se fosse $f^{-1}(X) \cap f^{-1}(Y) \neq \emptyset$, esisterebbe $a \in f^{-1}(X) \cap f^{-1}(Y)$. Allora $f(a) \in X$ e $f(a) \in Y$, e quindi $X \cap Y \neq \emptyset$, contraddizione. La contraddizione dimostra che $f^{-1}(X) \cap f^{-1}(Y) = \emptyset$.

7.22. (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) Abbiamo già visto in (b) che se $y = 0$, allora $\psi^{-1}(y) = \emptyset$. Supponiamo quindi $y \neq 0$ e distinguiamo i tre casi $y < y^{-1}$, $y = y^{-1}$, $y > y^{-1}$.

Se $y < y^{-1}$, allora $\psi^{-1}(y) = \emptyset$.

Se $y = y^{-1}$, allora $\psi^{-1}(y) = \{y\}$.

Se $y > y^{-1}$, allora $\psi^{-1}(y) = \{y, y^{-1}\}$ ha cardinalità 2.

Pertanto $|\psi^{-1}(y)| = 1$ se e solo se $y = y^{-1}$, ossia se e solo se $y^2 = 1$, vale a dire se e solo se $y = 1$ o $y = -1$.

(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 $a \sim_\psi b$.

7.23. 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 $\pi^{-1}(\pi(B)) \subseteq B$.

7.24. (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 $f, g, h \in \mathbb{N}^A$ tali che $f \sim g$ e $g \sim h$. Allora $\{a \in A \mid f(a) \neq g(a)\} \cup \{a \in A \mid g(a) \neq h(a)\}$ 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 $f(b) = h(b)$, 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 \mathbb{N}^A . Allora per ogni $f, g \in \mathbb{N}^A$, $\{a \in A \mid f(a) \neq g(a)\}$ è un insieme finito. Siano in particolare $f, g: A \rightarrow \mathbb{N}$ 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 $f, g \in \mathbb{N}^A$ 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 $f, g \in \mathbb{N}^A$, cioè \sim è la relazione banale su \mathbb{N}^A .

(c) Siano $n, m \in \mathbb{N}$ 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 in questo caso $f_n(a) = n \neq m = f_m(a)$ per ogni $a \in A$), e $\{a \in A \mid f_n(a) \neq f_m(a)\} = \emptyset$ 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 $n = m$.

7.25. (a) *Transitività.* Siano $f, g, h \in B^{\mathbb{N}}$ tali che $f \sim g$ e $g \sim h$. Allora esistono $n, m \in \mathbb{N}$ 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 $f(i) = g(i) = h(i)$ 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 $B^{\mathbb{N}}$. 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 $f_a, f_b : \mathbb{N} \rightarrow B$ le applicazioni definite da $f_a(n) = a$ per ogni $n \in \mathbb{N}$ e $f_b(n) = b$ per ogni $n \in \mathbb{N}$. Dato che \sim è la relazione banale su $B^{\mathbb{N}}$, si deve avere $f_a \sim f_b$. Quindi esiste $n \in \mathbb{N}$ 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 $f : \mathbb{N} \rightarrow B$, cioè $|B^\mathbb{N}| = 1$. Dato che sull'insieme $B^{\mathbb{N}}$ 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 $n \in \mathbb{N}$ 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 φ è iniettiva.

7.26. Per dimostrare che f e g sono due biiezioni, una inversa dell'altra, è sufficiente dimostrare che $g \circ f = \iota_{\mathcal{E}}$ e $f \circ g = \iota_{\mathcal{P}}$.

Mostriamo che $g \circ f = \iota_{\mathcal{E}}$. Si osservi intanto che le due applicazioni $g \circ f$ e $\iota_{\mathcal{E}}$ hanno entrambe dominio e codominio uguali a \mathcal{E} . Quindi per dimostrare che le due applicazioni coincidono si deve dimostrare che $g \circ f(\sim) = \iota_{\mathcal{E}}(\sim)$ per ogni $\sim \in \mathcal{E}$. Ora

$$g \circ f(\sim) = g(f(\sim)) = g(A/\sim) = \sim_{A/\sim}$$

e $\iota_{\mathcal{E}}(\sim) = \sim$. Pertanto dobbiamo dimostrare che $\sim_{A/\sim} = \sim$, cioè che le due equivalenze $\sim_{A/\sim}$ 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 $\sim_{A/\sim}$ si ha che $a \sim_{A/\sim} b$ se e sono 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 sono 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 $a \sim b$, 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 $\sim_{A/\sim}$ e \sim sono uguali.

Dimostriamo ora che $f \circ g = \iota_{\mathcal{P}}$. Osserviamo intanto che le due applicazioni $f \circ g$ e $\iota_{\mathcal{P}}$ hanno entrambe dominio e codominio uguali a \mathcal{P} . Quindi per dimostrare che le due applicazioni sono uguali si deve far vedere che $f \circ g(\mathcal{F}) = \iota_{\mathcal{P}}(\mathcal{F})$ per ogni $\mathcal{F} \in \mathcal{P}$. Ora $f \circ g(\mathcal{F}) = f(g(\mathcal{F})) = f(\sim_{\mathcal{F}}) = A/\sim_{\mathcal{F}} = \iota_{\mathcal{P}}(\mathcal{F}) = \mathcal{F}$. 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 $t \in X = [a]_{\sim_{\mathcal{F}}} = \{x \mid x \in A, x \sim_{\mathcal{F}} a\}$, 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 $a \in Y$, 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 $A / \sim_{\mathcal{F}} = \mathcal{F}$.

7.27. (a) Supponiamo che \sim_f sia la relazione banale ω . Allora $x \sim_f y$ per ogni $x, y \in \mathbb{Z}$, cioè $f(x) = f(y)$ per $x, y \in \mathbb{Z}$. Sia $a = f(1) \in A$. Allora $f(x) = a$ per ogni $x \in \mathbb{Z}$.

Viceversa supponiamo che esista $a \in A$ tale che $f(x) = a$ per ogni $x \in \mathbb{Z}$. Allora $f(x) = f(y)$ per ogni $x, y \in \mathbb{Z}$, cioè $x \sim_f y$ per ogni $x, y \in \mathbb{Z}$. Equivalentemente, la relazione \sim_f coincide con la relazione banale ω .

(b) Supponiamo che \sim_f sia la relazione di uguaglianza $=$. Questo vuol dire che per ogni $x, y \in \mathbb{Z}$ si ha $x \sim_f y$ se e solo se $x = y$. Equivalentemente, per ogni $x, y \in \mathbb{Z}$ si ha $f(x) = f(y)$ se e solo se $x = y$. Questo vuol dire che $f: \mathbb{Z} \rightarrow A$ è iniettiva. Ma se esiste un'applicazione iniettiva $f: \mathbb{Z} \rightarrow A$, l'insieme A è certamente infinito.

8.7. Supponiamo $ab \equiv ac \pmod{n}$. Per il corollario 4.5 esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha a + \beta n = 1$. Quindi $\alpha a \equiv 1 \pmod{n}$. Ma allora $b = 1b \equiv \alpha ab \equiv \alpha ac \equiv 1c = c \pmod{n}$ per l'esercizio 8.2.

8.11. (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 $x \in [a]_{} \rightleftharpoons$ 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 $x \in f^{-1}([f(a)]_{\equiv_n})$.

8.12. Siano $a, b \in \mathbb{Z}$ tali che $[a]_{\equiv_3} = [b]_{\equiv_3}$. Allora $a \equiv b \pmod{3}$, cioè $3|(a - b)$, vale a dire esiste $c \in \mathbb{Z}$ tale che $a - b = 3c$. Ne segue che $2a - 2b = 6c$, ossia $6|(2a - 2b)$, 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 ψ 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 $6|(2a - 2b)$, cioè esiste $d \in \mathbb{Z}$ tale che $2a - 2b = 6d$. Ma allora $a - b = 3d$, ossia $3|(a - b)$, da cui $[a]_{\equiv_3} = [b]_{\equiv_3}$. Questo dimostra che ψ è iniettiva.

8.13. (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 ϱ sono

$$[1]_{\varrho} = \{1\}, \quad [2]_{\varrho} = \{2, -3\}, \quad [3]_{\varrho} = \{3, 23, -7, 28\}, \quad [4]_{\varrho} = \{4, -1, 14\}.$$

In particolare A / ϱ 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) Si, in quanto $\varphi([1]_Q) = [1]_{\equiv_5}$, $\varphi([2]_Q) = [2]_{\equiv_5}$, $\varphi([3]_Q) = [3]_{\equiv_5}$, $\varphi([4]_Q) = [4]_{\equiv_5}$, 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 $C \in A/Q$ tale che $\varphi(C) = [0]_{\equiv_5}$.

9.5. Si semplifichi prima di moltiplicare. Si trova che $\binom{10}{8} = \frac{10!}{8! \cdot 2!} = \frac{9 \cdot 10}{2!} = \frac{90}{2} = 45$ e $\binom{n+1}{n-2} = \frac{(n+1)!}{(n-2)! \cdot 3!} = \frac{(n-1)n(n+1)}{6}$.

$$9.8. 26^2 \cdot 10^3 \cdot 26^2 = 456\,976\,000.$$

9.9. (d) $\binom{m}{2}$.

(e) mn .

(f) Dato che $A \cap B = \emptyset$, i due casi $y \in A$ e $y \in B$ si escludono l'un l'altro. Ci sono $\binom{m}{2}$ insiemi $\{x, y\}$ con $x \in A$, $y \in A$ e $x \neq y$. Ci sono mn insiemi $\{x, y\}$ con $x \in A$ e $y \in B$ (e quindi $x \neq y$). Pertanto ci sono $\binom{m}{2} + mn$ insiemi $\{x, y\}$ con $x \in A$, $y \in A \cup B$ e $x \neq y$.

9.10. (a) I divisori interi di $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ sono tutti e soli i numeri del tipo $\pm p_1^{i_1} p_2^{i_2} \cdots p_t^{i_t}$ con $0 \leq i_j \leq \alpha_j$ per ogni $j = 1, 2, \dots, t$. Ora il segno può essere scelto in 2 modi (+ o -), i_1 può essere scelto in $\alpha_1 + 1$ modi, i_2 può essere scelto in $\alpha_2 + 1$ modi, e così via. In definitiva i divisori possono essere costruiti in $2(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)$ modi.

(b) I numeri naturali che dividono n sono tutti e soli del tipo $p_1^{i_1} p_2^{i_2} \cdots p_t^{i_t}$ con $0 \leq i_j \leq \alpha_j$ per ogni $j = 1, 2, \dots, t$. Quindi ce ne sono $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)$. Se n è un quadrato, tutti gli α_j sono pari, quindi tutti gli $\alpha_j + 1$ sono dispari, e pertanto $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)$ è dispari.

(c) Se n non è un quadrato, non tutti gli esponenti α_j sono pari, ossia almeno un α_j è dispari. Quindi almeno un $\alpha_j + 1$ è pari e pertanto $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)$ è pari.

9.12. Invece di contare le relazioni di equivalenza su X , si contano le partizioni di X .

(a) Se $X = \{x_0\}$ ha un solo elemento, c'è un'unica partizione di X , la $\{\{x_0\}\}$.

(b) Se $X = \{x_0, x_1\}$ ha due elementi, le partizioni di X sono due, $\{\{x_0\}, \{x_1\}\}$ e $\{\{x_0, x_1\}\}$.

(c) Se $X = \{x_0, x_1, x_2\}$ ha tre elementi, le partizioni di X sono cinque:

$$\{\{x_0, x_1, x_2\}\}, \quad \{\{x_0\}, \{x_1, x_2\}\}, \quad \{\{x_1\}, \{x_0, x_2\}\}, \quad \{\{x_2\}, \{x_0, x_1\}\} \quad \text{e} \quad \{\{x_0\}, \{x_1\}, \{x_2\}\}.$$

9.13. Nella seconda dimostrazione della proposizione 9.7, per dimostrare che σ è suriettiva si è fatto vedere che dato f nel codominio $\{0, 1\}^A$ di σ , si ha $\chi_{f^{-1}(1)} = f$, cioè $\sigma(f^{-1}(1)) = f$. Quindi σ manda $f^{-1}(1)$ in f . L'inversa σ^{-1} di σ deve pertanto mandare f in $f^{-1}(1)$. Quindi $\sigma^{-1}: \{0, 1\}^A \rightarrow \mathcal{P}(A)$ è definita da $\sigma^{-1}(f) = f^{-1}(1)$ per ogni $f \in \{0, 1\}^A$.

9.18. (a) $b - 1$.

(b) Ve ne sono b . La decina eccezionale è costituita dai b numeri $1, 2, 3, \dots, b - 1, (b - 1)b$.

(c) $b - 2$.

(d) $\binom{b-2}{2}$.

(e) $b - 1$.

(f) b .

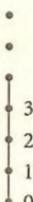
(g) $2b - 2$ se $c \neq b - 1$. La cifra di $b - 1$ ha invece b elementi.

(h) $(b - 1)b/2$.

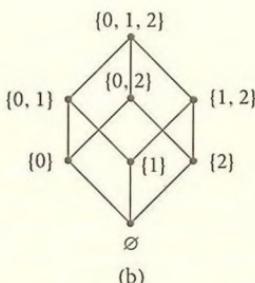
(i) $(b - 1)b/2$.

9.19. Tante quante i sottoinsiemi di cardinalità 6 di un insieme di 90 elementi, ossia $\binom{90}{6} = 622\,614\,630$.

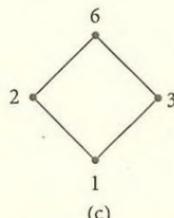
10.8.



(a)



(b)



(c)

10.10. Non è totalmente ordinato; gli elementi massimali sono a e b ; non esiste il massimo; d è l'unico elemento minimale; d è il minimo; c è l'estremo inferiore di $\{a, b\}$; non esistono né massimo, né minimo, né estremo superiore di $\{a, b\}$; i maggioranti di $\{c, d\}$ sono a , b e c .

10.17. (a) L'estremo superiore non esiste, l'estremo inferiore è 0.

(b) L'estremo superiore non esiste, l'estremo inferiore è 0.

(c) Non esistono né l'estremo superiore né quello inferiore.

(d) Non esistono né l'estremo superiore né quello inferiore.

(e) L'estremo superiore è 2, l'estremo inferiore è -2.

(f) L'estremo superiore è 2, l'estremo inferiore è -2.

10.23. (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 è \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} : $B = \{1/z \mid z \in \mathbb{N}, z \neq 0\}$, $C = A \cup \{0\}$, $D = B \cup \{0\}$, eccetera.

10.24. (a) Sia (Z, m) un maggiorante di \mathcal{G} in \mathcal{F} . Allora Z è un sottoinsieme di A , $m: Z \rightarrow B$ è un'applicazione, e per ogni $(X, f) \in \mathcal{G}$ si ha $(X, f) \leq (Z, m)$; per come è definito l'ordine parziale \leq su \mathcal{F} questo significa che $X \subseteq Z$ e che $f(x) = m(x)$ per ogni $(X, f) \in \mathcal{G}$ ed ogni $x \in X$. Ma allora per ogni $(X, f), (Y, g) \in \mathcal{G}$ ed ogni $a \in X \cap Y$ si ha che $a \in Z$ e che $f(a) = m(a) = g(a)$.

(b) Supponiamo ora che per ogni $(X, f), (Y, g) \in \mathcal{G}$ ed ogni elemento $a \in X \cap Y$ 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 φ 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 φ è ben definita.

Dato che $S \subseteq A$ e $\varphi: S \rightarrow B$ è un'applicazione, la coppia (S, φ) è un elemento di \mathcal{F} . Per dimostrare che (S, φ) 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 $(Z, m) \geq (X, f)$ 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 $x \in X$ si ha $\varphi(x) = f(x)$. Quindi $(S, \varphi) \geq (X, f)$ per ogni $(X, f) \in \mathcal{G}$. 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 ogni $(X, f) \in \mathcal{G}$ 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 $(Z, m) \geq (S, \varphi)$. Questo dimostra che (S, φ) 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, φ) 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} .

10.28. (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 τ , quello che si deve dimostrare è che se $a \sigma a'$ e $b \sigma b'$, ove $a, a', b, b' \in A$, allora $a \varrho b$ se e solo se $a' \varrho b'$. Per come è definita la relazione σ , dobbiamo mostrare pertanto che da $a \varrho a', a' \varrho a, b \varrho b', b' \varrho b$ e $a \varrho b$ segue $a' \varrho b'$, e che da $a \varrho a', a' \varrho a, b \varrho b', b' \varrho b$ e $a' \varrho b'$ segue $a \varrho b$. Queste implicazioni sono ovvie perché ϱ è transitiva.

(c) *Riflessività.* Per ogni $a \in A$ si ha $a \varrho a$ perché ϱ 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 $a \varrho b$ e $b \varrho a$, da cui $a \sigma b$, e pertanto $[a]_\sigma = [b]_\sigma$.

Transitività. Siano $a, b, c \in A$ tali che $[a]_\sigma \tau [a]_\sigma$ e $[a]_\sigma \tau [c]_\sigma$. Allora $a \varrho b$ e $b \varrho c$, da cui $a \varrho c$ perché ϱ è transitiva. Quindi $[a]_\sigma \tau [c]_\sigma$.

11.20. Per ogni $x, y \in L$ si ha $\varphi(x \vee y) = (x \vee y) \vee a = x \vee (y \vee a) = x \vee (a \vee y) = x \vee ((a \vee a) \vee y) = x \vee (a \vee (a \vee y)) = x \vee (a \vee (y \vee a)) = (x \vee a) \vee (y \vee a) = \varphi(x) \vee \varphi(y)$ e $\varphi(x \wedge y) = (x \wedge y) \vee a = (x \vee a) \wedge (y \vee a) = \varphi(x) \wedge \varphi(y)$. Quindi φ è un omomorfismo di reticolati.

(a) \Rightarrow (b) Supponiamo che φ sia un isomorfismo di reticolati, cioè che φ sia biiettiva. 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 φ è l'applicazione identica di L in L .

(c) \Rightarrow (a) Ovvio.

11.23. (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 $Z \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$, $A \subseteq Z$ e $B \subseteq Z$, allora $A \cup B \subseteq Z$. Tutte queste affermazioni sono ovvie.

Per la seconda affermazione distinguiamo 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 $Z \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$, $Z \subseteq A$ 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 $Z \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$, $Z \subseteq A$ e $Z \subseteq B$, allora $Z \subseteq \emptyset$. Le prime due di queste affermazioni sono ovvie. Per la terza si osservi che se $Z \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$, $Z \subseteq A$ 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 $1_L = \mathbb{Z}$ perché $A \subseteq \mathbb{Z}$ per ogni $A \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$, e $0_L = \emptyset$ perché $\emptyset \subseteq A$ per ogni $A \in \mathcal{P}_\infty(\mathbb{Z}) \cup \{\emptyset\}$. Quindi il reticolo L è limitato.

(c) Sia $A \in L$ tale che $\mathbb{Z} \setminus A$ 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 $A \cup B = \mathbb{Z}$. 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 $B = [A \cup (\mathbb{Z} \setminus A)] \cap B = (A \cap B) \cup [(\mathbb{Z} \setminus A) \cap B] \subseteq (A \cap B) \cup (\mathbb{Z} \setminus A)$ 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 $A \cup B = \mathbb{Z}$ segue che $A = \mathbb{Z}$ e quindi $\mathbb{Z} \setminus A$ 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) $(2\mathbb{Z}_{\geq 0} \wedge 2\mathbb{Z}_{\leq 0}) \vee \mathbb{D} = \emptyset \vee \mathbb{D} = \emptyset \cup \mathbb{D} = \mathbb{D}$ e $(2\mathbb{Z}_{\geq 0} \vee \mathbb{D}) \wedge (2\mathbb{Z}_{\leq 0} \vee \mathbb{D}) = (2\mathbb{Z}_{\geq 0} \cup \mathbb{D}) \wedge (2\mathbb{Z}_{\leq 0} \cup \mathbb{D})$. Dato che $(2\mathbb{Z}_{\geq 0} \cup \mathbb{D}) \cap (2\mathbb{Z}_{\leq 0} \cup \mathbb{D}) = \mathbb{D} \cup \{0\}$ è un insieme infinito ne segue che $(2\mathbb{Z}_{\geq 0} \cup \mathbb{D}) \wedge (2\mathbb{Z}_{\leq 0} \cup \mathbb{D}) = (2\mathbb{Z}_{\geq 0} \cup \mathbb{D}) \cap (2\mathbb{Z}_{\leq 0} \cup \mathbb{D}) = \mathbb{D} \cup \{0\}$.

11.32. (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 $x \wedge y \in K$.

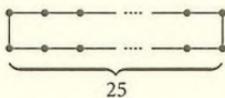
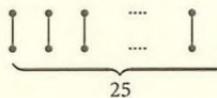
(d) Siano $x, x', y, y' \in B$ tali che $[x]_{\sim_f} = [x']_{\sim_f}$ e $[y]_{\sim_f} = [y']_{\sim_f}$. Allora $x \sim_f x'$ e $y \sim_f y'$, cioè $f(x) = f(x')$ e $f(y) = f(y')$. Quindi $f(x) \leq f(y)$ se e solo se $f(x') \leq f(y')$.

(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 $[x]_{\sim_f} \preceq [z]_{\sim_f}$.

12.4. No, in un grafo con 100 vertici si deve avere $d(v) < 100$ per ogni vertice v , e quindi non può essere $d(v_{100}) = 100$.

12.5. Sì, ad esempio

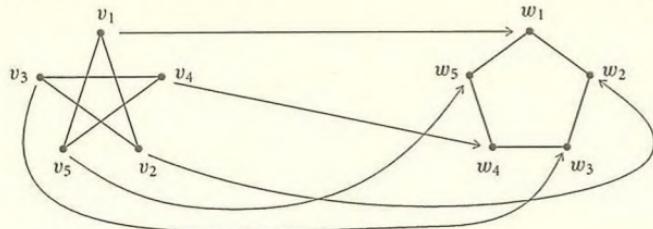


12.6. No. I numeri naturali dispari $i \leq 98$ sono $98/2 = 49$, che è dispari, mentre ogni grafo deve avere un numero pari di vertici dispari.

12.11. (a) Etichettiamo gli insiemi

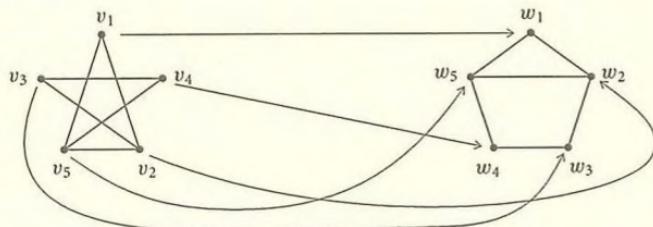
$$V = \{v_1, v_2, v_3, v_4, v_5\} \quad e \quad W = \{w_1, w_2, w_3, w_4, w_5\}$$

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 φ 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 3. 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 φ 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 φ 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 φ appena descritto.

12.14. 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 quello di figura 48.2(a). Per $d = 0$ il grafo deve essere quello di figura 48.2(b).

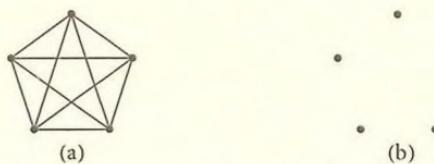


FIGURA 48.2.

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 ℓ_0 e ℓ_1 . Siano v_0 e v_2 i vertici diversi da v_1 di ℓ_0 e ℓ_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 $v \neq v_2$ e $v \neq v_1$. Se fosse $v = v_0$, il grafo G avrebbe come sottografo il grafo di figura 48.3(a). 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 di figura 48.3(b). 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 quello di figura 48.3(c).

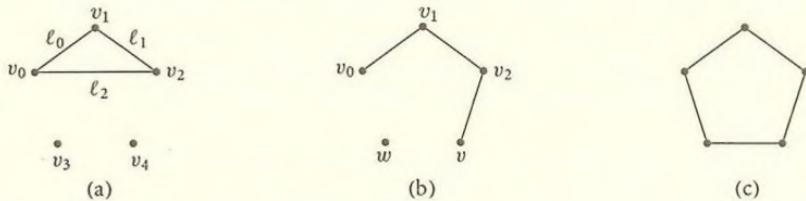


FIGURA 48.3.

Abbiamo così dimostrato che a meno di isomorfismi ci sono esattamente tre grafi regolari con 5 vertici, aventi grado 0, 2 e 4 rispettivamente.

12.15. Siano $G = (V, L)$ e $G' = (V', L')$ due grafi orientati. Un *isomorfismo* (di grafi orientati) di G in G' è una biezione $\varphi: V \rightarrow V'$ tale che per ogni $v, w \in V$ si ha $(v, w) \in L$ se e solo se $(\varphi(v), \varphi(w)) \in L'$.

12.16. (a) Se ϱ è la relazione di uguaglianza $=$, il suo grafo è $G_0 = G_\varrho = (V, \varrho)$ dove $\varrho = \{(a, b) \mid a, b \in V, a \varrho b\} = \{(a, b) \mid a, b \in V, a = b\} = \{(a, a) \mid a \in V\} = D_V$. Quindi $G_0 = (V, D_V)$.

(b) Si deve dimostrare che se ϱ è un'equivalenza su V , allora $\varrho = (\pi \times \pi)^{-1}(D_{V/\varrho})$, cioè che per ogni coppia $(v, v') \in V \times V$ si ha $(v, v') \in \varrho$ se e solo se $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\varrho})$.

Si ha $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\varrho})$ se e solo se $(\pi \times \pi)(v, v') \in D_{V/\varrho}$, cioè se e solo se $(\pi(v), \pi(v')) \in D_{V/\varrho}$, ossia se e solo se $\pi(v) = \pi(v')$. Ma $\pi(v) = [v]_\varrho$ e $\pi(v') = [v']_\varrho$. Quindi $(v, v') \in (\pi \times \pi)^{-1}(D_{V/\varrho})$ se e solo se $[v]_\varrho = [v']_\varrho$, e questo accade se e solo se $v \varrho v'$, cioè se e solo se $(v, v') \in \varrho$.

13.3. Non è possibile percorrere esattamente una volta i sette ponti della città perché il multgrafo della figura 13.5 ha vertici dispari.

13.7. (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 12.4 il grafo 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 che anche 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 è sottografo di sé stesso. 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.

13.11. Siano $1 \leq m \leq n$ numeri interi.

(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 intero arbitrario.

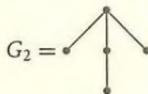
14.2. Per il teorema 14.3 un albero con 5 vertici deve avere 4 lati. Vediamo quindi in quanti e quali modi si possono disegnare quattro lati per ottenere un albero. In un grafo con 5 vertici ogni vertice deve avere grado ≤ 4 . Se c'è un vertice v_0 di grado 4 il grafo, avendo solo 4 lati, dovrà essere isomorfo al grafo



Se c'è un vertice v_0 di grado 3, il grafo dovrà avere un sottografo del tipo



e il quarto lato dovrà essere incidente in uno dei vertici disegnati in basso. Comunque si scelga uno dei vertici disegnati in basso, il grafo sarà sempre isomorfo al grafo



Se tutti i vertici hanno grado ≤ 2 , l'albero, essendo connesso, dovrà essere necessariamente isomorfo al grafo



Ecco quindi che ci sono esattamente tre alberi con 5 vertici a meno di isomorfismi, perché ogni albero con 5 vertici è isomorfo a G_1 o a G_2 o a G_3 , e questi tre grafi non sono a due a due isomorfi tra loro.

14.4. Applichiamo la formula del lemma 12.3. Sia n il numero cercato, ossia il numero di vertici di grado 1. L'albero ha quindi $|V| = n + 2 + 3 + 4 = n + 9$ vertici e si ha

$$\sum_{v \in V} d(v) = n \cdot 1 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 = n + 29.$$

Per il teorema 14.3 l'albero ha $n + 8$ lati, e quindi per la formula del lemma 12.3 si ha $n + 8 = \frac{1}{2}(n + 29)$, da cui $n = 13$.

Nella figura 48.4 è disegnato un albero soddisfacente a queste condizioni.

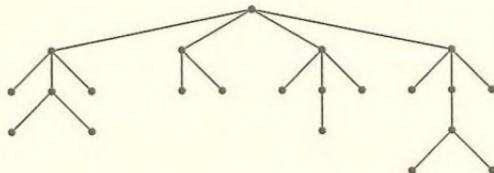


FIGURA 48.4.

14.5. Si ragioni come per l'esercizio precedente. Sia n_1 il numero cercato, di modo che l'albero ha $|V| = n_1 + n_2 + \dots + n_k$ vertici. Si ha

$$\sum_{v \in V} d(v) = n_1 + 2n_2 + 3n_3 + \dots + kn_k.$$

Dato che l'albero ha $n_1 + n_2 + \dots + n_k - 1$ lati, dal lemma 12.3 si ottiene

$$n_1 + n_2 + n_3 + \dots + n_k - 1 = \frac{1}{2}(n_1 + 2n_2 + 3n_3 + \dots + kn_k),$$

da cui

$$n_1 = n_3 + 2n_4 + 3n_5 + \dots + (k-2)n_k + 2.$$

Se ne deduce in particolare che ogni albero finito con almeno due vertici ha almeno due vertici di grado 1. Questo migliora la proposizione 14.2.

14.7. (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 "interni" 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 $(3,2)$. In tutti e tre i casi G ha un cammino euleriano.

14.9. (a) Figura 48.5.

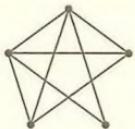


FIGURA 48.5.

(b) Lo stesso di (a), in quanto ogni grafo finito con 8 lati è planare per l'esercizio 14.8.

15.6. (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) Si supponga che S sia un semigruppo commutativo. Per dimostrare che anche S^X è un semigruppo 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.

15.13. 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

$$\begin{aligned} ((s, t)(s', t'))(s'', t'') &= (ss', tt')(s'', t'') = ((ss')s'', (tt')t'') = (s(s's''), t(t't'')) \\ &= (s, t)(s's'', t't'') = (s, t)((s', t')(s'', t'')). \end{aligned}$$

15.15. (a) Per ogni $(a, b), (a', b'), (a'', b'') \in \mathbb{R} \times \mathbb{R}$ si ha $((a, b) * (a', b')) * (a'', b'') = (aa', ab' + b) * (a'', b'') = (aa'a'', aa'b'' + ab' + b)$ e $(a, b) * ((a', b') * (a'', b'')) = (a, b) * (a'a'', a'b'' + b') = (aa'a'', a(a'b'' + b') + b) = (aa'a'', aa'b'' + ab' + b)$. 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 $\{1\} \times \mathbb{R}$ di $\mathbb{R} \times \mathbb{R}$ è un sottosemigruppo di $(\mathbb{R} \times \mathbb{R}, *)$, in quanto per ogni $b, b' \in \mathbb{R}$ si ha $(1, b) * (1, b') = (1, b' + b) \in \{1\} \times \mathbb{R}$. Analogamente $\mathbb{R} \times \{0\}$ è un sottosemigruppo di $(\mathbb{R} \times \mathbb{R}, *)$, in quanto per ogni $a, a' \in \mathbb{R}$ si ha $(a, 0) * (a', 0) = (aa', 0 + 0) = (aa', 0) \in \mathbb{R} \times \{0\}$.

(d) Sia $b \in \mathbb{R}$. 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 $n > 1$ e che l'uguaglianza sia vera per $n - 1$, cioè che $(1, b)^{n-1} = (1, (n-1)b)$. Allora $(1, b)^n = (1, b)^{n-1} * (1, b) = (1, (n-1)b) *$

$(1, b) = (1, b + (n - 1)b) = (1, nb)$. Per 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 $n > 1$ e 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.

16.5. 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 solo 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 destre.

In particolare A è un monoide se e solo se A ha un'identità sinistra e destra, se e solo se $|A| = 1$.

16.20. (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 $(x, y) = (x', y')$.

16.22. (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 φ è un endomorfismo del monoide (\mathbb{R}, \cdot) tale che $\varphi(0) = 0$ e $\varphi(\alpha) = -1$ per ogni numero reale negativo α , allora per ogni numero reale positivo β 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 φ 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 φ 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 φ è un endomorfismo di monoidi.

(c) Si ha $\varphi(\mathbb{R}) = \{1, 0, -1\} = S$.

16.23. (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 ≥ 2 e quindi $a + b \in M$.

(b) Ragioniamo per assurdo e supponiamo che il monoide M sia ciclico. 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 $3 \in M$.

17.6. (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 $x^{nm} = (x^n)^m = (y^n)^m = y^{nm} = (y^m)^n = (z^m)^n = z^{nm}$. Quindi $x \sim z$.

(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 $x \sim 1_M$.

17.7. (a) Riflessività. Per ogni $a \in \mathbb{Z}$ si ha $2^0a = 2^0a$, e quindi $a \sim a$.

Transitività. Siano $a, b, c \in \mathbb{Z}$ 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 $2^{n+p} a = 2^p 2^n b = 2^p 2^m b = 2^m 2^q c = 2^{m+q} c$. Quindi $a \sim c$.

(b) Siano $a, b, c, d \in \mathbb{Z}$ 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 $X \in \mathbb{Z}/\sim$. Allora esiste $x \in \mathbb{Z}$ 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 $a \in \mathbb{Z}$ dispari. Si ha $2^0 x = 2^n a$, e quindi $x \sim a$, da cui $[x]_\sim = [a]_\sim$. Ma allora $a \in D$ è un elemento tale che $\phi(a) = [a]_\sim = [x]_\sim = X$.

ϕ è un omomorfismo di monoidi. Si ha $\phi(1) = [1]_\sim = 1_{\mathbb{Z}/\sim}$ e $\phi(ab) = [ab]_\sim = [a]_\sim[b]_\sim = \phi(a)\phi(b)$ per ogni $a, b \in D \cup \{0\}$.

17.11. (c) Si deve dimostrare che da $(n, m) \sim (n', m')$ e $(r, s) \sim (r', s')$ segue $(n, m) \cdot (r, s) \sim (n', m') \cdot (r', s')$.

$(n', m') \cdot (r', s')$ per ogni $n, m, n', m', r, s, r', s' \in \mathbb{N}$. Ora $(n, m) \sim (n', m')$ equivale a

$$(48.1) \quad n + m' = m + n',$$

$(r, s) \sim (r', s')$ equivale a

$$(48.2) \quad r + s' = s + r',$$

e $(n, m) \cdot (r, s) \sim (n', m') \cdot (r', s')$, cioè $(nr + ms, ns + mr) \sim (n'r' + m's', n's' + m'r')$, equivale a

$$(48.3) \quad nr + ms + n's' + m'r' = ns + mr + n'r' + m's'.$$

Quindi si deve dimostrare che dalla (48.1) e dalla (48.2) segue la 48.3. Ora dalla 48.1 si ottiene l'uguaglianza tra interi $n - m = n' - m'$ e dalla 48.2 si ottiene $r - s = r' - s'$. Moltiplicando membro a membro queste uguaglianze si ottiene $nr - mr - ns + ms = n'r' - m'r' - n's' + m's'$, e da questa segue subito la (48.3).

17.13. (c) Si deve dimostrare che da $(z, w) \sim (z', w')$ e $(p, q) \sim (p', q')$ segue $(z, w) + (p, q) \sim (z', w') + (p', q')$ per ogni $(z, w), (z', w'), (p, q), (p', q') \in \mathbb{Z} \times \mathbb{Z}^*$. Ora $(z, w) \sim (z', w')$ equivale a

$$(48.4) \quad zw' = wz',$$

$(p, q) \sim (p', q')$ equivale a

$$(48.5) \quad pq' = qp',$$

e $(z, w) + (p, q) \sim (z', w') + (p', q')$, cioè $(zq + wp, wq) \sim (z'q' + w'p', w'q')$, equivale a

$$(48.6) \quad zqw'q' + wpw'q' = wqz'q' + wqw'p'.$$

Quindi si deve dimostrare che dalla (48.4) e dalla (48.5) segue la (48.6). Ma se valgono le (48.4) e (48.5), si ha $zqw'q' + wpw'q' = (zw')(qq') + (pq')(ww') = (wz')(qq') + (qp')(ww') = wqz'q' + wqw'p'$, che è la (48.6).

17.14. (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 $1_{A^\sim} = \iota_A \in S$ perché ovviamente $x \sim y$ implica $\iota_A(x) \sim \iota_A(y)$.

(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 $\varphi(1_S) = \iota_{A/\sim}$. 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 $(\tilde{f} \circ \tilde{g})([a]) = \tilde{f} \circ \tilde{g}([a])$ per ogni $a \in A$. Ma $(\tilde{f} \circ \tilde{g})([a]) = \tilde{f}(\tilde{g}([a])) = \tilde{f}([g(a)]) = [f(g(a))] = [(f \circ g)(a)] = \tilde{f} \circ \tilde{g}([a])$. Inoltre $\varphi(1_S) = \varphi(\iota_A) = \tilde{\iota}_A$ è uguale a $1_{(A/\sim)^{(A/\sim)}} = \iota_{A/\sim}$, perché per ogni $a \in A$ si ha $\tilde{\iota}_A([a]) = [\iota_A(a)] = [a] = \iota_{A/\sim}([a])$.

18.4. *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 18.1), in corrispondenza all'applicazione $\tilde{f} = h \circ \varphi = h' \circ \varphi: A \rightarrow M$ esiste un *unico* omomorfismo di monoidi $\tilde{f}: W \rightarrow M$ tale che $\tilde{f} \circ \varphi = f$. Dato che h, h' sono entrambi due omomorfismi di W in M tali che $h \circ \varphi = h' \circ \varphi = f$, ne segue che $\tilde{f} = h = h'$.

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 $\widehat{f}: W \rightarrow M$ tale che $\widehat{f} \circ \varphi = f$. Allora $\widehat{f} \in \text{Hom}(W, M)$ e $\Phi(\widehat{f}) = \widehat{f} \circ \varphi = f$.

19.9. Se $m\mathbb{Z} \supseteq n\mathbb{Z}$, allora $n = n \cdot 1 \in n\mathbb{Z} \subseteq m\mathbb{Z}$, e quindi esiste $t \in \mathbb{Z}$ tale che $n = mt$. Ne segue che $m \mid n$.

Viceversa se $m \mid n$, cioè se esiste $t \in \mathbb{Z}$ tale che $n = mt$, verifichiamo che vale l'inclusione $m\mathbb{Z} \supseteq n\mathbb{Z}$: se $x \in n\mathbb{Z}$, allora $x = nz$ per qualche $z \in \mathbb{Z}$, e quindi $x = nz = m(tz) \in m\mathbb{Z}$.

19.11. (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 $mnx = mn(g + h) = mng + mnh = n(mg) + m(nh) = n \cdot 0_G + m \cdot 0_G = 0_G$. 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 4.5 esistono $\alpha, \beta \in \mathbb{Z}$ 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 $x = \alpha(nx) + \beta(mx) \in S$.

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 α e β sono interi tali che $\alpha n + \beta m = 1$ (esistono per il corollario 4.5), allora $x = \alpha nx + \beta mx = 0_G$. Questo dimostra che $G[m] \cap G[n] = \{0_G\}$.

19.12. (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 sottosemigruppo di M . Se $x, y \in eMe$, allora $x = eme$ e $y = em'e$ per opportuni $m, m' \in M$, e quindi $xy = emem'e$. 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 semigruppo. Resta da dimostrare che possiede un'identità. Il suo elemento $e1_{eMe} = e^2 = e$ 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 $ex = eeme = eme = x$.

19.19. (a) Il gruppo (\mathbb{C}^*, \cdot) non ha la proprietà: ad esempio l'elemento $i \in \mathbb{C}^*$ è tale che $i^4 = 1$, mentre $i \neq 1$. Invece il gruppo $(\mathbb{C}, +)$ ha la proprietà: se $x \in \mathbb{C}$, 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 tali che $x^n = x^m$. Per simmetria si può supporre che $n \geq m$. Allora $x^{n-m} = x^n x^{-m} = x^n (x^m)^{-1} = x^n (x^n)^{-1} = 1_G$. Se fosse $n > m$ 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 $n = m$.

(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 $x^1 = x = y^n = (x^m)^n = x^{mn}$, 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.

20.4. (a) La relazione ϱ è definita, per ogni $a, b \in \mathbb{Z}$, da $a \varrho b$ se $a = b$ oppure $a = -b$, e quindi $a \varrho b$ se e solo se $|a| = |b|$. È immediato verificare che questa è un'equivalenza. La relazione σ 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 σ non è simmetrica, e quindi, in particolare, non è un'equivalenza. La relazione τ 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 τ se e solo se sono uguali oppure appartengono entrambi a $\{1, 5\}$ oppure appartengono entrambi a $\{-1, -5\}$. Ne segue quindi che τ è la relazione di equivalenza $\sim_{\mathcal{F}}$ associata alla partizione

$$\mathcal{F} = \{\{1, 5\}, \{-1, -5\}, \{z\} \mid z \in \mathbb{Z} \setminus \{1, 5, -1, -5\}\}.$$

(b) In (a) abbiamo visto che ϱ e τ sono equivalenze, mentre σ non lo è. Per la proposizione 20.1 le relazioni di equivalenza su \mathbb{Z} compatibili con l'addizione sono tutte e sole le congruenze modulo un numero naturale. Dato che né ϱ né τ sono congruenze, ne segue che nessuna delle equivalenze trovate in (a) è compatibile con l'addizione tra numeri interi.

(c) L'equivalenza ϱ è compatibile con la moltiplicazione tra numeri interi, 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 τ , 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 $(2 \cdot 1) \tau (2 \cdot 5)$.

20.5. (a) Riflessività. Per ogni $a \in \mathbb{Z}$ si ha $(aa - 3)(a - a) = 0$, e quindi $a \varrho a$.

Simmetria. Se $a \varrho b$, allora $(ab - 3)(a - b) = 0$, e quindi $(ba - 3)(b - a) = 0$, vale a dire $b \varrho a$.

Transitività. Siano $a, b, c \in \mathbb{Z}$ tali che $a \varrho b$ e $b \varrho c$. Allora $(ab - 3)(a - b) = 0$ e $(bc - 3)(b - c) = 0$. Se $a = b$ o $b = c$, allora $a \varrho c$. 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 $a \varrho c$.

(b) Sia $a \in \mathbb{Z}$. Allora

$$\begin{aligned} [a]_{\varrho} &= \{x \mid x \in \mathbb{Z}, x \varrho a\} = \{x \mid x \in \mathbb{Z}, (xa - 3)(x - a) = 0\} \\ &= \{x \mid x \in \mathbb{Z}, xa = 3 \text{ oppure } x = a\}. \end{aligned}$$

Quindi se a è uguale a 1 o 3 si ha che $[a]_{\varrho} = \{1, 3\}$ ha due elementi, se a è uguale a -1 o -3 si ha che $[a]_{\varrho} = \{-1, -3\}$ ha ancora due elementi, mentre se a è diverso da $1, 3, -1, -3$ allora $[a]_{\varrho} = \{a\}$ ha un solo elemento.

(c) No, perché la relazione ϱ non coincide con nessuna congruenza modulo un numero naturale.

20.6. L'unica è la congruenza modulo 1, cioè la relazione banale ω .

20.7. Sono quattro: le congruenze modulo 2, 3, 6, e relazione banale ω .

20.8. Sono tre: $\sim_{0,1}$ (cioè la relazione banale ω), $\sim_{1,1}$ e $\sim_{2,1}$.

20.9. Sono dodici: $\sim_{0,1}$ (cioè la relazione banale ω), $\sim_{1,1}$, $\sim_{2,1}$, $\sim_{0,2}$, $\sim_{1,2}$, $\sim_{2,2}$, $\sim_{0,3}$, $\sim_{1,3}$, $\sim_{2,3}$, $\sim_{0,6}$, $\sim_{1,6}$, $\sim_{2,6}$.

20.10. (a) Dimostriamo che φ 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 φ 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 φ 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 φ 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 .

20.12. Abbiamo già osservato prima dell'enunciato della proposizione 20.5 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 $\mathbb{N}/\sim_{k,n} = \{[mt]_{\sim_{k,n}} \mid m \in \mathbb{N}\} = \{[mt]_{\sim_{k,n}} \mid m \in \mathbb{N}\}$, 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 $n \geq 1$.

20.15. Si ha $[Y] = \{Y^n \mid n \in \mathbb{N}\}$. Ora $Y^n = 1_{\mathcal{P}(X)} = X$ se $n = 0$ e $Y^n = \underbrace{Y \cap Y \cap \cdots \cap Y}_{n \text{ volte}} = Y$ se $n > 0$. Quindi $[Y] = \{X, Y\}$ ha due elementi se $Y \neq X$ e 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 $\mathbb{N}/\sim_{0,1}$.

20.16. È isomorfo a $\mathbb{N}/\sim_{0,4}$.

20.17. È isomorfo a \mathbb{N} .

20.19. (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 $(i\sqrt{2})^0 = 1 \not\sim i\sqrt{2}$, in quanto $1/(i\sqrt{2}) = -i\sqrt{2}/2 \notin \mathbb{R}$, mentre $(i\sqrt{2})^0 = 1 \sim (i\sqrt{2})^2 = -2$, in quanto $1/(-2) \in \mathbb{R}$. Quindi $[i\sqrt{2}]_0^0 = [(i\sqrt{2})^0]_{\sim} = [1]_{\sim} \neq [i\sqrt{2}]_0^1 = [(i\sqrt{2})^1]_{\sim} = [i\sqrt{2}]_{\sim}$, mentre $[i\sqrt{2}]_0^0 = [1]_{\sim}$ è uguale a $[-2]_{\sim} = [(i\sqrt{2})^2]_{\sim} = [i\sqrt{2}]_0^2$. Da $[i\sqrt{2}]_0^0 = [i\sqrt{2}]_0^2 = [1]_{\sim}$ segue che $[i\sqrt{2}]_0^n = [1]_{\sim}$ per ogni $n \geq 0$ pari, mentre $[i\sqrt{2}]_0^n = [i\sqrt{2}]_{\sim}$ per ogni n dispari. In particolare il sottomonoide ciclico $[(i\sqrt{2})_{\sim}]$ di $(\mathbb{C}^*/\sim, \cdot)$ generato da $[i\sqrt{2}]_{\sim}$ ha due elementi.

(d) È isomorfo a $\mathbb{N}/\sim_{0,2}$.

20.20. (a) *Riflessività di \equiv .* Sia $a_1 a_2 \dots a_n \in W$. Per la riflessività di $=$ 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 $=$ e \sim sono simmetriche, 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 $=$ e 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 $\widehat{f}: W \rightarrow \overline{W}$. Se $a \in W$ è una parola di lunghezza 1 si ha $\widehat{f}(a) = \widehat{f}(\varphi(a)) = (\widehat{f} \circ \varphi)(a) = f(a) = (\overline{\varphi} \circ \pi)(a) = \overline{\varphi}(\pi(a)) = \overline{\varphi}([a]_\sim) = [a]_\sim$. Quindi \widehat{f} fa corrispondere alla parola $a \in W$ di lunghezza 1 la parola $[a]_\sim \in \overline{W}$ 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 \widehat{f} si ottiene $\widehat{f}(a_1 a_2 \dots a_n) = \widehat{f}(a_1 \circ a_2 \circ \dots \circ a_n) = \widehat{f}(a_1) \circ \widehat{f}(a_2) \circ \dots \circ \widehat{f}(a_n) = [a_1]_\sim \circ [a_2]_\sim \circ \dots \circ [a_n]_\sim = [a_1]_\sim [a_2]_\sim \dots [a_n]_\sim$. Quindi $\widehat{f}: W \rightarrow \overline{W}$ fa corrispondere alla parola $a_1 a_2 \dots a_n \in W$ la parola $[a_1]_\sim [a_2]_\sim \dots [a_n]_\sim \in \overline{W}$. È ora evidente che l'applicazione \widehat{f} è suriettiva.

(d) Siano $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in W$. Si ha

$$a_1 a_2 \dots a_n \sim_{\widehat{f}} b_1 b_2 \dots b_m$$

se e solo se $\widehat{f}(a_1 a_2 \dots a_n) = \widehat{f}(b_1 b_2 \dots b_m)$, 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 $a_1 a_2 \dots a_n \sim_{\widehat{f}} b_1 b_2 \dots b_m$ 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 $\sim_{\widehat{f}}$ coincidono.

(e) Applicando il teorema fondamentale di omomorfismo per i monoidi all'omomorfismo suiettivo $\widehat{f}: W \rightarrow \overline{W}$, si vede che $W / \sim_{\widehat{f}} \cong \overline{W}$. Si è già dimostrato in (d) che le due equivalenze \equiv e $\sim_{\widehat{f}}$ coincidono. Pertanto i monoidi W / \equiv e \overline{W} sono isomorfi.

21.4. (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 $g = \iota$. Pertanto l'unico elemento g di S_4 tale che $f \circ g = f$ è l'identità.

21.12. (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 $f(h) = \psi^{-1}\varphi(h) = \psi^{-1}\varphi(z_h) = \psi^{-1}(z_{2+h}) = 2+h$ per ogni $h = 1, 2, \dots, 6$, $f(7) = 1$, $f(8) = 2$. Nella notazione delle 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.

21.13. (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 .

(c) Se $d \geq 4$ è pari e $f = (a_1 \ a_2 \ a_3 \ \dots \ a_d)$, allora

$$f^2 = (a_1 \ a_3 \ a_5 \ \dots \ a_{d-3} \ a_{d-1}) \circ (a_2 \ a_4 \ a_6 \ \dots \ a_{d-2} \ a_d)$$

è il prodotto di due cicli disgiunti ciascuno dei quali ha lunghezza $d/2$.

22.6. $[\mathbb{C} : \mathbb{R}] = \infty$.

22.13. (a) No. Si è visto nel lemma 19.15 che se $f: G \rightarrow G'$ è un omomorfismo di gruppi allora $f(1_G) = 1_{G'}$. Quindi per ogni sottogruppo H' di G' si ha $f(1_G) \in H'$, e pertanto $1_G \in f^{-1}(H')$. Questo dimostra che l'insieme $f^{-1}(H')$ è sempre non vuoto.

(b) Sì. Ad esempio siano G un gruppo qualunque, G' un gruppo non banale (cioè con più di un elemento), $H' = \{1_{G'}\}$, e $f: G \rightarrow G'$ l'omomorfismo definito da $f(x) = 1_{G'}$ per ogni $x \in G$. Allora le classi laterali sinistre di G' modulo H' sono gli insiemi $\{g'\}$, $g' \in G'$. Sia g' un elemento di G' diverso da $1_{G'}$ e sia $C = \{g'\}$. Allora $f^{-1}(C) = \emptyset$.

22.14. (a) *Chiusura.* Se $f, g \in H$, allora $(f \circ g)(10) = f(g(10)) = f(10) = 10$, e quindi $f \circ g \in H$.

Identità. L'identità di S_{10} è l'applicazione identica ι , e si ha $\iota(10) = 10$. Quindi ι appartiene ad H .

Inverso. Sia $f \in H$. Allora $f(10) = 10$, e quindi $10 = f^{-1}(10)$. Pertanto $f^{-1} \in H$.

(b) Si consideri l'applicazione $\varphi: H \rightarrow S_9$ definita da $\varphi(f)(n) = f(n)$ per ogni $f \in H$ e ogni $n = 1, 2, \dots, 9$. Si tratta evidentemente di una biiezione di H in S_9 la cui inversa $\varphi^{-1}: S_9 \rightarrow H$ è definita, per ogni $g \in S_9$, da $\varphi^{-1}(g)(m) = g(m)$ se $m = 1, 2, \dots, 9$ e $\varphi^{-1}(g)(10) = 10$. Dimostriamo che φ è un omomorfismo di gruppi. Si deve dimostrare che per ogni $f, f' \in H$ si ha $\varphi(f \circ f') = \varphi(f) \circ \varphi(f')$. Quindi si deve dimostrare che per ogni $n = 1, 2, \dots, 9$ si ha $(\varphi(f \circ f'))(n) = (\varphi(f) \circ \varphi(f'))(n)$. Un facile conto mostra che $(\varphi(f \circ f'))(n) = (f \circ f')(n) = f(f'(n)) = f(\varphi(f')(n)) = (\varphi(f))(\varphi(f')(n)) = (\varphi(f) \circ \varphi(f'))(n)$.

(c) Si ha $|S_{10}| = 10!$ e $|H| = |S_9| = 9!$, e quindi $[S_{10} : H] = |S_{10}|/|H| = 10!/9! = 10$.

22.16. (b) $|G| = 2 \cdot (n - 2)!$.

(c) $[G : H] = (n - 2)!$.

22.19. (a) Sia $x \in G$ un elemento fissato. Dimostriamo che $C(x)$ è un sottogruppo di G .

Chiusura. Se $g, h \in C(x)$, allora

$$(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh),$$

e quindi $gh \in C(x)$.

Identità. Si ha $1_G x = x 1_G$, e quindi $1_G \in C(x)$.

Inverso. Sia $g \in C(x)$. Allora $gx = xg$. Moltiplicando questa uguaglianza a sinistra e a destra per g^{-1} si ottiene $g^{-1}g x g g^{-1} = g^{-1}x g g^{-1}$, cioè $x g^{-1} = g^{-1}x$. Quindi $g^{-1} \in C(x)$.

(b) *Riflessività.* Se $x \in G$, allora $1_G^{-1} x 1_G = x$, e quindi $x \sim x$.

Simmetria. Se $x, y \in G$ e $x \sim y$, esiste $g \in G$ tale che $g^{-1}xg = y$. Moltiplicando questa uguaglianza a sinistra per g e a destra per g^{-1} si ottiene che $gg^{-1}xgg^{-1} = gyg^{-1}$, ossia $x = gyg^{-1}$. Dato che $g^{-1} \in G$ si ottiene quindi che $y \sim x$.

Transitività. Siano $x, y, z \in G$ tali che $x \sim y$ e $y \sim z$. Allora esistono $g, h \in G$ tali che $g^{-1}xg = y$ e $h^{-1}yh = z$. Ma allora $z = h^{-1}yh = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$, e quindi $x \sim z$.

(c) Si deve dimostrare che se $g, g' \in G$ e $C(x)g = C(x)g'$, allora $g^{-1}xg = g'^{-1}xg'$. Ora se $g, g' \in G$ e $C(x)g = C(x)g'$, si ha $g = 1_G \cdot g \in C(x)g = C(x)g'$, e quindi $g = cg'$ per qualche $c \in C(x)$. Ma allora $g^{-1}xg = (cg')^{-1}x(cg') = g'^{-1}c^{-1}xcg'$. Infine da $c \in C(x)$ segue che $cx = xc$, e quindi $g^{-1}xg = g'^{-1}c^{-1}xcg' = g'^{-1}c^{-1}cxg' = g'^{-1}1_Gxg' = g'^{-1}xg'$, come si voleva dimostrare.

(d) *Iniettività.* Siano $g, g' \in G$ tali che $\varphi(C(x)g) = \varphi(C(x)g')$. Si deve dimostrare che $C(x)g = C(x)g'$, cioè si deve verificare la doppia inclusione. Per simmetria è sufficiente far vedere che $C(x)g \subseteq C(x)g'$. Ora se $y \in C(x)g$, esiste $c \in C(x)$ tale che $y = cg$, e si deve far vedere che esiste $c' \in C(x)$ tale che $y = c'g'$. Si osservi che $y = cg = c'g'$ se e solo se $c' = cgg'^{-1}$. Quindi si deve far vedere solamente che l'elemento $c' = cgg'^{-1}$ di G appartiene a $C(x)$, cioè che $cgg'^{-1}x = xcgg'^{-1}$. Si consideri l'uguaglianza $\varphi(C(x)g) = \varphi(C(x)g')$, cioè la $g^{-1}xg = g'^{-1}xg'$. Moltiplicandola a sinistra per g e a destra per g'^{-1} si ricava che $gg^{-1}xgg'^{-1} = gg'^{-1}xg'g'^{-1}$, cioè $xgg'^{-1} = gg'^{-1}x$. Quindi $cgxg'^{-1} = xcgg'^{-1} = xcgg'^{-1}$, come desiderato.

Suriettività. Sia a un qualunque elemento di $[x]_\sim$. Allora $x \sim a$, e quindi, per come è definita la relazione \sim , esiste $g \in G$ tale che $g^{-1}xg = a$. Ma allora $C(x)g$ è un elemento del dominio \mathcal{D}_x di φ tale che $\varphi(C(x)g) = g^{-1}xg = a$. Questo dimostra che φ è suriettiva.

(e) Si è visto in (d) che φ è biiettiva, e quindi $|[x]_\sim| = |\mathcal{D}_x| = [G : C(x)]$. Dimostrando il teorema di Lagrange si è visto poi che $|G| = [G : C(x)][C(x)]$. Pertanto $|[x]_\sim|$ divide $|G|$.

22.21. $|G/N|$ e $[G : N]$ sono entrambe notazioni per denotare la cardinalità dell'insieme $\{gN \mid g \in G\}$, e quindi sono certamente uguali. Il lettore osservi comunque che la costruzione del gruppo quoziante G/N è possibile solo quando N è sottogruppo normale di G , e quindi si può scrivere $|G/N|$ solo quando N è normale. La notazione $[G : N]$ ha invece significato per ogni sottogruppo N di G .

22.22. (a) Sia $x \in \mathbb{Q}/\mathbb{Z}$. Allora esiste $q \in \mathbb{Q}$ tale che $x = q + \mathbb{Z}$. Inoltre $q = s/t$ per opportuni $s, t \in \mathbb{Z}$, $t \neq 0$. Si può evidentemente supporre che $t > 0$, cioè che $t \in \mathbb{N}^*$. Ma allora $tx = t(q + \mathbb{Z}) = tq + \mathbb{Z} = s + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$.

(b) Si ha $tx = 0$ se e solo se $t(a/b + \mathbb{Z}) = 0_{\mathbb{Q}/\mathbb{Z}} = \mathbb{Z}$, cioè se e solo se $ta/b + \mathbb{Z} = \mathbb{Z}$. Questo accade se e solo se $ta/b \in \mathbb{Z}$, vale a dire se e solo se b divide ta . Ma dato che a e b sono primi tra loro, b divide ta se e solo se b divide t . Abbiamo così dimostrato che $tx = 0$ se e solo se b divide t . Quindi il più piccolo numero naturale $t \in \mathbb{N}^*$ tale che $tx = 0$ è il più piccolo numero naturale $t \in \mathbb{N}^*$ tale che b divide t , cioè il più piccolo multiplo positivo di b , ossia $|b|$.

23.4. (a) *Associatività.* Per ogni $(x, \varphi), (y, \psi), (z, \omega) \in L$ si ha $((x, \varphi) * (y, \psi)) * (z, \omega) = (x\varphi(y), \varphi \circ \psi) * (z, \omega) = (x\varphi(y)(\varphi \circ \psi)(z), \varphi \circ \psi \circ \omega) = (x\varphi(y)\varphi(\psi(z)), \varphi \circ \psi \circ \omega)$ e $(x, \varphi) * ((y, \psi) * (z, \omega)) = (x, \varphi) * (y\psi(z), \psi \circ \omega) = (x\varphi(y\psi(z)), \varphi \circ \psi \circ \omega) = (x\varphi(y)\varphi(\psi(z)), \varphi \circ \psi \circ \omega)$.

Identità. Per ogni $(x, \varphi) \in L$ si ha

$$(x, \varphi) * (1_G, \iota_G) = (x\varphi(1_G), \varphi \circ \iota_G) = (x1_G, \varphi) = (x, \varphi)$$

e

$$(1_G, \iota_G) * (x, \varphi) = (1_G \iota_G(x), \iota_G \circ \varphi) = (1_G x, \varphi) = (x, \varphi).$$

Inverso. Per ogni $(x, \varphi) \in L$ l'elemento $((\varphi^{-1}(x))^{-1}, \varphi^{-1}) \in L$ è l'inverso di (x, φ) , perché

$$\begin{aligned} (x, \varphi) * ((\varphi^{-1}(x))^{-1}, \varphi^{-1}) &= (x(\varphi(\varphi^{-1}(x))^{-1}), \varphi \circ \varphi^{-1}) \\ &= (x(\varphi(\varphi^{-1}(x^{-1}))), \iota_G) = (xx^{-1}, \iota_G) = (1_G, \iota_G) \end{aligned}$$

e

$$((\varphi^{-1}(x))^{-1}, \varphi^{-1}) * (x, \varphi) = ((\varphi^{-1}(x))^{-1}(\varphi^{-1}(x)), \varphi^{-1} \circ \varphi) = (1_G, \iota_G).$$

(b) Per ogni elemento $(x, \varphi) \in L$ e $(y, \iota_G) \in G \times \{\iota_G\}$ si ha

$$\begin{aligned} (x, \varphi) * (y, \iota_G) * (x, \varphi)^{-1} &= (x\varphi(y), \varphi) * ((\varphi^{-1}(x))^{-1}, \varphi^{-1}) \\ &= (x\varphi(y)\varphi(\varphi^{-1}(x))^{-1}, \iota_G) \in G \times \{\iota_G\}. \end{aligned}$$

Questo dimostra (b).

(c) Per ogni $(x, \varphi), (y, \psi) \in L$ si ha $\pi_2((x, \varphi) * (y, \psi)) = \pi_2(x\varphi(y), \varphi \circ \psi) = \varphi \circ \psi = \pi_2(x, \varphi) \circ \pi_2(y, \psi)$. Questo dimostra che π_2 è un omomorfismo. Inoltre $\ker \pi_2 = \{(x, \varphi) \in L \mid \pi_2(x, \varphi) = \iota_G\} = \{(x, \varphi) \in L \mid \varphi = \iota_G\} = \{(x, \iota_G) \mid x \in G\} = G \times \{\iota_G\}$.

23.7. (a) Per ogni $x, x' \in \mathbb{Q}$ si ha $\varphi(x+x') = 3(x+x') + \mathbb{Z} = 3x+3x'+\mathbb{Z} = (3x+\mathbb{Z})+(3x'+\mathbb{Z}) = \varphi(x)+\varphi(x')$.

(b) Un generico elemento y del codominio \mathbb{Q}/\mathbb{Z} di φ è del tipo $y = q + \mathbb{Z}$ per qualche $q \in \mathbb{Q}$. Si noti che allora anche $x = q/3$ è un elemento di \mathbb{Q} , cioè un numero razionale, e si ha $\varphi(x) = 3x + \mathbb{Z} = q + \mathbb{Z} = y$. Questo dimostra che φ è suriettiva.

(c) Il nucleo $\ker \varphi$ dell'omomorfismo φ è certamente un sottogruppo del dominio \mathbb{Q} di φ . Quindi c'è solo da dimostrare che $\ker \varphi$ contiene \mathbb{Z} , vale a dire che se z è un qualunque numero intero allora $\varphi(z) = 0_{\mathbb{Q}/\mathbb{Z}}$. Un semplice calcolo mostra che se $z \in \mathbb{Z}$ allora $\varphi(z) = 3z + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$.

(d) Si ha $\ker \varphi = \{q \in \mathbb{Q} \mid \varphi(q) = 0\} = \{q \in \mathbb{Q} \mid 3q + \mathbb{Z} = \mathbb{Z}\} = \{q \in \mathbb{Q} \mid 3q \in \mathbb{Z}\} = \{q \in \mathbb{Q} \mid \text{esiste } z \in \mathbb{Z} \text{ tale che } 3q = z\} = \{z/3 \mid z \in \mathbb{Z}\}$. Quindi $\ker \varphi/\mathbb{Z} = \{z/3 + \mathbb{Z} \mid z \in \mathbb{Z}\}$. Mostriamo che questo coincide con l'insieme $\{z/3 + \mathbb{Z} \mid z = 0, 1, 2\}$. Chiaramente $\ker \varphi/\mathbb{Z} = \{z/3 + \mathbb{Z} \mid z \in \mathbb{Z}\} \supseteq \{z/3 + \mathbb{Z} \mid z = 0, 1, 2\}$. Viceversa si fissi un elemento $z/3 + \mathbb{Z} \in \ker \varphi/\mathbb{Z}$, dove z denota un arbitrario numero intero. Si divida z per 3. Allora se q, r sono numeri interi tali che $z = 3q + r$ e $0 \leq r < 3$, si ha $z/3 + \mathbb{Z} = (3q + r)/3 + \mathbb{Z} = r/3 + q + \mathbb{Z} = r/3 + \mathbb{Z}$. Dato che r è uguale a 0 o 1 o 2, si ha $z/3 + \mathbb{Z} = r/3 + \mathbb{Z} \in \{z/3 + \mathbb{Z} \mid z = 0, 1, 2\}$. Ora per dimostrare che $\ker \varphi/\mathbb{Z} = \{z/3 + \mathbb{Z} \mid z = 0, 1, 2\}$ ha ordine 3 resta solo da far vedere che i suoi tre elementi $0/3 + \mathbb{Z} = \mathbb{Z}$, $1/3 + \mathbb{Z}$, $2/3 + \mathbb{Z}$ sono tutti distinti tra loro. Ma se due tra questi fossero uguali, allora due tra 0, 1/3, 2/3 differirebbero tra loro per un intero, il che non è.

23.8. (a) Si deve dimostrare che se $x, x' \in \mathbb{R}^*$ e $xH = x'H$, allora $x^2H = x'^2H$. Ora se $x, x' \in \mathbb{R}^*$ e $xH = x'H$, allora $x^{-1}x' \in H$, e quindi $(x^2)^{-1}(x')^2 = x^{-2}x'^2 = (x^{-1}x')^2 \in H$. Pertanto $x^2H = x'^2H$.

(b) Per ogni $x, x' \in \mathbb{R}^*$ si ha

$$\varphi((xH)(x'H)) = \varphi(xx'H) = (xx')^2H = x^2x'^2H = (x^2H)(x'^2H) = \varphi(xH)\varphi(x'H).$$

(c) $\ker \varphi = \{xH \mid x \in \mathbb{R}^*, \varphi(xH) = 1_{\mathbb{R}^*/H}\} = \{xH \mid x \in \mathbb{R}^*, x^2H = H\} = \{xH \mid x \in \mathbb{R}^*, x^2 \in H\} = \{xH \mid x \in \mathbb{R}^*, \text{ esiste } z \in \mathbb{Z} \text{ tale che } x^2 = 1/2^z\} = \{(1/(\sqrt{2})^z)H \mid z \in \mathbb{Z}\}$. In modo del tutto analogo a quanto fatto nel punto (d) dell'esercizio 23.7 si vede poi che $\ker \varphi = \{H, (1/\sqrt{2})H\}$ ha esattamente due elementi.

23.14. Si osservi innanzitutto che l'applicazione π è ben definita perché se $g, g' \in G$ e $gN = g'N$, allora $g'^{-1}g \in N$, e quindi $g'^{-1}g \in M$, da cui $gM = g'M$. Inoltre π è un omomorfismo di gruppi, in quanto $\pi(gN)\pi(g'N) = (gM)(g'M) = gg'M = \pi(gg'N) = \pi((gN)(g'N))$, ed è suriettivo perché ogni elemento del codominio di π è del tipo gM per qualche $g \in G$, e quindi $\pi(gN) = gM$. Calcoliamo il nucleo di π . Si ha

$$\begin{aligned} \ker \pi &= \{gN \mid g \in G, \pi(gN) = 1_{G/M}\} = \{gN \mid g \in G, gM = M\} \\ &= \{gN \mid g \in G, g \in M\} = \{gN \mid g \in M\} = M/N. \end{aligned}$$

Ma allora $M/N = \ker \pi$ è un sottogruppo normale di G/N , e applicando il teorema fondamentale di omomorfismo per i gruppi all'omomorfismo suriettivo $\pi: G/N \rightarrow G/M$ si ricava che $(G/N)/\ker \pi \cong G/M$. Pertanto i gruppi $(G/N)/\ker \pi = (G/N)/(M/N)$ e G/M sono isomorfi.

23.22. (a) Il sottoinsieme H non è un sottogruppo di $\mathbb{Z}^\mathbb{N}$. Ad esempio l'applicazione $i: \mathbb{N} \rightarrow \mathbb{Z}$ definita da $i(n) = n$ per ogni $n \in \mathbb{N}$ è un elemento di H che non è invertibile in H . Infatti l'elemento neutro di $\mathbb{Z}^\mathbb{N}$ è l'applicazione $z: \mathbb{N} \rightarrow \mathbb{Z}$ definita da $z(n) = 0$ per ogni $n \in \mathbb{N}$, e quindi l'opposto di i in $\mathbb{Z}^\mathbb{N}$ è l'applicazione $-i: \mathbb{N} \rightarrow \mathbb{Z}$ definita da $(-i)(n) = -n$ per ogni $n \in \mathbb{N}$. Dato che $-i$ non è un omomorfismo di insiemi ordinati di \mathbb{N} in \mathbb{Z} ne segue che $-i \notin H$. Quindi H non è un sottogruppo di $\mathbb{Z}^\mathbb{N}$.

(b) Si osservi intanto che H è un sottoinsieme chiuso di $\mathbb{Z}^\mathbb{N}$ in quanto se $f, g \in H$ anche $g + f \in H$, perché per ogni $n, m \in \mathbb{N}$ con $n \leq m$ si ha $f(n) \leq f(m)$ e $g(n) \leq g(m)$, e quindi $f(n) + g(n) \leq f(m) + g(m)$, vale a dire $(f + g)(n) \leq (f + g)(m)$.

Inoltre l'elemento neutro di $\mathbb{Z}^{\mathbb{N}}$ è l'applicazione $z: \mathbb{N} \rightarrow \mathbb{Z}$ definita da $z(n) = 0$ per ogni $n \in \mathbb{N}$. Dato che z è un omomorfismo di insiemi ordinati di \mathbb{N} in \mathbb{Z} , si ha che $z \in H$. Quindi H è un sottomonoide di $(\mathbb{Z}^{\mathbb{N}}, +)$.

(c) Si deve dimostrare che $\varphi(f+g) = \varphi(f) + \varphi(g)$ per ogni $f, g \in \mathbb{Z}^{\mathbb{N}}$; quindi si deve far vedere che $\varphi(f+g)(n) = (\varphi(f) + \varphi(g))(n)$ per ogni $f, g \in \mathbb{Z}^{\mathbb{N}}$ e ogni $n \in \mathbb{N}$. Si ha $\varphi(f+g)(n) = \sum_{i=0}^n (f+g)(i) = \sum_{i=0}^n (f(i) + g(i)) = \sum_{i=0}^n f(i) + \sum_{i=0}^n g(i) \stackrel{?}{=} \varphi(f)(n) + \varphi(g)(n)$.

(d) Mostriamo che φ è iniettiva. Si deve dimostrare che $\ker \varphi = \{z\}$, cioè che se $f \in \mathbb{Z}^{\mathbb{N}}$ e $\varphi(f) = z$ allora $f = z$. Ora se $f \in \mathbb{Z}^{\mathbb{N}}$ e $\varphi(f) = z$, allora $\varphi(f)(n) = 0$ per ogni $n \in \mathbb{N}$, cioè $\sum_{i=0}^n f(i) = 0$ per ogni $n \in \mathbb{N}$. Ma allora per $n = 0$ si ricava che $f(0) = 0$ e per $n > 0$ si ha $f(n) = (\sum_{i=0}^n f(i)) - (\sum_{i=0}^{n-1} f(i)) = 0 - 0 = 0$. Quindi $f = 0$.

Mostriamo che φ è suriettiva. Fissiamo $g \in \mathbb{Z}^{\mathbb{N}}$. Si deve dimostrare che esiste $f \in \mathbb{Z}^{\mathbb{N}}$ tale che $\varphi(f) = g$, cioè tale che $\varphi(f)(n) = g(n)$ per ogni $n \in \mathbb{N}$. Definiamo $f(n)$ per induzione su $n \geq 0$ in questo modo: si ponga $f(0) = g(0)$; supposto poi di aver già definito $f(0), f(1), f(2), \dots, f(n-1)$, si ponga $f(n) = g(n) - f(0) - f(1) - f(2) - \dots - f(n-1)$ per ogni $n > 0$. Allora f è una funzione di \mathbb{N} in \mathbb{Z} , e inoltre $\varphi(f)(n) = \sum_{i=0}^n f(i) = g(n)$ per ogni $n \in \mathbb{N}$. Quindi $\varphi(f) = g$. Pertanto l'endomorfismo φ è una biiezione, cioè è un automorfismo di $\mathbb{Z}^{\mathbb{N}}$.

23.23. (c) Si è visto in (b) 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 $\{1, -1\}$. Quindi il nucleo di π_2 è un sottogruppo normale di $G = \mathbb{Z} \times \{1, -1\}$. Ma si ha $\ker(\pi_2) = \{g \mid g \in G, \pi_2(g) = 1\} = \{(a, x) \mid (a, x) \in \mathbb{Z} \times \{1, -1\}, \pi_2(a, x) = 1\} = \{(a, x) \mid (a, x) \in \mathbb{Z} \times \{1, -1\}, x = 1\} = \{(a, 1) \mid a \in \mathbb{Z}\} = H$.

(d) $[G : H] = |G/H|$ per l'esercizio 22.21. Inoltre

$$G/H = G/\ker(\pi_2) \cong \pi_2(G) = \{1, -1\},$$

e quindi $|G/H| = 2$. Pertanto $[G : H] = 2$.

23.26. Sia (G, \cdot) un gruppo ciclico. Allora esiste $g \in G$ tale che $G = \langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$ (esercizio 23.2(c)). Consideriamo l'applicazione $\varphi: \mathbb{Z} \rightarrow G$ definita da $\varphi(t) = g^t$ per ogni $t \in \mathbb{Z}$ dell'esercizio 23.2. L'applicazione φ è un omomorfismo suriettivo del gruppo $(\mathbb{Z}, +)$ nel gruppo (G, \cdot) . Dal teorema fondamentale di omomorfismo per i gruppi si ha che $\mathbb{Z}/\ker \varphi \cong G$, dove $\ker \varphi$ denota il nucleo di φ . Ma il nucleo di un omomorfismo è sempre un sottogruppo del dominio, e abbiamo visto nell'esempio 19.11 che i sottogruppi del gruppo $(\mathbb{Z}, +)$ sono tutti e soli del tipo $n\mathbb{Z}$ per qualche $n \in \mathbb{N}$. Pertanto G è isomorfo al gruppo $\mathbb{Z}/n\mathbb{Z}$ per qualche $n \in \mathbb{N}$.

24.22. (a) Lo zero dell'anello è il numero 2, in quanto per ogni $x \in \mathbb{R}$ si ha $x \oplus 2 = x + 2 - 2 = x$.

(b) L'identità dell'anello è il numero 3, in quanto per ogni $x \in \mathbb{R}$ si ha $3 \otimes x = 3x - 6 - 2x + 6 = x$ e l'anello $(\mathbb{R}, \oplus, \otimes)$ è commutativo.

(c) Chiedere se l'anello commutativo con identità in questione è un campo equivale a chiedere se ogni elemento $x \in \mathbb{R}$ diverso da 2 è invertibile, cioè se per ogni $x \in \mathbb{R}$, $x \neq 2$, esiste $y \in \mathbb{R}$ tale che $x \otimes y = 3$. Ma $x \otimes y = xy - 2x - 2y + 6$, e se $x \neq 2$ si ha $xy - 2x - 2y + 6 = 3$ se e solo se $y = (2x - 3)/(x - 2)$. Questo significa che ogni $x \in \mathbb{R}$, $x \neq 2$, ha un inverso nell'anello uguale a $(2x - 3)/(x - 2)$. Pertanto l'anello $(\mathbb{R}, \oplus, \otimes)$ è un campo.

25.4. (a) Sono le applicazioni $f \in \mathbb{R}^X$ tali che $f(x) = 0$ per qualche $x \in X$ e $f(x') \neq 0$ per qualche $x' \in X$.

(b) Sono le applicazioni $f: X \rightarrow \mathbb{R}$ tali che $f(x) \neq 0$ per ogni $x \in X$.

27.5. Sia I un ideale di R tale che $1_R \in I$. Certamente $I \subseteq R$. Se poi $r \in R$, allora $r = r \cdot 1_R \in I$ perché $1_R \in I$. Quindi $I = R$.

Siano invece I un ideale di R e $u \in I$ un elemento invertibile in R . Allora $1_R = u^{-1}u \in I$ perché $u^{-1} \in R$ e $u \in I$. Per quanto visto nel paragrafo precedente si ha quindi $I = R$.

27.8. Soluzione per \mathbb{Z}_6 : gli ideali dell'anello \mathbb{Z}_6 sono $6\mathbb{Z}/6\mathbb{Z}$ (l'ideale nullo), $3\mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$ e $\mathbb{Z}/6\mathbb{Z}$ (l'ideale improprio).

27.10. (a) R ha $4 \cdot 4 \cdot 4 = 64$ elementi.

(b) È $(\bar{1}, \bar{0}, \bar{0})$.

(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 $\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = (\bar{n}, \bar{0}, \bar{0})$, e pertanto $\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = 0_R$ 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 $\text{char } R = 4$.

27.11. (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

$$(z \cdot i)(x) = (\underbrace{i + i + \cdots + i}_{z \text{ volte}})(x) = \underbrace{i(x) + i(x) + \cdots + i(x)}_{z \text{ volte}} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{z \text{ volte}} = \bar{z} = f_z(x)$$

quando $z > 0$,

$$\begin{aligned} (z \cdot i)(x) &= ((-i) + (-i) + \cdots + (-i))(x) = \underbrace{(-i)(x) + (-i)(x) + \cdots + (-i)(x)}_{-z \text{ volte}} \\ &= \underbrace{(-\bar{1}) + (-\bar{1}) + \cdots + (-\bar{1})}_{-z \text{ volte}} = z \cdot \bar{1} = \bar{z} = f_z(x) \end{aligned}$$

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 maggiore di 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, contraddizione.

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 $P_R \cong \mathbb{Z}_n$ perché $\text{char } \mathbb{Z}_n^X = n$. Pertanto $\mathbb{Z}_n^X \cong \mathbb{Z}_n$ è un campo perché n è primo.

27.13. 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 $a = -a$.

27.30. Dato che \mathbb{R} è un campo, \mathbb{R} ha i soli due ideali $\{0\}$ e \mathbb{R} . Per il teorema 25.4 ci sono esattamente due equivalenze su \mathbb{R} compatibili con l'addizione e la moltiplicazione. La prima è $\sim_{\{0\}}$, definita, per ogni $a, b \in \mathbb{R}$, da $a \sim_{\{0\}} b$ se $a - b \in \{0\}$, cioè se e solo se $a = b$; quindi $\sim_{\{0\}}$ è l'uguaglianza $=$. La seconda è $\sim_{\mathbb{R}}$, definita, per ogni $a, b \in \mathbb{R}$, da $a \sim_{\mathbb{R}} b$ se $a - b \in \mathbb{R}$. Quindi $a \sim_{\mathbb{R}} b$ per ogni $a, b \in \mathbb{R}$, vale a dire $\sim_{\mathbb{R}}$ è l'equivalenza banale ω su \mathbb{R} . Abbiamo così dimostrato che le uniche due relazioni di equivalenza su \mathbb{R} compatibili sia con l'addizione che con la moltiplicazione sono l'uguaglianza $=$ e la relazione banale ω .

27.31. 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 $\underbrace{1_R + 1_R + \cdots + 1_R}_{\frac{5}{3} \text{ volte}} = q$ 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

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = \underbrace{\frac{3}{5} + \frac{3}{5} + \cdots + \frac{3}{5}}_{n \text{ volte}} = \frac{3n}{5},$$

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 φ è chiaramente una biiezione. Inoltre si ha

$$\varphi(x+y) = \frac{5}{3}(x+y) = \frac{5}{3}x + \frac{5}{3}y = \varphi(x) + \varphi(y),$$

$$\varphi(x*y) = \varphi\left(\frac{5}{3}xy\right) = \frac{5}{3}\left(\frac{5}{3}xy\right) = \left(\frac{5}{3}x\right)\left(\frac{5}{3}y\right) = \varphi(x)\varphi(y)$$

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 φ è un isomorfismo dell'anello $(\mathbb{Q}, +, *)$ nel campo $(\mathbb{Q}, +, \cdot)$. In particolare, anche $(\mathbb{Q}, +, *)$ è un campo.

27.32. (a) Si ha $0_R = (0, \bar{0})$ e $1_R = (1, \bar{1})$. I due elementi $(0, \bar{1})$ e $(1, \bar{0})$ di R non sono nulli, ma il loro prodotto è nullo. Quindi R non è un dominio d'integrità.

(b) Si consideri la proiezione canonica sul primo fattore $\pi_{\mathbb{R}}: \mathbb{R} \times \mathbb{Z}_8 \rightarrow \mathbb{R}$ definita da $\pi_{\mathbb{R}}(a, \bar{b}) = a$ per ogni $a \in \mathbb{R}$, $\bar{b} \in \mathbb{Z}_8$. Allora $\pi_{\mathbb{R}}$ è un omomorfismo suriettivo d'anelli, come è immediato verificare, e il suo nucleo è

$$\begin{aligned}\ker \pi_{\mathbb{R}} &= \{(a, \bar{b}) \mid a \in \mathbb{R}, \bar{b} \in \mathbb{Z}_8, \pi_{\mathbb{R}}(a, \bar{b}) = 0\} \\ &= \{(a, \bar{b}) \mid a \in \mathbb{R}, \bar{b} \in \mathbb{Z}_8, a = 0\} = \{(0, \bar{b}) \mid \bar{b} \in \mathbb{Z}_8\} = \{0\} \times \mathbb{Z}_8.\end{aligned}$$

Applicando il teorema fondamentale di omomorfismo per gli anelli all'omomorfismo $\pi_{\mathbb{R}}: \mathbb{R} \times \mathbb{Z}_8 \rightarrow \mathbb{R}$ si deduce che

$$\mathbb{R} \times \mathbb{Z}_8 / \{0\} \times \mathbb{Z}_8 = \mathbb{R} \times \mathbb{Z}_8 / \ker \pi_{\mathbb{R}} \cong \mathbb{R}$$

è un campo. Pertanto $\{0\} \times \mathbb{Z}_8$ è un ideale massimale di $\mathbb{R} \times \mathbb{Z}_8$.

(c) Si consideri l'elemento $(0, \bar{4})$ di R . Si ha $(0, \bar{4}) \notin \mathbb{R} \times \{\bar{0}\}$ mentre $(0, \bar{4})(0, \bar{4}) = (0, \bar{16}) = (0, \bar{0}) \in \mathbb{R} \times \{\bar{0}\}$. Quindi $\mathbb{R} \times \{\bar{0}\}$ non è un ideale primo di R .

(d) Per ogni $n \in \mathbb{N}$, $n > 0$, si ha

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = \underbrace{(1, \bar{1}) + (1, \bar{1}) + \cdots + (1, \bar{1})}_{n \text{ volte}} = (n, \bar{n}),$$

e questo è sempre diverso da $(0, \bar{0}) = 0_R$. Quindi $\text{char } R = 0$.

27.33. (a) Chiaramente $1 = 1 + 0 \in S + M$.

Se $s + m, s' + m' \in S + M$ con $s, s' \in S$ e $m, m' \in M$, allora $(s + m) - (s' + m') = (s - s') + (m - m') \in S + M$ e $(s + m)(s' + m') = ss' + (sm' + s'm + mm') \in S + M$ perché $sm' + s'm + mm' \in M$. Questo dimostra che $S + M$ è un sottoanello dell'anello con identità R .

(b) Si osservi intanto che M è un ideale di $S + M$, perché è un ideale di R contenuto in $S + M$. Inoltre l'ideale M di $S + M$ è proprio, perché se per assurdo fosse $S + M = M$, allora $S \subseteq M$, da cui $1 \in M$. Ma allora $M = R$ (esercizio 25.7), 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 $x, y \in S + M$ e $xy \in M$, allora $x, y \in R$ e $xy \in M$, e da questo segue che o x o y devono appartenere ad M . Pertanto M è un ideale primo di $S + M$.

27.34. (a) Dimostriamo equivalentemente che se $\text{char } R = n \neq 0$, allora anche $\text{char } S \neq 0$. Se $\text{char } R = n \neq 0$, allora $\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}} = 0_R$. Ne segue che

$$\underbrace{1_S + 1_S + \cdots + 1_S}_{n \text{ volte}} = \underbrace{f(1_R) + f(1_R) + \cdots + f(1_R)}_{n \text{ volte}} = f(\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}}) = f(0_R) = 0_S.$$

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 $n \cdot 1_S = \underbrace{1_S + 1_S + \cdots + 1_S}_{n \text{ volte}} = 0_S$. Dividiamo n per m . Allora $n = qm + r$ con $q, r \in \mathbb{Z}$ e $0 \leq r < m$,

e quindi $0_S = n \cdot 1_S = (qm + r) \cdot 1_S = (qm) \cdot 1_S + r \cdot 1_S = q(m \cdot 1_S) + r \cdot 1_S = q \cdot 0_S + r \cdot 1_S = r \cdot 1_S$

perché $\text{char } S = m$. Se fosse $r > 0$, allora $\underbrace{1_S + 1_S + \cdots + 1_S}_{r \text{ volte}} = 0_S$, e questo è assurdo perché $\text{char } S = m > r$. Quindi si deve avere $r = 0$ ed $n = qm$.

$$29.3. \text{ (a)} \frac{1}{2+x} = \frac{1}{2} \cdot \frac{1}{1 - \left(-\frac{x}{2}\right)} = \frac{1}{2} \sum_{n \geq 0} \left(-\frac{x}{2}\right)^n = \sum_{n \geq 0} \frac{(-1)^n}{2^{n+1}} x^n.$$

$$\text{(b)} \frac{1}{(2+x)^2} = \frac{1}{4} \cdot \frac{1}{\left(1 + \frac{x}{2}\right)^2} = \frac{1}{4} \left(1 + \frac{x}{2}\right)^{-2} = \frac{1}{4} \sum_{n \geq 0} \binom{-2}{n} \left(\frac{x}{2}\right)^n \text{ (serie binomiale). Ora}$$

$$\binom{-2}{n} = \frac{(-2)(-3)(-4) \cdots (-n+1)}{n!} = \frac{(-1)^n (n+1)!}{n!} = (-1)^n (n+1),$$

$$\text{e quindi } \frac{1}{(2+x)^2} = \frac{1}{4} \sum_{n \geq 0} (-1)^n (n+1) \frac{1}{2^n} x^n = \sum_{n \geq 0} \frac{(-1)^n (n+1)}{2^{n+2}} x^n.$$

$$\text{(c)} \frac{1}{(2+x)^3} = \frac{1}{8} \left(1 + \frac{x}{2}\right)^{-3} = \frac{1}{8} \sum_{n \geq 0} \binom{-3}{n} \left(\frac{x}{2}\right)^n = \sum_{n \geq 0} \binom{-3}{n} \frac{x^n}{2^{n+3}}. \text{ Ma}$$

$$\binom{-3}{n} = \frac{(-3)(-4) \cdots (-2-n)}{n!} = \frac{(-1)^n (n+2)!}{2(n!)^2} = \frac{(-1)^n (n+1)(n+2)}{2},$$

$$\text{e quindi } \frac{1}{(2+x)^3} = \sum_{n \geq 0} \frac{(-1)^n (n+1)(n+2)}{2^{n+4}} x^n.$$

29.4. (a) Derivando l'uguaglianza $g \cdot \frac{1}{g} = 1$ si trova che $g' \cdot \frac{1}{g} + g \cdot \frac{d}{dx} \left(\frac{1}{g}\right) = 0$, e da questa (a) segue immediatamente.

29.6. Si deve verificare che $\exp(-x) \exp(x) = 1$, e questo segue immediatamente dall'esercizio 29.2.

29.7. Poniamo

$$\exp(\log(1+x)) = \sum_{n \geq 0} a_n x^n.$$

Confrontando i termini noti di questa uguaglianza si trova che $1 = a_0$, mentre derivandola si trova che

$$\exp(\log(1+x)) \cdot \frac{1}{1+x} = \sum_{n \geq 1} n a_n x^{n-1}.$$

Quindi $\sum_{n \geq 0} a_n x^n = (\sum_{n \geq 1} n a_n x^{n-1}) (1+x)$. Confrontando i coefficienti di x^n in questa uguaglianza si vede (per $n=0$) che $a_0 = a_1$, e che $a_n = (n+1)a_{n+1} + n a_n$ per ogni $n \geq 1$, cioè che $a_{n+1} = \frac{1-n}{n+1} a_n$ per ogni $n \geq 1$. Ne segue (per $n=1$) che $a_2 = 0$, e quindi, per induzione, che $a_n = 0$ per ogni $n \geq 2$. Quindi $\exp(\log(1+x)) = \sum_{n \geq 0} a_n x^n = 1+x$.

29.8. La derivata della serie $\log(1 + (\exp(x) - 1))$ è la serie

$$\frac{1}{1 + (\exp(x) - 1)} \exp(x) = 1.$$

Quindi le due serie $\log(1 + (\exp(x) - 1))$ e x differiscono per una costante, ossia $\log(1 + (\exp(x) - 1)) = x + c$ per qualche $c \in F$. Confrontando i termini costanti si trova che $c = 0$. Quindi $\log(1 + (\exp(x) - 1)) = x$.

29.9. Si ha

$$\frac{1}{(1-x)^n} = (1+(-x))^{-n} = \sum_{i \geq 0} \binom{-n}{i} (-x)^i.$$

Ora

$$\begin{aligned} \binom{-n}{i} &= \frac{(-n)(-n-1) \cdots (-n-i+1)}{i!} = (-1)^i \frac{n(n+1) \cdots (n+i-1)}{i!} \\ &= (-1)^i \frac{(n+i-1)!}{i!(n-1)!} = (-1)^i \binom{n+i-1}{i}, \end{aligned}$$

e quindi $1/(1-x)^n = \sum_{i \geq 0} \binom{n+i-1}{i} x^i$.

29.10. Per ogni $n \geq 1$ si ha $a_n = a_{n-1} + n$, e quindi, moltiplicando per x^n e sommando,

$$(48.7) \quad \sum_{n \geq 1} a_n x^n = \sum_{n \geq 1} a_{n-1} x^n + \sum_{n \geq 1} n x^n.$$

Si osservi ora che

$$\sum_{n \geq 1} n x^n = x \sum_{n \geq 1} n x^{n-1} = x \frac{d}{dx} \sum_{n \geq 0} x^n = x \frac{d}{dx} \frac{1}{1-x} = \frac{x}{(1-x)^2}.$$

Sia $f = \sum_{n \geq 0} a_n x^n$ la funzione generatrice. La (48.7) si riscrive allora nella forma

$$f = xf + \frac{x}{(1-x)^2},$$

da cui $f = x/(1-x)^3$.

29.11. Se f è la funzione generatrice, si ha $f = xf + \sum_{n \geq 1} n^2 x^n$ e $\sum_{n \geq 1} n^2 x^n = (x+x^2)/(1-x)^3$. Se ne ricava che

$$f = \frac{x+x^2}{(1-x)^4},$$

da cui $a_n = n(n+1)(2n+1)/6$.

29.12. (a) $f = -1 - x - x^2 + x^4 + x^5 + x^6$;

$$(b) f = \sum_{n \geq 0} (-1)^n x^n = \sum_{n \geq 0} (-x)^n = \frac{1}{1-(-x)} = \frac{1}{1+x};$$

$$(c) f = c \sum_{n \geq 0} x^n = \frac{c}{1-x}.$$

29.13. Sia A_n l'insieme delle n -uple (c_1, c_2, \dots, c_n) dove c_i è uguale a 0 o a 1 per ogni $i = 1, 2, \dots, n$ e in cui non appaiono due 0 consecutivi, e sia a_n la cardinalità di A_n . Per $n = 1, 2$ si ha ovviamente $a_1 = 2$ e $a_2 = 3$. Supponiamo $n \geq 3$ e determiniamo a_n . Sia $(c_1, c_2, \dots, c_n) \in A_n$. L' n -upla (c_1, c_2, \dots, c_n) termina con 1 o con 1,0. Se termina con 1, allora $(c_1, c_2, \dots, c_n) = (c_1, c_2, \dots, c_{n-1}, 1)$ dove $(c_1, c_2, \dots, c_{n-1}) \in A_{n-1}$. Quindi ci sono esattamente a_{n-1} n -uple in A_n che terminano in 1. Analogamente se $(c_1, c_2, \dots, c_n) \in A_n$ termina con 1,0, si

ha $(c_1, c_2, \dots, c_n) = (c_1, c_2, \dots, c_{n-2}, 1, 0)$ dove $(c_1, c_2, \dots, c_{n-2}) \in A_{n-2}$. Quindi ci sono esattamente a_{n-2} n -uple in A_n che terminano in 1, 0. In definitiva $a_n = a_{n-1} + a_{n-2}$ per ogni $n \geq 3$, che è proprio la relazione di ricorrenza dei numeri di Fibonacci. Però $a_1 = 2 = F_3$ e $a_2 = 3 = F_4$. Quindi $a_n = F_{n+2}$ per ogni $n \geq 1$.

29.14. La relazione di ricorrenza dei numeri di Fibonacci $F_i + F_{i+1} = F_{i+2}$, $i \geq 0$, si può riscrivere $F_i = F_{i+2} - F_{i+1}$. Sommando per $i = 0, 1, \dots, n$ si ha $F_0 + F_1 + \dots + F_n = F_2 + F_3 + \dots + F_{n+2} - F_1 - F_2 - \dots - F_{n+1} = F_{n+2} - F_1 = F_{n+2} - 1$.

29.15. Il caso $n = 0$ è ovvio. Se è vero per $n - 1$, allora $F_0 + F_1 + \dots + F_n = (F_0 + F_1 + \dots + F_{n-1}) + F_n = (F_{n+1} - 1) + F_n = F_{n+2} - 1$.

29.17. Per la proposizione 29.8 si ha $F_n = (\alpha^n - \beta^n)/\sqrt{5}$ con $\alpha = (1 + \sqrt{5})/2$ e $\beta = (1 - \sqrt{5})/2$. Quindi

$$\begin{aligned} F_n^2 &= \frac{1}{5}(\alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n) \quad \text{e} \quad F_{n-1}F_{n+1} = \frac{1}{5}(\alpha^{n-1} - \beta^{n-1})(\alpha^{n+1} - \beta^{n+1}) \\ &\quad = \frac{1}{5}(\alpha^{2n} - \alpha^{n-1}\beta^{n+1} - \alpha^{n+1}\beta^{n-1} + \beta^{2n}). \end{aligned}$$

Ne segue che

$$F_n^2 - F_{n-1}F_{n+1} = \frac{1}{5}(-2\alpha^n\beta^n + \alpha^{n-1}\beta^{n+1} + \alpha^{n+1}\beta^{n-1}) = \frac{\alpha^{n-1}\beta^{n-1}}{5}(-2\alpha\beta + \beta^2 + \alpha^2).$$

Ora $\alpha\beta = -1$ e $\alpha^2 + \beta^2 = 3$. Pertanto $F_n^2 - F_{n-1}F_{n+1} = \frac{(-1)^{n-1}}{5}(2 + 3) = (-1)^{n-1}$.

29.18. L'equazione caratteristica è $x^3 - 3x + 2 = 0$. Dato che $x^3 - 3x + 2 = (x - 1)^2(x + 2)$, l'equazione caratteristica ha la radice 1 di molteplicità 2 e la radice semplice -2. Quindi le successioni che soddisfano la relazione di ricorrenza $a_n = 3a_{n-2} - 2a_{n-3}$ per ogni $n \geq 3$ sono le $a_n = \lambda_1 \cdot 1^n + \lambda_2 n \cdot 1^n + \lambda_3(-2)^n = \lambda_1 + \lambda_2 n + \lambda_3(-2)^n$, $n \geq 0$. Dalle condizioni iniziali si ricava $\lambda_1 = \frac{10}{9}$, $\lambda_2 = -\frac{1}{3}$, $\lambda_3 = -\frac{1}{9}$. Quindi la successione cercata è la $a_n = \frac{1}{9}(10 - 3n - (-2)^n)$, $n \geq 0$.

29.19. Si osservi che il problema è equivalente al seguente. Sia $n \in \mathbb{N}$. Si calcoli quante sono le soluzioni $(m_1, m_2, m_3, m_4) \in \mathbb{N}^4$ del sistema

$$\begin{cases} m_1 + m_2 + m_3 + m_4 = n, \\ m_1 \geq 8, \\ m_2 \geq 3, \\ m_3 \geq 3, \\ m_4 \geq 3. \end{cases}$$

Sia a_n il numero di modi cercato per ogni $n \in \mathbb{N}$. Se calcoliamo il coefficiente di x^n nel prodotto

$$(x^8 + x^9 + x^{10} + \dots)(x^3 + x^4 + x^5 + \dots)(x^3 + x^4 + x^5 + \dots)(x^3 + x^4 + x^5 + \dots)$$

troviamo che il coefficiente di x^n è uguale al numero a_n di modi cercato. Quindi la funzione generatrice cercata è

$$(x^8 + x^9 + x^{10} + \dots)(x^3 + x^4 + x^5 + \dots)^3 = x^8 \cdot x^3 \cdot x^3 \cdot x^3 \cdot (1 + x + x^2 + \dots)^4 = \frac{x^{17}}{(1-x)^4}.$$

Per l'esercizio 29.9

$$\frac{x^{17}}{(1-x)^4} = \sum_{i \geq 0} \binom{i+3}{i} x^{i+17}.$$

Quindi $a_n = 0$ se $n < 17$ e $a_n = \binom{n-14}{n-17} = \frac{(n-14)(n-15)(n-16)}{6}$ se $n \geq 17$.

29.20. (b) I sottoinsiemi di k elementi di $X_n = \{1, 2, \dots, n\}$ possono o non contenere n o conterlo. Quelli che non lo contengono sono $a_{n-1,k}$. Quelli che lo contengono sono $a_{n-1,k-1}$.

(c) Per ogni n c'è un unico sottoinsieme di zero elementi di un insieme di n elementi. Quindi $f_0 = 1 + x + x^2 + \dots$

(d) Se si moltiplica l'identità dimostrata in (b) per x^n e si somma per $n = k, k+1, k+2, \dots$ si trova che $f_k = xf_k + xf_{k-1}$.

29.21. (a) Sia P_n l'insieme di tutte le parole nell'alfabeto A di lunghezza n con un numero pari di x_1 . Dato che P_0 contiene la sola parola vuota e questa ha zero x_1 si ha $a_0 = 1$. Supponiamo $n \geq 1$. Una qualunque parola appartenente a P_n finisce con una delle t lettere di A . Quindi possiamo ripartire P_n in t sottoinsiemi disgiunti P_{n,x_i} , $i = 1, 2, \dots, t$, dove P_{n,x_i} è l'insieme di tutte le parole appartenenti a P_n che finiscono in x_i . Per ogni $i = 2, 3, \dots, t$, si ha che una parola appartiene a P_{n,x_i} se e solo se è una parola appartenente a P_{n-1} seguita dalla lettera x_i . Quindi P_{n,x_i} ha a_{n-1} elementi per ogni $i = 2, 3, \dots, t$. Per $i = 1$, invece, una parola appartiene a P_{n,x_1} se e solo se è una parola di $n - 1$ lettere con un numero dispari di x_1 seguita dalla lettera x_1 . Dato che ci sono t^{n-1} parole di lunghezza $n - 1$ in un alfabeto di t lettere, si vede che ci sono $t^{n-1} - a_{n-1}$ parole di lunghezza $n - 1$ nell'alfabeto A con un numero dispari di x_1 . Quindi P_{n,x_1} ha cardinalità $t^{n-1} - a_{n-1}$. In definitiva quindi $a_n = t^{n-1} - a_{n-1} + (t-1)a_{n-1}$. La relazione di ricorrenza cercata è quindi $a_n = t^{n-1} + (t-2)a_{n-1}$ per ogni $n \geq 1$.

(b) Sia $f = \sum_{n \geq 0} a_n x^n$ la funzione generatrice. Dato che $a_n = t^{n-1} + (t-2)a_{n-1}$ per ogni $n \geq 1$, moltiplicando per x^n e sommando per $n \geq 1$ si trova che $\sum_{n \geq 1} a_n x^n = \sum_{n \geq 1} t^{n-1} x^n + \sum_{n \geq 1} (t-2)a_{n-1} x^n$, ossia $f - a_0 = x \sum_{n \geq 1} (tx)^{n-1} + (t-2)x \sum_{n \geq 1} a_{n-1} x^{n-1}$, vale a dire

$$f - 1 = x \frac{1}{1-tx} + (t-2)xf.$$

Se ne ricava che

$$f = \frac{(1-t)x + 1}{(1-tx)(1-(t-2)x)}.$$

(c) Per $t = 1$ la formula trovata in (b) diventa $f = 1 / ((1-x)(1+x))$, da cui $f = 1 / (1-x^2) = \sum_{i \geq 0} x^{2i}$. Quindi il coefficiente di x^n in f è 1 per n pari ed è 0 per n dispari.

(d) Per $t = 2$ la relazione di ricorrenza trovata in (a) dice che $a_n = 2^{n-1}$ per ogni $n \geq 1$.

29.22. (b) Un qualunque elemento di T_{k_1, \dots, k_n} , cioè una partizione $\mathcal{F} \in T_{k_1, \dots, k_n}$, che è immagine di una permutazione $\sigma \in S_n$, è immagine anche di tutte le permutazioni che si ottengono da σ scambiando tra loro le k_1 classi di 1 elemento ($k_1!$ possibilità), scambiando tra loro le k_2 classi di 2 elementi ($k_2!$ possibilità), eccetera. Si possono poi scambiare in σ tra loro gli elementi delle classi di 2 elementi ($(2!)^{k_2}$ possibilità), scambiare tra loro gli elementi delle classi di 3 elementi ($(3!)^{k_3}$ possibilità), e così via. In definitiva l'antiimmagine mediante Φ di un qualunque elemento $\mathcal{F} \in T_{k_1, \dots, k_n}$ è un sottoinsieme di S_n avente $k_1!(1!)^{k_1} k_2!(2!)^{k_2} \dots k_n!(n!)^{k_n}$ elementi.

(c) Dato che $\Phi: S_n \rightarrow T_{k_1, \dots, k_n}$ è suriettiva, S_n ha $n!$ elementi e l'antiimmagine di ogni elemento di T_{k_1, \dots, k_n} ha cardinalità $k_1!(1!)^{k_1} k_2!(2!)^{k_2} \dots k_n!(n!)^{k_n}$, ne segue che T_{k_1, \dots, k_n} ha

$$\frac{n!}{k_1!(1!)^{k_1} k_2!(2!)^{k_2} \dots k_n!(n!)^{k_n}}$$

elementi. L'asserto (c) segue ora immediatamente.

30.3. Sono le applicazioni $f: X \rightarrow \mathbb{R}$ tali che $f(X) \subseteq \{0, 1\}$.

30.11. (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 $a \oplus b = a + b - 2ab$ di R appartiene a E_R , cioè che se a e b sono idempotenti anche $a + b - 2ab$ è idempotente. Un semplice calcolo mostra che $(a + b - 2ab)^2 = a^2 + b^2 + 4a^2b^2 + 2ab - 4a^2b - 4ab^2 = a + b + 4ab + 2ab - 4ab - 4ab = a + b - 2ab$.

(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 $a \oplus (b \oplus c) = a \oplus (b + c - 2bc) = a + b + c - 2bc - 2a(b + c - 2bc) = a + b + c - 2bc - 2ab - 2ac + 4abc$ e $(a \oplus b) \oplus c = (a + b - 2ab) \oplus c = a + b - 2ab + c - 2(a + b - 2ab)c = a + b - 2ab + c - 2ac - 2bc + 4abc$. Quindi \oplus è associativa. L'operazione \oplus è anche commutativa in quanto $a \oplus b = a + b - 2ab = b + a - 2ba = b \oplus a$. Per quanto riguarda lo zero si ha che $0_R \in E_R$ e $0_R \oplus a = 0_R + a - 2 \cdot 0_R a = a$. Inoltre in E_R ogni elemento è l'opposto di sé stesso, in quanto per ogni $a \in E_R$ si ha $a \oplus a = a + a - 2a^2 = 0_R$. Quindi (E_R, \oplus) è un gruppo abeliano.

Abbiamo già dimostrato in (c) che E_R è un sottomonoide 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 $a, b, c \in R$, $a(b \oplus c) = a(b + c - 2bc) = ab + ac - 2abc = ab + ac - 2(ab)(ac) = ab \oplus ac$. Infine ogni elemento di E_R è idempotente come elemento dell'anello R , e quindi è idempotente anche come elemento dell'anello E_R .

30.12. (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

$$\begin{aligned} a_0 + a_1x + a_2x^2 + \dots + a_nx^n &= a_2x^2 + a_3x^3 + \dots + a_nx^n \\ &= x^2(a_2 + a_3x + \dots + a_nx^{n-2}) = x^2f \end{aligned}$$

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 opportuni $n \in \mathbb{N}$ e $b_0, b_1, \dots, b_n \in \mathbb{Z}_2$. Pertanto $x^2f = b_0x^2 + b_1x^3 + \dots + b_nx^{n+2} = 0 + 0 \cdot x + b_0x^2 + b_1x^3 + \dots + b_nx^{n+2} \in I$.

(b) Se $g, g' \in I$, allora $g = x^2f$, $g' = x^2f'$ per opportuni $f, f' \in \mathbb{Z}_2[x]$, 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.

30.15. (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 reticolati booleani finiti sono isomorfi se e solo se sono equipotenti.

(e) $6 \oplus 10 = (6 \wedge 10') \vee (6' \wedge 10) = (6 \wedge 33) \vee (55 \wedge 10) = 3 \vee 5 = 15$; $6 \odot 10 = 6 \wedge 10 = 2$.

30.16. Ogni anello booleano 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 avente otto elementi.

30.17. 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 φ è iniettiva si avrà pertanto $a+b=1_R$.

31.2. 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) .

31.12. (a) Dato che $330 = 2 \cdot 3 \cdot 5 \cdot 11$, i divisori positivi di 330 sono tutti e soli del tipo $2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdot 11^{n_4}$ con n_1, n_2, n_3, n_4 uguali a 0 o 1. Sia $\varphi: L \rightarrow \mathcal{P}(X)$ definita da $\varphi(2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdot 11^{n_4}) = \{i \in X \mid n_i = 1\}$. Allora φ è una biiezione, ed è un isomorfismo di insiemi parzialmente ordinati perché $2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdot 11^{n_4} \mid 2^{n'_1} \cdot 3^{n'_2} \cdot 5^{n'_3} \cdot 11^{n'_4}$ se e solo se per ogni $i \in X$, $n_i = 1$ implica $n'_i = 1$, ossia se e solo se $\varphi(2^{n_1} \cdot 3^{n_2} \cdot 5^{n_3} \cdot 11^{n_4}) \subseteq \varphi(2^{n'_1} \cdot 3^{n'_2} \cdot 5^{n'_3} \cdot 11^{n'_4})$.

(b) Per (a) i reticolati (L, \mid) e $(\mathcal{P}(X), \subseteq)$ sono isomorfi, e sappiamo che il reticolo $(\mathcal{P}(X), \subseteq)$ è booleano. Quindi anche il reticolo (L, \mid) è booleano.

(c) 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 $a' = 330/a$.

(d) Non lo è.

(e) Lo è.

(f) Lo è.

31.14. Un isomorfismo è $\varphi: \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ definito da $\varphi(I) = \{y_i \mid i \in I\}$ per ogni $I \in \mathcal{P}(X)$.

31.16. (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 $x \in \mathbb{R}$.

(c) Un isomorfismo è $\varphi: L \rightarrow \mathcal{P}(\mathbb{R})$ definito da $\varphi(f) = f^{-1}(1)$ per ogni $f \in L$.

31.21. 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 $2^{2^3} = 2^8$ elementi (corollario 31.15) 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.

32.2. Sono tutte vere.

32.9. 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 .

33.4. (d) è falsa.

(e) è vera: basta prendere per y il numero reale $-x$.

33.5. Ci sono varie soluzioni possibili. La più semplice di queste è $\forall x (\neg(x = 0) \rightarrow \exists y (xy = 1))$.

33.6. Una soluzione possibile è $(\forall x \forall y ((x' = y') \rightarrow (x = y))) \wedge \neg(\forall y \exists x (x' = y))$.

35.4. (a) non è lineare; (b) non è lineare; (c) è lineare, ma non è un isomorfismo; (d) è lineare ed è un isomorfismo; (e) non è lineare; (f) è lineare, ma non è un isomorfismo; (g) non è lineare; (h) non è lineare; (i) non è lineare; (l) è lineare ed è un isomorfismo.

35.9. No, era sufficiente che $ak = ka$ per ogni $k \in K$, cioè che a commutasse con ogni elemento di K .

36.18. Sia $B = \{v_1 + v_2, v_2 + v_3, \dots, v_{n-1} + v_n, v_n + v_1\}$. Dato che B ha tanti elementi quanto è la dimensione di V , B è una base di V se e solo se i vettori di B sono linearmente indipendenti. Siano $\lambda_1, \lambda_2, \dots, \lambda_n \in K$. Si ha $\lambda_1(v_1 + v_2) + \lambda_2(v_2 + v_3) + \dots + \lambda_{n-1}(v_{n-1} + v_n) + \lambda_n(v_n + v_1) = 0$ se e solo se $(\lambda_1 + \lambda_n)v_1 + (\lambda_1 + \lambda_2)v_2 + (\lambda_2 + \lambda_3)v_3 + \dots + (\lambda_{n-2} + \lambda_{n-1})v_{n-1} + (\lambda_{n-1} + \lambda_n)v_n = 0$, cioè se e solo se

$$(48.8) \quad \left\{ \begin{array}{l} \lambda_1 + \lambda_n = 0 \\ \lambda_1 + \lambda_2 = 0 \\ \lambda_2 + \lambda_3 = 0 \\ \vdots \\ \lambda_{n-2} + \lambda_{n-1} = 0 \\ \lambda_{n-1} + \lambda_n = 0. \end{array} \right.$$

Si ha quindi che B è una base di V se e solo se i vettori di B sono linearmente indipendenti, se e solo se il sistema (48.8) ha solo la soluzione nulla. Risolvendo il sistema, dalle ultime $n - 1$ equazioni si ricava che $\lambda_i = -\lambda_{i+1}$ per ogni $i = 1, 2, \dots, n - 1$, e quindi $\lambda_2 = -\lambda_1$, $\lambda_3 = \lambda_1$, $\lambda_4 = -\lambda_1$, eccetera, vale a dire $\lambda_i = \lambda_1$ se i è dispari e $\lambda_i = -\lambda_1$ se i è pari. In particolare dalle ultime $n - 1$ equazioni si ha che $\lambda_n = \lambda_1$ se n è dispari e $\lambda_n = -\lambda_1$ se n è pari. Consideriamo quindi separatamente i due casi di n dispari e n pari. Supponiamo n dispari. Dal sistema (48.8) segue quindi che

$$\left\{ \begin{array}{l} \lambda_1 + \lambda_n = 0 \\ \lambda_n = \lambda_1, \end{array} \right.$$

e pertanto, sostituendo, $2\lambda_1 = 0$; più precisamente, il sistema (48.8) nelle incognite $\lambda_1, \lambda_2, \dots, \lambda_n$ ha una soluzione non nulla se e solo se l'equazione $2\lambda_1 = 0$ ha una soluzione λ_1 non nulla. Ecco

quindi che B è una base se e solo se i suoi vettori sono linearmente indipendenti, se e solo se il sistema (48.8) non ha una soluzione non nulla, se e solo se l'equazione $2\lambda_1 = 0$ non ha una soluzione λ_1 non nulla. Occorre ora ricordare che $2 = 0$ se il campo K ha caratteristica due, mentre $2 \neq 0$ se K ha caratteristica diversa da 2. Quindi se $\text{char } K = 2$, si ha $2 = 0$, e quindi ogni $\lambda \in K$ è soluzione dell'equazione $2\lambda_1 = 0$. Si ha quindi che se $\text{char } K = 2$, l'equazione $2\lambda_1 = 0$ ha una soluzione non nulla, e quindi B non è una base di V . Se invece $\text{char } K \neq 2$, allora $2 \neq 0$ in K , e quindi moltiplicando l'equazione $2\lambda_1 = 0$ per l'inverso di 2 si trova che quell'equazione è equivalente a $\lambda_1 = 0$ che chiaramente ha solo la soluzione nulla $\lambda_1 = 0$. Pertanto se $\text{char } K \neq 2$ il sistema (48.8) ha solo la soluzione nulla, e quindi B è una base.

Supponiamo invece n pari. In questo caso il sistema (48.8) è equivalente al sistema

$$\begin{cases} \lambda_1 + \lambda_n = 0 \\ \lambda_n = -\lambda_1, \end{cases}$$

ossia, sostituendo, $\lambda_1 - \lambda_1 = 0$, che è un'equazione soddisfatta da ogni valore di λ_1 , e quindi in particolare il sistema (48.8) ha soluzioni non nulle. Ne segue che in questo caso B non è una base di V .

Riassumendo, B è una base di V se n è dispari e $\text{char } K \neq 2$, mentre non è una base in tutti gli altri casi, ossia se n è pari o $\text{char } K = 2$.

37.8. È vero. Mostriamolo con la doppia inclusione.

$(A) + \langle B \rangle \subseteq \langle A \cup B \rangle$: Dato che $A \subseteq A \cup B \subseteq \langle A \cup B \rangle$, abbiamo che $\langle A \cup B \rangle$ è un sottospazio di V che contiene A , e quindi $\langle A \cup B \rangle$ deve contenere $\langle A \rangle$ perché $\langle A \rangle$ è il più piccolo sottospazio di V che contiene A . Quindi $\langle A \rangle \subseteq \langle A \cup B \rangle$. Analogamente $\langle B \rangle \subseteq \langle A \cup B \rangle$. Da queste due ultime inclusioni segue che $\langle A \rangle + \langle B \rangle \subseteq \langle A \cup B \rangle$.

$\langle A \cup B \rangle \subseteq \langle A \rangle + \langle B \rangle$: Si ha che $A \subseteq \langle A \rangle \subseteq \langle A \rangle + \langle B \rangle$. Analogamente $B \subseteq \langle A \rangle + \langle B \rangle$, e quindi $\langle A \rangle + \langle B \rangle$ è un sottospazio di V che contiene $A \cup B$. Dato che $\langle A \cup B \rangle$ è il più piccolo sottospazio di V che contiene $A \cup B$, si deve avere pertanto che $\langle A \cup B \rangle \subseteq \langle A \rangle + \langle B \rangle$.

37.9. Dall'esercizio 37.2(e) sappiamo che $V/U = W \oplus U/U \cong W$. Analogamente $V/U = W' \oplus U/U \cong W'$. Quindi $W \cong V/U \cong W'$.

38.6. $f(1, -1, 3) = 3 - 2x - x^2 + 3x^3$.

38.7. $f(1, -1, 3) = 3 + x + x^3$.

38.8. $f(0, 2, 2) = -2x + 2x^2$.

38.16. Sia $\{e_1, e_2, \dots, e_n\}$ la base canonica di K^n . Per il teorema 38.1 esiste un'unica applicazione lineare $g: W \rightarrow K^n$ tale che $g(w_i) = e_i$ per ogni $i = 1, 2, \dots, n$. Per il lemma 38.3 l'applicazione g è un isomorfismo.

Si osservi come si calcola l'immagine di un arbitrario vettore $w \in W$. Dato $w \in W$, il vettore w si scrive in modo unico come combinazione lineare degli elementi w_1, w_2, \dots, w_n della base di W , ossia esistono $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ univocamente determinati tali che $w = \sum_{i=1}^n \alpha_i w_i$. Allora $g(w) = g(\sum_{i=1}^n \alpha_i w_i) = \sum_{i=1}^n \alpha_i g(w_i) = \sum_{i=1}^n \alpha_i e_i = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Quindi g manda un generico vettore $w \in W$, che si scrive in modo unico nella forma $w = \sum_{i=1}^n \alpha_i w_i$, in $(\alpha_1, \alpha_2, \dots, \alpha_n)$.

39.4. Soluzione di (b):

$$\begin{pmatrix} 5 & 5 & 0 \\ 0 & 3 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 5 \end{pmatrix}.$$

39.12. È

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

39.14. 2.

39.16. 1.

40.3. Si ha

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

41.3. Il rango di A è 3 per il sistema (1), 2 per il sistema (2), 3 per il sistema (3) e 2 per il sistema (4).

42.2. $\det B = -2$.

42.5. Si ha $B = A^*$, e quindi $\det B = \det A$. Le matrici C e A si ottengono l'una dall'altra scambiando la prima e la quarta colonna, e quindi $\det C = -\det A$. La matrice D ha la prima e la quarta colonna uguali, e quindi $\det D = 0$. Infine $\det F = \det A + \det E$.

43.12. La matrice associata ad f rispetto alle basi canoniche è

$$\begin{pmatrix} 1 & -1 & -1 \\ 2 & -2 & -2 \\ -1 & 0 & -1 \\ 0 & 5 & 10 \end{pmatrix}.$$

La seconda riga è il doppio della prima, e la quarta riga è la somma della prima e della terza riga moltiplicata per -5 . Quindi il massimo numero di righe linearmente indipendenti è 2 (sono la prima e la terza riga; la seconda e la quarta riga sono combinazioni lineari della prima e della terza). Quindi la matrice associata ad f ha rango 2, ossia f ha rango 2. Ma allora $\dim \ker f = \dim(\mathbb{R}^3) - \dim(f(\mathbb{R}^3)) = 3 - 2 = 1$.

43.14. Dal teorema 38.1 sappiamo che se $\{(\lambda, 1, 0), (1, \lambda, 0), (0, 0, 1)\}$ è una base di \mathbb{Z}_5^3 , esiste un unico endomorfismo φ_λ con le proprietà richieste. Vediamo quindi per quali valori di $\lambda \in \mathbb{Z}_5$ l'insieme $\{(\lambda, 1, 0), (1, \lambda, 0), (0, 0, 1)\}$ è una base di \mathbb{Z}_5^3 . Per l'esercizio 43.5 l'insieme $\{(\lambda, 1, 0), (1, \lambda, 0), (0, 0, 1)\}$ è una base di \mathbb{Z}_5^3 se e solo se

$$\begin{vmatrix} \lambda & 1 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & 1 \end{vmatrix} \neq 0.$$

Ora

$$\begin{vmatrix} \lambda & 1 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} \lambda & 1 \\ 1 & \lambda \end{vmatrix} = \lambda^2 - 1 = (\lambda - 1)(\lambda + 1).$$

Quindi per $\lambda \neq 1$ e $\lambda \neq -1$ (ossia, dato che $\lambda \in \mathbb{Z}_5$, per $\lambda = 0, 2, 3$), si ha che $\{(\lambda, 1, 0), (1, \lambda, 0), (0, 0, 1)\}$ è una base di \mathbb{Z}_5^3 , e quindi esiste un unico endomorfismo φ_λ con le proprietà richieste. Supponiamo $\lambda = 1$. Allora $(\lambda, 1, 0) = (1, \lambda, 0)$ e $(\lambda, 1, 0) \neq (0, 1, 0)$, e quindi non esiste nessuna applicazione che manda $(\lambda, 1, 0)$ in $(\lambda, 1, 0)$ e $(1, \lambda, 0)$ in $(0, 1, 0)$. Infine se $\lambda = -1$, si ha $-(\lambda, 1, 0) = (1, \lambda, 0)$, e quindi ogni applicazione lineare che manda $(\lambda, 1, 0)$ in $(\lambda, 1, 0)$ deve mandare $(1, \lambda, 0) = -(\lambda, 1, 0)$ in $-(\lambda, 1, 0)$. Ma $-(\lambda, 1, 0) = (1, 1, 0)$. Quindi non esiste nessuna applicazione lineare che manda $(\lambda, 1, 0)$ in $(\lambda, 1, 0)$ e $(1, \lambda, 0)$ in $(0, 1, 0)$. Si è così dimostrato che esiste un'applicazione φ_λ con le proprietà richieste se e solo se $\lambda \neq 1$ e $\lambda \neq -1$.

Supponiamo ora $\lambda \neq 1$ e $\lambda \neq -1$ e cerchiamo per quali λ l'endomorfismo φ_λ è un isomorfismo. L'endomorfismo φ_λ è un isomorfismo se e solo se manda la base $\{(\lambda, 1, 0), (1, \lambda, 0), (0, 0, 1)\}$ di \mathbb{Z}_5^3 in una base di \mathbb{Z}_5^3 . Quindi φ_λ è un isomorfismo se e solo se $\{(\lambda, 1, 0), (0, 1, 0), (0, 0, 1)\}$ è una base di \mathbb{Z}_5^3 . Questo accade se e solo se

$$\begin{vmatrix} \lambda & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \neq 0.$$

Ora

$$\begin{vmatrix} \lambda & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = \lambda.$$

Quindi φ_λ è un isomorfismo se e solo se $\lambda \neq 0$ (e, ovviamente, $\lambda \neq 1$ e $\lambda \neq -1$).

44.8. Se A e B sono due matrici simili $n \times n$, esiste una matrice $n \times n$ invertibile P tale che $B = P^{-1}AP$. Quindi $\text{tr } A = \text{tr } B$ per l'esercizio 40.1(c). Poi

$$\begin{aligned} \det B &= \det(P^{-1}AP) = (\det P^{-1})(\det A)(\det P) = (\det P^{-1})(\det P)(\det A) \\ &= \det(P^{-1}P)(\det A) = \det(I_n)(\det A) = \det A. \end{aligned}$$

Per quanto riguarda il polinomio caratteristico si ha

$$\begin{aligned} p_B(x) &= \det(B - xI_n) = \det(P^{-1}AP - xI_n) = \det(P^{-1}AP - P^{-1}xI_nP) = \det(P^{-1}(A - xI_n)P) \\ &= (\det P^{-1})(\det(A - xI_n))(\det P) = (\det P^{-1})(\det P)(\det(A - xI_n)) \\ &= \det(P^{-1}P) \det(A - xI_n) = 1 \cdot \det(A - xI_n) = p_A(x). \end{aligned}$$

In particolare A e B hanno gli stessi autovalori, perché $p_A(x) = p_B(x)$ hanno le stesse radici.

44.9. Come si è visto nell'esercizio 44.8 due matrici simili hanno la stessa traccia, lo stesso determinante e gli stessi autovalori. Quindi la traccia di A è $d_1 + d_2 + \dots + d_n$, il determinante è $d_1 d_2 \dots d_n$, e gli autovalori sono d_1, d_2, \dots, d_n .

44.11. Cerchiamo innanzitutto gli autovettori di A . Il polinomio caratteristico di A è

$$p_A(x) = \begin{vmatrix} -1-x & -1 \\ 1 & 1-x \end{vmatrix} = (-1-x)(1-x) + 1 = x^2.$$

Quindi l'unico autovalore di A è 0. Se A fosse diagonalizzabile, A sarebbe simile a una matrice diagonale

$$D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}.$$

Per l'esercizio 44.8 le matrici A e D devono avere gli stessi autovalori, che sono 0 per A e d_1, d_2 per D . Quindi $d_1 = d_2 = 0$, e pertanto D deve essere la matrice nulla. Ma l'unica matrice simile alla matrice nulla è la stessa matrice nulla. Quindi A stessa dovrebbe essere la matrice nulla, contraddizione. La contraddizione deriva dal fatto di aver supposto A diagonalizzabile. Quindi la matrice A non è diagonalizzabile.

44.16. Non hanno gli stessi autovettori in generale. Ad esempio gli autovettori della matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sono tutti e soli gli $\begin{pmatrix} \alpha \\ 0 \end{pmatrix}$ con $\alpha \neq 0$, mentre gli autovettori della sua matrice trasposta $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ sono tutti e soli i $\begin{pmatrix} 0 \\ \beta \end{pmatrix}$ con $\beta \neq 0$.

45.6. Per il teorema 45.2 l'anello $\mathbb{Q}[\sqrt{2}]$ è un campo e $\{1, \sqrt{2}\}$ è una base di $\mathbb{Q}[\sqrt{2}]$ su \mathbb{Q} . Se $a, b \in \mathbb{Q}$ e $a + b\sqrt{2} \neq 0$, allora o a o b sono $\neq 0$, e quindi anche $a - b\sqrt{2} \neq 0$. Ma allora l'inverso di $a + b\sqrt{2}$ è

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2} \sqrt{2},$$

e si ha $a/(a^2 - 2b^2), -b/(a^2 - 2b^2) \in \mathbb{Q}$.

45.12. $b_j = -a_0^{-1}a_{j+1}$.

INDICE ANALITICO

A

- abeliano, gruppo, 167
- additivamente chiuso, sottoinsieme, 173
- addizione, 142, 209
- adiacenti, vertici, 109
- albero, 125
 - con radice, 135
 - di supporto, 128
 - ordinato con radice, 136
- alfabeto valutato, 165
- algebra:
 - di Boole, 274
 - — duale, 279
 - di tipo 1, 298
- algebricamente chiuso, campo, 394
- algebrico, elemento, 388
- algoritmo di Euclide, 30
- analisi combinatoria, 79
- anello, 209
 - banale, 215
 - booleano, 265
 - commutativo, 209
 - degli endomorfismi, 213, 347
 - degli interi di Gauss, 223, 242
 - dei polinomi, 217, 224
 - delle classi resto, 227
 - delle parti di un insieme, 265
 - delle serie formali, 245
- di Boole, 265
- integro, 211
- quoziente, 218
- anomalia di un numero complesso, 47
- antiimmagine, 15
- antiperiodo, 40
- antisimmetrica, relazione, 87
- applicazione, 14
 - biettiva, 16
 - canonica, 62, 162, 165
 - composta, 20
 - di inclusione, 20
 - identica, 17
 - iniettiva, 16
 - inversa, 23
 - lineare, 308
 - multilineare alternante, 361
 - prodotto, 20
 - suriettiva, 16
- argomento di un numero complesso, 47
- arietà di un'operazione, 138, 141
- asse:
 - immaginario, 46
 - reale, 46
- associatività, 167
- automorfismo, 101, 109, 151, 170, 219, 308
 - di Frobenius, 397
 - interno, 173

- autospazio, 384
- autovalore, 377, 378
- autovettore, 377, 378
- B
- base, 314
- bene ordinato, insieme, 92
- biiettiva, applicazione, 16
- biiezione, 16
- Binet, teorema di, 370
- binomiale, coefficiente, 76
- binomio, formula del, 78
- bipartito, grafo, 120
- Boole:
 - algebra di, 274
 - anello di, 265
- booleano:
 - anello, 265
 - reticolo, 102
- buona definizione, 70, 156, 179
- C
- cammino, 111, 117
- euleriano, 117
- — orientato, 119
- hamiltoniano, 118
- — orientato, 119
- nullo, 111
- orientato, 112
- campo, 212
- algebricamente chiuso, 394
- di riducibilità completa, 394
- cappio, 60, 110, 111
- caratteristica:
 - di un anello, 231
 - di un'applicazione lineare, 342
 - di una matrice, 340
 - equazione, 253
 - funzione, 74 *
- cardinalità, 71
- catena, 88, 121
- Cayley, teorema di, 155, 204
- centro di un gruppo, 204
- chiusura:
 - algebrica, 394
 - transitiva, 66
 - cicli disgiunti, 183
 - ciclico:
 - gruppo, 203
 - monoide, 150
 - ciclo, 182
 - cifra, 38
 - circuito, 111
 - euleriano, 117
 - — orientato, 119
 - orientato, 112
 - classe, 3
 - di equivalenza, 62
 - di una permutazione, 188
 - laterale, 191, 218
 - codominio, 15
 - coefficiente, 217, 221
 - binomiale, 76
 - direttivo, 221
 - cofinito, sottoinsieme, 106
 - colonna, 51
 - dei termini noti, 353
 - colorazione, 130
 - combinatoria, 79
 - combinazione, 79
 - lineare, 302
 - commutativo:
 - anello, 209
 - gruppo, 167
 - compatibili (operazione ed equivalenza), 156
 - complementato, reticolo, 102
 - complemento, 102
 - completamento delle basi, teorema del, 318
 - completo:
 - grafo, 112
 - multigrafo orientato, 119
 - componente connessa, 111
 - composizione:
 - di applicazioni, 20
 - di relazioni, 174
 - composta, applicazione, 20
 - concatenazione, 162
 - condizione iniziale, 250, 253
 - confrontabili, elementi, 88
 - congiunzione, 284
 - coniugato di un numero complesso, 46, 50
 - coniugio, 154
 - connessa, componente, 111
 - connesso, grafo, 111
 - connettivo logico, 284

contraddizione, 288
 controimmagine, 15
 coppia ordinata, 12
 corpo, 212
 corrispondenza, 13, 59
 — biunivoca, 11, 16
 costante, 165, 292
 Cramer:
 — regola di, 372
 — teorema di, 353

D

De Moivre, formula di, 47
 derivata:
 — di un polinomio, 244
 — di una serie, 246
 determinante, 359, 363
 diagonale, 116
 — principale, 53
 diagramma, 112
 — commutativo, 112
 diametro di un grafo, 120
 differenza:
 — di insiemi, 5
 — simmetrica, 5
 digrafo, 110
 dimensione:
 — di uno spazio vettoriale, 318
 — finita, 318
 — infinita, 318
 dimostrazione:
 — diretta, 290
 — indiretta, 290
 — per assurdo, 290
 — per contrapposizione, 290
 — per induzione, 31
 direttivo, coefficiente, 224
 disgiunti:
 — cicli, 183
 — insiemi, 5
 disgiunzione, 284
 distanza tra due vertici, 120
 divisione euclidea fra polinomi, 225
 divisore, 28, 240
 — dello zero, 211
 — improprio, 241
 — proprio, 241

dominio, 15, 211
 — di integrità, 211
 — euclideo, 239
 doppia implicazione, 284
 doppia inclusione, 6
 doppiamente connesso, 124
 duale, enunciato, 98

E

elemento:
 — di un insieme, 3
 — invertibile, 212
 — irriducibile, 241
 — neutro, 147
 endomorfismo, 151, 170, 219, 308
 — di Frobenius, 238
 — nonsingolare, 329
 — singolare, 329
 enunciato duale, 98
 equazione caratteristica, 253
 equipotenti, 71
 — polinomi booleani, 276
 equivalenza, 61
 — associata ad un'applicazione, 62
 — banale, 66
 — classe di, 62
 esponenziale, serie, 247
 estensione:
 — di un campo, 387
 — per linearità, 326, 327
 estremo inferiore, superiore, 90
 Euclide, algoritmo di, 30
 euleriano:
 — cammino, 117, 119
 — circuito, 117, 119

Eulero:
 — formula di, 129
 — teorema di, 117

F

faccia di un multigrafo, 129
 falso, 284
 famiglia, 3, 8
 fattoriale, 35, 74
 fattorizzazione unica nei domini euclidei,
 — teorema di, 241
 Fermat, piccolo teorema di, 398
 filtro, 281

- foglia, 135
 foresta, 125, 126
 forma:
 — normale disgiuntiva, 277
 — trigonometrica di un numero complesso, 47
 formula:
 formula del binomio, 78
 — di De Moivre, 47
 — di Eulero, 129
 — di Grassmann, 322
 — in logica predicativa, 295
 — in logica proposizionale, 287
 — di De Morgan per i reticolati booleani, 103
 Frobenius:
 — automorfismo di, 397
 — endomorfismo di, 238
 funzione, 14
 — caratteristica, 74
 — generatrice, 249
 — esponenziale, 257
 — ordinaria, 257
- G**
 generatore di un monoide ciclico, 150
 generatrice, funzione, 249
 giustapposizione, 162
 grado, 221, 240, 389
 — complessivo, 112
 — di entrata, 112
 — di un polinomio, 224
 — di un vertice, 109
 — di uscita, 112
 grafi isomorfi, 109
 grafo, 108
 — bipartito, 120
 — completo, 120
 — complementare, 114
 — completo, 112
 — connesso, 111
 — di una relazione, 116
 — diretto, 110
 — nullo, 131
 — orientato, 60, 110
 — connesso, 112
 — di una funzione, 116
 — di una permutazione, 181
- — regolare, 116
 — regolare, 110
 — sconnesso, 111
 Grassmann, formula di, 322
 gruppi isomorfi, 170
 gruppo, 167
 — abeliano, 167
 — alterno, 190
 — banale, 171
 — ciclico, 203
 — degli automorfismi, 173
 — degli elementi invertibili (o delle unità), 212
 — delle permutazioni, 181
 — delle radici n -esime dell'unità, 170
 — di Galois, 393
 — identico, 171
 — quoziante, 194
 — simmetrico, 168, 181
- H**
 Hamilton-Cayley, teorema di, 382
 hamiltoniano, cammino, 118, 119
- I**
 ideale, 216
 — di un reticolo, 279
 — di un'algebra di Boole, 281
 — improprio, 217
 — massimale, 233
 — nullo, 217
 — primo, 233
 — principale, 223, 240, 279
 — proprio, 217
 idempotente, 172, 265
 identica, applicazione, 17
 identità, 17, 147, 167, 168, 209
 — destra, 210
 — sinistra, 210
 immaginario, asse, 46
 immagine, 15
 — di un'applicazione, 15
 — inversa, 15
 immersione, 20
 implicazione, 284
 incidenti, lati, 109
 inclusione, applicazione di, 20
 indeterminata, 217
 indice, 6, 8, 192

- indotto, ordinamento, 89
- infinito, insieme, 79
- iniettiva, applicazione, 16
- insieme, 3
 - bene ordinato, 92
 - complementare, 5
 - delle classi resto, 68
 - delle parti, 5
 - di generatori di uno spazio vettoriale, 302
 - finito, 71
 - infinito, 79
 - linearmente ordinato, 88
 - numerabile, 79
 - parzialmente ordinato, 88
 - quoziante, 62
 - semiordinato, 88
 - totalmente ordinato, 88
 - vuoto, 4
- insiemi disgiunti, 5
- insiemi ordinatamente isomorfi, 88
- interno, automorfismo, 173
- intersezione di insiemi, 5
- inversa, applicazione, 23
- inverso, 166–168
- invertibile, 166, 212
 - a destra, 166
 - a sinistra, 166
- ipotesi induttiva, 32
- irriducibile, elemento, 241
- isomorfi, 102, 151, 219, 308
- isomorfismo:
 - di anelli, 219
 - di grafi, 109
 - — orientati, 419
 - di gruppi, 170
 - di insiemi ordinati, 88
 - di multigrafi orientati, 113
 - di reticolati, 101
 - di semigruppi o di monoidi, 151
 - di spazi vettoriali, 308
 - lineare, 308
- K
 - Kronecker, simbolo di, 54
 - Kuratowski, teorema di, 130
- L
 - Lagrange, teorema di, 192
- laterale, classe, 191, 218
- lato:
 - di un grafo, 108
 - di un multigrafo, 111
 - multiplo, 111
 - orientato, 60
 - — di un multigrafo orientato, 110
- legge di composizione, 141
- limitato, reticolo, 102
- lineare:
 - applicazione, 308
 - combinazione, 302
- linearmente ordinato, insieme, 88
- linguaggio, 293
- livello, 135
- logaritmo, serie, 247
- logica proposizionale, 283
- lunghezza:
 - di un cammino, 111
 - di un ciclo, 182
 - di una catena, 121
 - di una parola, 81
- M
 - maggiorante, elemento, 90
 - mappa, 14
 - massimo comun divisore, 29, 243
 - massimo, elemento, 90
 - matrice, 51
 - (0, 1), 174
 - associata ad un'applicazione
 - lineare, 332, 333
 - colonna, 308
 - completa, 353
 - di adiacenza, 121
 - di una corrispondenza, 56
 - diagonale, 381
 - diagonalizzabile, 381
 - incompleta, 352
 - inversa, 57, 338
 - invertibile, 338
 - quadrata, 53
 - simmetrica, 55
 - trasposta, 55
 - triangolare superiore, 368
 - matrici simili, 349
 - minimale, elemento, 90

minimo comune multiplo, 30
 minimo, elemento, 90
 minorante, elemento, 90
 minore, 373
 modulo, 34, 46
 modus ponens, 288
 molteplicità:
 — di un lato, 113
 — di una radice, 242
 moltiplicazione, 142, 209
 monico, polinomio, 224
 monoide, 148
 — ciclico, 150
 — delle parole, 162
 — libero, 162
 — quoziante, 156
 monomio, 224
 multigrafo, 110
 — finito, 117
 — orientato, 110
 — — completo, 119
 — — semplice, 110
 — piano, 128
 — planare, 129
 multilineare alternante, applicazione, 361
 multiplo, 28, 143, 240

N

negazione, 284
 neutro, elemento, 147
 nonsingolare, endomorfismo, 329
 norma, 154, 242
 notazione:
 — a infisso, 138
 — additiva, 142
 — binaria, 42
 — moltiplicativa, 142
 — polacca, 138
 nucleo, 198, 220
 nullo, cammino, 111
 numerabile, insieme, 79
 numeri:
 — complessi, 43
 — — coniugati, 46, 50
 — di Bell, 257
 — di Fibonacci, 250
 — interi, 3

 — — congrui (modulo n), 67
 — naturali, 3
 — primi, 28
 — — tra loro, 30
 — razionali, 3
 — reali, 3
 — relativamente primi, 30

O

omomorfismo:
 — di algebre di Boole, 275
 — di anelli, 219
 — di gruppi, 170
 — di insiemi ordinati, 88
 — di monoidi, 151
 — di reticoli, 101
 — di semigruppi, 151
 — di spazi vettoriali, 308
 operazione, 138, 141, 166
 — associativa, 142
 — binaria, 141, 166, 274
 — indotta, 143
 — n -aria, 141, 274
 — per componenti, 215
 — unaria, 166, 274

opposto, 167

ordinamento:

 — parziale, 87
 — totale, 88
 — usuale, 87
 ordinata, coppia, 12
 ordine, 170
 — alfabetico, 83
 — di un minore, 373
 — di una matrice quadrata, 53
 — lineare, 88
 — parziale, 87
 — — inverso, 90
 — totale, 88

orientato:

 — cammino, 112
 — circuito, 112

P

parola, 81, 162
 — vuota, 81
 parte:
 — frazionaria, 39

- immaginaria, 46
- intera, 39
- reale, 46
- partizione, 63
- parzialmente ordinato, insieme, 88
- periodo, 40
- permutazione, 75, 76
 - con ripetizioni, 82
 - di classe dispari, 188
 - di classe pari, 188
 - senza punti fissi, 258
- piano di Argand-Gauss, 46
- piccolo teorema di Fermat, 398
- polinomi booleani equivalenti, 276
- polinomio, 217, 224
 - booleano, 276
 - caratteristico, 378
 - minimo, 389
 - monico, 224
- potenza, 143, 149, 168
- principio:
 - di dualità per i reticolati, 99
 - di dualità per i reticolati di Boole, 107
 - di identità dei polinomi, 244
 - di induzione, 31, 32
- problema dei ponti di Königsberg, 123
- prodotto, 142, 209
 - cartesiano, 12
 - diretto, 152
 - — di algebre di Boole, 280
 - — di anelli, 215
 - — di reticolati, 280
 - — di semigruppi, 146
 - lessicografico, 95
 - righe per colonne, 52
 - scalare, 53, 299
 - applicazione, 20
- proiezione canonica, 20, 62, 156, 194, 219, 220, 310
- proposizione, 284
- proprietà:
 - di cancellazione, 173, 214
 - distributiva, 6
 - distributiva nei reticolati, 99
 - riflessiva, 61
 - simmetrica, 61
 - transitiva, 61

- universale dei monoidi liberi, 162
- universale del gruppo additivo ($\mathbb{Z}, +$), 202
- universale del monoide ($\mathbb{N}, +$), 207
- universale del semigruppo ($\mathbb{N}^*, +$), 207
- universale dell'anello dei polinomi, 224
- punto di taglio, 121
- Q
- quantificatore:
 - esistenziale, 292
 - universale, 292
- quattro colori, teorema dei, 130
- quo, 28, 39, 240
- R
- radice:
 - di un polinomio, 242
 - in un albero, 135
 - n -esima dell'unità, 48
- rango, 340, 342
- reale, asse, 46
- reciproco, 166
- regola di Cramer, 372
- regolare, grafo, 110
- relazione, 59
 - composta, 66
 - di equivalenza, 61
 - di ricorrenza, 249
 - — lineare, 252
 - di uguaglianza, 61
 - inversa, 66
- resto, 28, 39, 240
- restrizione, 161
- reticolati isomorfi, 102
- reticolo, 96
 - booleano, 102
 - complementato, 102
 - delle equivalenze, 107
 - di Boole, 102
 - distributivo, 100
 - duale, 279
 - limitato, 102
- riducibilità completa, campo di, 394
- riflessiva, proprietà, 61
- riga, 51
- Rouché-Capelli, teorema di, 354
- Ruffini, teorema di, 242

- S
 scalare, 299
 sconnesso, grafo, 111
 segnatura, 187
 semigruppo, 142
 — commutativo, 142
 — libero, 165
 — quoziante, 156
 semiordinamento, 87
 semiordinato, insieme, 88
 serie:
 — binomiale, 248
 — formale di potenze, 245
 — formali, anello delle, 245
 — geometrica, 246
 simbolo:
 — funzionale, 292
 — logico, 293
 — predicativo, 292
 simmetrica:
 — matrice, 55
 — proprietà, 61
 singolare, endomorfismo, 329
 sistema:
 — di coordinate, 11
 — omogeneo, 354
 — — associato, 354
 solido platonico, 132
 soluzione di un sistema, 353
 somma:
 — di spazi vettoriali, 321
 — diretta esterna, 323
 — diretta interna, 323, 326
 — in un anello, 209
 — in un semigruppo, 142
 sostituzione, teorema di, 316
 sottoalgebra di Boole, 275
 sottoanello, 211
 — fondamentale, 232
 sottocampo, 387
 sottografo, 109
 sottogruppo, 168
 — alterno, 200
 — banale, 168
 — identico, 168
 — improprio, 168
 — normale, 193
 — proprio, 168
 sottoinsieme, 4
 — chiuso per un'operazione, 142
 — improprio, 4
 — ordinato, 89
 — proprio, 4
 sottomonoide, 149
 — generato da un elemento, 150
 sottoreticolo, 101
 sottosemigruppo, 143
 sottospazio vettoriale, 301
 — generato da un sottoinsieme, 302
 — invariante, 377
 spazio vettoriale, 299
 — duale, 339
 — nullo, 299
 — quoziante, 307
 struttura algebrica, 142
 suriettiva, applicazione, 16
- T
 tautologia, 288
 tavola di verità, 285
 teorema:
 — cinese del resto, 230
 — dei quattro colori, 130
 — del completamento delle basi, 318
 — di Binet, 370
 — di Cayley per i gruppi, 204
 — di Cayley per i monoidi, 155
 — di corrispondenza per gli ideali, 221
 — di corrispondenza per i gruppi, 201
 — di Cramer, 353
 — di Eulero, 117
 — di fattorizzazione unica nei domini euclidei, 241
 — di Hamilton-Cayley, 382
 — di Kuratowski, 130
 — di Lagrange, 192
 — di Rouché-Capelli, 354
 — di Ruffini, 242
 — di sostituzione, 316
 — di Wilson, 397
 — fondamentale:
 — — dell'algebra, 394
 — — dell'aritmetica, 28
 — — di omomorfismo per gli anelli, 220

- — di omomorfismo per gli spazi vettoriali, 309
 — — di omomorfismo per i gruppi, 200
 — — di omomorfismo per i semigruppi e i monoidi, 157
 termine costante, 245
 totalmente ordinato, insieme, 88
 traccia, 349, 350
 transitiva, proprietà, 61
 trascendente, elemento, 388
 trasformazione lineare, 308
 trasposizione, 186
 trasposta, matrice, 55
 triangolare superiore, matrice, 368
 triangolo di Tartaglia o di Pascal, 77
- U**
 uguaglianza tra insiemi, 4
 unione di insiemi, 5
 unità, 166, 212
 — immaginaria, 44
- V**
 valore, 15
 — assoluto, 34, 46
- di verità, 284
 valutazione, 165
 variabile, 165, 276
 — proposizionale, 287
 vero, 284
 vertice:
 — di un grafo, 60, 108
 — di un multigrafo, 111
 — — orientato, 110
 — dispari, 109
 — isolato, 109
 — pari, 109
 vettore, 299, 300
 vettori linearmente dipendenti, 312
 vettori linearmente indipendenti, 312
- W**
 Wilson, teorema di, 397
- Z**
 zero:
 — di un polinomio, 242
 — in un anello, 209
 — in un gruppo, 167
 — in un monoide, 148

Alfabeto greco

α, A	alfa
β, B	beta
γ, Γ	gamma
δ, Δ	delta
ε, E	epsilon
ζ, Z	zeta

η, H	eta
$\theta, \vartheta, \Theta$	theta ^(†)
ι, I	iota
κ, K	cappa
λ, Λ	lambda
μ, M	mi

ν, N	ni
ξ, Ξ	xi
o, O	òmicron
π, Π	pi
ϱ, P	ro
$\sigma, \varsigma, \Sigma$	sigma

τ, T	tau
υ, Y	ipsilon
ϕ, φ, Φ	phi
χ, X	chi ^(‡)
ψ, Ψ	psi
ω, Ω	oméga

^(†) "th" aspirato come in inglese;^(‡) "ch" aspirato come in tedesco.