APPUNTI ED ESERCIZI DI MATEMATICA DISCRETA

Margherita Roggero

A.A. 2005/2006

Introduzione

Queste note contengono gli appunti del corso di Matematica Discreta del primo anno della Laurea triennale in Matematica dell'A.A. 2005/06.

Gli argomenti sono quasi sempre presentati nello stesso ordine e con lo stesso grado di approfondimento con cui sono presentati a lezione, per cui il contenuto di queste note può essere considerato a tutti gli effetti il programma d'esame.

Gli esercizi che si trovano al termine di ogni capitolo non sono invece, in generale, gli stessi che vengono svolti durate le ore di esercitazione in classe, pur essendo di tipo e grado di difficoltà del tutto analoghi; lo scopo è quello di lasciare allo studente, durante tutta la durata del corso, materiale per quel momento di lavoro autonomo, che riteniamo indispensabile per un efficace ed effettivo apprendimento (e controllo della comprensione) degli argomenti teorici affrontati a lezione.

Infine, gli esercizi di riepilogo proposti nell'ultimo capitolo sono ripresi da compiti d'esame e intendono fornire allo studente, oltre all'occasione per una verifica finale della preparazione, anche un saggio diretto di quanto viene richiesto in sede d'esame.

Di alcuni di questi esercizi è fornita anche una proposta di risoluzione.

Desidero ringraziare tutti coloro che mi hanno aiutato durante la stesura di questi appunti, in modo particolare il Dott. Mario Valenzano, per l'accurato lavoro di revisione, e il Dott. Andrea Mori, cui si devono molti degli esercizi proposti.

Indice

Capitolo 1

Il linguaggio degli insiemi

1.1 Insiemi ed elementi

Indicheremo abitualmente gli insiemi con lettere maiuscole $A, B, \ldots$ e gli elementi di un insieme con lettere minuscole.

(Nota bene: NON diamo una definizione formale di insieme.)
"a è un elemento dell'insieme A" si scrive in simboli "$a \in A$" e si legge "a appartiene ad A".

Idea intuitiva: un insieme è costituito e caratterizzato esclusivamente dai suoi elementi, ossia: due insiemi sono uguali se e solo se contengono gli stessi elementi.

Pur non avendoli ancora definiti in modo rigoroso, useremo già da ora gli insiemi numerici $\mathbb{N}$ (numeri naturali), $\mathbb{Z}$ (numeri interi relativi), $\mathbb{Q}$ (numeri razionali) ed $\mathbb{R}$ (numeri reali), soprattutto per poter costruire qualche esempio significativo.

Un insieme può essere assegnato elencando i suoi elementi.

Esempio 1.1.1. *$A = \{0, 1\}$ è l'insieme costituito dai due numeri 0 e 1.*

Un altro modo per assegnare un insieme è quello di indicare una sua **proprietà caratteristica** ossia una proprietà soddisfatta da tutti gli elementi dell'insieme e solo da essi:

$$B = \{x \in X \mid x \text{ soddisfa la proprietà } P\}.$$

Se si usa la proprietà caratteristica:

- è sempre **necessario** indicare esplicitamente l'insieme X degli elementi da prendere in considerazione;
- la proprietà P usata non deve essere in alcun modo vaga o ambigua.

Esempio 1.1.2. *Non hanno alcun senso espressioni quali:*
$X = \{$*multipli di* $2\}$,
$Y = \{$*numeri naturali grandi*$\}$,
$Z = \{$*soluzioni dell'equazione* $x^4 - 1 = 0\}$.
L'insieme $V = \{x \in \mathbb{R} \mid x^2 + 1 = 0\}$ *è invece perfettamente definito.*

Poiché nessun numero reale ha quadrato negativo, l'insieme V ora considerato è privo di elementi:

V si chiama **insieme vuoto** e si denota $\emptyset$.

L'insieme vuoto è unico: $\{x \in \mathbb{R} \mid x^2 + 1 = 0\} = \emptyset = \{n \in \mathbb{N} \mid n > n\}$.

Nei paragrafi successivi vedremo come a partire da insiemi noti se ne possano costruire altri mediante alcune costruzioni standard (unione, intersezione, complementare, insieme delle parti, prodotto cartesiano, quoziente).

Per indicare che un elemento a non appartiene ad un insieme A scriviamo $a \notin A$.

Preso un qualsiasi elemento a, a non appartiene all'insieme vuoto. In simboli: $\forall a$: $a \notin \emptyset$.

$\forall$ significa "per ogni", "ogni", "per tutti" ...

Ad eccezione dell'insieme vuoto, tutti gli altri insiemi contengono qualche elemento.

In simboli: $A \neq \emptyset \iff \exists\ a$ tale che $a \in A$.

Il simbolo $\exists$ significa "esiste", "c'è almeno un/o/a..."; a volte si usa anche il simbolo $\exists!$ col significato di "esiste uno ed un solo" o "esiste un unico".

$\iff$ si legge "se e soltanto se" e significa che l'affermazione che lo precede e l'affermazione che lo segue sono equivalenti ossia che sono entrambe vere oppure entrambe false.

1.2 Sottoinsiemi

Si dice che l'insieme A è un **sottoinsieme** dell'insieme B, oppure che A è contenuto in B, se e solo se ogni elemento di A è anche elemento di B. In simboli:

$A \subseteq B \iff (a \in A \implies a \in B)$.

Il simbolo $\implies$ si legge "implica". Se F_1 e F_2 sono due affermazioni, l'implicazione $F_1 \implies F_2$ significa che se (oppure ogni volta che) l'affermazione F_1 è vera, allora è vera anche F_2. Quindi l'implicazione è corretta quando F_1 e F_2 sono entrambe vere ed anche quando F_1 è falsa (indipendentemente dal fatto che F_2 sia vera o falsa).

Esempio 1.2.1. *L'implicazione* $\forall n \in \mathbb{N}\ (n > 3 \implies 2n$ *è pari*$)$ *è corretta.*

Invece $\forall n \in \mathbb{N}\ (n > 3 \implies n^2 > 20)$ *è falsa perché esiste almeno un caso in cui la prima affermazione è vera e la seconda no:* $4 > 3$*, ma* $4^2 \leq 20$.

NOTA BENE: **Una affermazione è vera se e soltanto se è vera in tutti i casi; la dimostrazione deve comprendere tutti i casi possibili e non soltanto alcuni casi particolari.**
Una affermazione è falsa se e solo se è falsa in almeno un caso; per provarlo è sufficiente esibire esplicitamente un controesempio.

L'insieme vuoto è sottoinsieme di ogni insieme; ogni insieme è sottoinsieme di se stesso: se A è un insieme, allora $\emptyset \subseteq A$ e $A \subseteq A$.

1.3 Unione, intersezione, complementare

Definizione 1.3.1. *Siano A, B, C insiemi.*

Si dice **unione** *di A e B e si denota $A \cup B$ l'insieme i cui elementi sono tutti gli elementi che stanno in almeno uno tra A e B:*

$$x \in A \cup B \Longleftrightarrow (x \in A \ \ oppure \ \ x \in B).$$

Si dice **intersezione** *di A e B e si denota $A \cap B$ l'insieme i cui elementi sono tutti gli elementi che stanno contemporaneamente in A e in B:*

$$x \in A \cap B \Longleftrightarrow (x \in A \ \ e \ x \in B).$$

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

L'unione e l'intersezione di insiemi non dipendono dall'ordine in cui gli insiemi vengono considerati e soddisfano le seguenti **proprietà distributive**:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \qquad (A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

Esempio 1.3.2. *Siano $A = \{x \in \mathbb{R} \mid x^2 - 1 = 0\}$ e $B = \{x \in \mathbb{R} \mid x^2 + 3x + 2 = 0\}$.*

Allora:

$$A \cup B = \{x \in \mathbb{R} \mid (x^2 - 1)(x^2 + 3x + 2) = 0\}$$

$$A \cap B = \{x \in \mathbb{R} \mid \left\{ \begin{array}{l} x^2 - 1 = 0 \\ x^2 + 3x + 2 = 0 \end{array} \right. \}$$

Unione, intersezione e relative proprietà possono essere generalizzati a famiglie qualsiasi di insiemi.

Definizione 1.3.3. *Sia I un insieme non vuoto e, per ogni $i \in I$, sia A_i un insieme:*

$$a \in \bigcup_{i \in I} A_i \Longleftrightarrow (\exists i \in I \ t.c. \ a \in A_i), \qquad a \in \bigcap_{i \in I} A_i \Longleftrightarrow (\forall i \in I \ si \ ha \ \ a \in A_i).$$

Esempio 1.3.4. *Il dominio della funzione reale di variabile reale $y = \tan(x)$ è:*

$$\bigcup_{k \in \mathbb{Z}} (-\frac{\pi}{2} + k\pi, \ \frac{\pi}{2} + k\pi).$$

Esempio 1.3.5. *Per ogni $n \in \mathbb{N}$ indichiamo con A_n l'insieme dei numeri interi relativi che sono multipli di n. Allora $\bigcap_{n \in \mathbb{N}} A_n = \{0\}$ e $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{Z}$.*

Definizione 1.3.6. *Siano X un insieme e A un suo sottoinsieme. Si dice* **complementare** *di A in X e si indica con $\mathcal{C}_X(A)$ l'insieme di tutti gli elementi di X che non appartengono ad A:*

$$\mathcal{C}_X(A) = \{x \in X \mid x \notin A\}.$$

Il complementare di A si denota anche con $\mathcal{C}(A)$ se dal contesto è chairo quale insieme X si sta considerando.

L'insieme complementare $\mathcal{C}_X(A)$ è l'unico insieme che verifica le due condizioni

$$A \cap \mathcal{C}_X(A) = \emptyset \quad \text{e} \quad A \cup \mathcal{C}_X(A) = X.$$

Valgono inoltre le **Leggi di De Morgan**: se A e B sono sottoinsiemi di X, allora:

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

Proprietà analoghe valgono relativamente ad unioni ed intersezioni di famiglie di insiemi.

Definizione 1.3.7. *Dati gli insiemi A e B, si dice* **insieme differenza** *di B ed A, e si denota $B \setminus A$, l'insieme formato da tutti gli elementi di B che non appartengono ad A, ossia:*

$$x \in B \setminus A \iff x \in B \text{ e } x \notin A \quad ovvero \quad B \setminus A = \mathcal{C}_{A \cup B}(A).$$

1.4 Insieme delle parti e partizioni

Gli insiemi possono a loro volta essere considerati come elementi di altri insiemi.

Esempio 1.4.1. *L'insieme $A = \{1, \{2, 3\}\}$ ha due elementi: il numero 1 e l'insieme formato dai numeri 2 e 3.*

L'insieme $X = \{5, \{5\}\}$ ha due elementi: il numero 5 e l'insieme che ha 5 come unico elemento (un insieme come $\{5\}$ che ha un solo elemento si dice anche **singleton***).*

Definizione 1.4.2. *Si dice* **insieme delle parti** *di un insieme X, l'insieme $\mathcal{P}(X)$ i cui elementi sono i sottoinsiemi di X:*

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

Attenzione alle notazioni: $a \in A \iff \{a\} \subseteq A \iff \{a\} \in \mathcal{P}(A)$.

Esempio 1.4.3. *Sia $A = \{0, 5, 7\}$. Allora $\mathcal{P}(A) = \{\emptyset, \{0\}, \{5\}, \{7\}, \{0, 5\}, \{0, 7\}, \{5, 7\}, A\}$.*

L'insieme delle parti di un insieme non è mai l'insieme vuoto poiché in ogni caso contiene almeno l'elemento $\emptyset$. In particolare $\mathcal{P}(\emptyset) = \{\emptyset\}$ ha 1 elemento.

Se X è un insieme con n elementi, l'insieme delle parti $\mathcal{P}(X)$ ha 2^n elementi. Vedremo in seguito una dimostrazione (anzi tre diverse dimostrazioni) di questa affermazione.

Definizione 1.4.4. *Si dice* **partizione** *di X una famiglia di suoi sottoinsiemi tali che:*
- *nessuno di essi è vuoto,*
- *sono due a due disgiunti,*
- *la loro unione è tutto X.*

In modo piu formale possiamo dire che una partizione $\mathcal{Q}$ di X è un sottoinsieme di $\mathcal{P}(X)$ tale che:
- $\emptyset \notin \mathcal{Q}$
- $\forall\ Y, Y' \in \mathcal{Q}$ *si ha* $Y \cap Y' = \emptyset$ *oppure* $Y = Y'$
- $\bigcup_{Y \in \mathcal{Q}} Y = X$.

Un insieme $\mathcal{Q}$ siffatto si dice anche **quoziente** *di X.*

Esempio 1.4.5. a. *I sottoinsiemi $P = \{n \in \mathbb{Z} \mid n \text{ è pari}\}$ e $D = \{n \in \mathbb{Z} \mid n \text{ è dispari}\}$ costituiscono una partizione di $\mathbb{Z}$. Il quoziente $\mathcal{Q} = \{P, D\}$ ha due elementi.*

b. *I sottoinsiemi $A = \{n \in \mathbb{Z} \mid n < 0\}$, $B = \{0, 1, 2\}$ e $C = \{n \in \mathbb{Z} \mid n \geq 3\}$ costituiscono una partizione di $\mathbb{Z}$. Il quoziente $\mathcal{Q} = \{A, B, C\}$ ha tre elementi.*

c. *Per ogni numero naturale $k \geq 1$ si consideri il sottoinsieme Y_k di $\mathbb{N}$ definito da:*

$$Y_k = \{x \in \mathbb{N} \mid \text{ la notazione posizionale di } x \text{ in base } 10 \text{ ha } k \text{ cifre}\}.$$

I sottoinsiemi Y_k formano una partizione di $\mathbb{N}$. Il quoziente $\mathcal{Q} = \{Y_k \mid k \in \mathbb{N}, k \geq 1\}$ ha infiniti elementi.

d. *I sottoinsiemi $Y_p = \{x \in \mathbb{Z} \mid x \text{ è multiplo di } p\}$, al variare di p nei numeri primi positivi di $\mathbb{Z}$, non costituiscono una partizione di $\mathbb{Z}$, poiché la loro unione non contiene il numero intero 1 (oppure perché non sono due a due disgiunti).*

Il Paradosso di Russell. *Secondo la "definizione informale-intuitiva per cui un insieme è dato semplicemente dai suoi elementi (senza ulteriori condizioni), risulta essere un insieme anche quello i cui elementi sono tutti i possibili insiemi: indichiamo un tale "insieme" con X. Per X vale la strana proprietá: $X \in X$.*
Potremmo allora classificare tutti gli "insiemi" secondo i due tipi:

- *insiemi A tali che $A \notin A$*
- *insiemi A tali che $A \in A$.*

Gli insiemi del primo tipo formano un "sottoinsieme" Y di X. A quale dei due tipi apparterrà Y? Se $Y \in Y$ allora Y è un insieme del primo tipo e quindi $Y \notin Y$.
D'altra parte se $Y \notin Y$, allora Y è un insieme del secondo tipo ossia $Y \in Y$.
Da questa contraddizione non c'è via d'uscita, se non quella di definire con grande attenzione il concetto di insieme, in modo da evitare che "cose" come X e Y siano degli insiemi.

1.5 Prodotto cartesiano

Definizione 1.5.1. *Siano A, B, $A_1, \ldots, A_n$ insiemi.*
Si dice **prodotto cartesiano** *di A e B e si denota $A \times B$ l'insieme i cui elementi sono le* **coppie ordinate** *(a, b) dove a varia tra tutti gli elementi di A e b tra quelli di B:*

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

(Osserviamo che la "coppia ordinata" (a, b) può essere definita in modo rigoroso nel linguaggio degli insiemi come l'insieme $\{\ a,\ b,\ \{a\}\ \}$, diverso dall'insieme $\{\ a,\ b,\ \{b\}\ \}$ che corrisponde alla coppia (b, a).)

Analogamente il prodotto cartesiano di $A_1, \ldots, A_n$ è l'insieme delle $n-$uple di elementi presi ordinatamente uno in ciascun insieme:

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

Se $A \neq \emptyset$ e $B \neq \emptyset$, allora anche $A \times B \neq \emptyset$. Infatti esiste almeno un elemento $a_0 \in A$ e almeno un elemento $b_0 \in B$ e quindi il prodotto cartesiano contiene almeno l'elemento (a_0, b_0). Lo stesso vale per il prodotto cartesiano di n insiemi non vuoti.

Definiremo in seguito il prodotto cartesiano di una famiglia qualsiasi di insiemi (cfr. Esempio 3.1.6 g.).

1.6 Esercizi

Gli esercizi contrassegnati con un asterisco, in questo e nei capitoli seguenti, sono di una difficoltà maggiore rispetto agli altri.

Nei seguenti problemi A, B, C, ... denotano sottoinsiemi arbitrari di un insieme X fissato.

1.1. Siano $X = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid x^2 + x - 2 = 0\}$, $B = \{1, -1, 2\}$ e $C = \{1, \{2, 3\}\}$.

a. Determinare l'insieme delle parti di B e l'insieme delle parti di C.

b. Dire quali delle seguenti affermazioni sono vere e quali false:

$$\begin{array}{ccccccc} \{1\} \not\subseteq A & & 1 \in C & & \{1\} \in A & & 2 \in C \\ 1 \in A & & \{1\} \in C & & A \subseteq B & & \{2,3\} \in C \end{array} \qquad \begin{array}{ccc} 1 \subseteq A & & 3 \in C \\ B \subseteq A & & \{2\} \in C \end{array}$$

1.2. Siano $X = \mathbb{N}$, $A = \{x \in \mathbb{N} \mid x < 20\}$ e $B = \{x \in \mathbb{N} \mid x \geq 10\}$. Calcolare:

$$A \cap B, \quad A \cup B, \quad A \setminus B, \quad B \setminus A, \quad \mathcal{C}_X(A), \quad \mathcal{C}_X(B).$$

1.3. Siano $X = \mathbb{R}$, $Y = \{x \in \mathbb{R} \mid x \leq 3\}$ e $Z = \{x \in \mathbf{R} \mid 5 \leq x < 21\}$. Determinare $\mathcal{C}_{\mathbb{R}}(Y \cup Z)$, $\mathcal{C}_{\mathbb{R}}(Y)$, $\mathcal{C}_{\mathbb{R}}(Z)$ e verificare che $\mathcal{C}_{\mathbb{R}}(Y \cup Z) = \mathcal{C}_{\mathbb{R}}(Y) \cap \mathcal{C}_{\mathbb{R}}(Z)$.

1.4. Provare che le seguenti affermazioni sono false esibendo dei controesempi espliciti:

i) $A \cap B = A \cap C \Longrightarrow B = C$;
ii) $(B \cup A) \cap C = B \cup (A \cap C)$;
iii) $A \setminus \mathcal{C}_X(B) = \mathcal{C}_X(\mathcal{C}_X(A) \setminus B)$.

1.5. Enunciare e verificare le proprietà distributive per l'unione finita e l'intersezione finita di insiemi. Generalizzare all'unione e intersezione di famiglie qualsiasi di insiemi.

1.6. Enunciare e verificare le Leggi di De Morgan per l'unione finita e l'intersezione finita di insiemi. Generalizzare all'unione e intersezione di famiglie qualsiasi di insiemi.

1.7*. Siano $X = \mathbb{R}$, $Y = \{x \in \mathbb{R} \mid x \leq a\}$ e $Z = \{x \in \mathbb{R} \mid b \leq x < c\}$, dove a, b, c sono numeri reali qualsiasi, non necessariamente distinti. Determinare $\mathcal{C}_{\mathbb{R}}(Y \cup Z)$ come unione di sottoinsiemi disgiunti di $\mathbb{R}$.

1.8. Per ogni $n \in \mathbf{N}$, sia $A_n = \{x \in \mathbb{N} \mid x \neq n + 1\}$. Calcolare $\bigcup_{n\in\mathbb{N}} A_n$ e $\bigcap_{n\in\mathbb{N}} A_n$.

1.9. Per ogni $n \in \mathbb{N}$ poniamo $B_n = \{x \in \mathbb{N} \mid x \neq 2n\}$. Calcolare $\bigcap_{n\in\mathbb{N}} B_n$ e $\bigcup_{n\in\mathbb{N}} B_n$.

1.10. Per ogni $n \in \mathbb{N}$ poniamo $C_n = \{x \in \mathbb{N} \mid x \neq 2n + 3\}$. Calcolare $\bigcap_{n\in\mathbb{N}} C_n$ e $\bigcup_{n\in\mathbb{N}} C_n$.

1.11. Per ogni $n \in \mathbb{N}^* = \mathbb{N}\setminus\{0\}$ poniamo $I_n = (0, \frac{1}{n})$, intervallo aperto di $\mathbb{R}$. Dimostrare che $\bigcap_{n\in\mathbb{N}} I_n = \emptyset$. Determinare $\bigcup_{n\in\mathbb{N}} I_n$?

1.12. Per ogni $n \in \mathbb{N}^*$ poniamo $I_n = [0, \frac{1}{n}]$, intervallo chiuso di $\mathbb{R}$. Dimostrare che $\bigcap_{n\in\mathbb{N}} I_n = \{0\}$. Determinare $\bigcup_{n\in\mathbb{N}} I_n$?

1.13. Per ogni $n \in \mathbb{N}^*$ poniamo $I_n = [-n, \frac{1}{2n})$. Provare che non esistono due numeri naturali distinti n, m tali che $I_n \subseteq I_m$.Calcolare $\bigcap_{n\in\mathbb{N}} I_n$ e $\bigcup_{n\in\mathbb{N}} I_n$ e

1.14*. Trovare esplicitamente (oppure provare che non esistono) degli intervalli chiusi $I_n = [a_n, b_n]$ di $\mathbb{R}$, tali che $\bigcup_{n\in\mathbb{N}} I_n = (-1, 1)$.

1.15*. Trovare esplicitamente (oppure provare che non esistono) degli intervalli aperti $I_n = (a_n, b_n)$ di $\mathbb{R}$, tali che $\bigcup_{n\in\mathbb{N}} I_n = [-1, 1]$.

1.16. Dimostrare le uguaglianze $A \cap \mathcal{C}_X(B) = A \setminus B$ e $A \cup \mathcal{C}_X(B) = \mathcal{C}_X(B \setminus A)$.

1.17. Siano $A = \{1, 2, \sqrt{3}, -2, 0, \{2\}\}$ e $B = \{x \in \mathbb{R} \mid x^4 - 2x^2 - 3x - 2 = 0\}$. Determinare $A \cap B$, $\mathcal{C}_{\mathbb{R}}(B)$, $A \cap \mathcal{C}_{\mathbb{R}}(B)$, $A \setminus B$. Quali sono i sottoinsiemi di A che sono anche sottoinsiemi di B?

1.18. Dimostrare la seguente affermazione: $A \cap B = \emptyset$ se e solo se $\mathcal{C}_X(A) \cup \mathcal{C}_X(B) = X$.

1.19. Trovare esplicitamente dei sottoinsiemi A, B, C di $\mathbb{N}$ tali che $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$, $B \cap C \neq \emptyset$, $A \cap B \cap C = \emptyset$ e $A \cup B \cup C = \mathbb{N}$.

1.20. Siano D e P i sottoinsiemi dei numeri dispari e pari, rispettivamente. Dimostrare che $\{D, P\}$ è una partizione di $\mathbb{N}$.

1.21. Per ogni $r \in \{0, 1, 2\}$ si definisca A_r come il sottoinsieme dei numeri naturali la cui divisione per 3 dà resto r. Dimostrare che la famiglia $\{A_0, A_1, A_2\}$ è una partizione di $\mathbb{N}$.

1.22*. Per generalizzare la situazione dei due problemi precedenti, si fissi un numero naturale d maggiore di 1 e per ogni $r \in \{0, 1, \ldots, d-1\}$ si definisca A_r come il sottoinsieme dei numeri naturali la cui divisione per d dà resto r. Dimostrare che $\{A_1, A_2, \ldots, A_{d-1}\}$ definisce una partizione di $\mathbb{N}$.

1.23. Scrivere esplicitamente l'insieme delle parti dell'insieme $A = \{x, y, z\}$ e tutte le partizioni di A.

1.24. Dimostrare oppure confutare mediante controesempi le seguenti uguaglianze tra insiemi:

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B), \qquad \mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B).$$

1.25. Sia X l'insieme di tutti i numeri naturali multipli di 3. Scrivere una partizione di X costituita da 2 sottoinsiemi. Scrivere una partizione di X costituita da infiniti sottoinsiemi.

1.26*. Per ogni numero intero relativo n, sia A_n l'intervallo chiuso $[n + \sqrt{2}, n + 1 + \sqrt{2}]$. Calcolare $\bigcup_{n\in\mathbb{Z}} A_n$ e $\bigcap_{n\in\mathbb{Z}} A_n$. Gli insiemi A_n costituiscono una partizione di $\mathbb{R}$? Gli insiemi $A_n \cap \mathbb{Q}$ costituiscono una partizione di $\mathbb{Q}$?

1.27. È vero che per ogni coppia di insiemi $A, B \subset X$, la famiglia $\{A \cap B, A \setminus B, B \setminus A, \mathcal{C}_X(A \cup B)\}$ è una partizione di X?

1.28. È vero che $B \subseteq A$ se e soltanto se $\{B, A \setminus B, \mathcal{C}_X(A)\}$ è una partizione di X?

1.29*. Siano A un insieme, B un suo sottoinsieme e $\{A_i\}_{i\in I}$ una famiglia di sottoinsiemi di A. Provare oppure confutare mediante controesempi le seguenti affermazioni:

- **a.** se $\{A_i\}_{i\in I}$ è una partizione di A allora $\{B \cap A_i\}_{i\in I}$ è una partizione di B;
- **b.** se $\{B \cap A_i\}_{i\in I}$ è una partizione di B allora $\{A_i\}_{i\in I}$ è una partizione di A.

1.30. Esprimere l'insieme delle soluzioni reali della disequazione $\frac{x+2}{x+1} > 2$ in termini dei sottoinsiemi $A = \{x \in \mathbb{R} \mid x < 0\}$, $B = \{x \in \mathbb{R} \mid x > -1\}$.

1.31. Esprimere l'insieme delle soluzioni reali della disequazione $\sqrt{x^2 - 1} > x - 2$ in termini dei sottoinsiemi $A = (-1, 1)$, $B = \{x \in \mathbb{R} \mid x > 5/4\}$ e $C = \{x \in \mathbb{R} \mid x < 2\}$.

1.32*. Si generalizzi la discussione del problema precedente esprimendo l'insieme delle soluzioni reali della disequazione $\sqrt{P(x)} > Q(x)$ in termini degli insiemi $A = \{x \in \mathbb{R} \mid P(x) \geq 0\}$, $B = \{x \in \mathbb{R} \mid P(x) > Q(x)^2\}$ e $C = \{x \in \mathbb{R} \mid Q(x) < 0\}$.

1.33. Sia X l'insieme dei punti del piano cartesiano Oxy.

- **i)** Provare che le rette parallele all'asse x formano una partizione del piano X.
- **ii)** È vero che le rette passanti per l'origine formano una partizione di X?
- **iii)** Si può ottenere una partizione del piano mediante circonferenze con centro nell'origine?

1.34. Siano $A = \{-1, 0, 1\}$ e $B = \{1, 2\}$. Scrivere esplicitamente $A \times B$, $A \times A$, $(A \times A) \cap (A \times B)$, $A \times (A \cap B)$, $(A \times A) \cup (A \times B)$, $A \times (A \cup B)$, $\mathcal{P}(B \times B)$ e $\mathcal{P}(B) \times \mathcal{P}(B)$.

1.35*. Siano A, B due insiemi non vuoti e siano $\{A_1, A_2\}$ una partizione di A, $\{B_1, B_2\}$ una partizione di B.

- **i)** Provare che $\{A_1 \times B_1, A_2 \times B_2\}$ non è una partizione di $A \times B$.
- **ii)** Provare che $\{A_1 \times B_1, A_1 \times B_2, A_2 \times B_1, A_2 \times B_2\}$ è una partizione di $A \times B$.
- **iii)** Mostrare che esistono sempre altre partizioni di $A \times B$ oltre a quella del punto **ii)**.

Capitolo 2

Corrispondenze e relazioni

2.1 Corrispondenze

Definizione 2.1.1. *Siano A, B due insiemi. Si dice* **corrispondenza** *da A a B un qualsiasi sottoinsieme R del prodotto cartesiano $A \times B$.*
Se $A = B$, una corrispondenza in $A \times A$ si dice anche **relazione** *in A (o in $A \times A$).*

Per indicare che una certa coppia appartiene alla corrispondenza R, invece che $(a, b) \in R$, usualmente scriveremo aRb e diremo che a è in corrispondenza con b.

Esempio 2.1.2.

- *Siano $A = \{1, 4, -17\}$ e $B = \{0, 1, 2\}$. Il sottoinsieme $R = \{(1, 1),\ (4, 0),\ (4, 1)\}$ di $A \times B$ è una corrispondenza da A a B.*
- *L'insieme $T = \{(n, m) \in \mathbb{N} \times \mathbb{Z} \mid n = m^2\}$ è una corrispondenza da $\mathbb{N}$ a $\mathbb{Z}$.*
- *$R = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n + m$ è pari$\}$ è una relazione in $\mathbb{Z}$.*
- *Il semipiano $S = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$ del piano cartesiano $\mathbb{R}^2$ è una relazione in $\mathbb{R} \times \mathbb{R}$.*

Spesso una corrispondenza o una relazione sono assegnate individuando il sottoinsieme R mediante una sua proprietà caratteristica; in tal caso spesso si "confondono" la corrispondenza (o relazione) con la proprietà caratteristica stessa.

Esempio 2.1.3.

- *La circonferenza del piano cartesiano $\mathbb{R}^2$ di equazione $x^2 + y^2 = 1$ è una relazione in $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.*
- *La relazione "essere multiplo" in $\mathbb{N}$ è $\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m = nk$ per un qualche $k \in \mathbb{N}\}$.*

Definizione 2.1.4. *Dato un insieme A, la relazione $\Delta = \{(a,a) \in A \times A \mid a \in A\}$ si dice* **diagonale** *(o relazione identica) di $A \times A$.*

Definizione 2.1.5. *Sia R una corrispondenza in $A \times B$. Si dice* **corrispondenza inversa** *di R (relazione inversa nel caso $A = B$) la corrispondenza in $B \times A$ data da*

$$R^{-1} = \{(b,a) \in B \times A \mid (a,b) \in R\}.$$

Di particolare interesse nello studio di una relazione è stabilire se verifica alcune particolari proprietà. Diremo che una relazione R in A soddisfa la:

R) Proprietà riflessiva se $\forall\ a \in A$ si ha $(a,a) \in R$

S) Proprietà simmetrica se $\forall\ a,\ b \in A:\ (a,b) \in R \implies (b,a) \in R$

A) Proprietà antisimmetrica se $\forall\ a,\ b \in A:\ (a,b) \in R$ e $(b,a) \in R \implies a = b$

T) Proprietà transitiva se $\forall\ a,\ b,\ c \in A:\ (a,b) \in R$ e $(b,c) \in R \implies (a,c) \in R$

Esempio 2.1.6. *Vediamo quali delle proprietà R, S, A, T soddisfano alcune relazioni:*

a. *nell'insieme delle rette del piano, la relazione "essere incidente" ossia avere esattamente 1 punto in comune soddisfa soltanto S;*

b. *nell'insieme delle parti $\mathcal{P}(A)$ di un insieme A la relazione "essere sottoinsieme" gode delle proprietà R, A e T;*

c. *nell'insieme $\mathbb{Z}$ dei numeri interi la relazione "avere somma dispari" soddisfa solo S mentre "avere somma pari" soddisfa R, S, T.*

2.2 Relazioni d'ordine

Definizione 2.2.1. *Una relazione R in A si dice* **relazione d'ordine** *se soddisfa le proprietà riflessiva, antisimmetrica e transitiva (RAT).*
Una relazione d'ordine R in A si dice **ordine totale** *se due elementi qualsiasi $a,\ b \in A$ sono sempre* **confrontabili**, *ossia vale sempre (almeno) una tra $a\ R\ b$ e $b\ R\ a$. Una relazione d'ordine non totale si dice* **ordine parziale**.

Esempio 2.2.2.

a. *La relazione "divide" in $\mathbb{N}$ è una relazione d'ordine, ma è parziale: i numeri 2 e 3, ad esempio, non sono confrontabili tra loro in quanto nè 2 divide 3, nè 3 divide 2 in $\mathbb{N}$.*

b. *La relazione "divide" in $\mathbb{Z}$ non è una relazione d'ordine perché non soddisfa la proprietà antisimmetrica: 2 e -2 sono divisori l'uno l'altro in $\mathbb{Z}$, ma non sono uguali.*

c. *Se A è un insieme che ha almeno 2 elementi, l'inclusione in $\mathcal{P}(A)$ è una relazione d'ordine parziale. Se infatti a e b sono due elementi distinti di A, allora i due singleton $\{a\}$ e $\{b\}$ non sono confrontabili tra loro.*

d. *In $\mathbb{Z}$ la relazione "successore" nRm se $m = n+1$ non è una relazione d'ordine perché non soddisfa la proprietà transitiva.*

e. *$R = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid m = n + 2k$ con $k \in \mathbb{N}\}$ è una relazione d'ordine parziale in $\mathbb{Z}$.*

f. *Se R è una relazione d'ordine in A allora anche la relazione inversa R^{-1} è una relazione d'ordine. Inoltre se R è un ordine totale, anche R^{-1} lo è.*

Proprietà importante (che approfondiremo in seguito). Gli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ con le rispettive relazioni d'ordine "$\leq$" sono totalmente ordinati.

Definizione 2.2.3. *Sia R una relazione d'ordine in X e sia $A \subseteq X$. Si dice che m è il* **minimo** *di A se $m \in A$ e $\forall x \in A$ si ha mRx.*

Si dice che M è il **massimo** *di A se $M \in A$ e $\forall x \in A$ si ha xRM.*

Esempio 2.2.4.

a. *In $\mathbb{Z}$ dotato della relazione d'ordine $\leq$, il sottoinsieme dei numeri pari non ammette nè massimo nè minimo.*

b. *In $\mathbb{R}$ dotato della relazione d'ordine $\leq$, l'insieme dei numeri strettamente positivi non ammette nè minimo nè massimo.*

c. *Sia A un insieme. Consideriamo $X = \mathcal{P}(A)$ dotato della relazione d'ordine $\subseteq$. Allora X ha minimo $\emptyset$ e massimo A.*

Proposizione 2.2.5. *Siano R una relazione d'ordine in X e $A \subseteq X$.*
Se esiste un minimo m di A, allora è unico.
Se esiste un massimo M di A, allora è unico.

Dim: Supponiamo che m e m' soddisfino entrambi le condizioni per essere minimo di A. Allora in particolare scelto $x = m' \in A$, avremo che $m\ R\ m'$; allo stesso modo, preso $x = m \in A$, avremo che $m'\ R\ m$. Poiché R è una relazione d'ordine, R soddisfa la proprietà antisimmetrica e quindi $m = m'$.

La verifica relativa al massimo è del tutto analoga. $\diamond$

Definizione 2.2.6. *Un insieme X dotato di una relazione d'ordine R si dice* **ben ordinato** *se ogni sottoinsieme non vuoto di X ammette minimo.*

Definizione 2.2.7. *Sia A un sottoinsieme di un insieme X dotato di una relazione d'ordine R. Un elemento $x \in X$ si dice un* **minorante** *di A se per ogni $a \in A$ si ha xRa; analogamente un elemento $y \in X$ si dice un* **maggiorante** *di A se per ogni $a \in A$ si ha aRy.*

Risulta evidente dalla definizione che il minimo di A (se esiste) è un minorante di A ed anzi è l'unico minorante di A che appartiene ad A stesso. Analogamente, il massimo di A (se esiste) è un maggiorante di A ed anzi è l'unico maggiorante di A che appartiene ad A.

2.3 Relazioni di equivalenza

Definizione 2.3.1. *Una relazione R in un insieme A si dice* **relazione di equivalenza** *se soddisfa le proprietà riflessiva, simmetrica e transitiva (RST). Se R è una relazione di equivalenza, spesso si scrive $a \sim b$ invece che $(a, b) \in R$ oppure $a\ R\ b$.*

Esempio 2.3.2. *La relazione di parallelismo nell'insieme delle rette del piano è una relazione di equivalenza, mentre la relazione di ortogonalità non lo è.*

Definizione 2.3.3. *Sia $\sim$ una relazione di equivalenza in un insieme X e sia a un elemento di X. Si dice* **classe di equivalenza** *di a, e si denota $[a]$ (oppure $\overline{a}$) il sottoinsieme di X degli elementi che sono in relazione con a, ossia: $[a] = \{b \in X \mid a \sim b\}$.*
Un elemento a che appartiene ad una classe di equivalenza si dice anche **un rappresentante** *di quella classe.*

Si noti che tra gli elementi che appartengono a $[a]$ vi è anche a stesso, poiché, grazie alla proprietà riflessiva, si ha $a \sim a$; quindi a è in ogni caso un rappresentante di $[a]$.

Le relazioni di equivalenza in un insieme X ora definite corrispondono esattamente alle partizioni di X, di cui si è già parlato, come mostrano i due risultati seguenti.

Teorema 2.3.4. *Sia $\mathcal{Q} = \{Y_i \mid i \in I\}$ una partizione di X. Allora la relazione in X definita da:*

$$a\ R\ b \Longleftrightarrow \exists Y_i \in \mathcal{Q} \text{ tale che } a, b \in Y_i$$

è una relazione di equivalenza in X.

Dim: Dobbiamo verificare che sono soddisfatte le proprietà RST.

R) Poiché $\bigcup Y_i = X$, preso un qualsiasi $a \in X$ esiste sempre un sottoinsieme Y_i tale che $a \in Y_i$ e quindi $a\ R\ a$.

S) La validità della proprietà simmetrica è del tutto evidente: se $a, b \in Y_i$ allora $b, a \in Y_i$.

T) Siano a, b, c elementi di X e supponiamo che $a\ R\ b$ e che $b\ R\ c$, ossia che esistano Y_i e Y_j in $\mathcal{Q}$ tali che $a, b \in Y_i$ e $b, c \in Y_j$. Allora $b \in Y_i \cap Y_j$; poiché due sottoinsiemi distinti in una partizione non possono avere elementi in comune, allora $Y_i = Y_j$ e $a, c \in Y_i$ ossia $a\ R\ c$. $\diamond$

Teorema 2.3.5. *Sia $\sim$ una relazione di equivalenza in X. Allora le classi di equivalenza soddisfano le seguenti condizioni:*

i) $\forall a \in X\ [a] \neq \emptyset$*;*

ii) $\forall a, b \in X$ *si ha* $[a] = [b]$ *oppure* $[a] \cap [b] = \emptyset$*;*

iii) $\bigcup_{a \in X} [a] = X$*.*

Dim: Verifichiamo le tre condizioni.

i) $[a] \neq \emptyset$ poiché, come già visto, $a \in [a]$.

ii) Supponiamo $[a] \cap [b] \neq \emptyset$ e sia c un elemento di $[a] \cap [b]$. Proviamo che $[a] \subseteq [b]$.

Se $x \in [a]$, ossia se $a \sim x$, allora si ha:

$x \sim a$ (ottenuta usando la proprietà simmetrica)

$a \sim c$ perché $c \in [a]$ e $b \sim c$ perché $c \in [b]$ e quindi

$c \sim b$ (di nuovo usando la proprietà simmetrica).

Da queste relazioni, applicando due volte la proprietà transitiva, segue $x \sim b$ ossia $x \in [b]$.

In modo analogo si prova $[b] \subseteq [a]$ e quindi l'uguaglianza delle classi.

iii) È del tutto evidente che l'unione delle classi è contenuta in X. Proviamo allora che vale anche l'altra inclusione.

Sia $x \in X$; come già visto $x \in [x]$ e quindi x appartiene all'unione di tutte le classi. $\diamond$

Corollario 2.3.6. *Se $\sim$ è una relazione di equivalenza in X, allora le classi di equivalenza costituiscono una partizione di X: $\mathcal{Q} = \{[a] \mid a \in X\}$.*

Definizione 2.3.7. *Sia $\sim$ una relazione di equivalenza in X. Si dice* **insieme quoziente** *di X rispetto a (oppure modulo) l'equivalenza $\sim$, denotato $X_{/\sim}$, la partizione $\mathcal{Q}$ i cui elementi sono le classi di equivalenza: $X_{/\sim} = \{[a] \mid a \in X\}$.*

Esempio 2.3.8.

a. *La relazione di similitudine tra i triangoli del piano euclideo è una relazione di equivalenza. Se a è un triangolo con angoli interni α, β, γ, allora $[a] = \{$triangoli con angoli interni $\alpha, \beta, \gamma\}$.*

b. *La relazione in $\mathbb{Z}$: $n \sim m$ se $n - m$ è pari, è una relazione di equivalenza. La classe di un numero n è: $[n] = \{\ldots, n-4, n-2, n, n+2, n+4, \ldots\}$; le classi distinte sono quindi due, una contenente tutti i numeri pari e l'altra tutti i dispari.*

2.4 Esercizi

2.1. Sia $A = \{1, 2, 3, 4, 5, 6\}$ e siano ρ e σ le relazioni in A date da:

$x\rho y$ se e solo se $2x + 3y$ è multiplo di 5 e $x\sigma y$ se e solo se $2x - 3y$ è multiplo di 5.

a. Verificare che ρ è una relazione di equivalenza e scrivere esplicitamente tutte le classi di equivalenza.

b. Provare che invece σ non è una relazione di equivalenza. È una relazione d'ordine?

2.2. Siano $A = \{-1, 0, 1\}$ e $B = \{1, 2\}$.

a. Scrivere esplicitamente tutti gli elementi di $A \times B$, $A \times A$ e della diagonale Δ in $A \times A$.

b. Data la relazione $R = \{(-1, 1), (1, 0), (-1, -1), (1, 1), (0, 0)\}$ in $A \times A$, dire quali delle proprietà R, S, T, A tale relazione soddisfa.

c. È una relazione d'ordine? È un ordine totale?

d. Scrivere la relazione inversa R^{-1}.

2.3. Eseguire tutte le verifiche necessarie a completare quanto affermato nell'Esempio 2.2.2.

2.4. Sia X un insieme, A un suo sottoinsieme e R una relazione in X. Indichiamo con ρ la relazione in A indotta da R ossia:

$$\forall a, b \in A \text{ si ha } a\rho b \text{ se e solo se } aRb.$$

Verificare la validità delle seguenti proprietà:

i) se R è una relazione di equivalenza, anche ρ lo è,

ii) se R è una relazione di ordine, anche ρ lo è,

iii) se R è un ordine totale, anche ρ lo è.

iv) È vero che se X è ben ordinato mediante R, anche A lo è mediante ρ?

v) È vero che se $\{X_i\,,\, i \in I\}$ è una partizione di X, allora $\{A_i = X_i \cap A\,,\, i \in I\}$ è una partizione di A?

2.5. Trovare esplicitamente esempi di sottoinsiemi di $\mathbb{Z}$, $\mathbb{Q}$ ed $\mathbb{R}$ tali che, rispetto all'ordinamento usuale $\leq$:

a. non ammettono nè minimo nè massimo;

b. non ammettono minimo, ma hanno massimo;

c. ammettono minimo e massimo;

d. ammettono minimo m e massimo M tali che $m = M$.

2.6. In $\mathbb{N}$ si consideri la relazione: $x\rho y$ se x divide y ossia se $\exists k \in \mathbb{N}$ tale che $y = kx$.

a. Verificare che ρ è una relazione d'ordine.

b. È un ordine totale? È un buon ordinamento?

c. Dire se i sottoinsiemi $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{2, 3, 4, 12\}$ di $\mathbb{N}$ ammettono minimo e/o massimo rispetto alla relazione ρ.

d. $\mathbb{N}$ ammette minimo e/o massimo rispetto alla relazione ρ?

2.7. In $\mathbb{Z}$ si consideri la relazione: $x\rho y$ se x divide y ossia se $\exists k \in \mathbb{Z}$ tale che $y = kx$.

a. Provare che ρ non è nè una relazione d'ordine nè una relazione di equivalenza.

b. Sia $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x\rho y\}$ ossia il sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$ che individua (è) la relazione ρ. Determinare esplicitamente $S = R \cap R^{-1}$ e provare che S è una relazione di equivalenza.

2.8. In $\mathbb{Z}$ si consideri la relazione: $x\sigma y$ se $\exists k \in \mathbb{N}$ tale che $y = kx$.

a. Verificare che σ è una relazione d'ordine.

b. È un ordine totale? È un buon ordinamento?

c. Esiste un elemento di $\mathbb{Z}$ confrontabile con tutti gli altri?

d. Quali elementi sono confrontabili con -3?

e. Trovare oppure provare che non esistono il massimo e il minimo rispetto a σ dei seguenti sottoinsiemi:
$\{x \in \mathbb{Z} \mid x \geq 0\}$, $\{x \in \mathbb{Z} \mid x \leq 0\}$, $\{x \in \mathbb{Z} \mid x < 0\}$,
$P = \{x \in \mathbb{Z} \mid x \text{ è pari}\}$, $D = \{x \in \mathbb{N} \mid x \text{ è dispari}\}$.

2.9. Sia A un insieme dotato di una relazione d'ordine ρ rispetto alla quale A risulta ben ordinato. Provare che ρ è necessariamente un ordine totale.

2.10. Trovare esempi di relazioni in $\mathbb{N}$ che godano:

i) della proprietà R e non di S, T, A;

ii) della proprietà S e non di R, T, A;

iii) della proprietà T e non di R, S, A;

iv) della proprietà A e non di R, S, T.

2.11. In $\mathbb{N}$ si consideri la relazione $x\rho y$ se $x = y$ oppure se $2x$ divide y.

a. Provare che si tratta di una relazione d'ordine. È un ordine totale?

b. Provare che $\{2^k \mid k \in \mathbb{N}\}$ è un sottoinsieme totalmente ordinato rispetto a ρ.

c. Sia D il sottoinsieme di $\mathbb{N}$ dei numeri dispari. Provare che ρ ristretta a D è una relazione di equivalenza e caratterizzare le classi di equivalenza.

2.12. In $\mathbb{N} \times \mathbb{N}$ si consideri la relazione $(a, b)\rho(c, d)$ se $a + b < c + d$ oppure $a + b = c + d$ e $a \leq c$.

i) Verificare che si tratta di una relazione d'ordine totale;

ii) provare che $(0, 0)$ è il minimo di $\mathbb{N} \times \mathbb{N}$;

iii) scrivere le 6 coppie successive a $(0, 0)$ rispetto all'ordine ρ;

iv) provare che per ogni coppia (a, b) ci sono solo un numero finito di coppie che la precedono rispetto alla relazione ρ

2.13. In $\mathbb{N} \times \mathbb{N}$ si consideri la relazione $(a, b)\sigma(c, d)$ se $a < c$ oppure $a = c$ e $b \leq d$. Verificare che si tratta di una relazione d'ordine totale e provare che $(0, 0)$ è il minimo di $\mathbb{N} \times \mathbb{N}$. Provare che ogni coppia ha un successore immediato, ma che non esiste nessuna coppia di cui $(3, 0)$ sia il successore.

2.14. Dire quali delle proprietà R, S, T, A soddisfa la relazione ρ in A nei seguenti casi:

a. $A = \mathbb{Z}$, $x\rho y$ se $x - y = n^2$ per un qualche $n \in \mathbb{Z}$;

b. $A = \mathbb{Z}$, $x\rho y$ se $x - y = n^5$ per un qualche $n \in \mathbb{Z}$;

c. $A = \mathbb{R}$, $x\rho y$ se $|x| = |y|$;

d. $A = \mathbb{R}$, $x\rho y$ se $|x| \leq |y|$;

e. $A = \mathbb{Q} \setminus \{0\}$, $x\rho y$ se xy^{-1} può essere scritto come frazione $\frac{m}{n}$ con m, n interi dispari;

f. $A = \mathbb{N}$, $x\rho y$ se $x - y = 3n$ per un qualche $n \in \mathbb{N}$;

g. $A = \mathbb{N}$, $x\rho y$ se $x - y = 3n$ per un qualche $n \in \mathbb{Z}$.

In caso si tratti di una relazione d'ordine, dire se si tratta di un ordine totale. In caso si tratti di una relazione di equivalenza, determinare esplicitamente gli elementi di una classe a scelta.

2.15. Si consideri in $\mathbb{R}$ la relazione $x\rho y$ se e solo se $x - y \in \mathbb{Z}$. Verificare che è una relazione di equivalenza e scrivere esplicitamente $[1]$, $[\sqrt{2}]$, $[1.5]$. Provare che ogni classe di equivalenza $[x]$ ha uno ed un solo rappresentante x_0 tale che $0 \leq x_0 < 1$.

2.16. Si consideri in $\mathbb{R}$ la relazione $x\rho y$ se e solo se $x - y \in \mathbb{Q}$. Verificare che è una relazione di equivalenza e scrivere esplicitamente $[1]$, $[\sqrt{2}]$, $[1.5]$. È vero che ogni classe di equivalenza $[x]$ ha uno ed un solo rappresentante x_0 tale che $0 \leq x_0 < 1$?

2.17. Siano X un insieme non vuoto e ρ una relazione in X (ossia $\rho \subseteq X \times X$). Provare che:

a. ρ soddisfa le 4 proprietà R, S, T, A $\iff$ $\rho = \Delta$;

b. ρ è riflessiva $\iff$ $\Delta \subseteq \rho$;

c. ρ è simmetrica $\iff$ $\rho = \rho^{-1}$;

d. ρ è antisimmetrica $\iff$ $\rho \cap \rho^{-1} = \Delta$.

2.18. Siano A un insieme con almeno 3 elementi e $X = A \times A \times A$. Consideriamo la relazione τ in X data da:

$$(a, b, c)\tau(a', b', c') \text{ se } \{a, b, c\} = \{a', b', c'\}.$$

a. Verificare che τ è una relazione di equivalenza.

b. Fissati 3 elementi distinti a, b, c di A determinare esplicitamente le classi di equivalenza di (a, b, c), (a, b, a) e (c, c, c).

c. posto $A = \{1, 2, 3\}$, elencare tutti gli elementi di X e scrivere la partizione di X associata a τ.

Le relazioni presentate nei seguenti esercizi permettono di definire oggetti di particolare rilevanza in geometria.

2.19. Nel piano cartesiano $\mathbb{R}^2$ consideriamo la relazione $(x_1, y_1)\rho(x_2, y_2)$ se $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

Provare che si tratta di una relazione di equivalenza e caratterizzare geometricamente le classi di equivalenza.

2.20*. Nel piano cartesiano privato dell'origine $\pi^* = \mathbb{R}^2 \setminus \{O\}$ consideriamo la relazione:

$$P\rho Q \text{ se esiste una retta passante per l'origine che contiene } P \text{ e } Q.$$

a. Provare che ρ è una relazione di equivalenza.

b. Caratterizzare geometricamente la classe di equivalenza $[P]$ di un punto $P \in \pi^*$.

c. Sia C la circonferenza del piano di centro l'origine e raggio 1 e sia $P = (a, b)$ un punto qualsiasi. Determinare le coordinate di tutti i punti di $C \cap [P]$.

d. Sia r una retta del piano non passante per l'origine. Dire quanti elementi ha $r \cap [P]$, al variare di P in π^*.

e. Trovare un sottoinsieme di π^* che contenga esattamente 1 rappresentante per ciascuna classe di equivalenza.

2.21. Nel piano cartesiano $\mathbb{R}^2$ consideriamo la circonferenza Γ di centro l'origine e raggio 1 e in Γ la relazione

$$(x_1, y_1)\sigma(x_2, y_2) \text{ se } x_1 = -x_2 \text{ e } y_1 = -y_2 \text{ oppure } (x_1, y_1) = (x_2, y_2).$$

i) Provare che si tratta di una relazione di equivalenza e caratterizzare geometricamente le classi di equivalenza.

ii) Verificare che σ coincide con la relazione in Γ indotta dalla relazione ρ in π^* dell'esercizio precedente.

Il quoziente Γ/σ si chiama retta proiettiva.

2.22. Nell spazio cartesiano $\mathbb{R}^3$ consideriamo la superficie sferica Σ di centro l'origine e raggio 1 e in Σ la relazione

$$(x_1, y_1, z_1)\sigma(x_2, y_2, z_2) \text{ se } x_1 = -x_2,\ y_1 = -y_2 \text{ e } z_1 = -z_2 \text{ oppure } (x_1, y_1, z_1) = (x_2, y_2, z_2)\ .$$

Provare che si tratta di una relazione di equivalenza e caratterizzare geometricamente le classi di equivalenza.

Il quoziente Σ/σ si chiama piano proiettivo.

2.23. Nel piano cartesiano $\mathbb{R}^2$ consideriamo la relazione

$$(x_1, y_1)R(x_2, y_2) \text{ se } x_1 - x_2 \in \mathbb{Z} \text{ e } y_1 - y_2 \in \mathbb{Z}.$$

i) Provare che si tratta di una relazione di equivalenza.

ii) Verificare che $\mathbb{Z} \times \mathbb{Z}$ è la classe di $(0, 0)$.

iii) Determinare la classe di $(0.5, 2.3)$.

iv) Provare che ogni classe di equivalenza ha un rappresentante che appartiene al quadrato con vertici $(0, 0)$, $(0, 1)$, $(1, 0)$ e $(1, 1)$.

Il quoziente $\mathbb{R}^2/R$ si chiama toro.

2.24. Sia E l'insieme i cui elementi sono le equazioni lineari in due incognite a coefficienti in $\mathbb{R}$ ossia le equazioni del tipo $ax + by + c = 0$ con $a, b, c \in \mathbb{R}$. Si considerino la relazione σ in E data da "$e_1\sigma e_2$ se e_1 ed e_2 hanno le stesse soluzioni " e la relazione P in E data da "$e_1 P e_2$ se esiste $\lambda \in \mathbb{R}$, $\lambda \neq 0$ tale che $e_1 = \lambda e_2$ ". Verificare che σ eP coincidono e sono relazioni di equivalenza in S.

2.25. Sia S l'insieme dei sistemi lineari di due equazioni in due incognite. Verificare che la relazione "avere le stesse soluzioni è una relazione di equivalenza in S.

Capitolo 3

Le funzioni

3.1 Generalità sulle applicazioni o funzioni

Definizione 3.1.1. *Una* **applicazione o funzione** f *è una terna* $f = (A, B, \Gamma)$*, dove* A *e* B *sono insiemi non vuoti e* Γ *è una corrispondenza da* A *a* B *(cioè un sottoinsieme del prodotto cartesiano* $A \times B$*) che è ovunque definita e funzionale ossia che gode della seguente proprietà:*

$$\forall\ a \in A\ \exists!\ b \in B \text{ tale che } (a, b) \in \Gamma.$$

Notazioni e terminologia: A si dice **dominio** di f, B si dice **codominio** di f e Γ si dice **grafico** di f. Per indicare che f è una funzione da A in B invece che $f = (A, B, \Gamma)$ abitualmente si usa la notazione $f\colon A \longrightarrow B$. Fissato un elemento $a \in A$, per indicare che b è l'unico elemento di B tale che $(a, b) \in \Gamma$ si scrive $b = f(a)$ e si dice che b è **l'immagine** di a.

Definizione 3.1.2. *Si dice* **immagine** *di una funzione* $f\colon A \longrightarrow B$ *e si denota* $\mathrm{Im}f$ *oppure* $f(A)$ *il sottoinsieme di* B *degli elementi che sono immagine di qualche elemento di* A *ossia:*

$$\mathrm{Im}f = \{b \in B \mid b = f(a) \text{ per qualche } a \in A\}.$$

Più generalmente, dato un sottoinsieme C *di* A*, si dice* **immagine di** C *il sottoinsieme di* B*:*

$$f(C) = \{b \in B \mid b = f(a) \text{ per qualche } a \in C\}.$$

NOTA BENE Spesso per assegnare una funzione $f\colon A \longrightarrow B$ si fornisce una "legge" ossia una qualche formula che permette di associare a ciascun elemento del dominio la sua immagine. Si faccia però attenzione al fatto che la funzione è caratterizzata soltanto dal dominio A, dal codominio B e dal grafico Γ e non dalla eventuale "formulazione della legge".

I due esempi seguenti mostrano come una stessa"legge "può definire funzioni diverse e come, d'altra parte, "leggi diverse possono definire la stessa funzione.

Esempio 3.1.3. *La funzione* $f\colon \mathbb{Z} \longrightarrow \mathbb{N}$ *data da* $f(n) = n^2$ *e la funzione* $g\colon \mathbb{N} \longrightarrow \mathbb{Z}$ *data da* $g(n) = n^2$ *sono diverse, perché non hanno lo stesso dominio e lo stesso codominio, ma, oltre a questo, hanno anche proprietà molto diverse. Usando la terminologia che definiremo in seguito,* f *non è iniettiva, mentre* g *lo è.*

Esempio 3.1.4. *Siano* $A = \{0, 1, 2\}$ *ed* $f, g\colon A \longrightarrow \mathbb{R}$ *le funzioni definite rispettivamente da* $f(x) = x-7$ *e* $g(x) = x^3-3x^2+3x-7$*. Queste funzioni, per quanto espresse mediante "leggi" diverse, sono la stessa funzione, ossia* $f = g$*, poiché hanno lo stesso dominio* A*, lo stesso codominio* $\mathbb{R}$ *e lo stesso grafico:* $\Gamma_f = \Gamma_g = \{(0,-7),\ (1,-6),\ (2,-5)\}$.

NOTA BENE Particolare attenzione è necessario prestare alla definizione di funzioni mediante "leggi" nel caso in cui il dominio sia un insieme quoziente. In questi casi è sempre opportuno controllare che per ogni elemento del dominio, che è una classe di equivalenza, la sua immagine sia univocamente determinata, ossia non cambi se si cambia rappresentante della classe.

Esempio 3.1.5. *Sia* ρ *la relazione di equivalenza in* $\mathbb{Z}$ *data da* $x\rho y$ *se* $x - y$ *è multiplo di* 3*. Indichiamo con* $[x]$ *la classe di equivalenza di un elemento* x *nel quoziente* $\mathbb{Z}/\rho$*.*

Allora $[x] \mapsto [2^x]$ *non definisce una funzione* $f\colon \mathbb{Z}/\rho \to \mathbb{Z}/\rho$*, poiché* $[0] = [3]$*, ma* $[2^0] = [1] \neq [2^3] = [8]$*. Invece* $g\colon \mathbb{Z}/\rho \to \mathbb{Z}/\rho$ *data da* $[x] \mapsto [x^2]$ *è* **ben definita**. *Siano infatti* a *e* b *due rappresentanti di una stessa classe* $[a] = [b]$*, ossia* a *e* b *siano tali che* $a - b = 3k$ *per un qualche* $k \in \mathbb{Z}$*. Allora* $g([a]) = [a^2] = [(b+3k)^2] = [b^2+3(2bk+3k^2)] = [b^2]$.

Una riflessione importante suggerita dall'esempio precedente: esibire un esempio esplicito di classe la cui immagine non è univocamente definita mostra in modo rigoroso e completo che quella di f non è una buona definizione. Per provare che la funzione g è ben definita, invece, è stato necessario esaminare tutti gli elementi del dominio dimostrando con un ragionamento generale che le immagini sono univocamente determinate; un modo alternativo, (possibile soltanto perchè il dominio è un insieme finito) sarebbe stato quello di esaminare singolarmente, ossia uno alla volta, tutti gli elementi del dominio.

Quelli che seguono sono esempi di funzioni particolarmente importanti e che capiterà spesso di usare.

Esempio 3.1.6.

a. Le funzioni costanti. *Siano* A *e* B *insiemi e* $b_0 \in B$ *un elemento fissato. La funzione costante* b_0 *è* $f_{b_0}\colon A \longrightarrow B$ *definita da* $f_{b_0}(a) = b_0$ *per ogni* $a \in A$*. Se* $A = B = \mathbb{R}$*, la funzione costante* b_0 *ha come grafico la retta "orizzontale" di equazione* $y = b_0$*.*

b. Le funzioni identità. *Sia A un insieme; la funzione identità di A è $id_A\colon A \longrightarrow A$ definita da $id_A(a) = a$ per ogni $a \in A$. Se $A = B = \mathbb{R}$, la funzione identità $id_{\mathbb{R}}$ ha come grafico la retta bisettrice del primo e terzo quadrante di equazione $y = x$. Si faccia attenzione a non confondere la funzione identità con la funzione costante* 1.

c. Le funzioni proiezione su un fattore. *Siano A e B insiemi e $A \times B$ il loro prodotto cartesiano; si dice* **proiezione sul primo fattore** *la funzione $\pi_1\colon A \times B \longrightarrow A$ definita da $\pi_1((a, b)) = a$. Analogamente la* **proiezione sul secondo fattore** *è la funzione*
$\pi_2\colon A \times B \longrightarrow B$ *data da $\pi_2((a, b)) = b$.*

Se Γ è il grafico di una funzione f reale di variabile reale, allora $\pi_1(\Gamma)$ è il campo di esistenza di f e $\pi_2(\Gamma)$ è l'immagine di f.

d. Le funzioni proiezione sul quoziente. *Sia A un insieme dotato di una relazione di equivalenza ρ; indichiamo con A/ρ il relativo quoziente. Si dice* **proiezione di A sul quoziente** *la funzione $\pi\colon A \longrightarrow A/\rho$ definita da $\pi(a) = [a]$, dove $[a]$ indica la classe di equivalenza dell'elemento a.*

e. Le operazioni. *Una operazione binaria interna in un insieme A è una funzione $*\colon A \times A \longrightarrow A$. L'immagine di un elemento $*((a_1, a_2))$ di solito si denota $a_1 * a_2$.*

f. Le successioni. *Una successione è una funzione $f\colon \mathbb{N} \longrightarrow \mathbb{R}$; il termine $n-$esimo a_n della successione è l'immagine $f(n)$ del numero naturale n.*

g. *Sia I un insieme qualsiasi (che chiameremo* **insieme di indici***) e per ogni $i \in I$ sia A_i un insieme. Il prodotto cartesiano degli insiemi A_i denotato $\Pi_{i\in I}A_i$ è l'insieme i cui elementi sono le funzioni $f\colon I \to \cup A_i$ tali che $f(i) \in A_i$ per ogni $i \in I$.*

L'assioma della scelta *Contariamente a quanto accade nel caso del prodotto cartesiano di due insiemi non è possibile dimostrare che $\Pi_{i\in I}A_i$ è un insieme non vuoto quando tutti gli A_i sono non vuoti. Anzi l'affermazione:*

$$(\forall i \in I \ : \quad A_i \neq \emptyset) \quad \Longrightarrow \quad \Pi_{i\in I}A_i \neq \emptyset \tag{3.1}$$

non è nè vera nè falsa. Tale affermazione si chiama **Assioma della scelta** *e ogni matematico può liberamente scegliere se accettarlo come vero oppure rifiutarlo (con le relative conseguenze). Nel seguito noi assumeremo come vero l'Assioma della scelta.*

Definizione 3.1.7. *Siano $f\colon A \longrightarrow B$ una funzione, b un elemento di B e D un sottoinsieme di B. Si dice* **controimmagine di** *b il sottoinsieme di A così definito:*

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}.$$

Analogamente si dice **controimmagine di** *D il sottoinsieme di A:*

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

La controimmagine di un elemento b del codominio non è altro che la controimmagine del sottoinsieme singleton $\{b\}$, ossia $f^{-1}(b) = f^{-1}(\{b\})$. La controimmagine di un elemento è quindi sempre definita (ossia esiste sempre) ed è un sottoinsieme del dominio che, a seconda dei casi, può essere l'insieme vuoto $\emptyset$, oppure un singleton (ossia un sottoinsieme con un solo elemento), oppure un sottoinsieme con più elementi.

Esempio 3.1.8. *Siano* $A = \{0, 1, 2, 3\}$, $B = \mathbb{R}$ *e* $g\colon A \longrightarrow \mathbb{R}$ *l'applicazione definita da:* $g(0) = 5$, $g(1) = \sqrt{5}$, $g(2) = -\pi$, $g(3) = -\pi$.
Consideriamo i seguenti sottoinsiemi di $\mathbb{R}$*:* $D_1 = [3, +\infty)$, $D_2 = (-\infty, 0)$, $D_3 = [-10, -8]$.
Allora:

$$f^{-1}(D_1) = \{0\}\,,\ f^{-1}(D_2) = \{2, 3\}\,,\ f^{-1}(D_3) = \emptyset\ ,$$

$$f^{-1}(-\pi) = \{2, 3\}\,,\ f^{-1}(\sqrt{5}) = \{1\}\,,\ f^{-1}(27) = \emptyset.$$

Definizione 3.1.9. *Una funzione* $f\colon A \longrightarrow B$ *si dice:*

- **iniettiva** *se* $\forall\ a_1, a_2 \in A$: $\quad a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$*;*
- **suriettiva** *se* $\mathrm{Im}f = B$ *ossia se* $\forall\, b \in B\ \exists\ a \in A$ *tale che* $f(a) = b$*;*
- **biunivoca o biiettiva** *se è sia iniettiva sia suriettiva.*

Una funzione biunivoca si dice anche **biiezione oppure corrispondenza biunivoca ooppure corrispondenza** $1 - 1$.

Possiamo riformulare le precedenti definizioni usando le controimmagini.

Proposizione 3.1.10. *Sia* $f\colon A \longrightarrow B$ *una funzione. Allora:*

1) f *è iniettiva* $\iff \forall\, b \in B\ \ f^{-1}(b)$ *contiene al massimo un elemento.*

2) f *è suriettiva* $\iff \forall\, b \in B\ \ f^{-1}(b)$ *contiene almeno un elemento.*

3) f *è biunivoca* $\iff \forall\, b \in B\ \ f^{-1}(b)$ *contiene uno e un solo elemento.*

Dim: 1) Supponiamo f iniettiva e sia b un elemento qualsiasi di B. Se $b \notin \mathrm{Im}f$ allora $f^{-1}(b) = \emptyset$; se invece $b \in \mathrm{Im}f$ ossia se $b = f(a)$ per un qualche $a \in A$, allora per ogni $a' \neq a$ si ha $f(a') \neq f(a) = b$ e quindi $f^{-1}(b) = \{a\}$ contiene un solo elemento.

Supponiamo ora che la controimmagine di ciascun elemento del codominio contenga al massimo un elemento; se a_1, a_2 sono elementi distinti di A, allora le loro immagini $b_1 = f(a_1)$ e $b_2 = f(a_2)$ sono distinte perché in caso contrario $f^{-1}(b_1)$ conterrebbe più di un elemento.

2) L'equivalenza segue subito dall'osservazione che $f^{-1}(b) \neq \emptyset$ se e solo se $b \in \mathrm{Im}f$.

Infine 3) si ottiene immediatamente dalle precedenti. $\diamond$

Esempio 3.1.11.

a. *Le funzioni costanti da A in B non sono mai nè iniettive (tranne nel caso molto particolare in cui A abbia un solo elemento) nè suriettive (tranne nel caso molto particolare in cui B abbia un solo elemento).*

b. *Le funzioni identità $id_A \colon A \longrightarrow A$ sono sempre biunivoche.*

c. *Le funzioni proiezione su un fattore π_1 e π_2 dal prodotto cartesiano $A \times B$ su A e su B rispettivamente, sono sempre suriettive. Inoltre π_1 (risp. π_2) è anche iniettiva soltanto in caso B (risp. A) abbia un solo elemento.*

d. *La funzione proiezione sul quoziente $\pi \colon A \longrightarrow A/\rho$ è sempre suriettiva, poiché (per definizione) le classi di equivalenza non sono mai vuote. L'unico caso in cui π risulta anche iniettiva è quello che riguarda la relazione "identità": $a_1 \rho a_2$ se e solo se $a_1 = a_2$.*

3.2 Funzioni composte

Definizione 3.2.1. *Siano $f \colon A \longrightarrow B$ e $g \colon B \longrightarrow C$ funzioni. Si dice* **funzione composta di f e g** *la funzione: $g \circ f \colon A \longrightarrow C$ data da $(g \circ f)(a) = g(f(a))$.*

La lettura corretta di $g \circ f$ è "f composto g" in quanto f è la prima funzione che agisce e g la seconda; per evitare una (per noi) poco naturale lettura da destra verso sinistra e, nello stesso tempo, rispettare il significato matematico del simbolo, evitando confusione ed errori, si può leggere $g \circ f$ anche "g dopo f.

Si noti che la composizione di due funzioni è definita solo nel caso in cui il codominio della prima coincide col dominio della seconda.

Proposizione 3.2.2. (Proprietà associativa della composizione)
Siano $f \colon A \longrightarrow B$, $g \colon B \longrightarrow C$ e $h \colon C \longrightarrow D$ funzioni. Allora: $(h \circ g) \circ f = h \circ (g \circ f)$.

Dim: Per la verifica è sufficiente osservare che le due funzioni hanno lo stesso dominio A, lo stesso codominio D e assegnano a ciascun elemento a di A la stessa immagine $h(g(f(a)))$. $\diamond$

Grazie a tale proprietà associativa, potremo scrivere senza ambiguità la composizione di più funzioni come $h \circ g \circ f$, senza l'uso di parentesi.

Non valgono invece per la composizione di funzioni quelle che potremmo chiamare proprietà commutativa e proprietà di cancellazione, come mostrano gli esempi che seguono.

Esempio 3.2.3. *Siano A, B e C insiemi due a due distinti e siano $f \colon A \longrightarrow B$, $g \colon B \longrightarrow C$ e $h \colon B \longrightarrow A$ funzioni. La composizione $g \circ f$ è definita, mentre non lo è la composizione $f \circ g$ poiché il codominio di g e il dominio di f non coincidono.*

Le composizioni $h \circ f$ e $f \circ h$ sono entrambe definite, ma sono funzioni diverse, perché la prima ha dominio A e la seconda ha dominio B.

Esempio 3.2.4. *Siano $f, g\colon \mathbb{N} \longrightarrow \mathbb{N}$ le funzioni date da $f(n) = n^2$ e $g(n) = n + 3$. Le funzioni composte $g \circ f$ e $f \circ g$ sono entrambe definite, sono entrambe funzioni da $\mathbb{N}$ in $\mathbb{N}$, ma sono funzioni diverse poiché ad esempio $(g \circ f)(0) = g(f(0)) = g(0) = 3$, mentre $(f \circ g)(0) = f(g(0)) = f(3) = 9$.*

Esempio 3.2.5. *Sia $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ la funzione $f(n) = n + 1$. Per ogni fissato numero naturale k, consideriamo la funzione $g_k\colon \mathbb{N} \longrightarrow \mathbb{N}$ data da $g_k(m) = m - 1$ se $m > 0$, $g_k(0) = k$. Al variare del numero naturale k, si ottengono tante funzioni g_k diverse (poiché $g_k(0) = k$ varia al variare di k); però le funzioni composte $g_k \circ f$ sono tutte coincidenti, in quanto $g_k \circ f = id_{\mathbb{N}}$ per ogni k. Allora, per $h \neq k$ si ha $g_h \circ f = g_k \circ f$ ma $g_h \neq g_k$.*

D'altra parte se $f_7\colon \mathbb{N} \longrightarrow \mathbb{N}$ è la funzione costante 7, allora per $h \neq k$ si ha $f_7 \circ g_h = f_7 \circ g_k$ ma $g_h \neq g_k$.

I risultati seguenti stabiliscono legami tra le proprietà di una funzione definite nel paragrafo precedente e la composizione.

Proposizione 3.2.6. *Siano $f\colon A \longrightarrow B$ e $g\colon B \longrightarrow C$ due funzioni. Allora:*

i) *$g \circ f$ iniettiva $\Longrightarrow$ f iniettiva;*

ii) *$g \circ f$ suriettiva $\Longrightarrow$ g suriettiva.*

Dim: i) Proviamo che se f non è iniettiva, neppure $g \circ f$ può esserlo.

Supponiamo che a_1, a_2 siano elementi distinti di A tali che $f(a_1) = f(a_2) = b$; allora si ha:

$$(g \circ f)(a_1) = g(f(a_1)) = g(b) = g(f(a_2)) = (g \circ f)(a_2)$$

e quindi $g \circ f$ non è iniettiva.

ii) Supponiamo $g \circ f$ suriettiva; vogliamo provare che $\mathrm{Im}g = C$, ossia che $\forall\, c \in C$ si ha $c \in \mathrm{Im}g$.

Per ipotesi esiste $a \in A$ tale che $(g \circ f)(a) = c$. In tal caso, posto $b = f(a)$, si ha $g(b) = c$, come volevasi. $\diamond$

Dall'iniettività della funzione composta, invece, nulla segue riguardo all'iniettività della seconda funzione e, allo stesso modo, dalla suriettività della funzione composta nulla segue riguardo alla suriettività della prima funzione.

Esempio 3.2.7. *Siano $f\colon \mathbb{N} \longrightarrow \mathbb{Z}$, $g\colon \mathbb{Z} \longrightarrow \mathbb{N}$ le funzioni date rispettivamente da $f(n) = n^2$ e $g(m) = \sqrt{m}$ se $\sqrt{m}$ è un numero intero, $g(m) = 5$ in caso contrario. La funzione composta $g \circ f$ non è altro che la funzione identità $id_{\mathbb{N}}\colon \mathbb{N} \longrightarrow \mathbb{N}$ ed è quindi sia iniettiva sia suriettiva. Però f non è suriettiva, in quanto ad esempio $2 \notin \mathrm{Im}f$ e g non è iniettiva in quanto ad esempio $g(2) = g(3) = 5$.*

I due esempi seguenti mostrano il comportamento di due funzioni importanti rispetto alla composizione.

Esempio 3.2.8. *Siano A, B insiemi, id_A e id_B le rispettive funzioni identità e sia infine $g\colon A \longrightarrow B$ una funzione qualsiasi. Allora si ha $id_B \circ g = g$ ed anche $g \circ id_A = g$.*

Esempio 3.2.9. *Siano A un insieme, a un suo elemento fissato e $f_a\colon A \longrightarrow A$ la corrispondente funzione costante. Se $g\colon A \longrightarrow A$ è una funzione qualsiasi, allora $f_a \circ g = f_a$ e $g \circ f_a = f_{g(a)}$.*

3.3 Funzioni inverse

Definizione 3.3.1. *Si dice* **funzione inversa** *di una funzione $f\colon A \longrightarrow B$ una funzione $g\colon B \longrightarrow A$ tale che valgano le due condizioni $g \circ f = id_A$ e $f \circ g = id_B$.*

Teorema 3.3.2. *Sia $f\colon A \longrightarrow B$ una funzione. Sono equivalenti:*

1) *esiste una funzione g inversa di f;*

2) *f è biunivoca;*

3) *esistono due funzioni h_1, $h_2\colon B \longrightarrow A$ tali che $h_1 \circ f = id_A$ e $f \circ h_2 = id_B$.*

Dim: Per provare l'equivalenza delle condizioni seguiremo lo schema: 1) $\Longrightarrow$ 3) $\Longrightarrow$ 2) $\Longrightarrow$ 1).

Per provare che 1) $\Longrightarrow$ 3) basta scegliere $h_1 = h_2 = g$.

L'implicazione 3) $\Longrightarrow$ 2) segue dalla Proposizione 3.2.6, ricordando che le funzioni identità sono iniettive e suriettive.

Proviamo infine 2) $\Longrightarrow$ 1). Supponiamo f biunivoca e costruiamo esplicitamente la funzione inversa $g\colon B \longrightarrow A$, assegnando l'immagine ad ogni elemento b del dominio. Per ipotesi l'insieme controimmagine di b contiene uno ed un solo elemento a ossia esiste uno ed uno solo $a \in A$ tale che $f(a) = b$. Poniamo allora $g(b) = a$. Per costruzione si ha $(g \circ f)(a) = g(f(a)) = g(b) = a$ per ogni $a \in A$ e $(f \circ g)(b) = f(g(b)) = f(a) = b$ per ogni $b \in B$. $\diamond$

Notiamo che la funzione inversa costruita esplicitamente nella dimostrazione del precedente teorema non è altro che la corrispondenza inversa della funzione $f\colon A \longrightarrow B$ pensata come corrispondenza in $A \times B$. Non sempre la corrispondenza inversa di una funzione risulta essere a sua volta una funzione; il teorema precedente mostra che ciò accade se e soltanto se f è biunivoca.

Di solito la funzione inversa di f (naturalmente se esiste) viene denotata col simbolo f^{-1}.

NOTA BENE Con la notazione ora introdotta l'immagine di un elemento $b \in B$ mediante la funzione f^{-1} si scriverà, seguendo la notazione generale, $f^{-1}(b)$. Purtroppo questo stesso simbolo è stato usato anche per denotare l'insieme controimmagine di b rispetto alla funzione f e la notazione risulta quindi ambigua.
Per evitare pasticci si tenga sempre presente che:
- l'insieme controimmagine $f^{-1}(b)$ esiste sempre, mentre non sempre esiste la funzione inversa: in mancanza di indicazioni esplicite, è sempre meglio interpretare $f^{-1}(b)$ come insieme controimmagine;
- in caso la funzione inversa esista, ossia quando f è biunivoca, avremo $f^{-1}(b) = \{a\}$, se interpretiamo il simbolo come insieme controimmagine di b rispetto alla funzione f, e $f^{-1}(b) = a$ se interpretiamo il simbolo come immagine di b rispetto alla funzione inversa f^{-1}.

Osservazione 3.3.3. *Risulta chiaro dalla dimostrazione del teorema precedente, che* **la funzione inversa, se esiste, è unica**. *In particolare si può notare che se esistono due funzioni h_1 e h_2 come nella condizione 3) del teorema, allora tali funzioni conincidono tra loro e sono proprio la funzione inversa f^{-1}. Si ha infatti*

$$h_1 = h_1 \circ id_B = h_1 \circ (f \circ h_2) = (h_1 \circ f) \circ h_2 = id_A \circ h_2 = h_2.$$

Osservazione 3.3.4. *Per poter affermare che una funzione $f\colon A \longrightarrow B$ ammette l'inversa, non è sufficiente provare che vi è una funzione $h_1\colon B \longrightarrow A$ tale che $h_1 \circ f = id_A$ (oppure una funzione $h_2\colon B \longrightarrow A$ tale che $f \circ h_2 = id_B$). Si veda a questo proposito la funzione $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ dell'Esempio 3.2.5: f non ammette inversa in quanto non è suriettiva, ma ci sono addirittura infinite funzioni g_k che soddisfano la condizione $g_k \circ f = id_{\mathbb{N}}$. Oppure si vedano le funzioni f e g dell'Esempio 3.2.7: g non ammette inversa perché non è iniettiva, ma si ha $g \circ f = id_{\mathbb{N}}$.*

Concludiamo con una proprietà che ci sarà utile in seguito.

Proposizione 3.3.5. *Sia $g\colon B \longrightarrow C$ una applicazione. Prese comunque due applicazioni biunivoche $f\colon A \longrightarrow B$ e $h\colon C \longrightarrow D$, le seguenti affermazioni sono equivalenti:*

i) *g è iniettiva (risp. suriettiva, biunivoca);*

ii) *$g \circ f$ è iniettiva (risp. suriettiva, biunivoca);*

iii) *$h \circ g$ è iniettiva (risp. suriettiva, biunivoca);*

iv) *$h \circ g \circ f$ è iniettiva (risp. suriettiva, biunivoca).*

Dim: Osserviamo innanzi tutto che sarà sufficiente provare l'equivalenza per quel che riguarda l'iniettività e la suriettività.

Per l'iniettività ricordiamo che $iii) \implies i)$ segue dalla Proposizione 3.2.6 e l'implicazione inversa $i) \implies iii)$ segue dalla precedente osservando che esiste h^{-1} e si ha $g = h^{-1} \circ (h \circ g)$.

Proviamo ora direttamente $ii) \implies i)$.

Siano b_1, b_2 elementi distinti di B. Per ipotesi f è biunivoca, quindi esistono e sono unici a_1 e a_2 in A tali che $f(a_1) = b_1$ e $f(a_2) = b_2$ con $a_1 \neq a_2$. Allora per l'iniettività di $g \circ f$ si ha

$$g(b_1) = g(f(a_1)) = (g \circ f)(a_1) \neq (g \circ f)(a_2) = g(f(a_2)) = g(b_2)$$

ossia g è iniettiva.

L'implicazione inversa $i) \implies ii)$ segue dalla precedente osservando che esiste f^{-1} e si ha $g = (g \circ f) \circ f^{-1}$.

Infine usando in sequenza le due equivalenze già provate si ottiene $i) \iff iv)$.

La verifica per la suriettività è analoga ed è lasciata come esercizio al lettore. $\diamond$

3.4 Esercizi

Nel seguito $\mathbb{Z}_2$ indica il quoziente di $\mathbb{Z}$ rispetto alla relazione di equivalenza $n \,\rho\, m$ se $n - m$ è pari.

3.1. Si consideri la corrispondenza in $\mathbb{Z}_2 \times \mathbb{Z}$ costituita dalle coppie $([n], n)$ per ogni $n \in \mathbb{Z}$. Si tratta del grafico di una funzione $\mathbb{Z}_2 \to \mathbb{Z}$? La corrispondenza inversa è il grafico di una funzione $\mathbb{Z} \to \mathbb{Z}_2$?

3.2. Perché $f([n]) = 3n + 1$ non definisce una funzione $f\colon \mathbb{Z}_2 \to \mathbb{Z}$? È vero che $g([n]) = [3n + 1]$ definisce una funzione di $\mathbb{Z}_2$ in se stesso?

3.3. Verificare che $f(n) = [n]$ definisce una funzione $f\colon \mathbb{Z} \to \mathbb{Z}_2$. Determinare l'immagine dell'elemento 7, l'immagine dell'elemento 8, l'immagine di f, l'immagine dell'insieme $\{-2, -1, 0, 1\}$, la controimmagine di $[7]$ e la controimmagine dell'insieme $\{[7], [-1]\}$.

3.4. Dire se le seguenti operazioni in $\mathbb{Z}_2$ sono ben definite:

a. $[n] * [m] = [n + m^2]$;

b. $[n] * [m] = [nm]$;

c. $[n] * [m] = [n]$;

d. $[n] * [m] = [n^m]$;

e. $[n] * [m] = [k]$ dove k è il minore tra n e m.

3.5. Sia X il quoziente di $\mathbb{R}$ rispetto alla relazione di equivalenza $x \,\rho\, y$ se $x - y \in \mathbb{Z}$.

Dire se le seguenti operazioni in X sono ben definite:

a. $[a] * [b] = [a + b]$;

b. $[a] * [b] = [ab]$;

c. $[a] * [b] = [2a - b]$.

3.6. Si determini in ciascun caso la terna (A, B, Γ) che definisce le funzioni presentate negli esempi **a., b., c., d.** del primo paragrafo di questo capitolo.

3.7. Sia $f\colon \mathbb{Z} \to \mathbb{Z}$ data da $f(n) = n^2 - 3n + 5$. Determinare $f(0)$, $f^{-1}(5)$, $f^{-1}(0)$. Si tratta di una applicazione iniettiva? Si tratta di una applicazione suriettiva?

3.8. Sia $f\colon \mathbb{Z} \to \mathbb{Z}$ data da $f(n) = 2n^2 - 3n + 5$. Determinare $f(0)$, $f^{-1}(5)$, $f^{-1}(0)$. Si tratta di una applicazione suriettiva? Si tratta di una applicazione iniettiva?

3.9. Sia $f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ la funzione data da $f((n, m)) = \min\{m, n\}$.

- **a.** Determinare l'immagine dei sottoinsiemi $\mathbb{N} \times \{0\}$ e $\{0\} \times \mathbb{N}$.
- **b.** Determinare gli insiemi controimmagine $f^{-1}(n)$ per $n = 4$ e poi per un n generico.
- **c.** Dire se f è iniettiva, suriettiva, biunivoca.

3.10. Sia $f\colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ la funzione data da $f((n, m)) = m^2 + n$.

- **a.** Determinare $\mathrm{Im} f$ e l'immagine dei sottoinsiemi $\mathbb{Z} \times \{0\}$ e $\{0\} \times \mathbb{Z}$.
- **b.** Determinare gli insiemi controimmagine $f^{-1}(4)$ e $f^{-1}(\mathbb{Z}_-)$, dove $\mathbb{Z}_-$ è l'insieme dei numeri interi strettamente negativi.
- **c.** Dire se f è iniettiva, suriettiva, biunivoca.

3.11. Sia $f\colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ l'applicazione data da: $f((x, y)) = (y, 2)$ se x è dispari e $f((x, y)) = (y, x)$ se x è pari.

- **a.** Dire se f è iniettiva, suriettiva, biunivoca.
- **b.** Determinare $f^{-1}((1, 1))$, $f^{-1}((1, 2))$, $f^{-1}((11, 12))$, $f^{-1}((4, 6))$, $f^{-1}((4, 7))$.
- **c.** Determinare $f(2\mathbb{Z} \times 2\mathbb{Z})$ e $f^{-1}(2\mathbb{Z} \times 2\mathbb{Z})$, dove $2\mathbb{Z}$ è l'insieme dei numeri interi pari.

3.12. Determinare tutte le applicazioni $f\colon A \to B$ dove $A = \{1, 2, 3\}$ e $B = \{\alpha, \beta\}$. Quante sono quelle suriettive? Quante sono quelle iniettive?

3.13. Esiste una applicazione $f\colon \mathbb{R} \to \mathbb{R}$ tale che $f(\{1, 2\}) = \{1, \sqrt{2}, \pi\}$? Esiste una applicazione $g\colon \mathbb{R} \to \mathbb{R}$ tale che $g(\{1, \sqrt{2}, \pi\}) = \{1, 2\}$? (motivare le risposte; in caso affermativo esibire un esempio.)

3.14. La successione di **Fibonacci** è la funzione $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ data da $f(0) = 1$, $f(1) = 1$ e $f(n + 1) = f(n) + f(n - 1)$ per ogni $n \geq 2$. Determinare le immagini dei primi 6 numeri naturali. Si tratta di una funzione suriettiva? iniettiva?

3.15. Determinare l'immagine della funzione $\phi\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ data da $\phi((m, n)) = mn$. Vi sono elementi del codominio la cui controimmagine sia un singleton? Trovare tutti gli elementi di $\phi^{-1}(p)$, per ogni numero primo p.

3.16. Provare che la funzione $\phi\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ data da $\phi((x, y)) = (x + y, x - y)$ è biunivoca e determinare la sua inversa.

3.17. Siano A un insieme, B un suo sottoinsieme, $X = \mathcal{P}(A)$ e $\phi\colon X \longrightarrow X$ l'applicazione data da $\phi(C) = C \cap B$. Dire se ϕ è iniettiva, suriettiva, biunivoca e determinare $\mathrm{Im}(\phi)$.

Rispondere alle stesse domande relativamente a $\psi\colon X \longrightarrow X$ data da $\psi(C) = C \cup B$.

3.18. Siano X, Y e Z insiemi e $f\colon X \to Y$, $g\colon Y \to Z$ delle applicazioni.
Si determini la composizione $g \circ f\colon X \to Z$ in ciascuno dei casi seguenti:

a. $X = Y = Z = \mathbb{R}$, $f(x) = x^2 + 1$ e $g(x) = (x-1)^2$.

b. $X = Z = \mathbb{R}$, $Y = \mathbb{R}_+$, $f(x) = x^2$, $g(x) = \sqrt{x}$.

c. $X = \mathbb{R} \setminus \{0\}$, $Y = \mathbb{R}$, $Z = \mathbb{Z}$, $f(x) = x/|x|$ e $g(x) =$ il più piccolo numero pari $\geq x$.

3.19. Sia $f\colon \mathbb{N} \to \mathbb{N}$ l'applicazione definita da $f(n) = n^2$.
Provare che non esiste una applicazione $g\colon \mathbb{N} \to \mathbb{N}$ tale che $f \circ g = id_{\mathbb{N}}$. Costruire due diverse applicazioni $h\colon \mathbb{N} \to \mathbb{N}$ tali che $h \circ f = id_{\mathbb{N}}$.

3.20. Sia $f\colon \mathbb{Z} \to \mathbb{N}$ l'applicazione definita da $f(n) = n^2 - n$ se $n > 0$ e $f(n) = -n + 1$ se $n \leq 0$. Provare che non esiste una applicazione $g\colon \mathbb{N} \to \mathbb{Z}$ tale che $g \circ f = id_{\mathbb{Z}}$. Costruire due diverse applicazioni $h\colon \mathbb{N} \to \mathbb{Z}$ tali che $f \circ h = id_{\mathbb{N}}$.

3.21. Sia $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ l'applicazione data da $f(n) = 4n+1$ se n è pari e $f(n) = 3n-2$ se n è dispari. Dire se si tratta di una applicazione iniettiva, suriettiva, biunivoca. Determinare esplicitamente gli insiemi controimmagine di 0, 1, -3.

3.22*. Siano X e Y insiemi arbitrari (non vuoti) ed $f\colon X \to Y$ una data funzione. Definiamo in X una relazione ρ secondo la regola: $x \rho x' \Leftrightarrow f(x) = f(x')$. Dimostrare che ρ è una relazione di equivalenza e che la funzione $\phi([x]) = f(x)$ definisce una biiezione tra l'insieme quoziente X/ρ e l'immagine di f.

3.23. Sia $f\colon \mathbb{Z} \to \mathbb{N}$ l'applicazione definita da $f(n) = n^4$. Costruire esplicitamente il quoziente di $\mathbb{Z}$ e l'applicazione ϕ come nell'esercizio precedente.

3.24. Siano $f\colon A \longrightarrow B$ e $g\colon B \longrightarrow C$ due funzioni biunivoche. Verificare che anche la funzione inversa f^{-1} e la funzione composta $g \circ f$ sono funzioni biunivoche.

3.25. Trovare un esempio di insieme A e applicazione $f\colon A \longrightarrow A$ tali che $f \circ f = f$ (che non sia id_A).

3.26. Sia $f = (A, B, \Gamma)$ una funzione e siano π_1 e π_2 le proiezioni sui fattori del prodotto cartesiano $A \times B$. Provare che $\pi_1(\Gamma) = A$ e $\pi_2(\Gamma) = \mathrm{Im} f$.

3.27. Sia $f\colon \mathbb{R} \to \mathbb{R}$ ciascuna delle funzioni date da:

$$1)\ x^2 \quad , \quad 2)\ e^x \quad , \quad 3)\ sen(x) \quad , \quad 4)\ cos(x) \quad , \quad 5)\ arctan(x).$$

Dire se si tratta di una funzione iniettiva, suriettiva, biunivoca.
Esiste la funzione inversa?
Quali modifiche bisogna introdurre affinche la funzione $g(x)$ data rispettivamente da:

$$1)\ \sqrt{(x)} \quad , \quad 2)\ ln(x) \quad , \quad 3)\ arcsen(x) \quad , \quad 4)\ arccos(x) \quad , \quad 5)\ tan(x).$$

sia l'inversa di f.
Calcolare $g(f(-32))$.

Capitolo 4

Numeri naturali e Cardinalità

4.1 L'insieme dei numeri naturali $\mathbb{N}$ e l'induzione

L'insieme dei numeri naturali $\mathbb{N}$ è l'unico insieme numerico di cui ci occuperemo che risulta essere ben ordinato rispetto alla relazione d'ordine $\leq$. L'insieme $\mathbb{N}$ non può essere costruito a partire dagli assiomi della teoria degli insiemi, ma deve essere "postulato" e di tale postulazione l'essere ben ordinato è una delle richieste fondamentali. Inltre $\mathbb{N}$ è il "primo" insieme **infinito** che incontriamo; ogni altra costruzione di insieme infinito partirà direttamente o indirettamente da $\mathbb{N}$. Vogliamo sottolineare che nessun insieme infinito può essere costruito a partire dalla teoria degli insiemi, ma almeno uno di essi deve essere postulato con un nuovo salto concettuale.

Assiomi di Peano. L'insieme dei numeri naturali $\mathbb{N}$ è un insieme non vuoto dotato di una funzione $\sigma\colon \mathbb{N} \to \mathbb{N}$ (detta successore) che gode delle seguenti proprietà:

i) esiste un elemento in $\mathbb{N}$, denotato 0, tale che $Im\,\sigma = \mathbb{N} \setminus \{0\}$;

ii) σ è iniettiva;

iii) **Principio di induzione:** se U è un sottoinsieme di $\mathbb{N}$ tale che

1) $0 \in U$ (base dell'induzione o passo iniziale)

2) $n \in U \implies \sigma(n) \in U$ ossia $\sigma(U) \subseteq U$ (passo induttivo)

allora $U = \mathbb{N}$.

Non intendiamo approfondire la definizione assiomatica di $\mathbb{N}$; diciamo soltanto che a partire dagli assiomi si può costruire in modo formalmente perfetto tutto ciò che sappiamo su $\mathbb{N}$, come le operazioni di somma e prodotto e le loro proprietà. Ad esempio $n + 0 = n$ e $n + \sigma(0) = \sigma(n)$ ecc. In tal modo, come suggerisce il nome stesso, il "successore" di un numero naturale n ossia il numero n' tale che $\sigma(n) = n'$, non è altro che $n + 1$: d'ora in

poi scriveremo appunto $n+1$ invece che $\sigma(n)$.

Un'altra definizione assiomatica di $\mathbb{N}$ (del tutto equivalente a questa) si ottiene sostituendo la condizione iii) con la condizione:

iii') $\mathbb{N}$ è dotato di un buon ordinamento $\leq$ tale che $n \leq \sigma(n)$ per ogni elemento $n \in \mathbb{N}$.

Proviamo solo una parte dell'equivalenza tra i due sistemi di assiomi.

Proposizione 4.1.1. *Se $\mathbb{N}$ è un insieme che soddisfa i), ii), iii'), allora $\mathbb{N}$ soddisfa anche iii).*

Dim: Sia U un sottoinsieme di $\mathbb{N}$ che soddisfa le condizioni 1) e 2) del principio di induzione. Procediamo **per assurdo**. Supponiamo $U \neq \mathbb{N}$ e proviamo che ne discende una contraddizione.

Poniamo $V = \mathcal{C}_{\mathbb{N}}(U)$; per ipotesi $V \neq \emptyset$ e quindi, in virtù del buon ordinamento (assioma iii')) di $\mathbb{N}$, V ammette minimo che indicheremo con m.

Non può essere $m = 0$ in quanto $0 \in U$ e quindi $0 \notin V$.

Allora (assioma i)) esiste $k \in \mathbb{N}$ tale che $m = \sigma(k)$. Poiché k è minore di m che è il minimo di V, allora $k \notin V$ ossia $k \in U$. In virtù delle ipotesi fatte su U, se $k \in U$ allora anche $\sigma(k) = m \in U$ e quindi $m \notin V$: ciò non è, però, possibile perché m, essendo il minimo di V, sta in V. $\diamond$

Una delle principali applicazioni di tale principio è la **dimostrazione per induzione**.
Sia $P(n)$ una proprietà relativa ad un generico numero naturale n e sia $U = \{n \in \mathbb{N} \mid$ la proprietà $P(n)$ è vera
Se valgono le due condizioni seguenti:
1) $0 \in U$ (base dell'induzione)
2) $n \in U \implies n+1 \in U$ (passo induttivo)
allora per il principio di induzione $U = \mathbb{N}$, ossia la proprietà è vera per tutti gli $n \in \mathbb{N}$.

Esempio 4.1.2. *Sia X un insieme con n elementi. Proviamo mediante l'induzione che $\mathcal{P}(X)$ ha 2^n elementi.*

Dim: Passo iniziale: se X ha 0 elementi, ossia se $X = \emptyset$, allora $\mathcal{P}(X) = \{\emptyset\}$ ha $1 = 2^0$ elementi.

Passo induttivo: supponiamo che l'asserto sia vero per gli insiemi che hanno $n-1$ elementi e proviamolo per X, che ha $n > 0$ elementi.

Fissato un elemento $x_0 \in X$, abbiamo $X = Y \cup \{x_0\}$ dove $Y = X \setminus \{x_0\}$ è un insieme con $n-1$ elementi. Possiamo suddividere i sottoinsiemi di X tra quelli che non contengono x_0 e quelli che lo contengono: quelli del primo tipo sono tutti i sottoinsiemi di Y e quindi il loro numero è, grazie all'ipotesi induttiva, 2^{n-1}; quelli del secondo tipo si ottengono aggiungendo x_0 a ciascun insieme del primo tipo. Otteniamo così l'unione disgiunta:

$$\mathcal{P}(X) = \mathcal{P}(Y) \cup \{A \cup \{x_0\} \mid A \in \mathcal{P}(Y)\}.$$

Allora $\mathcal{P}(X)$ ha $2^{n-1} + 2^{n-1} = 2^n$ elementi. $\diamond$

Alcune varianti (equivalenti) dell'induzione:

I. Se valgono le condizioni:
1') $k_0 \in U$
2) $n \in U \implies n+1 \in U$
allora la proprietà $P(n)$ è vera $\forall n \geq k_0$.

II. (Detta: forma forte dell'induzione) Se valgono le due condizioni:
1') $k_0 \in U$
2') $(k \in U \ \ \forall k \ \text{ t.c. } \ k_0 \leq k \leq n) \implies n+1 \in U$
allora la proprietà $P(n)$ è vera $\forall n \geq k_0$.

Esempio 4.1.3. *Proviamo che per ogni numero naturale strettamente positivo n si ha*

$$1 + \cdots + n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Passo iniziale $n = 1$: la formula vale poiché $1 = \frac{1(1+1)}{2}$.
Passo induttivo: supposta vera la formula per un certo numero $n \geq 1$, proviamo che vale anche per il successivo $n+1$. Si ha:

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

Esempio 4.1.4. *Proviamo che in $\mathbb{N}$ esiste la* **divisione con resto** *ossia che presi due qualsiasi numeri $a, b \in \mathbb{N}$, $b \neq 0$, esistono $q \in \mathbb{N}$ (quoziente) ed $r \in \mathbb{N}$ (resto) tali che $a = bq + r$ e $r < b$.*

Dim: Procediamo per induzione sul dividendo a.
Passo iniziale: $a = 0$: l'asserto vale ponendo $q = r = 0$.
Passo induttivo: supponiamo l'asserto vero per ogni coppia di numeri naturali (a', b') con $a' < a$ e proviamo che vale anche per la coppia (a, b).
Se $a < b$, allora l'asserto vale ponendo $q = 0$ e $r = a$.
Se $a \geq b$, grazie all'ipotesi induttiva sappiamo che l'asserto vale per la coppia $(a-b, b)$ e che quindi esistono q' ed $r' < b$ tali che $a - b = bq' + r'$. L'asserto vale allora ponendo $q = q' + 1$ e $r = r'$. $\diamond$

Una successione si dice **definita ricorsivamente** se sono assegnate le immagini di alcuni numeri iniziali $f(0), f(1), \ldots, f(r)$ e poi l'immagine di un generico numero $n > r$ è data mediante una formula che coinvolge $f(n-1)$, o, più genericamente, $f(0), f(1), \ldots, f(n-1)$. È proprio grazie al principio di induzione che la ricorsione definisce una successione, ossia una funzione il cui dominio è tutto $\mathbb{N}$.

Esempio 4.1.5. *Siano a, b e k numeri reali qualsiasi. Si dice* **successione aritmetica** *o lineare la successione definita ricorsivamente da $a_0 = a$ e, per ogni $n \geq 1$, $a_{n+1} = a_n + k$. Si dice* **successione geometrica** *o esponenziale la successione definita ricorsivamente da $b_0 = b$ e, per ogni $n \geq 1$, $b_{n+1} = b_n k$.*

Esempio 4.1.6. *La* **successione di Fibonacci** *è la successione definita ricorsivamente da $f_0 = 1$, $f_1 = 1$ e per ogni $n \geq 2$, $f_{n+1} = f_{n-1} + f_n$.*

4.2 La cardinalità di un insieme

Come applicazione delle cose viste riguardo alle funzioni vogliamo ora definire in modo rigoroso il "numero di elementi" di un insieme, anche nel caso in cui l'insieme sia "infinito". Prima di poter fare ciò, è necessario precisare cosa intendiamo dicendo che un insieme è finito oppure che è infinito.

Definizione 4.2.1. *Si dice che due insiemi A e B sono* **equipollenti** *oppure hanno la stessa* **cardinalità** *se esiste una funzione biunivoca $f\colon A \longrightarrow B$.*

Consideriamo un insieme X i cui elementi sono insiemi. La relazione di equipollenza in X è una equivalenza. La classe di equivalenza di un insieme A si indica con $Card(A)$.

Intuitivamente possiamo dire che $Card(A) = Card(B)$ se A ha tanti elementi quanti B. Vogliamo ora mettere a confronto tra loro le cardinalità, per poter dire anche se un insieme ha più elementi (oppure ha meno elementi) di un altro. Molti dei risultati che useremo (contrassegnati con un asterisco) saranno soltanto enunciati, poiché una loro dimostrazione rigorosa richiede nozioni e tecniche non elementari (come ad esempio l'assioma della scelta).

Lemma* 4.2.2. *Siano A e B insiemi. Allora:*

esiste una funzione iniettiva $i\colon A \longrightarrow B \iff$ esiste una funzione suriettiva $p\colon B \longrightarrow A$.

Definizione 4.2.3. *Dati due insiemi A e B, diciamo che A* **ha cardinalità minore o uguale di** *B se esiste una applicazione iniettiva $i\colon A \longrightarrow B$ oppure (equivalentemente) se esiste una applicazione suriettiva $p\colon B \longrightarrow A$. In tal caso scriveremo $Card(A) \leq Card(B)$.*

Teorema* 4.2.4. *Siano A e B insiemi. Allora:*

$$Card(A) = Card(B) \iff Card(A) \leq Card(B) \text{ e } Card(B) \leq Card(A).$$

Definizione 4.2.5. *Un insieme A si dice* **finito** *se per ogni funzione $f\colon A \longrightarrow A$ si ha:*

$$f \text{ è iniettiva} \iff f \text{ è biunivoca} \iff f \text{ è suriettiva.}$$

A si dice **infinito** *in caso contrario, ossia se esiste una funzione $f\colon A \longrightarrow A$ iniettiva ma non suriettiva, oppure suriettiva ma non iniettiva.*

Possiamo riformulare tali definizioni dicendo che un insieme è infinito se è equipollente ad un suo sottoinsieme proprio ed è finito se questo non capita.

Esempio 4.2.6. *L'insieme dei numeri naturali $\mathbb{N}$ è un insieme infinito poiché la funzione "successore" $\sigma\colon \mathbb{N} \longrightarrow \mathbb{N}$, $\sigma(n) = n+1$ è iniettiva ma non suriettiva (Assiomi di Peano).*

Possiamo anche vedere che la funzione "doppio" $f\colon \mathbb{N} \longrightarrow P$ ($P = \{$numeri naturali pari$\}$) data da $f(n) = 2n$, è biunivoca e quindi $Card(\mathbb{N}) = Card(P)$, anche se P è un sottoinsieme proprio di $\mathbb{N}$.

Nel seguito del capitolo indicheremo con I_n ($n \geq 1$) l'insieme dei numeri naturali $\{1, \ldots, n\}$.

Il risultato seguente, tutt'altro che evidente come potrebbe sembrare a prima vista, è conosciuto come **principio dei cassetti** o **principio della piccionaia**.

Lemma 4.2.7. *1) Se $n \leq m$ allora $Card(I_n) \leq Card(I_m)$;*

2) $Card(I_n) = Card(I_m)$ se e solo se $n = m$.

Dim: 1) La funzione $f\colon I_n \longrightarrow I_m$ data da $f(i) = i$ per ogni $i \in I_n$ è iniettiva.

2) Proviamo solo l'implicazione non banale $Card(I_n) = Card(I_m) \Longrightarrow n = m$.

Sia A l'insieme dei numeri naturali m per cui questa implicazione è falsa per un qualche $n \in \mathbb{N}$. Vogliamo provare che A è vuoto, ossia che la proprietà è vera per tutti i numeri naturali ≥ 1.

Supponiamo (per assurdo) $A \neq \emptyset$; allora, in virtù del buon ordinamento di $\mathbb{N}$, esiste il minimo di A che indichiamo con m_0. Poiché $m_0 \in A$, esiste un numero $n \neq m_0$ tale che $Card(I_{m_0}) = Card(I_n)$: sia quindi $f\colon I_n \longrightarrow I_{m_0}$ una funzione biunivoca.

Il minimo m_0 non può essere 1, poiché l'unica applicazione $f\colon I_n \longrightarrow I_1$ è l'applicazione costante 1; se $n \neq 1$, allora $1, 2 \in I_n$ e quindi f non è iniettiva poiché $f(1) = f(2) = 1$.

Supponiamo allora $m_0 \neq 1$: in tal caso $m_0 - 1 \neq 0$ ed è definito I_{m_0-1}.

Sia $k = f(n)$ e sia $g\colon I_{m_0} \longrightarrow I_{m_0}$ la funzione biunivoca data da $g(i) = i$ se $i \neq k$ e $i \neq m_0$, $g(k) = m_0$, $g(m_0) = k$. La funzione $h = g \circ f\colon I_n \longrightarrow I_{m_0}$ è biunivoca e tale che $h(n) = m_0$. Mediante h possiamo costruire la funzione biunivoca $h'\colon I_{n-1} \longrightarrow I_{m_0-1}$ data da $h'(i) = h(i)$. Allora $m_0 - 1 \in A$, in contrasto con la minimalità di m_0. $\diamond$

Grazie a questo risultato potremo indicare senza ambiguità la cardinalità di I_n con n. Diremo inoltre che l'insieme vuoto ha cardinalità 0.

Condensiamo nel risultato seguente una serie di altri fatti di non facile dimostrazione.

Teorema* 4.2.8. a. *Per ogni numero $n \in \mathbb{N}$, I_n è un insieme finito.*

b. *Ogni insieme finito A è equipollente ad un I_n oppure è $\emptyset$: quindi $Card(A) \in \mathbb{N}$.*

c. *Se B è infinito, allora $Card(B) > n$ per ogni $n \in \mathbb{N}$: quindi $Card(B) \notin \mathbb{N}$.*

La cardinalità dell'insieme infinito $\mathbb{N}$ non è quindi un numero naturale. $Card(\mathbb{N})$ è detta **cardinalità numerabile** e viene indicata con $\aleph_0$ ($\aleph$ è la lettera ebraica alef). Un insieme equipollente a $\mathbb{N}$ si dice **insieme numerabile**.

Teorema* 4.2.9. *Siano A, B due insiemi.*

a. *Le cardinalità di A e B sono sempre confrontabili, ossia vale sempre $Card(B) \leq Card(A)$ oppure $Card(A) \leq Card(B)$.*

b. *Se A è un insieme infinito, allora $Card(A) \geq \aleph_0$, ossia $\aleph_0$ è il più piccolo cardinale infinito.*

Esempio 4.2.10. *$Card(\mathbb{Z}) = \aleph_0$. Una applicazione biunivoca $f\colon \mathbb{Z} \longrightarrow \mathbb{N}$ è data da $f(n) = 2n$ se $n \geq 0$, $f(n) = -2n - 1$ se $n < 0$.*

Esempio 4.2.11. *$Card(\mathbb{Q}) = \aleph_0$. Non è semplice definire una funzione biunivoca $\mathbb{Z} \longrightarrow \mathbb{Q}$; costruiamone allora una iniettiva e una suriettiva.*
Una funzione iniettiva è, ad esempio, $n \mapsto n$. Costruiamo ora quella suriettiva.
Consideriamo in $\mathbb{N} \times \mathbb{N}^*$ ($\mathbb{N}^* = \mathbb{N} \setminus \{0\}$) la relazione d'ordine totale:

$$(a, b) \leq (c, d) \text{ se } a + b < c + d \text{ oppure se } a + b = c + d \text{ e } a \leq c.$$

Concretamente si ha:

$$(0,1) < (0,2) < (1,1) < \cdots < (0,b) < (1,b-1) < (2,b-2) < \cdots < (b-1,1) < (0,b+1) < \cdots$$

Ogni elemento di $\mathbb{N} \times \mathbb{N}^*$ occupa in questa sequenza una ben precisa posizione che potrebbe essere anche calcolata mediante una formula ricorsiva. Sia allora $f\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ data da $f(n) = \frac{a}{b}$, se $n \geq 0$ e $f(n) = -\frac{a}{b}$, se $n \leq 0$, dove (a, b) è l'elemento che occupa il posto $n + 1$ nella fila. Tale funzione è chiaramente suriettiva, anche se non iniettiva.

Esempio 4.2.12. *$Card(\mathbb{R})$ detta anche* **cardinalità del continuo** *è strettamente maggiore di $\aleph_0 = Card(\mathbb{N})$.*

Come nell'esempio precedente l'applicazione $n \mapsto n$ mostra che $Card(\mathbb{N}) \leq Card(\mathbb{R})$.

Proviamo che non vale l'uguaglianza mostrando che nessuna funzione $f\colon \mathbb{N} \longrightarrow \mathbb{R}$ può essere suriettiva. Identifichiamo ogni numero reale con la sua scrittura posizionale in base 10 e indichiamo con $c_n(x)$ la $n-$esima cifra decimale del numero x.

Costruiamo un numero reale che non appartiene a $\mathrm{Im} f$. Sia y il numero reale con parte intera 0 tale che $c_n(y) = 2$ se $c_n(f(n-1)) \neq 2$ e $c_n(y) = 1$ se $c_n(f(n-1)) = 2$. Tale numero y differisce da ciascun numero reale appartenente a $\mathrm{Im} f$ in almeno una cifra decimale e quindi $y \notin \mathrm{Im} f$.

Esempio 4.2.13. *Sia $\mathcal{P}(A)$ l'insieme delle parti di A. Allora $Card(A) < Card(\mathcal{P}(A))$. La funzione iniettiva $a \mapsto \{a\}$ prova che $Card(A) \leq Card(\mathcal{P}(A))$.*
Proviamo che non vale l'uguaglianza. Supponiamo per assurdo che esista una funzione $f\colon A \longrightarrow \mathcal{P}(A)$ biunivoca e indichiamo con B il sottoinsieme di A degli elementi a tali che $a \notin f(a)$. Essendo f suriettiva, esiste un elemento $a_0 \in A$ tale che $f(a_0) = B$. Si perviene allora alla contraddizione:

$$a_0 \in f(a_0) \Longleftrightarrow a_0 \notin f(a_0).$$

Come conseguenza, si prova l'esistenza di infiniti cardinali infiniti diversi, ad esempio: $Card(\mathbb{N}) < Card(\mathcal{P}(\mathbb{N})) < Card(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \dots$.

4.3 Esercizi

4.1. Provare mediante l'induzione che le seguenti formule valgono per ogni $n \in \mathbb{N}$:

a. $1 + 4 + \cdots + n^2 = \frac{2n^3+3n^2+n}{6}$

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

c. $\left(\frac{1}{3}\right)^0 + \left(\frac{1}{3}\right)^1 + \cdots + \left(\frac{1}{3}\right)^n = \frac{3^{n+1}-1}{2\cdot 3^n}$

4.2. Sia $A = \{n \in \mathbb{N} \mid 1 + 2 + \cdots + n = (n+3)(n-2)/2\}$.

a. Provare che se n appartiene ad A allora anche $n+1$ appartiene ad A.

b. E' vero che $A = \mathbb{N}$?

4.3. Una delle regole del calcolo letterale è la proprietà commutativa del prodotto: $ab = ba$. Provare che allora si ha anche $(ab)^n = a^n b^n$ per ogni esponente intero positivo n.

4.4. Provare che per ogni numero naturale $k \geq 7$ si ha $(k-5)^4 > k$.
Determinare $\{k \in \mathbb{N} \mid (k-5)^4 > k\}$.

4.5*. Si considerino nel piano euclideo n rette generiche (ossia tali che tra esse non ci siano coppie di rette parallele oppure terne di rette passanti per uno stesso punto). Provare che tali rette suddividono il piano in $\frac{n^2+n+2}{2}$ parti.

4.6*. Per ogni coppia di numeri naturali n e m poniamo: $0 + m = m$, $\sigma(n) + m = \sigma(n+m)$.
Provare mediante l'induzione che in questo modo si definisce una operazione $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

4.7*. Per ogni coppia di numeri naturali n e m poniamo: $0m = 0$, $\sigma(n)m = nm + m$.
Provare mediante l'induzione che in questo modo si definisce una operazione $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.
Verificare che per ogni coppia di numeri naturali n, m, $n \neq 0, 1$, $m \neq 0$ si ha $nm > m$.

4.8. Esistono due applicazioni differenti di $\mathbb{N}$ in $\mathbb{N}$ aventi la stessa immagine?

4.9. Indichiamo con $6\mathbb{Z}$ il sottoinsieme di $\mathbb{Z}$ dei multipli interi di 6. Provare che $Card(6\mathbb{Z}) = Card(\mathbb{Z})$.

4.10. Indichiamo con Q il sottoinsieme di $\mathbb{N}$ dei numeri n^2, tali che $n \in \mathbb{N}$. Provare che $Card(Q) = \aleph_0$.

4.11. Sia A un insieme finito con 3 elementi. Provare che $Card(A \times \mathbb{N}) = \aleph_0$. Generalizzare il risultato al caso in cui A abbia k elementi con $k \in \mathbb{N}^*$.

4.12. Siano $(0, 1)$ e $(3, +\infty)$ un intervallo aperto e una semiretta di $\mathbb{R}$. Provare che hanno la stessa cardinalità di $\mathbb{R}$.

4.13. Siano γ e Γ le circonferenze del piano cartesiano con centro l'origine e raggio rispettivamente 1 e 2. Provare che γ e Γ hanno la stessa cardinalità, che è anche la stessa cardinalità della retta reale. È vero che nell'interno di γ vi sono infiniti punti a coordinate razionali?

4.14. In un teatro vi sono 500 persone. Provare che ce ne sono almeno 2 che festeggiano il compleanno lo stesso giorno.
Quante persone bisogna riunire per essere sicuri che almeno tre tra esse festeggino il compleanno lo stesso giorno?

4.15. Provare che in Italia esistono sicuramente due persone che festeggiano il compleanno nello stesso giorno, hanno lo stesso numero di scarpe ed anche la stessa altezza espressa in centimetri. E a Torino?

Capitolo 5

Elementi di calcolo combinatorio

5.1 Permutazioni e disposizioni

Indichiamo con S_X l'insieme di tutte le funzioni biunivoche di un insieme X in sè.
La composizione di funzioni è una operazione in S_X che gode delle seguenti proprietà:

- associativa: $h \circ (g \circ f) = (h \circ g) \circ f$;

- esistenza dell'identità id_X tale che $\forall f \in S_X \ \ (f \circ id_X = id_X \circ f = f)$;

- esistenza dell'inverso: $\forall f \in S_X$, $\exists f^{-1} \in S_X$ tale che $f \circ f^{-1} = f^{-1} \circ f = id_X$.

Un insieme dotato di una operazione che gode di tali proprietà si dice **gruppo**: $(S_X, \circ)$ è dunque un gruppo.

La teoria generale dei gruppi sarà affrontata nel corso di Algebra. Per ora ci limitiamo a contare quanti elementi ha S_X nel caso in cui X è un insieme finito.

Osserviamo intanto che la cardinalità di S_X non dipende dalla natura degli oggetti dell'insieme X, ma solo dalla cardinalità di X. Vale infatti la seguente proprietà:

Proposizione 5.1.1. *Siano A, A', B, B' insiemi tali che $Card(A) = Card(A')$ e $Card(B) = Card(B')$. Vi è allora corrispondenza biunivoca tra gli insiemi $\mathcal{H}$ delle funzioni $h\colon A \longrightarrow B$ e $\mathcal{H}'$ delle funzioni $h'\colon A' \longrightarrow B'$, corrispondenza che trasforma funzioni iniettive (risp. suriettive, biunivoche) in funzioni iniettive (risp. suriettive, biunivoche).*

Dim: Per ipotesi esistono due funzioni biunivoche $f\colon A \longrightarrow A'$ e $g\colon B \longrightarrow B'$. Una corrispondenza tra $\mathcal{H}$ e $\mathcal{H}'$ è data da $h \mapsto g \circ h \circ f^{-1}$; tale corrispondenza è certamente biunivoca, poiché ha come inversa $h' \mapsto g^{-1} \circ h' \circ f$.

L'ultima parte dell'asserto segue immediatamente dalla Proposizione 3.3.5. $\diamond$

In virtù di tale proprietà, nel seguito potremo , senza perdere in generalità, considerare, al posto di un generico insieme X con cardinalità n, l'insieme $I_n = \{1, \ldots, n\}$.

Definizione 5.1.2. *Si dice* **permutazione** *di n elementi ogni applicazione biunivoca di I_n in sè. L'insieme S_n di tutte le permutazioni di I_n (con l'operazione di composizione) si dice* **gruppo delle permutazioni di n elementi** *o* **gruppo simmetrico**.

Ogni elemento di S_n è una funzione biunivoca f di I_n in sè ed è quindi univocamente individuata dalle immagini $(f(1), f(2), \ldots, f(n))$, che costituiscono una $n-$upla ordinata in cui i numeri da 1 a n compaiono tutti una e una sola volta, in un ben preciso ordine. Da ora in poi capiterà spesso di identificare la funzione f con tale $n-$upla ordinata.

Notazione. Sia n un numero naturale ≥ 1. Col simbolo $n!$, che si legge n **fattoriale**, si denota il prodotto di tutti i naturali da 1 fino ad n: $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$. È utile dare significato ad $n!$ anche nel caso $n = 0$ ponendo per convenzione $0! = 1$.

Proposizione 5.1.3. *La cardinalità P_n del gruppo simmetrico S_n è $n!$.*

Dim: Proviamolo per induzione su n.

Se $n = 1$, l'unica permutazione di I_1 è la funzione identità e quindi S_1 ha $1! = 1$ elemento.

Supponiamo la formula vera per un certo n e proviamola per l'intero successivo $n+1$. Per ogni numero naturale j, $1 \leq j \leq n+1$, gli elementi f di S_{n+1} tali che $f(n+1) = j$ sono tanti quanti le applicazioni biunivoche tra I_n e l'insieme $I_{n+1} \setminus \{j\}$ che ha n elementi. In virtù della Proposizione 5.1.1 e dell'ipotesi induttiva, tali applicazioni sono $P_n = n!$ e quindi gli elementi di S_{n+1} sono $P_{n+1} = (n+1) \cdot P_n = (n+1) \cdot n! = (n+1)!$. $\diamond$

Esempio 5.1.4. *L'ordine di arrivo di una gara a cui partecipano* 20 *corridori (escludendo la possibilità di ritiri e di piazzamenti ex-aequo) è una permutazione dei partecipanti. I possibili ordini di arrivo diversi sono allora* 20!.

Intuitivamente possiamo dire che ci sono 20 possibili primi classificati; per ciascuno di questi ci sono 19 possibili secondi classificati (tutti meno il primo classificato), 18 possibili terzi classificati, e così via....

Definizione 5.1.5. *Siano k ed n due interi, $1 \leq k \leq n$, e siano A e B insiemi con cardinalità rispettivamente k ed n. L'insieme delle applicazioni iniettive $f\colon A \longrightarrow B$ si dice insieme delle* **disposizioni (semplici) di n elementi a k a k**.

Come già detto per le permutazioni, possiamo supporre senza perdere in generalità che A sia I_k e B sia I_n. Una disposizione $f\colon I_k \longrightarrow I_n$ è allora univocamente determinata dalla $k-$upla ordinata delle immagini $(f(1), \ldots, f(k))$ che è costituita da numeri compresi tra 1 e n, nessuno dei quali ripetuto.

Proposizione 5.1.6. *L'insieme delle disposizioni di n elementi a k a k ha cardinalità*

$$D_{n,k} = \frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1).$$

Dim: Procediamo per induzione su k.

Se $k = 1$, le applicazioni, tutte iniettive, di I_1 in I_n sono tante quante le possibili immagini dell'unico elemento del dominio, ossia sono $D_{n,1} = n = \frac{n!}{(n-1)!}$.
Se d'altra parte $k = n$, allora $D_{n,n} = P_n = n! = \frac{n!}{0!} = \frac{n!}{(n-n)!}$.

Supponiamo la formula vera per un certo $k < n$ e proviamola per l'intero successivo $k+1$.

Per ogni numero naturale j, $1 \leq j \leq n$, le disposizioni $f\colon I_{k+1} \longrightarrow I_n$ tali che $f(k+1) = j$ sono tante quante le applicazioni iniettive tra I_k e l'insieme $I_n \setminus \{j\}$ che ha $n-1$ elementi. In virtù della Proposizione 5.1.1 e dell'ipotesi induttiva, il numero di tali applicazioni è

$$D_{n-1,k} = \frac{(n-1)!}{(n-1-k)!}.$$

Complessivamente le disposizioni di n elementi a $k+1$ a $k+1$ sono:

$$D_{n,k+1} = n \cdot D_{n-1,k} = n \cdot \frac{(n-1)!}{(n-k-1)!} = \frac{n!}{(n-k-1)!} = n(n-1)\cdots(n-k).$$

$\diamond$

Esempio 5.1.7. *In una gara a cui partecipano* 20 *corridori (escludendo la possibilità di ritiri e di piazzamenti ex-aequo) i vincitori delle medaglie formano una terna ordinata di corridori. I possibili "podi" diversi sono tanti quante le disposizioni di* 20 *elementi a* 3 *a* 3*, ossia* $20 \cdot 19 \cdot 18$.

Intuitivamente possiamo dire che ci sono 20 possibili primi classificati, per ciascuno 19 possibili secondi classificati e 19 possibili terzi classificati.

Definizione 5.1.8. *Siano k ed n due interi ≥ 1 e siano A e B insiemi con cardinalità rispettivamente k ed n. L'insieme di tutte le applicazioni $f\colon A \longrightarrow B$ si dice insieme delle* **disposizioni con ripetizione di n elementi a k a k.**

Posto $A = I_k$ e $B = I_n$, una disposizione con ripetizione $f\colon I_k \longrightarrow I_n$ è univocamente determinata dalla $k-$upla ordinata delle immagini $(f(1), \ldots, f(k))$ che è costituita da numeri compresi tra 1 e n, eventualmente anche ripetuti.

Proposizione 5.1.9. *L'insieme delle disposizioni con ripetizione di n elementi a k a k ha cardinalità $D^r_{n,k} = n^k$.*

Dim: Proviamolo per induzione su k.

Se $k = 1$, le applicazioni di I_1 in I_n sono tante quante le possibili immagini dell'unico elemento del dominio, ossia sono $D^r_{n,1} = n = n^1$.

Supponiamo la formula vera per un certo k e proviamola per l'intero successivo $k+1$. Per ogni numero naturale j, $1 \leq j \leq n$, le disposizioni con ripetizione $f\colon I_{k+1} \longrightarrow I_n$ tali che $f(k+1) = j$ sono tante quante le applicazioni di I_k nell'insieme I_n.
Si ha allora $D^r_{n,k+1} = n \cdot D^r_{n,k} = n \cdot n^k = n^{k+1}$. $\diamond$

Esempio 5.1.10. *Le schedine del totocalcio sono sequenze in cui compaiono i simboli* $1, 2, X$ *in file ordinate di* 13*, ossia sono disposizioni con ripetizione di* 3 *elementi a* 13 *a* 13*. Il numero totale di tutte le possibili schedine è allora* $D^r_{3,13} = 3^{13}$*.*

Ci sono infatti 3 possibili risultati della prima partita; per ciascuno di essi ci sono 3 possibili risultati per la seconda partita, e così via per 13 volte.

Esempio 5.1.11. *Sia A un insieme con k elementi. Ogni sottoinsieme B di A è univocamente individuato da una funzione (la sua* **funzione caratteristica***) $f_B\colon A \longrightarrow \{0,1\}$ tale che $f_B(a) = 0$ se $a \notin B$ e $f_B(a) = 1$ se $a \in B$. Allora $\mathcal{P}(A)$ ha tanti elementi quante sono le applicazioni di A in $\{0,1\}$ e quindi $Card(\mathcal{P}(A)) = D^r_{2,k} = 2^k$.*

5.2 Combinazioni e binomiali

Definizione 5.2.1. *Siano k ed n due interi, $0 \leq k \leq n$, e sia A un insieme con cardinalità n (possiamo supporre, senza perdita di generalità, $A = I_n$). Le* **combinazioni (semplici) di n elementi a k a k** *sono tutti i possibili sottoinsiemi di A aventi esattamenti k elementi.*

Definizione 5.2.2. *Siano k ed n due interi, $0 \leq k \leq n$. Si dice* **binomiale n su k** *e si denota col simbolo $\binom{n}{k}$ il numero $\frac{n!}{k!\cdot(n-k)!}$.*

Proposizione 5.2.3. *L'insieme delle combinazioni di n elementi a k a k ha cardinalità*

$$C_{n,k} = \binom{n}{k}.$$

Dim: Osserviamo innanzi tutto che la formula vale se $k = 0$. Supponiamo allora $k \geq 1$.

Fissiamo un sottoinsieme B di I_n e consideriamo nell'insieme delle applicazioni iniettive da I_k in I_n quelle che hanno B come insieme immagine: il loro numero è pari al numero delle applicazioni biunivoche tra I_k e B ossia P_k. Al variare di B tra tutti i possibili sottoinsiemi di I_n con k elementi otteniamo il numero totale delle applicazioni iniettive di I_k in I_n. Avremo allora: $P_k \cdot C_{n,k} = D_{n,k}$. Sostituendo i valori già noti di P_k e $D_{n,k}$ si ricava $C_{n,k} = \binom{n}{k}$. $\diamond$

Esempio 5.2.4. *In una lotteria vengono assegnati* 3 *premi uguali per estrazione a sorte tra i* 20 *partecipanti. Il terzetto di vincitori è un insieme di* 3 *persone sorteggiate, che non tiene conto dell'eventuale ordine di estrazione. I possibili terzetti di vincitori sono allora tanti quante le possibili scelte di* 3 *elementi in un insieme di* 20*, ossia sono* $C_{20,3} = \binom{20}{3}$.

Esempio 5.2.5. *Vogliamo calcolare in quanti modi diversi si può scegliere una terna di numeri* (a, b, c) *compresi tra* 1 *e* 100 *ordinati in ordine crescente* $a < b < c$*. Osserviamo che ogni insieme di* 3 *numeri corrisponde ad una sola possibile terna e non a varie terne differenti a seconda dell'ordine; stiamo cioè considerando combinazioni (e non disposizioni) di elementi di* I_{100} *presi a* 3 *a* 3*. Allora le terne siffatte sono in numero di* $C_{100,3} = \binom{100}{3}$.

Corollario 5.2.6. *Se* k *ed* n *sono numeri interi,* $0 \leq k \leq n$*, allora* $\binom{n}{k}$ *è un numero intero.*

Dim: $\binom{n}{k}$ è definito come numero razionale, ma risulta essere un intero, poiché è la cardinalità di un insieme finito. ◇

Vediamo ora alcune proprietà dei binomiali.

Proposizione 5.2.7. *Siano* k *ed* n *numeri interi,* $0 \leq k \leq n$*. Allora:*

1) $$\binom{n}{k} = \binom{n}{n-k},$$

2) $$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Dim: Entrambe le proprietà si possono facilmente verificare mediante conti algebrici diretti. Preferiamo però darne una diversa dimostrazione mediante le proprietà degli insiemi.

1) Sia A un insieme con n elementi. $C_{n,k} = \binom{n}{k}$ e $C_{n,n-k} = \binom{n}{n-k}$ sono rispettivamente la cardinalità di $\mathcal{P}_k = \{B \subseteq A \mid B \text{ ha } k \text{ elementi}\}$ e di $\mathcal{P}_{n-k} = \{C \subseteq A \mid C \text{ ha } n-k \text{ elementi}\}$.

   L'applicazione $B \mapsto \mathcal{C}_A(B)$ stabilisce una corrispondenza biunivoca tra $\mathcal{P}_k$ e $\mathcal{P}_{n-k}$ e prova quindi che le loro cardinalità coincidono.

2) L'asserto equivale all'uguaglianza: $C_{n+1,k+1} = C_{n,k+1} + C_{n,k}$.

   L'insieme $H = \{B \subset I_{n+1} \mid B \text{ ha } k+1 \text{ elementi}\}$ è unione disgiunta di:

$$H' = \{B \in H \mid n+1 \notin B\} = \{B \subseteq I_n \mid B \text{ ha } k+1 \text{ elementi}\} \text{ e di}$$

$$H'' = \{B \in H \mid n+1 \in B\} = \{D \cup \{n+1\} \mid D \subseteq I_n \text{ e } D \text{ ha } k \text{ elementi}\}.$$

Si ha allora $C_{n+1,k+1} = Card(H) = Card(H') + Card(H'') = C_{n,k+1} + C_{n,k}$, come volevasi. ◇

Teorema 5.2.8. *I binomiali sono i coefficienti che compaiono nello sviluppo della potenza n−esima di un binomio (da cui il loro nome) ossia:*

$$(X+Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^{n-k}Y^k.$$

Dim: Procediamo per induzione su n.

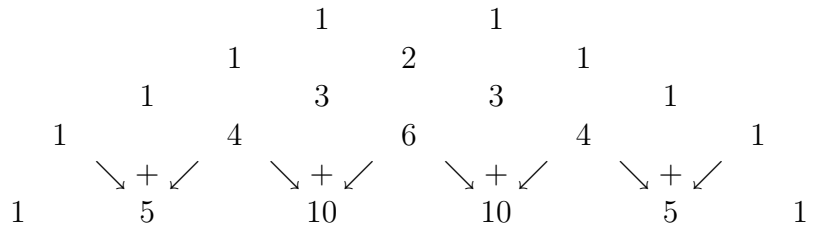
Se $n = 1$, allora $\binom{1}{0} = \binom{1}{1} = 1$ e quindi $(X+Y)^1 = \binom{1}{0}X + \binom{1}{1}Y$.

Supponiamo la formula vera per un certo n e proviamola per il successivo $n+1$. Si ha:

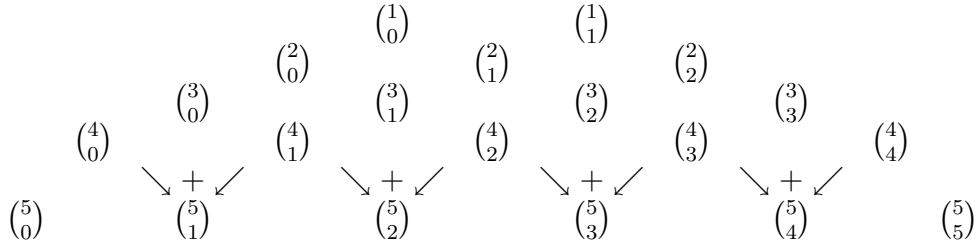
$$(X+Y)^{n+1} = (X+Y)^n(X+Y) = \left(\sum_{k=0}^{n} \binom{n}{k} X^{n-k}Y^k\right)(X+Y).$$

Nell'ultimo membro i monomi con parte letterale $X^{n+1-k}Y^k$ sono due: $\left(\binom{n}{k}X^{n-k}Y^k\right)X$ e $\left(\binom{n}{k-1}X^{n-k+1}Y^{k-1}\right)Y$. Il coefficiente di $X^{n+1-k}Y^k$ nello sviluppo di $(X+Y)^{n+1}$ è dunque $\binom{n}{k} + \binom{n}{k-1}$, che coincide proprio con $\binom{n+1}{k}$, come provato in Proposizione 5.2.7 2). ⋄

Il modo più conosciuto e veloce (almeno per valori bassi di n) per costruire i coefficienti dello sviluppo di $(X+Y)^n$ è il **Triangolo di Tartaglia**.



Osserviamo che la regoletta che permette di costruire il triangolo di Tartaglia non è altro che l'applicazione ripetuta riga dopo riga della Proposizione 5.2.7 2)



Corollario 5.2.9. *i)* $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

ii) Se A è un insieme con n elementi, allora $\mathcal{P}(A)$ ha 2^n elementi.

Dim: Per i) basta porre $X = Y = 1$ nella formula dello sviluppo del binomio.

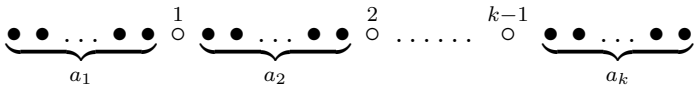
L'affermazione ii) segue da i); infatti $\binom{n}{k}$ è il numero di sottoinsiemi di A che hanno k elementi e quindi la somma $\sum_{k=0}^{n}\binom{n}{k} = 2^n$ dà il numero complessivo di tutti i possibili sottoinsiemi di A. $\diamond$

Definizione 5.2.10. *Si dice* **combinazione con ripetizione di n oggetti di k tipi diversi** *ogni $k-$upla $(a_1, a_2, \ldots, a_k)$ di numeri $a_i \in \mathbb{N}$ tali che $a_1 + a_2 + \cdots + a_k = n$.*

Proposizione 5.2.11. *Il numero delle possibili combinazioni con ripetizione di n oggetti di k tipi è:*

$$C^r_{n,k} = \binom{n+k-1}{k-1} = \binom{n+k-1}{n}.$$

Dim: Immaginiamo di disporre gli n oggetti in fila ponendo gli a_1 oggetti del primo seguiti da un posto vuoto, poi gli a_2 oggetti del secondo tipo seguiti da un posto vuoto e così via, secondo lo schema seguente.



Ogni configurazione di questo tipo, corrisponde alla scelta dei $k-1$ spazi vuoti in una sequenza di $n+k-1$ caselle. Allora, ricordando anche le proprietà dei binomiali:

$$C^r_{n,k} = C_{n+k-1,k-1} = \binom{n+k-1}{k-1} = \binom{n+k-1}{n}.$$

$\diamond$

Esempio 5.2.12. *L'esito di una votazione con 5 canditati e 300 elettori è dato dai numeri $V_1, V_2, \ldots, V_5$ dei voti ottenuti da ciascun candidato a cui si aggiungono le schede bianche B e le nulle N, cosicché $V_1 + V_2 + \cdots + V_5 + B + N = 300$. I possibili esiti sono allora $C^r_{300,7} = C_{306,6}$.*

5.3 Esercizi

5.1. Per **anagramma** di una certa parola, si intende un qualunque riordinamento delle lettere che costituiscono quella parola. Contrariamente a quanto succede in enigmistica, in matematica NON si richiede che il nuovo riordinamento delle lettere formi una parola di senso compiuto. Calcolare quanti sono gli anagrammi delle parole seguenti:

SE, ICS, ORO, TORINO, INSIEME, ANAGRAMMA.

5.2. Ad un campionato di calcio partecipano 20 squadre. Ogni squadra gioca una prima volta contro tutte le altre (girone di andata) e poi una seconda (girone di ritorno). Quante partite in totale si disputano nel girone d'andata? Qual'è la risposta per un torneo a n squadre, se $n \geq 2$?

5.3. Dati 5 punti del piano, a 3 a 3 non allineati, quante sono le rette che passano per 2 di tali punti? Cambia la risposta se anziché nel piano i 5 punti sono scelti nello spazio? Qual'è la risposta nel caso generale di $n \geq 2$ punti, con la medesima condizione che siano a 3 a 3 non allineati?

5.4. Sia A l'insieme $\{a, b, c, d\}$. Quante sono le applicazioni iniettive $f\colon A \to A$ tali che $f(b) = d$? Quante le suriettive con $f(a) = a$?

5.5. Si hanno a disposizione 6 vernici di colori diversi, con cui si vogliono dipingere le 4 pareti di una stanza, usando un solo colore per parete.

In quanti modi si possono dipingere le pareti se si decide di non usare più volte uno stesso colore? In quanti modi se si decide che è possibile usare più volte uno stesso colore? In quanti modi se si decide che è possibile usare più volte uno stesso colore, purché non su pareti adiacenti?

Generalizzare le risposte dei precedenti quesiti al caso di una stanza poligonale con n pareti.

5.6. Quanti sono i possibili prodotti di 6 fattori che si possono formare con i numeri 7, 17 e 37?

5.7. Nove persone si presentano ad un concorso per 4 posti. Quante sono le possibili graduatorie dei vincitori, se si escludono gli *ex-aequo*?

5.8. Si mettono dentro un'urna 30 palline di 4 colori diversi: rosso, verde, giallo e blu. In quanti modi differenti si possono combinare i colori? In quanti modi se si vuole che ci sia almeno una pallina per ciascun colore? In quanti se si vuole che non ci siano più di 15 palline di uno stesso colore? In quanti se si vuole che siano soddisfatte contemporaneamente le ultime due condizioni?

5.9. Siano $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 6, 4\}$, $C = \{1, 2\}$.

- **a.** Determinare il numero di applicazioni di C in C e il numero di applicazioni $\phi\colon A \to B$ tali che $\phi(C) \subseteq C$.
- **b.** Si fissi una applicazione suriettiva $f\colon A \to B$ a scelta. Quante sono le applicazioni $g\colon B \to A$ tali che $f \circ g = id_B$? È vero che lo stesso numero si sarebbe ottenuto per ogni altra applicazione suriettiva $f\colon A \to B$?
- **c.** Si fissi una applicazione suriettiva $f\colon A \to C$ a scelta. Quante sono le applicazioni $g\colon C \to A$ tali che $f \circ g = id_C$? È vero che lo stesso numero si sarebbe ottenuto per ogni altra applicazione suriettiva $f\colon A \to C$?
- **d.** Si fissi una applicazione iniettiva $h\colon B \to A$ a scelta. Quante sono le applicazioni $k\colon A \to B$ tali che $k \circ h = id_B$? È vero che lo stesso numero si sarebbe ottenuto per ogni altra applicazione iniettiva $f\colon B \to A$?
- **e.** Si fissi una applicazione iniettiva $h\colon C \to A$ a scelta. Quante sono le applicazioni $k\colon A \to C$ tali che $k \circ h = id_C$? È vero che lo stesso numero si sarebbe ottenuto per ogni altra applicazione iniettiva $f\colon C \to A$?

Capitolo 6

L'anello dei numeri interi

6.1 Costruzione dell'insieme dei numeri interi

Consideriamo il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ dell'insieme dei numeri naturali per sè ed in esso la relazione:

$$(n, m)\ \rho\ (n', m') \iff n + m' = n' + m.$$

Si può facilmente verificare che ρ è una relazione di equivalenza.

Osserviamo che sono in relazione con la coppia $(0, 0)$ tutte e sole le coppie del tipo (n, n). Inoltre, in ogni altra classe di equivalenza vi è una (e soltanto una) coppia in cui uno dei due elementi è lo 0. Se infatti $n > m$, ossia se $n = m + p$, allora $(n, m)\rho(p, 0)$ e, analogamente, se $n < m$, ossia se $m = n + q$, allora $(n, m)\rho(0, q)$.

Definizione 6.1.1. *Si dice insieme dei numeri interi relativi $\mathbb{Z}$ l'insieme quoziente $(\mathbb{N} \times \mathbb{N})/\rho$. Ogni classe di equivalenza $[(n, m)]$ si dice* **numero intero relativo**.
La classe di $(0, 0)$ si dice **zero di $\mathbb{Z}$** *e si indica con 0; la classe di $(p, 0)$ (dove $p \in \mathbb{N}$) si indica con $+p$ o semplicemente con p e si dice* **numero intero positivo**, *la classe di $(0, q)$ (dove $q \in \mathbb{N}$) si indica con $-q$ e si dice* **numero intero negativo**.

Possiamo definire le operazioni somma e prodotto in $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\rho$ a partire dalle operazioni di $\mathbb{N}$, nel modo seguente:

$$[(n, m)] + [(n', m')] = [(n + n', m + m')]$$

e

$$[(n, m)] \cdot [(n', m')] = [(nn' + mm', nm' + n'm)]$$

Possiamo inoltre definire in $\mathbb{Z}$ un ordine totale nel modo seguente:

$$[(n, m)] \leq [(n', m')] \text{ se in } \mathbb{N} \text{ vale la disuguaglianza } n + m' \leq n' + m.$$

Lasciamo per esercizio al lettore la verifica che queste operazioni sono **ben poste** (ossia che il risultato non dipende dai rappresentanti) e la dimostrazione del seguente risultato.

Proposizione 6.1.2. *L'applicazione* $i\colon \mathbb{N} \longrightarrow \mathbb{Z}$ *data da* $i(p) = [(p,0)]$ *è iniettiva e rispetta le operazioni e l'ordinamento ossia:*

$$i(p+q) = i(p) + i(q), \quad i(pq) = i(p)\cdot i(q), \quad p \leq q \text{ in } \mathbb{N} \text{ se e solo se } i(p) \leq i(q) \text{ in } \mathbb{Z}.$$

Grazie alla Proposizione 6.1.2 potremo identificare i numeri naturali con i numeri interi positivi e considerare $\mathbb{N}$ (identificato con $i(\mathbb{N})$) come un sottoinsieme di $\mathbb{Z}$.

6.2 Generalità sugli anelli

Definizione 6.2.1. *Si dice* **anello** *un insieme* A *dotato di due operazioni, usualmente denotate con* $+$ *e* $\cdot$ *e dette somma e prodotto, che soddisfano le seguenti proprietà:*

1. *Proprietà associativa della somma:* $\forall a,\ b,\ c \in A:\ (a+b)+c = a+(b+c)$

2. *Proprietà commutativa della somma:* $\forall a,\ b \in A:\ a+b = b+a$

3. *Esistenza dello zero o elemento neutro per la somma:*
$\exists$ *un elemento in* A*, di solito denotato* 0_A*, tale che* $\forall a \in A:\ a+0_A = 0_A+a = a$

4. *Esistenza dell'opposto rispetto alla somma:* $\forall a \in A\ \exists\ b \in A$ *t.c.:* $a+b = b+a = 0_A$
(di solito l'opposto di a *si indica con* $-a$*)*

5. *Proprietà associativa del prodotto:* $\forall a,\ b,\ c \in A:\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$

6. *Proprietà distributive del prodotto rispetto alla somma:*
$\forall a,\ b,\ c \in A:\quad (a+b)\cdot c = a\cdot c + b\cdot c, \qquad c\cdot(a+b) = c\cdot a + c\cdot b$

Un anello si dice **anello commutativo con identità** *se soddisfa anche le due ulteriori condizioni:*

7. *Proprietà commutativa del prodotto:* $\forall a,\ b \in A:\ a\cdot b = b\cdot a$

8. *Esistenza dell'identità o elemento neutro per il prodotto:*
$\exists$ *un elemento in* A*, di solito denotato* 1_A*, tale che* $\forall a \in A:\ a\cdot 1_A = 1_A\cdot a = a$

Proposizione 6.2.2. *L'insieme dei numeri interi* $\mathbb{Z}$ *dotato delle operazioni* $+$ *e* $\cdot$ *è un anello commutativo con identità. In particolare:*

i) $0_{\mathbb{Z}} = [(0,0)] = 0$;

ii) $-[(n,m)] = [(m,n)]$;

iii) $1_{\mathbb{Z}} = [(1,0)] = 1$.

A partire dalle definizioni date e dalle proprietà di $\mathbb{N}$ possono essere dimostrate in modo rigoroso tutte le proprietà dei numeri interi che usiamo abitualmente. Notiamo però che molte di esse non sono caratteristiche dei numeri interi, ma dipendono soltanto dalla struttura di anello, ossia valgono per tutti gli anelli (oppure per tutti gli anelli commutativi con identità). L'enunciato seguente presenta alcune proprietà di questo tipo ed altre sono inserite tra gli esercizi; una trattazione sistematica della teoria degli anelli non rientra però nelle finalità di questo corso.

Lemma 6.2.3. *Sia A un anello. Allora:*

i) *l'elemento neutro rispetto alla somma è unico;*

ii) $\forall a \in A$, $0_A \cdot a = a \cdot 0_A = 0_A$*;*

iii) *per ogni elemento $a \in A$ l'opposto è unico;*

iv) *vale la proprietà di cancellazione rispetto alla somma $a + c = b + c \Longrightarrow a = b$.*

Se inoltre A è un anello commutativo con identità 1_A, allora:

v) *l'elemento neutro rispetto al prodotto è unico;*

vi) *l'opposto $-a$ di un elemento $a \in A$ è $(-1_A) \cdot a$.*

Dim: i) Siano 0_A e $0'_A$ elementi di A che soddisfano entrambi le condizioni per essere un elemento neutro rispetto alla somma. Avremo allora $0_A + 0'_A = 0'_A$ poiché 0_A è elemento neutro, ma anche $0_A + 0'_A = 0_A$, poiché anche $0'_A$ è elemento neutro. Allora $0_A = 0'_A$.

ii) Sia a un qualsiasi elemento di A.
Si hanno le uguaglianze: $0_A \cdot a = (0_A + 0_A) \cdot a = 0_A \cdot a + 0_A \cdot a$. Sommando ai due membri estremi dell'uguaglianza l'opposto di $(0_A \cdot a)$ troviamo da un lato $(0_A \cdot a) + (-(0_A \cdot a)) = 0_A$ e dall'altro $0_A \cdot a + 0_A \cdot a + (-(0_A \cdot a)) = 0_A \cdot a + 0_A = 0_A \cdot a$ Allora $0_A = 0_A \cdot a$, come volevasi. Notiamo che abbiamo usato le proprietà distributive e di esistenza dell'opposto di ogni elemento.

iii) Siano b e b' elementi di A che soddisfano le condizioni per essere opposti di a. Allora $b = b + 0_A = b + (a + b') = (b + a) + b' = 0_A + b' = b'$. Si noti che nel punto centrale di tale verifica abbiamo fatto ricorso alla proprietà associativa della somma.

iv) Sommando ai due membri di $a + c = b + c$ l'opposto di c otteniamo $(a + c) + (-c) = (b + c) + (-c)$, da cui segue, grazie alla proprietà associativa della somma, $a = b$.

v) si prova in modo del tutto analogo a quello seguito per provare i).

vi) Proviamo che $(-1_A) \cdot a$ soddisfa le condizioni per essere l'opposto di a.
Si ha: $a + (-1_A) \cdot a = 1_A \cdot a + (-1_A) \cdot a = (1_A + (-1_A)) \cdot a = 0_A \cdot a$. In virtù di quanto provato nel punto ii), abbiamo $0_A \cdot a = 0_A$ e quindi $a + (-1_A) \cdot a = 0_A$. $\diamond$

Definizione 6.2.4. *Siano A e B due anelli (anelli commutativi con identità). Nel prodotto cartesiano $A \times B$ si possono introdurre due operazioni di somma e prodotto nel seguente modo: $\forall (a,b),(a',b') \in A \times B$*

$$(a,b) + (a',b') = (a+a', b+b'),$$
$$(a,b) \cdot (a',b') = (aa', bb').$$

Si verifica che con tali operazioni, dette **operazioni componente per componente**, *il prodotto cartesiano $A \times B$ assume la struttura di anello (anello commutativo con identità), che viene detto* ***anello prodotto*** *di A e B.*

Nel prossimo paragrafo vedremo alcune proprietà che valgono per l'anello $\mathbb{Z}$, ma non per tutti gli anelli commutativi con identità. Prima però introduciamo qualche altra definizione relativa ad un anello commutativo con identità A.

Nel seguito sottointenderemo quasi sempre il simbolo $\cdot$ del prodotto, ossia scriveremo ab invece di $a \cdot b$, e useremo la notazione abbreviata $a - b$ al posto di $a + (-b)$.

Definizione 6.2.5. *Si dice che un anello commutativo con identità A è un* **dominio di integrità** *o semplicemente un* **dominio** *se in A vale la* **legge di annullamento del prodotto** *ossia se $\forall\ a, b \in A$: $ab = 0_A \Longrightarrow a = 0_A$ oppure $b = 0_A$.*

Lemma 6.2.6. *Se A è un dominio di integrità, allora in A vale la legge di cancellazione per il prodotto ossia $\forall\ a,\ b,\ c \in A$, se $c \neq 0_A$ allora $ac = bc \Longrightarrow a = b$.*

Dim: Sommando ai due membri di $ac = bc$ l'opposto di bc si ottiene $ac - bc = 0_A$ ossia $(a-b)c = 0_A$. Poiché vale la legge di annullamento del prodotto e $c \neq 0$, allora $a - b = 0$ ossia (sommando b ai due membri) $a = b$. $\diamond$

Definizione 6.2.7. *Un elemento a di un anello A si dice* **zero-divisore** *di A se esiste $b \in A$, $b \neq 0_A$, tale che $ab = 0_A$.*

Concretamente gli zero-divisori sono quegli elementi per cui non vale la legge di cancellazione del prodotto. Un anello commutativo con identità A è un dominio se e solo se l'unico zero-divisore è 0_A.

Esempio 6.2.8. *In $\mathbb{Z}$ l'unico elemento per cui non vale la legge di cancellazione è 0 e quindi $\mathbb{Z}$ è un dominio di integrità.*

Definizione 6.2.9. *Un elemento $u \in A$ si dice* **unità** *o anche* **elemento invertibile** *di A se esiste in A un suo* **inverso rispetto al prodotto**, *ossia un elemento v tale che $uv = vu = 1_A$. Di solito l'inverso di un elemento a (che, se esiste, è sempre unico) si indica con a^{-1}.*

Due elementi a, b di A si dicono **associati** *l'uno all'altro se esiste una unità $u \in A$ tale che $a = ub$ (e quindi $b = u^{-1}a$).*

Esempio 6.2.10. *In $\mathbb{Z}$ gli unici elementi invertibili sono 1 e -1. Due elementi sono allora associati se sono uguali oppure sono opposti.*

Definizione 6.2.11. *Si dice che un anello commutativo con identità A è un* **campo** *se ogni elemento non nullo di A è una unità.*

Definizione 6.2.12. *Siano a, b elementi di A. Si dice che a* **divide** *b se esiste $c \in A$ tale che $b = ac$. In simboli "a divide b" si scrive a/b e "a non divide b" si scrive $a \not| b$.*

Lemma 6.2.13. *Siano $a, b \in A$. Se a e b sono associati allora a/b e b/a.*

Se inoltre A è un dominio di integrità, allora vale anche il viceversa ossia a/b e b/a se e solo se a e b sono associati.

Dim: La prima parte dell'affermazione segue subito dalla definizione di elementi associati.

Supponiamo allora che A sia un dominio e che si abbia a/b e b/a. Se $a = 0$ allora anche $b = 0$ e quindi $a = 1_A \cdot b$ e $b = 1_A \cdot a$.

Supponiamo allora $a \neq 0$ e siano $c, d \in A$ tali che $a = bc$ e $b = ad$. Sostituendo la seconda uguaglianza nella prima si ottiene $a = adc$ ossia $a \cdot 1_A = adc$. Poiché A è un dominio e $a \neq 0_A$, possiamo fare ricorso alla legge di cancellazione per il prodotto ottenendo $1_A = cd$. Questa relazione dice che c e d sono unità e quindi a e b sono associati. ◇

Definizione 6.2.14. *Sia A un anello commutativo con identità. Un elemento $a \in A$, che non è invertibile e che non è 0_A, si dice*

- **riducibile** *in A se può essere scritto come un prodotto $a = bc$, $b, c \in A$, in cui nè b nè c sono invertibili;*
- **irriducibile** *se e non è riducibile, ossia se non si può decomporre in un prodotto tranne che nel prodotto di una unità per un elemento associato ad a;*
- **primo** *in A se ogni volta che divide un prodotto allora divide uno dei due fattori. In simboli: $a/bc \Longrightarrow a/b$ oppure a/c.*

NOTA BENE Si faccia attenzione al fatto che 0_A e gli elementi invertibili di A **non sono mai, per definizione, nè riducibili, nè irriducibili, nè primi**.

Esempio 6.2.15. *In $\mathbb{Z}$ il numero 2 è un elemento irriducibile poiché non può essere scritto come prodotto, a meno di non usare i fattori 1, -1, 2 e -2 che sono rispettivamente unità di $\mathbb{Z}$ oppure associati a 2 in $\mathbb{Z}$.*

Il numero 2 *è anche primo in* $\mathbb{Z}$ *perché un prodotto è pari soltanto quando almeno uno dei due fattori è pari (ossia* 2 *è primo perché* $2/ab \Longrightarrow 2/a$ *oppure* $2/b$*).*

Invece 0 *e* 1 *e* -1 *non sono nè riducibili, nè irriducibili, nè primi.*

Osservazione 6.2.16. *Nelle scuole elementari e medie spesso si dice che un numero è primo se non è decomponibile in un prodotto, confondendo quindi primo con irriducibile. Questa confusione non porta ad errori poiché, come mostreremo nel prossimo paragrafo, l'insieme degli elementi irriducibili di* $\mathbb{Z}$ *coincide con l'insieme degli elementi primi di* $\mathbb{Z}$ *ossia, relativamente a* $\mathbb{Z}$*, queste due nozioni risultano essere equivalenti. Questa proprietà è parte del* **Teorema fondamentale dell'aritmetica** *ed è un fatto tutt'altro che ovvio o banale. Inoltre le due nozioni non sono per nulla equivalenti in generale.*

Definizione 6.2.17. *Un dominio* A *si dice* **dominio fattoriale** *o* **dominio a fattorizzazione unica** *(in breve* **U.F.D.***, dall'inglese Unique Factorization Domain) se ogni elemento* $a \in A$ *non nullo e non invertibile si decompone in modo unico (a meno dell'ordine e di fattori moltiplicativi invertibili) nel prodotto di elementi irriducibili, o equivalentemente, se si decompone nel prodotto di elementi primi.*

Osservazione 6.2.18. *L'equivalenza tra le due formulazioni della fattorialità presenti nella precedente definizione non è del tutto ovvia. Per verificare che dalla seconda discende la prima è sufficiente provare che ogni elemento primo è anche irriducibile (ma non viceversa!) e che ogni fatorizzazione in fattori primi è sempre essenzialmente unica. Per verificare che dalla prima discende la seconda bisogna verificare che se vale l'unicità della decomposizione in fattori irriducibili per tutti gli elementi di* A*, allora gli elementi irriducibili di* A *sono anche primi. Lasciamo queste verifiche al lettore. Nei prossimi paragrafi queste proprietà saranno provate per esteso nel caso dell'anello* $\mathbb{Z}$*.*

6.3 La divisione euclidea

La **divisione con resto** oggetto di questo paragrafo è semplicemente il primo tipo di divisione che si impara alle elementari (prima dell'introduzione delle frazioni), ma è anche un importantissimo strumento di calcolo e di dimostrazione per le proprietà dell'anello $\mathbb{Z}$.

Teorema 6.3.1. *Per ogni coppia* a, b *di numeri interi, con* $b \neq 0$*, esistono e sono univocamente determinati i numeri interi* q *(quoziente) ed* r *(resto), tali che* $a = bq + r$ *con* $0 \leq r < |b|$*.*

Dim: Per prima cosa dimostriamo che degli interi q ed r siffatti esistono e poi proveremo che sono univocamente determinati.

Osserviamo intanto che è sufficiente provare l'asserto nel caso $a \geq 0$ e $b > 0$. Se infatti $b < 0$ e si ha $a = (-b)q + r$ allora $a = b(-q) + r$; analogamente se $a < 0$, $b \geq 0$ e si ha

$(-a) = bq + r$ allora $a = b(-q-1) + (b-r)$ con $0 \leq b - r < |b|$ (oppure $a = b(-q)$ se $r = 0$). Siano, allora, $a \geq 0$ e $b > 0$. Procediamo per induzione su a.

Se $a = 0$, basta prendere $q = r = 0$.

Supponiamo l'asserto vero per tutti gli interi $a' < a$ e proviamolo per a.
Se $a < b$, è sufficiente prendere $q = 0$ ed $r = a$. Se $a \geq b$, l'asserto è vero per i numeri $(a-b)$ e b, ossia esistono q' e r' tali che $(a-b) = bq' + r'$ e $0 \leq r' < |b|$.
Allora $q = q' + 1$ e $r = r'$ soddisfano le condizioni volute.

Proviamo ora l'unicità di q ed r. Supponiamo che valgano le relazioni $a = bq + r$ e $a = bq' + r'$ con $0 \leq r \leq r' < |b|$. Sottraendo membro a membro si ottiene $b(q - q') = (r' - r)$ ossia $b/(r' - r)$. Essendo $|b| > r' - r \geq 0$, allora $r' - r = 0$ e quindi anche $q - q'$ deve essere nullo. $\diamond$

Definizione 6.3.2. *Siano k un numero intero ≥ 2 detto* **base** *e C un insieme di k simboli detti* **cifre** *associati ai numeri compresi tra 0 e $k-1$. Si dice* **scrittura posizionale** *di numero intero positivo a una sequenza ordinata $c_s c_{s-1} \dots c_1 c_0$ tale che $c_i \in C$ ed $a = c_s k^s + c_{s-1} k^{s-1} + \cdots + c_1 k + c_0$.*

La scrittura posizionale di un numero negativo b si ottiene premettendo il segno $-$ alla scrittura posizionale di $a = -b$.

Corollario 6.3.3. *Fissata una base k e un insieme di cifre C, ogni numero intero positivo a possiede una e una sola scrittura posizionale e ogni seuquenza del tipo $c_s c_{s-1} \dots c_1 c_0$ con $c_i \in C$ è la scrittura posizionale di un numero intero.*

Dim: Per provare che una tale scrittura esiste (ed anche per calcolarla) procediamo per induzione su a.

Se $0 \leq a \leq k-1$, allora $a = c_0$, con $c_0 \in C$.

Sia allora $a \geq k$ e supponiamo l'asserto vero per tutti in numeri minori di a. Eseguiamo la divisione di a per k: $a = qk + r$, con $0 \leq r \leq k-1$.
Per l'ipotesi induttiva, l'asserto è vero per il quoziente q. Se $q = c'_{s'} k^{s'} + c'_{s'-1} k^{s'-1} + \cdots + c'_1 k + c'_0$, la scrittura di a si ottiene ponendo $s = s' + 1$, $c_i = c'_{i-1}$ e $c_0 = r$.
Per i numeri negativi si usa la scrittura posizionale dell'opposto preceduta dal segno $-$. $\diamond$

Esempio 6.3.4. *Introduciamo le nuove cifre $*$ per il numero 10 e $\bullet$ per 11 oltre alle 10 cifre abituali. La notazione in base 12 del numero (che in base 10 si scrive) 419 è $2 * \bullet$ poiché $419 = 2 \cdot 12^2 + 10 \cdot 12 + 11$. Per calcolarla a partire da 419 si eseguono le divisioni:*

$419 = 34 \cdot 12 + 11$ *con resto* $11 = c_0 = \bullet$

$34 = 2 \cdot 12 + 10$ *con resto* $10 = c_1 = *$

$2 = 0 \cdot 12 + 2$ *con resto* $2 = c_2 = 2$.

Nel seguito di questo paragrafo e nel prossimo ci occuperemo dei divisori di un numero intero e supporremo sempre di lavorare con numeri positivi e con fattori positivi. Tutte le

proprietà dimostrate, però, valgono per tutti i numeri interi, anche per i negativi, poiché ogni numero intero è associato ad un numero positivo, cioè differisce da un positivo per un fattore moltiplicativo invertibile 1 o -1.

Definizione 6.3.5. *Si dice* **massimo comun divisore** *di due interi a e b non entrambi nulli il numero intero positivo $k = MCD(a, b)$ tale che k/a, k/b e $\forall h \in \mathbb{Z}$ t.c. h/a e h/b si ha h/k.*

Il MCD quindi è il più grande divisore comune ad a e b, non solo rispetto alla relazione d'ordine totale $\leq$, ma anche rispetto alla divisibilità.

Esempio 6.3.6. *Non ha senso definire il $MCD(0, 0)$ poiché l'insieme dei divisori di 0 coincide con $\mathbb{Z}$ e quindi non ha massimo. Invece, se $a \in \mathbb{Z}$, $a \neq 0$, allora $MCD(a, 0) = |a|$.*

L'aver richiesto che il MCD sia un numero positivo fa sì che, se esiste (cosa non ovvia ma che proveremo essere vera), allora è unico. Per provare che il massimo comun divisore esiste useremo il seguente lemma.

Lemma 6.3.7. *Siano $a, b \in \mathbb{Z}$, $b \neq 0$ e sia r il resto della divisione di a per b. Allora $MCD(a, b)$ e $MCD(b, r)$ (se esistono) coincidono.*

Dim: Sia $a = bq + r$. Ogni divisore comune a b e r divide anche a; d'altra parte si ha anche $r = a - bq$ e quindi ogni divisore comune ad a e b divide anche r. $\diamond$

Teorema 6.3.8. (Identità di Bézout) *Siano a, b due interi non entrambi nulli.*

Allora $MCD(a, b)$ esiste e può essere ottenuto come combinazione lineare di a e b, ossia $MCD(a, b) = ax + by$ per opportuni $x, y \in \mathbb{Z}$.

Dim: Supponiamo $a \geq b \geq 0$ e procediamo per induzione sul minimo tra a e b ossia su b.

Se $b = 0$, allora $MCD(a, 0) = a = a \cdot 1 + 0 \cdot 1$.

Supponiamo allora $b > 0$ e l'asserto vero per tutte le coppie (a', b') con $b' < b$. L'asserto è allora vero in particolare per la coppia $a' = b$ e $b' = r$, dove r è il resto della divisione di a per b, cioè esiste $d = MCD(b, r)$ ed inoltre si ha $d = bx' + ry'$ per opportuni $x', y' \in \mathbb{Z}$. In virtù del Lemma 6.3.7 si ha $MCD(a, b) = d$. Inoltre dalle relazioni $a = bq + r$ e $d = bx' + ry'$ si ricava $MCD(a, b) = ay' + b(x' - qy')$, ossia l'identità di Bézout con $x = y'$ e $y = x' - qy'$. $\diamond$

La dimostrazione precedente fornisce un metodo effettivo per il calcolo del massimo comun divisore e dei coefficienti x, y che compaiono nell'identità di Bézout, metodo noto come **algoritmo euclideo** o algoritmo delle divisioni successive.

Per calcolare il massimo comun divisore di due numeri a, b, con $b \neq 0$ si procede nel modo seguente:
$MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2) = \cdots = MCD(r_i, r_{i+1}) = \cdots = MCD(r_k, 0) = r_k$
dove r_1 è il resto della divisione di a per b, r_2 è il resto della divisione di b per r_1 e r_{i+1} è il resto della divisione di r_{i-1} per r_i.

Questo procedimento ha al più b passi (poiché $b > r_1 > r_2 > \cdots > r_k > 0$) e si ferma non appena si trova un resto nullo. Il $MCD(a, b)$ è l'ultimo resto non nullo trovato.

Procedendo a ritroso da $r_k = r_{k-2} - r_{k-1}q_{k-1}$ ed utilizzando le relazione trovate ad ogni divisione $r_i = r_{i-1}q_{i-1} + r_{i-2}$, si ricava l'identità di Bézout.

Esempio 6.3.9. *Procedimento per calcolare* $MCD(6852, 3997)$*:*

1) $6852 = 3997 \cdot 1 + 2855$

2) $3997 = 2855 \cdot 1 + 1142$

3) $2855 = 1142 \cdot 2 + 571$

4) $1142 = 571 \cdot 2 + 0$

Allora $MCD(6852, 3997) = 571$*. Procedimento per calcolare l'identità di Bézout:*

3) $571 = 2855 - 1142 \cdot 2$

2) $1142 = 3997 - 2855$ *da cui, sostituendo nella precedente,* $571 = 2855 - (3997 - 2855) \cdot 2$ *ossia* $571 = 2855 \cdot 3 + 3997 \cdot (-2)$

1) $2855 = 6852 - 3997$ *da cui, sostituendo nella precedente,* $571 = (6852 - 3997) \cdot 3 + 3997 \cdot (-2)$ *ossia* $571 = 6852 \cdot 3 + 3997 \cdot (-5)$.

Corollario 6.3.10. *Siano* $a, b, c \in \mathbb{Z}$*,* $(a, b) \neq (0, 0)$*. Allora:*

$$\exists x, y \in \mathbb{Z} \text{ tali che } c = ax + by \iff MCD(a, b)/c.$$

Dim: Siano $d = MCD(a, b)$ e $d = ax' + by'$ l'identità di Bézout. Se $c = ax + by$, ogni divisore comune ad a e b divide anche c; in particolare d/c.

Viceversa, se $c = dt$, allora $c = ax + by$, dove si ponga $x = x't$, $y = y't$. $\diamond$

Osseriviamo infine che il minimo comune multiplo di due numeri si ottiene facilmente a partire dal loro massimo comun divisore come: $mcm(a, b) = \frac{ab}{MCD(a,b)}$ e quindi può essere, anch'esso, calcolato mediante l'algoritmo euclideo.

6.4 Il teorema fondamentale dell'aritmetica

In questo paragrafo proveremo che ogni numero intero, non nullo e non invertibile, si fattorizza in modo essenzialmente unico (ossia a meno di permutazioni dei fattori e di cambiamenti di segno) nel prodotto di numeri primi.

Ci sarà utile la seguente

Definizione 6.4.1. *Sia a un elemento di un anello A commutativo con identità. Due fattorizzazioni $a = b_1 \cdots b_k$ e $a = c_1 \cdots c_h$ sono* **essenzialmente la stessa fattorizzazione** *di a se $k = h$ e per ogni $i = 1, \ldots, k$ si ha $b_i = u_i c_{\sigma(i)}$, dove le u_i sono unità di A e σ è una opportuna permutazione degli indici. In altre parole due fattorizzazioni sono essenzialmente la stessa se differiscono solo per l'ordine dei fattori e per eventuali fattori moltiplicativi invertibili.*

Lemma 6.4.2. *Sia a un numero intero $\neq 0, 1, -1$. Allora a può essere scritto come prodotto di numeri interi irriducibili $a = a_1 \cdot \cdots \cdot a_k$.*

Dim: Senza perdere in generalità, possiamo supporre $a \geq 2$ e considerare solo fattori ≥ 2.

Procediamo per induzione su a. Se $a = 2$, allora a è irriducibile, $k = 1$, $a = a_1$ e non c'è nulla da provare.

Supponiamo l'asserto vero per tutti gli interi n, $2 \leq n < a$ e proviamo che vale anche per a.
Se a è irriducibile, come prima $k = 1$, $a = a_1$. Se invece a si può scrivere come prodotto $a = bc$, con b, c non invertibili, allora i fattori sono tali che $2 \leq b, c < a$ e quindi grazie all'ipotesi induttiva possiamo scrivere $b = b_1 \cdots b_i$, $c = c_1 \cdots c_j$ e quindi $k = i + j$, $a = b_1 \cdots b_i \cdot c_1 \cdots c_j$. $\diamond$

Lemma 6.4.3. *Sia p un numero intero $\neq 0, 1, -1$. Allora :*

$$p \text{ è primo} \iff p \text{ è irriducibile.}$$

Dim: "$\Longrightarrow$" Supponiamo che p sia primo. Se $p = mn$ con $m, n \in \mathbb{Z}$, allora p/mn e quindi, essendo primo, deve dividere almeno uno dei fattori. Se $m = pq$, allora $p = pqn$, da cui, per la cancellazione, $qn = 1$. Questa uguaglianza dice che n è una unità di $\mathbb{Z}$ e quindi m è associato a p. Si conclude che p non ha decomposizioni effettive in un prodotto, cioè è irriducibile.

"$\Longleftarrow$" Sia p un numero irriducibile e siano a, b interi tali che p/ab e $p \not| a$. Proviamo che allora p/b. Dalle ipotesi fatte segue che $MCD(a, p) = 1$; possiamo allora scrivere l'identità di Bézout $1 = xa + yp$ (Teorema 6.3.8). Moltiplicando i due membri per b e ricordando che p/ab ossia che esiste $c \in \mathbb{Z}$ tale che $pc = ab$, troviamo: $b = xab + pyb = p(xc + yb)$ e quindi p/b. $\diamond$

Teorema 6.4.4. (Teorema fondamentale dell'aritmetica) *$\mathbb{Z}$ è un dominio a fattorizzazione unica ossia ogni numero intero $\neq 0, 1, -1$ si fattorizza in modo essenzialmente unico nel prodotto di numeri primi.*

Dim: I risultati precedenti mostrano che ogni numero intero a ($a \neq 0, 1, -1$) si fattorizza nel prodotto di irriducibili e che gli irriducibili in $\mathbb{Z}$ sono anche primi. Allora a si fattorizza nel prodotto di numeri primi.

Rimane da provare che la fattorizzazione è essenzialmente unica.

Supponiamo che tutti i fattori siano positivi (sostituendo eventualmente i negativi con i loro opposti). Sia $a = p_1p_2\cdots p_k = q_1q_2\cdots q_h$, con fattori p_i e q_j tutti primi.

Procediamo per induzione su k.
Se $k = 1$, allora $a = p_1$ è irriducibile e quindi anche $h = 1$ e $p_1 = q_1$.
Supponiamo che la scrittura sia unica per i prodotti di $k-1$ fattori irriducibili e proviamolo per i prodotti di k fattori irriducibili. Poiché p_k è primo e divide $q_1q_2\cdots q_h$, allora p_k divide uno dei q_i: possiamo supporre di riordinare i q_i in modo che p_k/q_h. Ma anche q_h è irriducibile e quindi $p_k = q_h$. Allora si ha $a = p_1p_2\cdots p_{k-1}p_k = q_1q_2\cdots q_{h-1}p_k$.

Mediante la cancellazione otteniamo $p_1p_2\cdots p_{k-1} = q_1q_2\cdots q_{h-1}$, che è un prodotto di $k-1$ fattori irriducibili. Dall'ipotesi induttiva segue che $k-1 = h-1$ (ossia $k = h$) e che, a meno dell'ordine, le due fattorizzazioni coincidono, ossia $p_1 = q_1, \ldots, p_{k-1} = q_{k-1}$. Avendo già provato che $p_k = q_k$, abbiamo dimostrato per intero l'unicità della fattorizzazione di a. $\diamond$

Un modo conveniente per scrivere la fattorizzazione di un intero a nel prodotto di fattori primi è quello di raccogliere mediante esponenti i fattori uguali, ottenendo scritture del tipo $a = p_1^{m_1}\cdots p_r^{m_r}$, dove i p_i sono primi distinti. L'esponente m_i si dice **molteplicità** di p_i in a.

Corollario 6.4.5. *In $\mathbb{Z}$ ci sono infiniti numeri primi.*

Dim: Supponiamo per assurdo che esistano solo un numero finito di primi $p_1, \ldots, p_r$.

L'intero $n = (p_1\cdots p_r) + 1$ non è divisibile esattamente per alcun p_i e quindi non è divisibile per alcun primo. Troviamo così un numero $\neq 0, 1, -1$ privo di fattori primi, in contrasto con quanto provato. $\diamond$

Si noti che la precedente è una vera dimostrazione per assurdo e non, come si potrebbe pensare, un metodo per costruire un ulteriore numero primo a partire da r primi assegnati. Ad esempio il numero $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1$ non è primo, ma si decompone nel prodotto di 59 e 509.

6.5 Esercizi

6.1. Provare mediante la definizione di $\mathbb{Z}$ come quoziente di $\mathbb{N} \times \mathbb{N}$ che il prodotto di due numeri positivi è positivo, il prodotto di due numeri negativi è positivo e il prodotto di un numero positivo per uno negativo è negativo.

6.2. Provare mediante la definizione di $\mathbb{Z}$ come quoziente di $\mathbb{N} \times \mathbb{N}$ che $\mathbb{Z}$ è un dominio di integrità.

6.3. Sia A un anello commutativo con identità 1_A. Provare per ogni $a, b \in A$ le seguenti relazioni (tra le quali la regoletta del "$- \times - = +$"):

a. $-(ab) = (-a)b = a(-b)$, $(-1_A)^2 = 1_A$, $(-a)^2 = a^2$, $(-a)(-b) = ab$,

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

c. $(-1_A)^n = 1_A$ se n è un intero pari e $(-1_A)^n = -1_A$ se n è un intero dispari.

6.4. Sia A un anello commutativo con identità. Provare che l'inverso di un elemento $a \in A$, se esiste, è unico.

6.5. Sia A un anello commutativo con identità. Provare che se u e v sono unità di A, anche uv e v^n, per ogni $n \in \mathbb{Z}$, lo sono.

6.6. Sia A un anello commutativo con identità e sia u un elemento invertibile di A. Provare che u è cancellabile ossia che $\forall a, b \in A : au = bu \Rightarrow a = b$.

6.7. Sia A un anello commutativo con identità. Provare l'equivalenza:

$$c \text{ è uno zero-divisore} \Leftrightarrow c \text{ non è cancellabile.}$$

6.8. Sia A un anello commutativo con identità e sia ρ la relazione $a\rho b$ se e solo se a e b sono associati.

- **a.** Provare che ρ è una relazione di equivalenza in A.
- **b.** Posto $A = \mathbb{Z}$, determinare $\mathbb{Z}/\rho$.
- **c.** È vero che $[a] + [b] = [a + b]$ è una operazione ben definita in $\mathbb{Z}/\rho$?

6.9. Sia A un anello commutativo con identità che possiede almeno un elemento invertibile $u \neq 1_A$. Provare che la relazione $a\sigma b$ se e solo se a/b non è nè una relazione d'ordine nè una relazione di equivalenza.

6.10. Siano A e B due anelli (oppure anelli commutativi con identità). Verificare che le operazioni definite componente per componente nel prodotto $A \times B$ soddisfano le proprietà di anello (rispettivamente: di anello commutativo con identità).

6.11. Generalizzare la definizione di anello prodotto ad un numero finito di anelli (anelli commutativi con identità) ed effettuare le necessarie verifiche.

6.12. Determinare la scrittura posizionale in base 7, 2 e 13 del numero (che nella abituale base 10 si scrive) 4581.
Scrivere nella abituale base 10 i numeri $(110101)_7$, $(110101)_2$, $(110101)_{13}$, dove l'indice indica la base usata.

6.13. Trovare il MCD di 39758 e di 54573 ed esplicitare l'identità di Bézout.

6.14. Determinare un numero $a \in \mathbb{Z}$ tale che $\{16h + 18k \mid h, k \in \mathbb{Z}\} = a\mathbb{Z}$, dove $a\mathbb{Z} = \{at \mid t \in \mathbb{Z}\}$.

6.15. Trovare il MCD e il mcm di 138788 e 62329, e quindi determinare un numero $a \in \mathbb{Z}$ tale che $\{138788\, x + 62329\, y \mid x, y \in \mathbb{Z}\} = a\mathbb{Z}$, dove $a\mathbb{Z} = \{at \mid t \in \mathbb{Z}\}$.

6.16. Determinare il MCD di 6120, 720 e 880.

6.17. Sia p un numero intero irriducibile. Provare che per ogni $a \in \mathbb{Z}$ si ha $MCD(a, p) = 1$ oppure $MCD(a, p) = p$.

6.18*. Siano $n_1, \ldots, n_r$ numeri interi non nulli. Definire il loro MCD e provare che esiste. Generalizzare l'algoritmo euclideo e l'identità di Bézout al caso di r numeri interi.

Capitolo 7

Gli anelli delle classi di resto

7.1 Definizione e prime proprietà di $\mathbb{Z}_n$

Sia n un intero fissato, $n \geq 2$.

Indichiamo con $n\mathbb{Z}$ l'insieme dei multipli interi di n, ossia $n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$. Possiamo associare a n (o a $n\mathbb{Z}$) la relazione di **congruenza modulo** n in $\mathbb{Z}$:

$$a \, R_n \, b \quad \text{se e solo se} \quad a - b \in n\mathbb{Z}.$$

Se $a \, R_n \, b$ si dice che a **è congruo a** b **modulo** n e si scrive $a \equiv b \bmod n$.
Un modo equivalente di esprimere la relazione di congruenza modulo n è la seguente:

$$a \equiv b \bmod n \quad \text{se e solo se} \quad \text{le divisioni di } a \text{ e di } b \text{ per } n \text{ hanno lo stesso resto } r.$$

Infatti, se $a = nq + r$ e $b = nq' + r$, allora $a - b = n(q - q') \in n\mathbb{Z}$; viceversa se $b = a + nt$ e $a = nq + r$, anche la divisione di b per n, ossia $b = n(q + t) + r$, ha lo stesso resto r.

La relazione di congruenza modulo n è una relazione di equivalenza in $\mathbb{Z}$. Il quoziente si dice **insieme delle classi di resto modulo** n (o delle classi di congruenza modulo n) e si indica abitualmente con $\mathbb{Z}_n$.

Lemma 7.1.1. i) *Se* $[a] \in \mathbb{Z}_n$, *allora* $[a] = \{a + nt \mid t \in \mathbb{Z}\}$.

ii) $\mathbb{Z}_n$ *ha esattamente* n *classi distinte. Più precisamente* $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Dim: La prima parte dell'asserto segue immediatamente dalla definizione di congruenza data inizialmente: $b \equiv a \bmod n$ se e solo se $b - a \in n\mathbb{Z}$ ossia se e solo se $b = a + nt$ con $t \in \mathbb{Z}$.

La seconda parte dell'asserto si ottiene ricordando che ogni classe di equivalenza $[a]$ è caratterizzata dal resto della divisione di a per n e che i resti possibili sono gli interi r tali che $0 \leq r < n$. $\diamond$

Possiamo definire in $\mathbb{Z}_n$ delle operazioni di somma e prodotto ponendo:

$$[a] + [b] = [a + b] \text{ e analogamente } [a] \cdot [b] = [ab].$$

Lasciamo come esercizio al lettore la verifica che queste operazioni sono ben definite, ossia che il risultato non dipende dai rappresentanti, e che con tali operazioni $\mathbb{Z}_n$ risulta essere un anello commutativo con $0_{\mathbb{Z}_n} = [0]$, $1_{\mathbb{Z}_n} = [1]$ e $-[a] = [-a]$.

Esempio 7.1.2. La prova del 9 *per una operazione tra numeri interi consiste nell'eseguire il calcolo in* $\mathbb{Z}_9$ *e controllare che il risultato trovato sia corretto come classe di* $\mathbb{Z}_9$*. Non è, quindi, un controllo del tutto sicuro, poiché non segnala eventuali errori che siano multipli interi di* 9*, ma in compenso è molto rapido.*

Ogni classe in $\mathbb{Z}_9$ *ha un rappresentante compreso tra* 0 *e* 8*, che si può velocemente calcolare seguendo il seguente procedimento.*

La scrittura posizionale in base 10 *di* a *è* $a = c_0 + 10c_1 + \cdots + 10^n c_n$*, dove le* c_i *sono cifre, ossia numeri compresi tra* 0 *e* 9*.*

Ma in $\mathbb{Z}_9$*, si ha* $[10^k] = [10]^k = [1]^k = [1^k] = [1]$ *e quindi, se* $a > 9$*:*

$$[a] = [c_0 + 10c_1 + \cdots + 10^n c_n] = [c_0] + [10][c_1] + \cdots + [10^n][c_n] = [c_0 + c_1 + \cdots + c_n] = [a_1]$$

con $0 \leq a_1 < a$*. Ripetendo il procedimento sui rappresentanti via via trovati, si perviene velocemente al rappresentante di* $[a]$ *compreso tra* 0 *e* 8*.*

I calcoli in $\mathbb{Z}_9$ *si riducono quindi a semplici calcoli tra numeri di* 1 *cifra che si possono eseguire velocemente anche a mente.*

Come potrebbe funzionare la prova del 10*? e la prova dell'*11*?*

Il risultato seguente caratterizza le unità e gli zero-divisori degli anelli $\mathbb{Z}_n$.

Proposizione 7.1.3. *Siano* $a, n \in \mathbb{Z}$*,* $n \geq 2$*. Allora:*

1) $[a]$ *è una unità in* $\mathbb{Z}_n \iff MCD(a, n) = 1$*;*

2) $[a]$ *è uno zero-divisore in* $\mathbb{Z}_n \iff MCD(a, n) > 1$*.*

Dim: 1) $[a]$ è una unità in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$ tale che $[a][b] = [ab] = [1]$ in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$ tale che $ab - 1 \in n\mathbb{Z} \iff \exists b, t \in \mathbb{Z}$ tali che $1 = ab + nt \iff MCD(a, n)/1$ (cfr. Lemma 6.3.10) $\iff MCD(a, n) = 1$.
2) $[a]$ è zero-divisore in $\mathbb{Z}_n \iff \exists [b] \in \mathbb{Z}_n$, $[b] \neq [0]$, tale che $[a][b] = [ab] = [0]$ in $\mathbb{Z}_n \iff \exists b \in \mathbb{Z}$, $0 < b < n$, tale che $ab \in n\mathbb{Z} \iff mcm(a, n) \leq ab < an \iff MCD(a, n) > 1$. $\diamond$

Ricordiamo ora la definizione di campo e una proprietà valida per ogni anello commutativo con identità:

Si dice che un anello commutativo con identità A è un **campo** se ogni elemento non nullo di A è una unità.

Lemma 7.1.4. *Sia* A *un anello commutativo con identità.*

i) *Se* u *è un elemento invertibile di* A*, allora* u *non è uno zero-divisore.*

ii) *Se* A *è un campo, allora* A *è un dominio di integrità.*

Dim: Proviamo che se u è invertibile e si ha $ub = 0_A$, allora necessariamente $b = 0_A$. Moltiplichiamo i due membri di $ub = 0_A$ per u^{-1}; si ottiene $b = 1_A \cdot b = u^{-1}ub = u^{-1} \cdot 0_A = 0_A$ ossia $b = 0_A$, come volevasi.

La seconda affermazione si ottiene subito dalla prima ricordando le definizioni di campo e di dominio. $\diamond$

Corollario 7.1.5. *Sia n un intero ≥ 2. Allora:*

$$\mathbb{Z}_n \text{ è un campo} \iff \mathbb{Z}_n \text{ è un dominio} \iff n \text{ è un numero primo.}$$

Dim: "$\mathbb{Z}_n$ è un campo $\Longrightarrow$ $\mathbb{Z}_n$ è un dominio" è un caso particolare del lemma precedente.

Per provare "$\mathbb{Z}_n$ è un dominio $\Longrightarrow$ n è un numero primo" basta ricordare che se n non è primo, allora è riducibile e osservare che i fattori di una sua fattorizzazione $n = ab$ corrispondono a classi $[a]$ e $[b]$ non nulle in $\mathbb{Z}_n$ ma tali che $[a][b] = [0]$ ossia a zero-divisori propri.

Infine "n è un numero primo $\Longrightarrow$ $\mathbb{Z}_n$ è un campo" si ottiene ricordando che ogni classe in $\mathbb{Z}_n$ è del tipo $[r]$ con $0 \leq r < n$; se n è primo, allora per ogni classe $[r]$ non nulla, ossia tale che $0 < r < n$, si ha $MCD(r, n) = 1$ e quindi $[r]$ è invertibile in $\mathbb{Z}_n$ (Proposizione 7.1.3). $\diamond$

Esempio 7.1.6. *In $\mathbb{Z}_{35}$ $[16]$ è invertibile poiché $MCD(16, 35) = 1$. Per determinarne l'inverso, calcoliamo (mediante l'algoritmo euclideo) l'identità di Bézout $1 = 16 \cdot (-24) + 35 \cdot 11$.*

In $\mathbb{Z}_{35}$ si ha allora $[16][-24] = [1]$ e quindi $[-24] = [16]^{-1}$.

Notiamo che i coefficienti dell'identità di Bézout non sono unicamente determinati; ad esempio si ha anche $1 = 16 \cdot 11 + 35 \cdot (-5)$; questo non contrasta con l'unicità dell'inverso poiché in $\mathbb{Z}_{35}$ si ha $[-24] = [11]$.

In $\mathbb{Z}_{35}$ $[15]$ è uno zero-divisore, poiché $MCD(15, 35) = 5 > 1$. Si ha infatti $[15][7] = [0]$, con $[7] \neq [0]$, avendo ottenuto 7 dalla divisione $35 : MCD(15, 35)$.

7.2 Congruenze e sistemi di congruenze lineari

Definizione 7.2.1. *Una congruenza lineare è una equazione in $\mathbb{Z}$ del tipo $aX \equiv b \bmod n$, con $a, b, n \in \mathbb{Z}$. Sono soluzioni della congruenza tutti i numeri interi x tali che $ax - b$ è multiplo di n.*

Risulta evidente dalla definizione che se x è soluzione della congruenza $aX \equiv b \bmod n$, anche $x + nt$ lo è, per ogni $t \in \mathbb{Z}$.

Risolvere la congruenza $aX \equiv b \bmod n$ equivale a risolvere in $\mathbb{Z}_n$ l'equazione lineare in una variabile $[a][X] = [b]$, oppure a risolvere in $\mathbb{Z} \times \mathbb{Z}$ l'equazione lineare in due variabili $aX + nY = b$.

Quest'ultimo modo di interpretare una congruenza lineare ci fornisce immediatamente il criterio per sapere se ammette soluzioni e, in caso affermativo, il metodo per calcolare le soluzioni stesse.

Teorema 7.2.2. *La congruenza lineare* $aX \equiv b \bmod n$ *ammette soluzioni se e solo se* $MCD(a, n)$ *divide* b.

Dim: L'asserto segue immediatamente dal Corollario 6.3.10. $\diamond$

Metodo risolutivo per le congruenze lineari. Se una congruenza lineare $aX \equiv b \bmod n$ soddisfa la condizione $MCD(a, n)/b$, possiamo dividere i coefficienti a, b, n per il $MCD(a, n)$ ottenendo una congruenza $a'X \equiv b' \bmod n'$ equivalente alla precedente (ossia con le stesse soluzioni) e tale che $MCD(a', n') = 1$.

Possiamo allora supporre $MCD(a, n) = 1$.

Risolviamo in $\mathbb{Z}_n$ l'equazione lineare $[a][X] = [b]$ moltiplicando i due membri per l'inverso $[c]$ di $[a]$ ($[c]$ esiste poiché $MCD(a, n) = 1$ e c può essere calcolato mediante l'algoritmo euclideo). In $\mathbb{Z}_n$ vi è l'unica soluzione $[bc]$.

L'insieme S delle soluzioni della congruenza è costituito da tutti i numeri $x \in \mathbb{Z}$ tali che $[x] = [bc]$ ed è quindi $S = \{bc + nt \mid t \in \mathbb{Z}\}$.

Osservazione 7.2.3. *Se* $MCD(a, n) = 1$*, l'insieme delle soluzioni di* $aX \equiv b \bmod n$ *è l'insieme* $x_0 + n\mathbb{Z} = \{x_0 + nt \mid t \in \mathbb{Z}\}$*, dove* x_0 *è una qualsiasi soluzione della congruenza. Per determinare tutte le soluzioni è quindi sufficiente conoscerne una qualsiasi.*

Osservazione 7.2.4. *Se* $MCD(a, n)/b$ *, la congruenza* $aX \equiv b \bmod n$ *è risolubile e il suo insieme delle soluzioni si può esprimere mediante una nuova congruenza con coefficiente direttivo* 1 *ossia del tipo* $X \equiv c \bmod m$*, dove* c *è una qualsiasi soluzione della congruenza e* $mMCD(a, n) = n$.

Definizione 7.2.5. *Un sistema di congruenze lineari è un sistema del tipo:*

$$\begin{cases} a_1X \equiv b_1 \bmod n_1 \\ a_2X \equiv b_2 \bmod n_2 \\ \cdots\cdots\cdots\cdots\cdots \\ a_kX \equiv b_k \bmod n_k \end{cases} \tag{7.1}$$

Sono soluzioni del sistema tutti i numeri $x \in \mathbb{Z}$ *che soddisfano contemporaneamente tutte le congruenze del sistema.*

Per risolvere un sistema di congruenze dovremo quindi determinare gli insiemi S_i delle soluzioni di ciascuna congruenza e poi la loro intersezione S, che in alcuni casi potrà anche essere $\emptyset$. La conoscenza di alcune proprietà generali permette, però, di semplificare talvolta il procedimento e di sapere in anticipo se e quante soluzioni un certo sistema avrà.

Procedimento risolutivo del sistema di congruenze lineari (13.3).

1) La risolubilità di ciascuna equazione è **una condizione necessaria** per la risolubilità del sistema (13.3). Se per ogni $i = 1, \ldots, k$, $MCD(a_i, n_i)/b_i$, allora ogni congruenza in (13.3) è risolubile; grazie all'Osservazione 7.2.4, il sistema (13.3) è equivalente ad un sistema più semplice della forma:

$$\begin{cases} X \equiv c_1 \bmod m_1 \\ X \equiv c_2 \bmod m_2 \\ \ldots\ldots\ldots\ldots\ldots \\ X \equiv c_k \bmod m_k \end{cases} \tag{7.2}$$

2) Se x_1 e x_2 sono due soluzioni di 7.2, allora per ogni $i = 1, \ldots, k$, $x - 1 - c_i$ e $x_2 - c_i$ sono entrambi multipli di m_i e quindi anche $x_1 - x_2$ è multiplo di m_i. Quindi $x - 1 - x_2$ è multiplo del minimo comune multiplo d di $m_1, \ldots, m_k$. Viceversa, se x_1 è una soluzione, allora anche $x_1 + td$ per ogni $t \in \mathbb{Z}$, è una soluzione del sistema. Se il sistema è risolubile, vi sarà allora una e una sola soluzione x_0 compresa tra 0 e $k-1$. Risolvere il sistema di congruenze si riduce allora alla ricerca di tale soluzione x_0. Tutte le soluzioni potranno allora esprimersi sotto forma di una congruenza $X \equiv x_0 \bmod d$.

3) Procediamo per induzione sul numero di congruenze nel sistema.

   Iniziamo a considerare il caso in cui il sistema sia costituito da due congruenze:

$$\begin{cases} X \equiv c_1 \bmod m_1 \\ X \equiv c_2 \bmod m_2 \end{cases} \tag{7.3}$$

   Poniamo $m' = mcm(m_1, m_2)$. Le soluzioni esistono se e solo se l'intersezione

$$\{c_1, c_1 + m_1, c_1 + 2m_1, \ldots, c_1 + (\frac{m'}{m_1} - 1)m_1\} \cap \{c_2, c_2 + m_2, c_2 + 2m_2, \ldots, c_2 + (\frac{m'}{m_2} - 1)m_2\}$$

   è non vuota (e in tal caso contiene un unico elemento, ossia la soluzione c').

4) Supponiamo di saper risolvere tutti i sistemi costituiti con $k - 1$, $k \geq 3$, congruenze ed esaminiamo il caso di un sistema con congruenze. In tal caso possiamo risolvere il sistema formato dalle prime due congruenze, sostituendo quindi ad esse le loro soluzioni scritte sotto forma di una congruenza del tipo $X \equiv c' \bmod m'$. Otteniamo in tal caso un nuovo sistema, equivalente al precedente, e con $k - 1$ congruenze.

Rimane aperta la questione dell'esistenza o meno delle soluzioni. In generale potremo sapere se le soluzioni di un sistema del tipo (7.3) esistono solo dopo aver cercato l'intersezione degli insiemi delle soluzioni delle due congruenze. Vi è però un caso in cui è possibile sapere a priori che le soluzioni esistono. Il risultato seguente fornisce infatti una condizione sufficiente per l'esistenza delle soluzioni.

Teorema 7.2.6. *Se $MCD(m_1, m_2) = 1$, allora:*

1) *il sistema di congruenze (7.3) è risolubile;*

2) *l'insieme delle soluzioni è $S = \{x_0 + m_1 m_2 t \mid t \in \mathbb{Z}\}$ dove x_0 è una qualsiasi soluzione;*

2) *una soluzione è $x_0 = c_1 m_2 r_2 + c_2 m_1 r_1$ dove r_2 è un rappresentante della classe inversa di $[m_2]$ in $\mathbb{Z}_{m_1}$ e r_1 è un rappresentante della classe inversa di $[m_1]$ in $\mathbb{Z}_{m_2}$.*

Dim: Iniziamo dal punto 3) (di cui il punto 1) è un'ovvia conseguenza).
Osserviamo per prima cosa che $[m_1]$ è invertibile in $\mathbb{Z}_{m_2}$, poiché $MCD(m_1, m_1) = 1$ (e analogamente $[m_2]$ in $\mathbb{Z}_{m_1}$).
Verifichiamo che x_0 è soluzione della prima congruenza del sistema (7.3) (la verifica relativa alla seconda congruenza è del tutto analoga): in $\mathbb{Z}_{m_1}$ si ha:

$$[x_0] = [c_1 m_2 r_2 + c_2 m_1 r_1] = [c_1 m_2 r_2] + [c_2 m_1 r_1] = [c_1 m_2 r_2] = [c_1][m_2][r_2] = [c_1]$$

dove l'ultima uguaglianza deriva dal fatto che, per costruzione, $[m_2][r_2] = [1]$ in $\mathbb{Z}_{m_1}$.

Per provare 2), infine, è sufficiente ricordare che, come già osservato, due soluzioni differiscono per un multiplo del minimo comune multiplo di , che in questo caso è proprio il loro prodotto, poichè m_1 e m_2 sono coprimi. $\diamond$

Grazie a quanto visto fino ad ora, possiamo enunciare il seguente criterio sufficiente per la risolubilità di un sistema del tipo più generale (13.3).

Teorema 7.2.7. *Siano a_i, b_i, n_i interi tali che $\forall i$, $1 \leq i \leq k$, si abbia $MCD(a_i, n_i) = 1$ e $\forall i, j$, $1 \leq i < j \leq k$, si abbia $MCD(n_i, n_j) = 1$. Allora:*

1) *il sistema di congruenze (13.3) è risolubile;*

2) *l'insieme delle soluzioni è $S = \{x_0 + n_1 n_2 \cdots n_k t \mid t \in \mathbb{Z}\}$ dove x_0 è una qualsiasi soluzione.*

NOTA BENE Le condizioni del precedente teorema sono condizioni sufficienti ma non necessarie per l'esistenza di soluzioni. In termini molto espliciti, tutti i sistemi che soddisfano tali condizioni hanno soluzioni; tra i sistemi che non le soddisfano, alcuni hanno soluzioni e altri no.

Quelli che seguono sono le traduzioni del precedente teorema nel linguaggio delle relazioni di congruenza e in quello degli anelli delle classi di resto $\mathbb{Z}_n$ e vanno sotto il nome di **Teorema cinese dei resti**.

Corollario 7.2.8. *Siano c_i, n_i, $i = 1, \ldots, k$, interi tali che $MCD(n_i, n_j) = 1$, per ogni i, j, $1 \leq i < j \leq k$.*

Esiste allora un intero x che è congruo a ciascun c_i modulo n_i.

Dim: Il numero x cercato è una soluzione del sistema 7.2. $\diamond$

Corollario 7.2.9. *Siano $n_1, \ldots, n_k$ interi ≥ 2 tali che $MCD(n_i, n_j) = 1$, per ogni i, j, $1 \leq i < j \leq k$. Allora l'applicazione:*

$$\alpha \colon \mathbb{Z}_{n_1 \cdots n_k} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

$$\alpha([x]_{n_1 \cdots n_k}) \;=\; ([x]_{n_1}, \ldots, [x]_{n_k})$$

è una applicazione biunivoca (che rispetta le operazioni).

Dim: Il dominio e il codominio di α hanno entrambi $n_1 \cdots n_k$ elementi. Per provare che α è biunivoca è allora sufficiente provare che è suriettiva.

Sia $([c_1]_{n_1}, \ldots, [c_k]_{n_k})$ un qualsiasi elemento del codominio; per trovare una classe $[x]$ tale che $\alpha([x]_{n_1 \cdots n_k}) = ([c_1]_{n_1}, \ldots, [c_k]_{n_k})$, è sufficiente scegliere una soluzione x del sistema (7.2). $\diamond$

7.3 La funzione di Eulero

Definizione 7.3.1. *Si chiama* **funzione di Eulero** *l'applicazione $\phi \colon \mathbb{N} \setminus \{0, 1\} \to \mathbb{N}$ data da $\phi(n) = Card\{k \in \mathbb{N} \mid 1 \leq k < n,\ MCD(n, k) = 1\}$, ossia $\phi(n)$ è il numero di interi tra 1 e $n - 1$ coprimi con n.*

La funzione di Eulero di un numero n coincide col numero di classi invertibili in $\mathbb{Z}_n$. Ad esempio, se p è un numero primo, $\phi(p) = p - 1$, poiché tutte le classi non nulle in $\mathbb{Z}_p$ sono invertibili.

Più in generale, se p^k è la potenza di un numero primo $\phi(p^k) = p^{k-1}(p - 1)$, poiché in $\mathbb{Z}_{p^k}$ sono invertibili tutte le classi tranne le p^{k-1} classi i cui rappresentanti compresi tra 0 e $p^k - 1$ sono i multipli di p, ossia $p \cdot 0$, $p \cdot 1$, $p \cdot 2$, $\ldots$, $p \cdot (p^{k-1} - 1)$.

Vediamo ora un metodo per calcolare il valore di $\phi(n)$ per ogni intero n a partire dalla fattorizzazione di n in fattori primi $p_1^{r_1} \cdots p_k^{r_k}$, con primi p_i tutti distinti.

Proposizione 7.3.2. (Moltiplicatività della funzione di Eulero) *Siano $p_1, \ldots, p_k$ primi distinti. Allora :*

$$\phi(p_1^{r_1} \cdots p_k^{r_k}) = \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k}) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_k^{r_k - 1}(p_k - 1).$$

Dim: La funzione α presentata nell'enunciato del Corollario 7.2.9 trasforma elementi invertibili di $\mathbb{Z}_n = \mathbb{Z}_{p_1^{r_1} \cdots p_k^{r_k}}$ in $k-$uple di elementi ciascuno dei quali è invertibile in $\mathbb{Z}_{p_i^{r_i}}$, e viceversa. Il numero di classi invertibili in $\mathbb{Z}_n$ coincide quindi col prodotto dei numeri di classi invertibili in $\mathbb{Z}_{p_i^{r_i}}$. $\diamond$

Terminiamo il capitolo sui numeri interi col seguente bel risultato.

Teorema 7.3.3. (Teorema di Eulero) *Siano a, n interi positivi tali che $MCD(a,n) = 1$.*

Allora $a^{\phi(n)} \equiv 1 \bmod n$.

Dim: La dimostrazione si articola in alcuni punti della cui prova diamo solo una breve traccia.

Sia p un numero primo.

I) $(x+y)^p \equiv x^p + y^p \bmod p$.

(Il coefficiente binomiale $\binom{p}{k} = \frac{p!}{k!\cdot(p-k)!}$ è multiplo di p per ogni k tale che $1 \leq k \leq p-1$.)

II) Piccolo teorema di Fermat. $a^p \equiv a \bmod p$.

(È sufficiente considerare gli interi $a \geq 0$. Per induzione su a. Se $a = 0$ è ovvio.

Se vale per $a-1$, allora $a^p = ((a-1)+1)^p \equiv (a-1)^p + 1^p \equiv (a-1)+1 = a \bmod p$.)

III) Se p è primo e $MCD(a,p) = 1$, allora $a^{p-1} \equiv 1 \bmod p$.

(In $\mathbb{Z}_p$ la classe di a è invertibile e quindi si può cancellare a nella relazione II.)

IV) Si generalizza al caso di un numero $n = p^r$ per induzione su r e la formula dello sviluppo della potenza $p-$esima di un binomio.

V) Si generalizza al caso di un numero qualsiasi usando la decomposizione in potenze di primi. Se $n = p^r t$, con $MCD(p,t) = 1$, allora $a^{\phi(n)} = a^{\phi(p^r)\phi(t)} \equiv 1^{\phi(t)} = 1 \bmod p^r$. Valendo questa relazione rispetto a tutti i primi nella decomposizione di n, allora vale anche modulo n.

$\diamond$

Esempio 7.3.4. *Consideriamo i due numeri $a = 2$ e $n = 7$ che sono coprimi. Poichè 7 è primo, si ha $\phi(7) = 7 - 1 = 6$.*

Verifichiamo il Teorema di Eulero in questo caso particolare mediante calcoli diretti:

$$2^6 = 64 = 7 \cdot 9 + 1 \ \textit{quindi}\ 64 \equiv 1 \bmod 7 \ \textit{ossia}\ 2^{\phi(7)} \equiv 1 \bmod 7.$$

Esempio 7.3.5. *Vogliamo calcolare la cifra x che indica le unità del numero 327^{81} scritta in forma posizionale.*

Anche un computer incontra grosse difficoltà ad eseguire questo calcolo e in ogni caso fornisce soltanto una approssimazione del risultato data dalle prime cifre a sinistra del numero accompagnate da una opportuna potenza di 10, non certo l'ultima cifra a destra.

Eseguiamo in altro modo questo calcolo facendo ricorso al Teorema di Eulero. Osserviamo che calcolare la cifra delle unità equivale a calcolare il resto della divisione per 10 ossia il numero x compreso tra 0 e 9 tale che $\overline{x} = \overline{327^{82}}$ in $\mathbb{Z}_{10}$.

Intanto $327 \equiv 7 \bmod 10$ quindi in $\mathbb{Z}_{10}$ si ha $\overline{x} = \overline{327}^{82} = \overline{7}^{82}$.
Ora, per il teorema di Eulero con $a = 7$, $n = 10$ e $\phi(n) = \phi(10) = 4$ vale la relazione

$7^{\phi(10)} = 7^4 \equiv 1 \bmod 10$. *Quindi* $\overline{x} = \overline{7}^{82} = \overline{7}^{80+2} = (\overline{7}^4)^{20} \cdot \overline{7^2} = \overline{1}^{20} \cdot \overline{49} = \overline{9}$.
La cifra finale di 327^{82} *è quindi* 9.

Esempio 7.3.6. *Vogliamo trovare le ultime due cifre decimali (ossia decine e unità) di* 3^{925}. *Le ultime due cifre decimali corrispondono al resto della divisione per* 100. *Come nell'esempio precedente usiamo il Teorema di Eulero:*

$$a^{\phi(100)} \equiv 1 \bmod 100.$$

Ora $\phi(100) = \phi(25 \cdot 4) = \phi(5^2 \cdot 2^2) = 5(5-1)2(2-1) = 40$ *dunque* $3^{40} \equiv 1 \bmod 100$.
Inoltre $925 = 40 \cdot 23 + 5$ *e quindi*

$$\overline{3}^{950} = \overline{3}^{23 \cdot 40 + 5} = (\overline{3}^{40})^{23} \cdot \overline{3}^5 = \overline{1} \cdot (\overline{3}^5) = \overline{243} = \overline{43}.$$

7.4 Crittografia

La **crittografia**, dal greco $\chi\rho\iota\pi\tau o\sigma$ = nascosto e $\gamma\rho\alpha\varphi\epsilon\iota\nu$ = scrivere, è lo studio dei metodi per garantire la segretezza del contenuto di un messaggio anche nel caso sia intercettato.

Un metodo crittografico ideale dovrebbe permettere al mittente di crittografare con molta facilità i messaggi e dovrebbe inoltre assicurare che solo il destinatario designato possa decifrarli con facilità.

Pur essendo una pratica antichissima (si trovano esempi già nei geroglifici egiziani e nella Bibbia), la crittografia è maturata definitivamente a rango di scienza solo nei primi del 1900 con l'avvento di nuove teorie e tecniche matematiche.

Attualmente è entrata a far parte della nostra vita quotidiana, poichè ne fanno uso tessere Bancomat, telefoni cellulari, trasmissioni televisive, internet e in genere ogni strumento di comunicazione elettronica.

Il cifrario di Cesare

Anche Giulio Cesare era solito cifrare i messaggi usando il metodo di **sostituzione**; ad ogni lettera dell'alfabeto ne faceva corrispondere un'altra traslata di un certo numero di posizioni. Se usiamo la chiave 3 tutte le lettere vengono scalate di 3 posizioni, quindi in corrispondenza del vecchio alfabeto troviamo il nuovo

A	B	C	D	E	F	G	H	$\ldots$	U	V	Z
U	V	Z	A	B	C	D	E	$\ldots$	R	S	T

Questa tabella è la **chiave** usata per la cifratura ed è la stessa che viene usata per la decifratura; si rende quindi necessaria una precedente comunicazione tra le due parti al fine di scambiarsi questa informazione. Nella necessità di un accordo preliminare sta una delle principali debolezze di questo e di ogni altro metodo crittografico ''vecchio stile'', perché anche la comunicazione iniziale corre il rischio di essere intercettata.

Possiamo generalizzare il metodo di Cesare ricorrendo alle classi di resto, così da ottenere permutazioni che non solo traslano, ma ''rimescolano'' le lettere e che sono anche facilmente ottenibili dalle due parti.

Associamo ad ogni lettera dell'alfabeto un numero da 1 a 21, o meglio una classe di resto modulo 21.

Fissati poi due numeri interi a e b (**i parametri di cifratura**) otteniamo la lettera che sostituirà la lettera individuata dalla classe $\overline{x}$ come quella individuata da $\overline{y}$ dove

$$y = ax + b$$

(in pratica basta eseguire il calcolo $ax + b$, dividere per 21 e prendere il resto y.)

Esempio 7.4.1. *Usiamo la chiave di cifratura* $y = 5x + 1$.
La lettera ***A*** *corrisponde a* $\overline{x} = \overline{1}$ *e quindi sarà sostituita dalla* ***F*** *corrispondente a* $\overline{y} = \overline{5 \cdot 1 + 1} = \overline{6}$.
La lettera ***H*** *corrisponde a* $\overline{x} = \overline{8}$ *e quindi sarà sostituita dalla* ***V*** *corrispondente a* $\overline{y} = \overline{5 \cdot 8 + 1} = \overline{41} = \overline{20}$.

Potremmo costruire in questo modo tutta la tabella della sostituzione ottenendo una ***permutazione delle lettere****. Chi deve decifrare può costruirsi l'intera tabella delle corrispondenze e usarla a rovescio, oppure può usare la formula inversa:* $x = 17y + 4$.

La lettera ***F*** *che corrisponde a* $\overline{y} = \overline{6}$ *deve essere decifrata come* ***A*** *corrispondente a* $\overline{x} = \overline{17 \cdot 6 + 4} = \overline{106} = \overline{1}$ *e così via.*

Esempio 7.4.2. *Usiamo ora una differente chiave di cifratura:* $y = 3x + 1$.
La lettera ***A*** *corrisponde a* $\overline{x} = \overline{1}$ *e quindi sarà sostituita dalla* ***D*** *corrispondente a* $\overline{y} = \overline{3 \cdot 1 + 1} = \overline{4}$.
La lettera ***H*** *corrisponde a* $\overline{x} = \overline{8}$ *e quindi sarà sostituita dalla* ***D*** *corrispondente a* $\overline{y} = \overline{3 \cdot 8 + 1} = \overline{25} = \overline{4}$.

Questa seconda chiave scelta non va bene perchè ***A*** *e* ***H*** *sono crittografate entrambe come* ***D****. Chi legge* ***D*** *non sa se interpretare come* ***A*** *o come* ***H****.*

Si pone allora naturale una domanda: quali formule del tipo $y = ax + b$ vanno bene?

La risposta sta nella chiave di decifratura $x = cy + d$; se una tale chiave esiste allora lettere diverse devono sicuramente essere state codificate mediante lettere diverse.

Se usiamo la chiave di cifratura $y = ax + b$, quali numeri c e d forniscono la chiave di decifratura $x = cy + d$?

Devono essere scelti in modo che la doppia sostituzione $x \mapsto ax + b \mapsto c(ax + b) + d$ dia sempre come risultato x stesso, almeno come classe di resto modulo 21 ossia $\overline{x} =$

$\overline{c(ax+b)+d}$. Svolgendo i calcoli otteniamo le relazioni:

$$\begin{cases} ca \equiv 1 \mod 21 \\ cb \equiv -d \mod 21 \end{cases}$$

La prima relazione dice che $\overline{c}$ deve essere l'inverso di $\overline{a}$ in $\mathbb{Z}_{21}$; trovato c, le seconda relazione dice che $\overline{d}$ sarà $\overline{-cb}$. Condizione necessaria e sufficiente perchè esista la chiave di decifratura è che $\overline{a}$ sia invertibile in $\mathbb{Z}_{21}$.

La risposta alla domanda precedente è quindi:

per avere una buona chiave di cifratura bisogna scegliere a in modo che esista $\overline{a}^{-1}$ in $\mathbb{Z}_{21}$.

Per quanto visto relativamente alle classi di resto, la condizione che a deve soddisfare è $MCD(a,n)=1$ e il numero di possibili scelte di una siffatta classe in $\mathbb{Z}_n$ è data dalla funzione di Eulero $\phi(n)$.

Il codice RSA

Il Teorema di Eulero è alla base di un metodo crittografico particolarmente ingegnoso che risolve il problema della segretezza nello scambio delle "chiavi" tra il mittente e il destinatario. I metodi crittografici **a chiave pubblica** non richiedono lo scambio di comunicazioni riservate in alcun momento tra mittente e destinatario. Nel seguito tutte le comunicazioni tra i due soggetti si intenderanno come disponibili a chiunque; ad esempio possono avvenire mediante pubblicazione su un giornale oppure su un sito internet completamente accessibile.

La prima metodologia crittografica di questo genere fu sviluppata nel 1978 da tre ricercatori: Ronald Rivest, Adi Shamir e Leo"RSA".
L'idea di base del codice RSA è la constatazione di quanto sia facile moltiplicare tra loro due numeri dati e di quanto sia invece difficile (o meglio calcolativamente lungo) risalire ai fattori dato il prodotto.

In teoria chiunque può decifrare un messaggio crittografato mediante il codice RSA, ma il tempo richiesto per la decifrazione è tanto da rendere il messaggio ormai privo di interesse. Il diretto destinatario possiede invece un metodo di decifratura molto veloce. Vediamo come questa ''doppia velocità'' possa essere praticamente realizzata.

Ci si accorda (pubblicamente!) su come trasformare i messaggi in sequenze di numeri ciascuno di lunghezza prefissata: sia m uno di questi numeri.

Il **destinatario** del messaggio prepara la chiave di decifrazione nel modo seguente:

- Costruisce un numero n moltiplicando due numeri primi p e q abbastanza grandi in modo che p e q siano sicuramente maggiori di m (e tra l'altro il resto della divisione per n di ogni numero m' congruo a m modulo n sia m stesso). Poichè il destinatario sa che $n=pq$, egli può facilmente calcolare la funzione di Eulero $\phi(n)=(p-1)(q-1)$.

- Il destinatario sceglie inoltre un altro numero h coprimo con $\phi(n)$ e calcola l'inverso $\overline{d}$ di $\overline{h}$ in $\mathbb{Z}_{\phi(n)}$, ossia calcola d tale che $hd = 1 + k\phi(n)$.

- Egli, infine, rende pubblici i due numeri n e h, mentre mantiene il più assoluto segreto sulla fattorizzazione $n = pq$, sul valore di $\phi(n)$ e su d.

Il **mittente** adopera queste informazioni, ossia n e h, per crittografare il messaggio m nel modo seguente:

- Calcola la potenza m^h e la divide per n ottenendo un resto c; comunica (pubblicamente) al destinatario il numero c che è il messaggio cifrato. La relazione tra il messaggio originale e la sua cifratura è data da:

$$c \equiv m^h \bmod n \quad \text{ovvero} \quad \overline{c} = \overline{m}^h \quad \text{in} \quad \mathbb{Z}_n.$$

- Il destinatario decodifica il messaggio con l'aiuto del numero d calcolando la potenza c^d e dividendola per n. Il resto della divisione è proprio il messaggio originale. Si ha infatti:

$$\overline{c}^d = \overline{m}^{hd} = \overline{m}^{1+k\phi(n)} = \overline{m} \cdot (\overline{m}^k)^{\phi(n)} = \overline{m} \cdot \overline{1} = \overline{m}.$$

Come si può vedere nell'ultimo passaggio la validità del Teorema di Eulero sta alla base di questa procedura. Infatti è grazie a tale risultato che possiamo affermare che $(\overline{m}^k)^{\phi(n)} = \overline{1}$. Notiamo che le ipotesi del teorema possono essere facilmente soddisfatte, operando se necessario piccole modifiche sul messaggio iniziale m in modo da renderlo coprimo con n.

A titolo di curiosità diciamo che i primi attualmente adoperati per l'RSA hanno un numero di cifre dell'ordine delle centinaia e che il metodo viene considerato del tutto sicuro. In un esperimento del 1994 per ''rompere'' una chiave RSA di 129 cifre, (ossia per fattorizzare un numero n di 129 cifre), sono stati necessari 8 mesi di lavoro coordinato effettuato da 600 gruppi di ricerca sparsi in 25 paesi, che hanno messo a disposizione 1600 computers, facendoli lavorare in parallelo collegati tra loro attraverso Internet!

Esempio 7.4.3. *Eseguiamo una simulazione di codifica e decodifica di un messaggio mediante RSA. Il destinatario del messaggio, chiamiamola Francesca, ha scelto i due primi* 5 *e* 11 *e li ha moltiplicati ottenendo* 55*. Perchè questa simulazione con numeri così piccoli abbia senso dobbiamo fingere che nessuno (a parte Francesca) sia in grado di calcolare in tempi brevi la fattorizzazione di* 55*.*

Francesca ha calcolato $\phi(55) = (5-1)\cdot(11-1) = 40$*, ha scelto* $h = 3$ *coprimo con* 40 *e ha determinato (mediante l'algoritmo euclideo) un numero* d *tale che* $dh \equiv 1 \bmod 40$*, ottenendo* $d = 27$ *(poichè* $3 \cdot 27 = 1 + 2 \cdot 40$*).*

Francesca comunica poi pubblicamente, a tutti coloro che vogliono scriverle in modo riservato, i due numeri $n = 55$ *e* $h = 3$*.*

Paolo vuole mandarle il messaggio $m = 7$*: calcola:* $m^h = 7^3 = 343$*, lo divide per* 55 *e ottiene il resto* $c = 13$ *che spedisce a Francesca. Nessuno è in grado di decodificare il messaggio* $c = 13$ *tranne Francesca che possiede la chiave di decifrazione* $d = 27$*.*

Francesca calcola allora 13^{27} *e quindi divide per* 55 *ottenendo il resto* 7 *che è il messaggio "in chiaro".*

Si noti che Francesca non deve necessariamente calcolare per intero la potenza 13^{27} *prima di eseguire la divisione per* 55*, ma può lavorare nelle classi di resto* $\mathbb{Z}_{55}$ *nel modo seguente:*

$$\overline{13}^{27} = (\overline{13}^3)^9 = \overline{52}^9 = \overline{-3}^9 = \overline{-19683} = \overline{-48} = \overline{7}.$$

7.5 Esercizi

7.1. Consideriamo $\mathbb{Z}_{54}$, l'anello delle classi di resto modulo 54.

- **a.** Trovare un intero n, $0 \leq n < 54$, tale che $[n] = [125]$. Ne esiste più d'uno?
- **b.** Esiste un intero pari nella classe di 125?
- **c.** Esiste un intero multiplo di 3 nella classe di 125?
- **d.** Sia m un intero fissato. Provare che esiste almeno un intero s, con $100 \leq s \leq 200$, tale che $[m] = [s]$.

7.2. Determinare esplicitamente l'insieme delle potenze della classe di 2 in $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$ e $\mathbb{Z}_{16}$.

7.3. Sia I l'insieme dei multipli di $[4]$ in $\mathbb{Z}_{18}$.

- **a.** Considerare la relazione di equivalenza in $\mathbb{Z}_{18}$: $[a] \sim [b]$ se e solo se $[a] - [b] \in I$. Quante sono le classi di equivalenza?
- **b.** Determinare esplicitamente l'insieme dei multipli di $[10]$ in $\mathbb{Z}_{18}$.
- **c.** Verificare che $[10] \cdot [13] = [10] \cdot [4]$ in $\mathbb{Z}_{18}$. È vero che $[13] = [4]$?

7.4. Provare che in $\mathbb{Z}_6$ $[2]$ è un elemento primo. Verificare l'uguaglianza $[2] = [-2] \cdot [2]$. È vero che $[2]$ in quanto elemento primo è anche irriducibile?

7.5. Nell'anello $\mathbb{Z}_{24}$:

- **a.** determinare tutti gli elementi invertibili e le loro classi;
- **b.** determinare tutti gli zero-divisori;
- **c.** trovare tutti gli elementi $[b]$ tali che $[b] \cdot [16] = [0]$.
- **d.** Provare che $[5^k]$ è invertibile in $\mathbb{Z}_{24}$ per ogni $k \in \mathbb{N}$. Possiamo allora dire che gli elementi invertibili di $\mathbb{Z}_{24}$ sono infiniti?

7.6. Dire se le seguenti equazioni hanno soluzioni intere:

$$35\,x + 84\,y = 6 \qquad 35\,x + 84\,y + 12\,z = 1975 \qquad 49\,x + 168\,y = 14.$$

7.7. L'equazione $[3522] \cdot [x] = [1]$ ha soluzioni in $\mathbb{Z}_{500}$?

7.8. Trovare un intero n tale che $([n]_4, [n]_9) = ([3]_4, [7]_9)$ in $\mathbb{Z}_4 \times \mathbb{Z}_9$. Ne esiste più d'uno?

7.9. Sia A l'anello prodotto $\mathbb{Z}_4 \times \mathbb{Z}_6$.

a. Verificare che $([1]_4, [2]_6)$ è uno zero-divisore e che

b. Verificare che $([1]_4, [5]_6)$ è una unità.

c. Trovare l'insieme degli elementi del tipo $6x$ (ossia $x + \cdots + x$, 6 volte) al variare di x in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

d. Trovare l'insieme degli elementi del tipo $6x$ (ossia $x + \cdots + x$, 6 volte) al variare di x in $\mathbb{Z}_{24}$.

e. Provare che non esiste alcuna applicazione biunivoca $f\colon A \to \mathbb{Z}_{24}$ tale che $f(x+y) = f(x) + f(y)$.

f. Determinare l'insieme dei multipli di $([2]_4, [2]_6)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

7.10. Risolvere le congruenze:

$$3x \equiv 7 \bmod 11 \qquad 8x \equiv 18 \bmod 30 \qquad 9x \equiv 12 \bmod 20$$

$$2x \equiv 11 \bmod 13 \qquad 8x \equiv 4 \bmod 10 \qquad 4x \equiv 7 \bmod 15$$

7.11. Provare che l'applicazione $f\colon \mathbb{Z}_{18} \to \mathbb{Z}_6$ data da $f([n]_{18}) = [n]_6$ è ben definita e rispetta le operazioni. Determinare $f^{-1}([0]_6)$ e $f^{-1}([1]_6)$.

7.12. Determinare tutti gli elementi invertibili e tutti gli zero-divisori di $\mathbb{Z} \times \mathbb{Z}_6$ dotato delle operazioni componente per componente.

7.13. Esiste un intero a tale che la sua classe sia l'inversa della classe di 3 sia in $\mathbb{Z}_{16}$, sia in $\mathbb{Z}_{35}$?

7.14. Verificare che l'applicazione $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ data da $\phi(a) = [a]$ rispetta le operazioni di somma e prodotto.

a. Provare che $\phi^{-1}([0]) = n\mathbb{Z}$.

b. Più in generale, verificare che $\phi^{-1}([a]) = a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$.

7.15. Provare che esiste un intero $a \in \mathbb{Z}$ (e determinarlo) tale che $18\mathbb{Z} \cap 24\mathbb{Z} = a\mathbb{Z}$.

7.16. Provare che in $\mathbb{Z}_4 \times \mathbb{Z}_2$ con le operazioni definite componente per componente ogni elemento è una unità oppure uno zero-divisore.

7.17. Siano n ed m due interi non nulli. Provare che in $\mathbb{Z}_n \times \mathbb{Z}_m$ ogni elemento è una unità oppure uno zero-divisore.

7.18. Mostrare che risolvere la congruenza $2x^2 \equiv 3x \bmod 11$ è un problema equivalente a risolvere l'equazione $[2]X^2 = [3]X$ in $\mathbb{Z}_{11}$, precisando anche in che senso si deve intendere l'equivalenza. Determinare tutti gli elementi di $\mathbb{Z}_{11}$ che soddisfano l'equazione $[2]X^2 = [3]X$ (mediante sostituzione diretta di ciascun elemento); dedurne quindi l'insieme delle soluzioni della congruenza $2x^2 \equiv 3x \bmod 11$.

7.19. Alla luce dell'esercizio precedente, determinare tutte le soluzioni delle seguenti congruenze non lineari:

$$2x^2 \equiv x \bmod 11 \qquad x^3 \equiv 4x \bmod 7 \qquad 2x^2 - 1 \equiv 5x \bmod 6$$

$$2x^3 \equiv 3x^2 \bmod 5 \qquad 2x^3 \equiv 1 + x \bmod 9 \qquad x^3 - 2x^2 \equiv 0 \bmod 10$$

7.20. Risolvere i seguenti sistemi di congruenze lineari:

$$\begin{cases} x \equiv 7 \bmod 11 \\ x \equiv 18 \bmod 30 \end{cases} \qquad \begin{cases} 3x \equiv 7 \bmod 11 \\ 8x \equiv 18 \bmod 30 \end{cases} \qquad \begin{cases} 6x \equiv 14 \bmod 22 \\ 8x \equiv 18 \bmod 30 \end{cases}$$

7.21. Provare che il seguente sistema di congruenze lineari non ha soluzioni:

$$\begin{cases} 2x \equiv 3 \bmod 5 \\ \\ x \equiv 3 \bmod 10 \end{cases}$$

7.22. Dire se il seguente il seguente sistema di congruenze lineari ha soluzioni ed in caso affermativo determinarle:

$$\begin{cases} 3x \equiv 3 \bmod 10 \\ \\ 2x \equiv 4 \bmod 15 \end{cases}$$

7.23. Risolvere i sistemi di congruenze lineari seguenti

$$\begin{cases} x \equiv 6 \bmod 11 \\ 3x \equiv 2 \bmod 8 \end{cases} \quad \begin{cases} 4x \equiv 6 \bmod 10 \\ 2x \equiv 5 \bmod 7 \end{cases} \quad \begin{cases} 5x \equiv 4 \bmod 12 \\ 11x \equiv 1 \bmod 20 \end{cases}$$

$$\begin{cases} 8x \equiv 3 \bmod 13 \\ 8x \equiv 6 \bmod 12 \end{cases} \quad \begin{cases} 4x \equiv 2 \bmod 6 \\ 10x \equiv 11 \bmod 25 \end{cases} \quad \begin{cases} 2x \equiv 7 \bmod 9 \\ 8x \equiv 6 \bmod 12 \end{cases}$$

7.24. Risolvere i seguenti sistemi di congruenze lineari

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 5 \bmod 7 \\ x \equiv 1 \bmod 11 \end{cases} \quad \begin{cases} 2x \equiv 3 \bmod 5 \\ 5x \equiv 2 \bmod 7 \\ x \equiv 1 \bmod 12 \end{cases} \quad \begin{cases} 4x \equiv 2 \bmod 6 \\ 3x \equiv 1 \bmod 5 \\ 4x \equiv 1 \bmod 13 \end{cases}$$

7.25. Fornire un esempio di sistema di congruenze lineari che non ammette nessuna soluzione.

7.26. Fornire un esempio esplicito di sistema di congruenze lineari per il quale non siano soddisfatte le ipotesi del Teorema cinese, ma che ammetta ugualmente soluzioni.

7.27. Determinare tutti gli interi n per i quali il sistema $\begin{cases} 2x \equiv 3 \bmod 15 \\ 3x \equiv n \bmod 12 \end{cases}$ ammette soluzioni.

7.28. Determinare tutti gli interi n per i quali il sistema $\begin{cases} 5x \equiv -1 \bmod 24 \\ 10x \equiv n \bmod 18 \end{cases}$ non ammette soluzioni.

7.29. Determinare tutti gli interi n per i quali il sistema $\begin{cases} 5x \equiv -1 \bmod 24 \\ 10x \equiv 3 \bmod n \end{cases}$ non ammette soluzioni.

7.30. Calcolare $\phi(36)$, $\phi(528)$ e $\phi(121)$, dove ϕ è la funzione di Eulero.

7.31. Determinare la cifra delle unità del numero 3477^{159}.

7.32. Determinare il numero n, $0 \leq n < 7$, tale che $[n] = [857342^{124}]$ in $\mathbb{Z}_7$.

7.33. Determinare il nucleo e l'immagine dell'applicazione $f\colon \mathbb{Z}_{24} \to \mathbb{Z}_6 \times \mathbb{Z}_4$ data da $f([x]_{24}) = ([x]_6, [x]_4)$.

7.34. Determinare il nucleo e l'immagine dell'applicazione $g\colon \mathbb{Z}_{24} \to \mathbb{Z}_3 \times \mathbb{Z}_8$ data da $f([x]_{24}) = ([x]_3, [x]_8)$.

Capitolo 8

Il campo $\mathbb{Q}$ dei numeri razionali

8.1 Costruzione dell'insieme dei numeri razionali

Definizione 8.1.1. *Consideriamo il prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}^*$ delle coppie di numeri interi (n, m) tali che $m \neq 0$ ed in esso la relazione:*

$$(n, m)\ \rho\ (n', m') \iff nm' = n'm.$$

Si dice insieme dei numeri razionali $\mathbb{Q}$ l'insieme quoziente $(\mathbb{Z} \times \mathbb{Z}^*)/\rho$.

Verifichiamo che tale definizione ha senso, ossia che ρ è effettivamente una relazione di equivalenza.

Le proprietà riflessiva e simmetrica sono ovvie; controlliamo soltanto la validità della proprietà transitiva.

T) Supponiamo che $(n, m)\rho(n', m')$ e che $(n', m')\rho(n'', m'')$ ossia che valgano le due uguaglianze $nm' = n'm$ e $n'm'' = n''m'$. Moltiplichiamo i due membri della prima uguaglianza per m'' e i due membri della seconda per m; otteniamo così le uguaglianze $nm'm'' = n'mm''$ e $n'm''m = n''m'm$ da cui $nm'm'' = n''m'm$. Poiché per costruzione m' è non nullo, possiamo cancellare m' ottenendo $nm'' = n''m$ e quindi $(n, m)\rho(n'', m'')$.

Ogni classe di equivalenza $[(n, m)]$ si dice **numero razionale** e si denota abitualmente sotto forma di **frazione** $\frac{n}{m}$. Il numero intero n si dice **numeratore** e il numero intero m si dice **denominatore**; numeratore e denominatore sono caratteristiche di una frazione ossia di un particolare rappresentante della classe e non della classe di equivalenza. Osserviamo che in ogni classe di equivalenza $[(n, m)]$ si trovano infinite coppie (ad esempio tutte le coppie (nt, mt) al variare di t in $\mathbb{Z}$) e tra queste una speciale (n', m') tale che n' e m' sono coprimi e $m' > 0$, che si dice **frazione ridotta**.

Proposizione 8.1.2. *Ogni numero razionale $\frac{n}{m}$ ha una e una sola rappresentazione come frazione ridotta.*

Dim: Moltiplicando, se necessario, numeratore e denominatore per -1, possiamo supporre intanto $m > 0$. Sia $t = MCD(m, n)$; allora $m = tm'$, $n = tn'$ e $MCD(n', m') = 1$. Otteniamo così una rappresentazione ridotta $\frac{n'}{m'}$ di $\frac{n}{m}$.

Supponiamo che $\frac{n''}{m''}$ sia un'altra rappresentazione ridotta di $\frac{n}{m}$; allora $\frac{n'}{m'} = \frac{n''}{m''}$ e quindi $n'm'' = n''m'$ in $\mathbb{Z}$. Per ipotesi m'' non ha nessun fattore in comune con n'' e quindi, per l'unicità della fattorizzazione in $\mathbb{Z}$, m''/m'; per lo stesso motivo m'/m'' e quindi m' e m'' sono associati in $\mathbb{Z}$: essendo m' e m'' entrambi positivi, coincidono. Semplificando in $n'm'' = n''m'$, si ottiene poi che anche n' e n'' coincidono. $\diamond$

Corollario 8.1.3. *Se $\frac{n}{m}$ è la rappresentazione come frazione ridotta del numero razionale x, allora ogni altra frazione che rappresenta x è del tipo $\frac{nt}{mt}$, con $t \in \mathbb{Z}$.*

Possiamo definire le operazioni somma e prodotto in $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\rho$ a partire dalle operazioni di $\mathbb{Z}$, nel modo seguente:

$$[(n, m)] + [(n', m')] = [(nm' + n'm, mm')] \quad \text{e} \quad [(n, m)] \cdot [(n', m')] = [(nn', mm')].$$

Possiamo inoltre definire in $\mathbb{Q}$ un ordine totale nel modo seguente:

$[(n, m)] \leq [(n', m')]$ se, scelti i rappresentanti in modo che $mm' > 0$, in $\mathbb{Z}$ si ha $nm' \leq n'm$.

Verifichiamo che la somma è **ben definita** ossia che il risultato non dipende dai rappresentanti.
Calcoliamo la somma $x + y$ di due numeri razionali usando due diverse frazioni per rappresentare x e due diverse frazioni per rappresentare y e proviamo che il risultato non cambia.
Siano $x = \frac{n}{m} = \frac{n'}{m'}$ e $y = \frac{a}{b} = \frac{a'}{b'}$. Allora per definizione risulta $nm' = n'm$ e $ab' = a'b$ in $\mathbb{Z}$. Calcoliamo $x + y = \frac{n}{m} + \frac{a}{b} = \frac{nb+am}{mb}$ e $x + y = \frac{n'}{m'} + \frac{a'}{b'} = \frac{n'b'+a'm'}{m'b'}$, ma in $\mathbb{Z}$ risulta (utilizzando le uguaglianze precedenti)

$$(nb + am)m'b' = nm'bb' + mm'ab' = n'mbb' + mm'a'b = (n'b' + a'm')mb$$

e quindi $\frac{nb+am}{mb} = \frac{n'b'+a'm'}{m'b'}$, ossia $\frac{n}{m} + \frac{a}{b} = \frac{n'}{m'} + \frac{a'}{b'}$.

Lasciamo per esercizio al lettore (in quanto analoghe alla precedente) le verifiche che il prodotto e la relazione d'ordine sono ben definite e le dimostrazioni delle seguenti proprietà.

Proposizione 8.1.4. *$\mathbb{Q}$ dotato delle operazioni di somma e di prodotto è un* **campo** *ossia è un anello commutativo con identità $1_{\mathbb{Q}} = \frac{1}{1}$ in cui ogni elemento $\frac{n}{m}$ non nullo (ossia diverso da $0_{\mathbb{Q}} = \frac{0}{1}$) ammette inverso $\frac{m}{n}$.*

Inoltre $\mathbb{Q}$ è un **campo ordinato** *(la relazione d'ordine $\leq$ rispetta le operazioni ossia le diseguaglianze si conservano se si somma ai due membri un qualsiasi numero razionale oppure se si moltiplicano i due membri per un qualsiasi numero razionale positivo).*

Proposizione 8.1.5. *L'applicazione* $i\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ *data da* $i(p) = \frac{p}{1}$ *è iniettiva e rispetta le operazioni e l'ordinamento ossia:*

1) $i(p+q) = i(p) + i(q)$;

2) $i(pq) = i(p) \cdot i(q)$;

3) $p \leq q$ *in* $\mathbb{Z} \Leftrightarrow i(p) \leq i(q)$ *in* $\mathbb{Q}$.

Grazie alla Proposizione 8.1.5 potremo identificare i numeri interi relativi con i numeri razionali in cui il denominatore divide il numeratore e pensare $\mathbb{Z}$ (identificato con $i(\mathbb{Z})$) come un sottoanello di $\mathbb{Q}$. Questa immersione rende $\mathbb{Z}$ un sottoinsieme proprio di $\mathbb{Q}$, anche se i due insiemi hanno la stessa cardinalità.

Infine il campo $\mathbb{Q}$ gode della **proprietà di densità** rispetto all'ordine $\leq$:

tra due numeri razionali distinti si trovano sempre altri (infiniti altri) numeri razionali.

Se infatti $x, y \in \mathbb{Q}$ e $x < y$, allora $x < \frac{1}{2}(x+y) < y$ (o più generalmente $x < x + \frac{n}{m}(y-x) < y$ per ogni $0 < n < m$.

8.2 La notazione posizionale dei numeri razionali

Introduciamo ora la notazione posizionale dei numeri razionali a partire da quella dei numeri interi e, nuovamente, facendo ricorso alla divisione con resto.

Ci sarà utile la seguente

Definizione 8.2.1. *La parte intera* d *di* x *è il più grande numero intero minore o uguale ad* x.

Se $x = \frac{a}{b}$ con $b > 0$, la divisione con resto di a per b dà $a = bq + r$ con $0 \leq r < b$. Allora $\frac{a}{b} = q + \frac{r}{b}$ con $q \in \mathbb{Z}$ e $0 \leq \frac{r}{b} < 1$. Quindi $d = q$ è la parte intera di $x = \frac{a}{b}$.

Fissiamo la base k e l'insieme delle k cifre. Vogliamo scrivere ogni numero razionale mediante una sequenza di queste cifre, generalizzando quanto fatto per i numeri interi.

La notazione posizionale di un numero razionale positivo x è composta da due parti: la scrittura posizionale della sua parte intera, formata da un numero finito di cifre, e una sequenza infinita di cifre $q_1 q_2 \dots q_i \dots$ $(i \in \mathbb{N}^*)$, che di solito separiamo dalle precedenti mediante una virgola.

Se d è la parte intera di x, la parte "dopo la virgola" sarà quindi la scrittura posizionale del numero $x - d$, compreso tra 0 e 1. In caso la base scelta sia 10, le cifre dopo la virgola si chiamano **decimali**.

La scrittura posizionale di un numero razionale negativo y si ottiene premettendo il segno meno alla scrittura posizionale di $-y$; si noti che in tal caso la parte intera di y differisce per una unità dalla parte "prima della virgola" nella scrittura posizionale di y. Vediamo ora come si procede per calcolare le cifre della scrittura posizionale di x $(x \geq 0)$.

i) Scegliamo come suo rappresentante una frazione $\frac{a}{b}$, con $a, b > 0$.

ii) Eseguita la divisione con resto di a per b: $a = bd + r_0$, la parte "prima della virgola" di $\frac{a}{b}$ è la scrittura posizionale in base k della parte intera d.

iii) Le cifre dopo la virgola si ottengono ricorsivamente nel modo seguente:

q_1 è il quoziente della divisione di $r_0 k$ per b: $r_0 k = bq_1 + r_1$;

q_i è il quoziente della divisione di $r_{i-1} k$ per b: $r_{i-1} k = bq_i + r_i$.

Notiamo che si ha $0 \leq r_{i-1} k < bk$ e quindi i quozienti q_i sono compresi tra 0 e $k - 1$ e sono perciò rappresentabili in base k mediante una cifra.

Osservazione 8.2.2. *Non forniremo algoritmi generali per l'esecuzione delle operazioni tra numeri razionali espressi in forma posizionale rispetto a una prefissata base k; ci limitiamo soltanto a mettere in evidenza i due fatti seguenti che ci saranno utili in seguito:*

(1) il numero razionale x ($x \geq 0$) è la somma del numero intero d, che è la sua parte intera, e del numero razionale $\frac{r_0}{b}$ compreso tra 0 e 1, che corrisponde alla sequenza di cifre dopo la virgola;

(2) il prodotto xk ha scrittura posizionale che si ottiene da quella di x spostando la virgola a destra di una posizione.

Se nella sequenza delle divisioni per b necessarie per passare dalla frazione $\frac{a}{b}$ alla sua scrittura posizionale si incontra un resto nullo, da quel momento in poi tutti i quozienti (e i resti) saranno nulli: di solito una tale sequenza tutta di zeri viene omessa ottenendo così una **scrittura finita**.

Se invece non si incontra mai un resto nullo, i possibili resti diversi r_i sono al massimo $b - 1$. Dopo al più b cifre dopo la virgola, capiterà certamente di ottenere come resto un resto già ottenuto in precedenza. La sequenza delle divisioni (dei quozienti e dei resti) ripeterà allora quella ottenuta a partire dalla prima volta che si è incontrato quello stesso resto e così via infinite volte. La scrittura posizionale sarà quindi costituita da alcune cifre prima della virgola, da alcune dopo la virgola e poi dall'infinita ripetizione di una stessa sequenza: **scrittura periodica**. Anche in questo caso si può evitare l'uso di scritture infinite, che sarebbero un ostacolo pratico insormontabile, indicando una sola volta la sequenza che si ripete (**periodo**) evidenziata con una soprallineatura.

Sintetizziamo le considerazioni precedenti nel seguente enunciato.

Proposizione 8.2.3. *I numeri razionali hanno tutti scrittura posizionale finita oppure periodica.*

Notiamo però che uno stesso numero razionale (se non è intero) ha scrittura finita oppure scrittura periodica a seconda della base scelta.

Esempio 8.2.4. *Il numero razionale* $\frac{1}{3}$ *in base* 10 *ha scrittura periodica* $(0,\overline{3})_{10}$ *mentre in base* 3 *ha scrittura finita* $(0,1)_3$.

Viceversa $\frac{1}{2}$ *in base* 10 *ha scrittura finita* $(0,5)_{10}$ *mentre in base* 3 *ha scrittura periodica* $(0,\overline{1})_3$.

Proposizione 8.2.5. *Un numero razionale* x *ha scrittura finita in base* k *se e solo se nella sua espressione come frazione ridotta* $\frac{a}{b}$ *ogni fattore primo di* b *divide* k.

Dim: In virtù dell'Osservazione 8.2.2, il numero razionale x ha scrittura finita con r cifre dopo la virgola se e soltanto se xk^r è un numero intero n. Allora x si scrive come frazione $\frac{n}{k^r}$ e quindi nella corrispondente frazione ridotta $\frac{a}{b}$ il denominatore b è un divisore di k^r. ◇

Proposizione 8.2.6. *Ogni scrittura finita o periodica su* k *cifre è la scrittura posizionale in base* k *di un numero razionale.*

Dim: Una scrittura finita con r cifre dopo la virgola, ossia del tipo $c_t \dots c_0, q_1 \dots q_r$, è la scrittura posizionale del numero $x = \frac{n}{k^r}$, dove $n = c_t \dots c_0 q_1 \dots q_r$ è il numero intero che si ottiene "cancellando la virgola" nella scrittura finita (cfr. Osservazione 8.2.2 (2)).

Consideriamo allora una scrittura periodica, con s cifre dopo la virgola seguite da un gruppo periodico di r cifre, ossia una scrittura del tipo $c_t \dots c_0, p_1 \dots p_s\overline{q_1 \dots q_r}$. Il numero razionale x che in base k ha quella scrittura posizionale (se esiste) ha la proprietà che xk^{r+s} e xk^s hanno la stessa parte "dopo la virgola" $0,\overline{q_1 \dots q_r}$.

La differenza $xk^{r+s} - xk^s$ è quindi il numero intero $m = c_t \dots c_0 p_1 \dots p_s q_1 \dots q_r - c_t \dots c_0 p_1 \dots p_s$ (cfr. Osservazione 8.2.2 (1)) e perciò $x = \frac{m}{k^{r+s}-k^s}$. Abbiamo costruito in modo esplicito il numero x e ciò prova la sua esistenza. ◇

Fissata la base k, la corrispondenza tra numeri razionali e scritture finite o periodiche è biunivoca, con un'unica eccezione: i numeri che hanno una scrittura finita hanno anche un'altra scrittura, che è periodica con periodo costituito solo dalla cifra $k-1$.

Esempio 8.2.7. *In base* 10 *il numero* $0,\overline{9}$ *è il numero* x *tale che (cfr. Osservazione 8.2.2)*

$$10x - x = 9,\overline{9} - 0,\overline{9} = 9 + 0,\overline{9} - 0,\overline{9} = 9$$

e quindi $x = 1$.

8.3 Generalità sui polinomi

Sia A un anello. Col simbolo $A[X]$ indicheremo l'insieme di tutti i polinomi in una indeterminata a coefficienti in A.

La trattazione generale delle proprietà dei polinomi non rientra negli scopi di questo corso e verrà affrontata nel corso di Algebra del II anno. Per ora ci accontenteremo di definire i polinomi come "scritture formali" del tipo $a_0 + a_1X + \dots + a_nX^n$ con $a_i \in A$ e ci occuperemo soltanto del caso in cui A è un anello di numeri: nel paragrafo successivo

$A = \mathbb{Z}$ oppure $A = \mathbb{Q}$; in seguito $A = \mathbb{R}$ e $A = \mathbb{C}$. A parte il caso $A = \mathbb{Z}$, A sarà quindi un campo di numeri K. Daremo per note le seguenti definizioni e proprietà dei polinomi a coefficienti in un campo K (valide però anche per polinomi a coefficienti in un dominio di integrità come è $\mathbb{Z}$), solitamente studiate nelle superiori.

I) Gli elementi di K si possono anche considerare come polinomi di $K[X]$, detti **polinomi costanti** e tra essi c'è anche il **polinomio nullo** che ha tutti i coefficienti nulli.

II) In $K[X]$ sono definite delle operazioni di somma e di prodotto, che estendono quelle di K e che rendono $K[X]$ un anello commutativo con identità. L'elemento neutro rispetto alla somma e l'identità rispetto al prodotto sono rispettivamente i polinomi costanti 0 e 1.

III) Per ogni polinomio non nullo $F(X)$, il **grado**, denotato $\partial F(X)$, è l'esponente massimo dell'indeterminata che compare in $F(X)$ con coefficiente non nullo.

Le costanti sono i polinomi di grado 0. Il prodotto di due polinomi di gradi c e d rispettivamente ha grado $c + d$.

IV) Se $F(X) = a_0 + a_1X + \cdots + a_nX^n$ è un polinomio di $K[X]$ e b è un elemento di K, con $F(b)$ si intende l'elemento di K che si ottiene sostituendo b al posto di X nella scrittura formale di $F(X)$, ossia $F(b) = a_0 + a_1b + \cdots + a_nb^n$.

Definizione 8.3.1. *Si dice che $\alpha \in K$ è una* **radice** *di $F(X)$ se $F(\alpha) = 0$ ossia se α è una* **soluzione dell'equazione polinomiale** $F(X) = 0$.

NOTA BENE Bisogna fare molta attenzione all'ambiguità della scrittura $F(X) = 0$: a volte viene usata per affermare che un certo polinomio $F(X)$ è il polinomio nullo altre volte per indicare l'equazione polinomiale corrispondente al polinomio $F(X)$ (ossia la ricerca delle radici di $F(X)$). Nel seguito, per evitare tale ambiguità, useremo la notazione $F(X) = 0$ solo nel senso di equazione, mentre scriveremo $F(X) = 0_{K[X]}$ per dire che $F(X)$ è il polinomio nullo.

Per le proprietà di $K[X]$ di cui tratteremo nel resto di questo paragrafo dovremo necessariamente supporre che K sia un campo.

La divisione con resto. Anche se la tecnica di calcolo dovrebbe già essere nota dalle superiori, proviamo esplicitamente l'esistenza della divisione con resto in $K[X]$, poiché (come già per l'anello $\mathbb{Z}$), si tratta di uno strumento di importanza fondamentale per comprendere le proprietà dei polinomi.

Teorema 8.3.2. *Siano $F(X), G(X)$ polinomi di $K[X]$, con K campo e $G(X) \neq 0_{K[X]}$. Esistono allora due polinomi $Q(X)$ e $R(X)$ in $K[X]$ tali che:*

$$F(X) = G(X)Q(X) + R(X)$$

con $R(X)$ polinomio nullo oppure di grado inferiore a quello $G(X)$.

Dim: Se $F(X)$ è il polinomio nullo, basta porre $Q(X) = R(X) = 0_{K[X]}$. Supponiamo $F(X)$ non nullo e procediamo per induzione su $\partial F(X)$.
Se $\partial F(X) < \partial G(X)$, basta porre $Q(X) = 0_{K[X]}$ e $R(X) = F(X)$.
Supponiamo allora $\partial F(X) \geq \partial G(X)$ e supponiamo l'asserto vero per tutte le coppie di polinomi $F'(X)$, $G'(X)$, con $\partial F'(X) < \partial F(X)$.
Siano a e b i coefficienti non nulli di grado massimo (**coefficienti direttivi**) di $F(X)$ e $G(X)$ rispettivamente. Per l'ipotesi induttiva, l'asserto è vero, in particolare, per la coppia di polinomi $F'(X) = F(X) - ab^{-1}X^{d-c}G(X)$ e $G'(X) = G(X)$ (dove $d = \partial F(X)$ e $c = \partial G(X)$), poiché risulta $\partial F'(X) < \partial F(X)$.
Avremo allora: $F(X) - ab^{-1}X^{d-c}G(X) = Q'(X)G(X) + R'(X)$ con $R'(X)$ nullo oppure di grado inferiore a $G(X)$, da cui $F(X) = (ab^{-1}X^{d-c} + Q'(X))G(X) + R(X)$ con $R(X) = R'(X)$ nullo oppure di grado inferiore a $G(X)$. $\diamond$

Facendo ricorso alla divisione con resto potremmo ripetere i ragionamenti fatti per l'anello $\mathbb{Z}$ e provare che per $K[X]$ valgono le seguenti importanti proprietà:

1) l'esistenza del MCD di due polinomi;

2) l'identità di Bézout;

3) l'algoritmo euclideo per il calcolo del MCD;

4) l'esistenza e l'unicità della fattorizzazione in fattori primi.

Le proprietà 1) e 4) sopra enunciate valgono anche per l'anello $\mathbb{Z}[X]$, ma la loro dimostrazione richiede ragionamenti più complicati; invece non esistono in generale quoziente e resto di due polinomi a coefficienti interi e di conseguenza per $\mathbb{Z}[X]$ le proprietà 2) e 3) proprio non valgono. Un caso particolare in cui esistono in $\mathbb{Z}[X]$ il quoziente e il resto di due polinomi a coefficienti interi si ha quando il polinomio divisore è monico; il risultato seguente, enunciato per un campo K, vale allora anche per $K = \mathbb{Z}$.

Teorema 8.3.3. (Teorema di Ruffini) *Siano $F(X)$ un polinomio di $K[X]$ e α un elemento di K. Allora:*

$$\alpha \text{ è una radice di } F(X) \iff X - \alpha \text{ divide } F(X) \iff F(X) = (X - \alpha)G(X).$$

Dim: Eseguiamo la divisione con resto di $F(X)$ per $X - \alpha$: $F(X) = (X - \alpha)G(X) + R(X)$, con resto $R(X)$ nullo oppure di grado 0 (ossia $R(X) = r$ è una costante). Se ora sostituiamo α nei due membri, otteniamo $F(\alpha) = (\alpha - \alpha)G(\alpha) + r = r$. Allora α è una radice di $F(X)$ se e soltanto se $r = 0$, ossia se e soltanto se $X - \alpha$ divide esattamente $F(X)$. $\diamond$

Definizione 8.3.4. *Si dice che α è una radice di $F(X)$ di molteplicità r se $(X - \alpha)^r$ divide $F(X)$ e $(X - \alpha)^{r+1}$ non lo divide.*

Corollario 8.3.5. *Un polinomio non nullo $F(X) \in K[X]$ di grado d ha al più d radici in K (anche contando ciascuna con la sua molteplicità).*

Così, $F(X)$ si decompone in $K[X]$ come un prodotto:

$$(X-\alpha_1)^{r_1} \cdot \cdots \cdot (X-\alpha_t)^{r_t} \cdot G_1(X) \cdot \cdots \cdot G_m(X)$$

dove le α_i sono le radici distinte di $F(X)$ di molteplicità r_i e i polinomi $G_j(X)$ sono polinomi di grado maggiore di 1, privi di radici in K e irriducibili in $K[X]$. Tale decomposizione è unica a meno dell'ordine dei fattori e di costanti moltiplicative.

Dim: Procediamo per induzione su d.

Se $d = 1$, allora $F(X) = aX + b$ (con $a \neq 0$) ha esattamente 1 radice $\alpha = -ba^{-1}$.

Supponiamo l'asserto vero per tutti i polinomi di grado $< \partial F(X)$ e proviamo che vale anche per $F(X)$. Supponiamo che $F(X)$ abbia una radice α di molteplicità r: allora $F(X) = (X-\alpha)^r G(X)$ e α non è radice di $G(X)$.

Se $F(X)$ ha anche un'altra radice $\beta \neq \alpha$, allora $0 = F(\beta) = (\beta-\alpha)^r G(\beta)$ e quindi $G(\beta) = 0$ ossia β è radice anche di $G(X)$. Viceversa, se β è radice di $G(X)$, allora $\beta \neq \alpha$ e si ha $F(\beta) = (\beta-\alpha)^r G(\beta) = 0$ ossia β è anche radice di $F(X)$.

Le radici di $F(X)$ sono allora α (con molteplicità r) e le radici di $G(X)$. Poiché il grado di $G(X)$ è $d-r$, per ipotesi induttiva le radici di $G(X)$ sono al più $d-r$ e quindi le radici di $F(X)$ sono al più d. $\diamond$

Si faccia sempre molta attenzione trattando con i polinomi a specificare sia l'anello in cui si stanno considerando i suoi coefficienti sia l'anello in cui si cercano le sue eventuali radici, in quanto le proprietà di un fissato polinomio dipendono fortemente dall'ambiente nel quale lo si sta considerano. Si consideri ad esempio il polinomio $F(X) = 2X^4 - 6$; tale polinomio:

- non ha radici ed è riducibile come come polinomio di $\mathbb{Z}[X]$;
- non ha radici ed è irriducibile come polinomio di $\mathbb{Q}[X]$;
- ha 2 radici e si spezza nel prodotto di 3 fattori irriducibili come polinomio di $\mathbb{R}[X]$;
- ha 4 radici e si spezza nel prodotto di 4 fattori irriducibili come polinomio di $\mathbb{C}[X]$.

8.4 Polinomi a coefficienti interi e razionali

Ci occupiamo ora dei polinomi di $\mathbb{Q}[X]$ e delle loro radici in $\mathbb{Q}$. Possiamo osservare, innanzi tutto, che le radici di $F(X)$ e di $aF(X)$, dove a è una qualsiasi costante non nulla, sono esattamente le stesse. Potremo allora limitarci a considerare, senza perdere in generalità, polinomi **monici** ossia con coefficiente direttivo 1 (moltiplicando $F(X)$ per l'inverso del suo coefficiente direttivo) oppure, se ciò risultasse più conveniente, polinomi a coefficienti interi ossia di polinomi di $\mathbb{Z}[X]$ (moltiplicando $F(X)$ per un multiplo comune dei denominatori delle frazioni che sono i suoi coefficienti).

Gli esempi seguenti mostrano che i polinomi di $\mathbb{Q}[X]$ di grado d possono avere un numero r di radici (contate con la loro molteplicità) per ogni intero r tale che $0 \leq r \leq d$, $r \neq d-1$.

Esempio 8.4.1. *Se $a_1, \ldots, a_d$ sono d numeri razionali, il polinomio $(X-a_1)\cdot\cdots\cdot(X-a_d)$ ha esattamente tante radici quanto è il suo grado.*

Esempio 8.4.2. *Per ogni $d \geq 2$, il polinomio $X^d - 2$ non ha nessuna radice in $\mathbb{Q}$.*

Supponiamo per assurdo che abbia una radice $x \in \mathbb{Q}$, che possiamo esprimere sotto forma di frazione ridotta $\frac{a}{b}$. Sostituendo x nel polinomio e moltiplicando per b^d si ottiene: $a^d - 2b^d = 0$ ossia $a^d = 2b^d$. Per la fattorialità di $\mathbb{Z}$, il fattore primo 2 deve dividere a ossia $a = 2c$. Dividendo per 2 i due membri si ottiene allora $2^{d-1}c^d = b^d$, con $d-1 \geq 1$; allora il fattore primo 2 deve dividere b, in contraddizione con la scelta di $\frac{a}{b}$ frazione ridotta.

Esempio 8.4.3. *Se $0 \leq r \leq d-2$ e $a_1, \ldots, a_r$ sono r numeri razionali, il polinomio $(X-a_1)\cdot\cdots\cdot(X-a_r)\cdot(X^{d-r}-2)$ ha esattamente r radici in $\mathbb{Q}$.*

NOTA BENE Un polinomio di grado 2 oppure 3 è riducibile (ossia decomponibile nel prodotto di fattori non costanti) se e soltanto se ha almeno una radice. Se infatti $F(X)$ ha una radice α, allora si spezza nel prodotto $(X-\alpha)G(X)$; viceversa, se si spezza in un prodotto di fattori non costanti $F(X) = G(X)H(X)$, allora almeno uno dei due fattori ha grado 1 e quindi ha una radice.

Invece per un polinomio di grado ≥ 4, avere una radice è in generale solo una condizione sufficiente per essere riducibile, ma non è assolutamente una condizione necessaria.

Ad esempio il polinomio $X^4 + 3X^2 + 2$ di $\mathbb{Q}[X]$ si decompone nel prodotto $(X^2+1)(X^2+2)$, ossia è riducibile, ma non ha radici in $\mathbb{Q}$.

Non ci occuperemo però in questo corso del problema generale di stabilire se un polinomio di $\mathbb{Q}[X]$ sia o meno riducibile. Il risultato seguente fornisce però un metodo generale per stabilire, teoricamente ed anche operativamente, quali e quante radici razionali abbia un qualsiasi polinomio di $\mathbb{Q}[X]$.

Proposizione 8.4.4. *Sia $F(X) = a_0 + a_1X + \cdots + a_dX^d$ un polinomio di grado d che possiamo supporre a coefficienti interi, ossia $a_i \in \mathbb{Z}$ e $a_d \neq 0$.*

Ogni radice $\alpha \in \mathbb{Q}$ di $F(X)$, si può scrivere come frazione $\frac{n}{m}$, con n/a_0 ed m/a_d.

Dim: Sia $\alpha \in \mathbb{Q}$ una radice di $F(X)$ e $\frac{n}{m}$ la sua espressione come frazione ridotta.

Moltiplicando i due membri di $F(\frac{n}{m}) = 0$ per m^d si trova $a_0m^d + a_1nm^{d-1} + \cdots + a_dn^d = 0$, da cui $m(a_0m^{d-1} + a_1nm^{d-2} + \cdots + a_{d-1}n^{d-1}) = -a_dn^d$. Poiché nessun fattore di m divide n, allora m divide a_d.

Analogamente da $a_0m^d = -n(a_1m^{d-1} + \cdots + a_dn^{d-1})$ si ricava che n divide a_0. $\diamond$

Esempio 8.4.5. *Vogliamo determinare tutte le radici razionali del polinomio* $\frac{5}{3}X^7+\frac{3}{2}X^6+\frac{7}{6}X^5-\frac{1}{2}X^4-\frac{1}{3}X^3$. *Poiché mancano i termini di grado* 2, 1 *e* 0, *il polinomio avrà la radice* 0 *con molteplicità* 3, *ossia* $F(X)=X^3G(X)$ *con* $G(X)=\frac{5}{3}X^4+\frac{3}{2}X^3+\frac{7}{6}X^2-\frac{1}{2}X-\frac{1}{3}$: *le radici non nulle di* $F(X)$ *sono esattamente le radici di* $G(X)$.

Per determinare le radici di $G(X)$, *moltiplichiamo tutti i coefficienti per un numero intero multiplo comune dei denominatori:* $G'(X)=6G(X)=10X^4+9X^3+7X^2-3X-2$.

Le radici di $G'(X)$ *sono elementi dell'insieme:*

$$\{\tfrac{n}{m}\in\mathbb{Q}\mid n/2 \text{ e } m/10\}=\{\pm1,\ \pm2,\ \pm\tfrac{1}{2},\ \pm\tfrac{1}{5},\ \pm\tfrac{2}{5},\ \pm\tfrac{1}{10}\}.$$

Sostituendo uno dopo l'altro questi 12 *numeri in* $G'(X)$ *si arriva a stabilire che le uniche radici razionali di* $G'(X)$ *sono* $\frac{1}{2}$ *e* $-\frac{2}{5}$. *Infine, facendo ricorso al teorema di Ruffini, si ottiene la fattorizzazione:* $F(X)=\frac{5}{3}X^3(X-\frac{1}{2})(X+\frac{2}{5})(X^2+X+1)$, *con* X^2+X+1 *privo di radici razionali. Le radici di* $F(X)$ *sono quindi* 0 *con molteplicità* 3 *e* $\frac{1}{2}$ *e* $-\frac{2}{5}$ *con molteplicità* 1.

Per concludere ricordiamo, senza dimostrarlo, un importante risultato noto come **Lemma di Gauss**.

Teorema 8.4.6. *Se un polinomio* $F(X)\in\mathbb{Z}[X]$ *si decompone nel prodotto* $F(X)=G_1(X)G_2(X)$ *con* $G_1(X),G_2(X)\in\mathbb{Q}[X]$, *allora si decompone anche nel prodotto* $F(X)=G_1'(X)G_2'(X)$ *con* $G_1'(X),G_2'(X)\in\mathbb{Z}[X]$.

8.5 Esercizi

8.1. Verificare che le operazioni in $\mathbb{Q}$ sono ben definite.

8.2. Verificare che l'ordine $\leq$ in $\mathbb{Q}$ rispetta la somma e rispetta il prodotto per numeri positivi.

8.3. Scrivere in forma decimale (ossia posizionale in base 10) i seguenti numeri razionali:

$$\frac{1}{17},\quad \frac{11}{18},\quad -\frac{23}{7},\quad -\frac{35}{121},\quad \frac{101}{13},\quad \frac{2005}{33}.$$

8.4. Scrivere i seguenti numeri razionali (scritti in forma posizionale in base 10) sotto forma di frazione:

$$0,58 \qquad 0,5\overline{8} \qquad 0,\overline{58} \qquad 1,0\overline{01} \qquad 1,\overline{001}$$

$$1,27\overline{31} \quad 1,273\overline{1} \quad -2,\overline{117} \quad -2,1\overline{17} \quad -2,11\overline{7}$$

8.5. Scelto un intero k con $2\leq k\leq 9$, scrivere in forma posizionale in base k i seguenti numeri espressi in base 10:

$$11 \quad -32 \quad 107 \quad 22,9 \quad 5,13 \quad 1,\overline{403} \quad 3,2\overline{60}.$$

8.6. I seguenti numeri sono scritti in base 12 con $A = 10$ e $B = 11$. Trascriverli in forma di frazione in base 12 e poi in forma posizionale e di frazione in base 10.

$$2A \quad AB \quad 2B0 \quad 709 \quad 26,61 \quad A,0\overline{A1} \quad B,A3\overline{B}.$$

8.7. Determinare tre basi diverse rispetto alle quali il numero $x = \frac{1}{4}$ ha scrittura posizionale finita e tre rispetto alle quali ha scrittura posizionale periodica; esprimere x rispetto a tali basi.

8.8. Esplicitare la relazione $x \leq y$ in $\mathbb{Q}$ usando la scrittura posizionale dei numeri razionali.

8.9. Calcolare quoziente e resto della divisione tra i polinomi $X^5 - 3X^2 + 6X + 2$ e $\frac{1}{2}X^2 + X + 4$ di $\mathbb{Q}[X]$.

8.10. Determinare il MCD dei polinomi dell'esercizio precedente mediante l'algoritmo euclideo.

8.11. Determinare il MCD dei polinomi $X^3 - 2X^2 + 2X + 5$ e $3X^2 - 4X - 7$ di $\mathbb{Q}[X]$ mediante l'algoritmo euclideo ed esplicitare l'identità di Bézout.

8.12. Provare che ogni equazione polinomiale di grado 1 a coefficienti in $\mathbb{Q}$ ammette esattamente una soluzione in $\mathbb{Q}$.

8.13. Provare (oppure confutare mediante un esempio) che ogni equazione polinomiale di grado 2 a coefficienti in $\mathbb{Q}$ ammette almeno una soluzione in $\mathbb{Q}$.

8.14. Dire per quali valori di n il polinomio $X^n - 5$ ammette una radice razionale.

8.15. Determinare (se esiste) un numero $a \in \mathbb{Q}$ tale che il polinomio $F_a(X) = 3X^5 - 5X^3 + aX - 5$:

i) non ammetta radici razionali, (si può dedurre che per tale valore di a il polinomio $F_a(X)$ è senza dubbio irriducibile?)

ii) ammetta radici razionali; si può dedurre che per tale valore di a il polinomio $F_a(X)$ è senza dubbio riducibile?)

iii) ammetta 2 radici razionali.

8.16. Trovare un esempio esplicito di polinomio di $\mathbb{Q}[X]$ irriducibile e di grado n, per ogni $n \geq 1$.

8.17. Provare che nessun polinomio di grado d di $\mathbb{Q}[X]$ può avere esattamente $d - 1$ radici, contando ciascuna con la sua molteplicità.

8.18*. Sia n un numero intero. Provare che l'equazione polinomiale $X^2 - n = 0$ ha soluzioni razionali se e solo se ha soluzioni intere ossia se e solo se n è un quadrato in $\mathbb{Z}$.

Capitolo 9

Il campo $\mathbb{R}$ dei numeri reali

9.1 Cenni alla costruzione formale dei numeri reali

Gli ampliamenti successivi dei numeri naturali ottenuti finora, ossia $\mathbb{Z}$ e $\mathbb{Q}$, sono stati la risposta a questioni prettamente algebriche ossia legate alle operazioni o, equivalentemente, alle equazioni polinomiali. In $\mathbb{N}$ è definita la somma, esiste l'elemento neutro 0 rispetto alla somma, ma non esistono gli opposti; così non sono risolubili le equazioni polinomiali moniche di grado 1: $X + n = 0$ (tranne se $n = 0$).

L'ampliamento da $\mathbb{N}$ a $\mathbb{Z}$ permettere di risolvere tutte queste equazioni, poiché in $\mathbb{Z}$ esistono gli opposti; in $\mathbb{Z}$, però, non è risolubile la generica equazione polinomiale di primo grado: $aX + b = 0$, poiché non esistono (in generale) gli inversi.

L'ampliamento da $\mathbb{Z}$ a $\mathbb{Q}$ permettere di risolvere tutte le equazioni di primo grado, poiché $\mathbb{Q}$ è un campo; però vi sono equazioni di grado superiore (ad esempio di grado 2) a coefficienti in $\mathbb{Q}$ che non ammettono soluzioni razionali.

Potremmo allora continuare in questa direzione cercando un ampliamento di $\mathbb{Q}$ in cui tutte le equazioni polinomiali di grado 2, oppure di ogni grado, siano risolubili. Un tale ampliamento esiste (ne accenneremo brevemente in seguito), ma non è $\mathbb{R}$.

I numeri reali nascono da problematiche di tipo un po' diverso. La diagonale del quadrato di lato 1 ha, per il teorema di Pitagora, misura x tale che $x^2 = 2$: come abbiamo visto, non esiste alcun numero razionale x che soddisfa questa condizione. Anche la misura della circonferenza di raggio 1 non è esprimibile mediante un numero razionale e non è neppure radice di un polinomio di $\mathbb{Z}[X]$ (ma provarlo non è semplice!)

Intuitivamente, vogliamo costruire un ampliamento di $\mathbb{Q}$ che non perda le buone proprietà algebriche di $\mathbb{Q}$ e che permetta di misurare la lunghezza dei segmenti. Le proprietà seguenti formalizzano questa idea intuitiva e forniscono una descrizione $\mathbb{R}$.

Assiomi dei numeri reali:

I) $\mathbb{R}$ **è un campo**: sono definite due operazioni (somma e prodotto) rispetto alle quali $\mathbb{R}$ è un anello commutativo con identità in cui ogni elemento non nullo possiede inverso.

II) $\mathbb{R}$ **è un campo ordinato**: $\mathbb{R}$ è dotato di un ordine totale compatibile con la somma e compatibile col prodotto per elementi maggiori di 0.

III) $\mathbb{R}$ **estende** $\mathbb{Q}$: $\mathbb{R}$ contiene un sottoinsieme in corrispondenza biunivoca con $\mathbb{Q}$ sul quale le operazioni e l'ordinamento di $\mathbb{R}$ coincidono con quelli di $\mathbb{Q}$.

IV) $\mathbb{R}$ **è completo**: se X e Y sono due sottoinsiemi di $\mathbb{R}$ tali che $\forall x \in X$, $\forall y \in Y$ si abbia $x \leq y$, allora esiste un elemento $z \in \mathbb{R}$ tale che $x \leq z \leq y$, $\forall x \in X$, $\forall y \in Y$.

Esempio 9.1.1. *La non razionalità del rapporto tra le misure del lato e della diagonale del quadrato (oppure del raggio e della circonferenza) mostra che* $\mathbb{Q}$ *non è completo. Siano infatti* $X = \{x \in \mathbb{Q}^+ \mid x^2 < 2\}$ *e* $Y = \{y \in \mathbb{Q}^+ \mid y^2 > 2\}$. *Allora* $\forall x \in X$ *e* $\forall y \in Y$ *si ha* $x^2 < 2 < y^2$ *e quindi (essendo* x *e* y *entrambi positivi)* $x < y$. *Però non esiste nessun numero razionale* z *tale che* $\forall x \in X$, $\forall y \in Y$, *si abbia* $x \leq z \leq y$, *poiché un tale numero dovrebbe coincidere con* $\sqrt{2}$ *che non è razionale.*

Si noti che una descrizione assiomatica non assicura che un oggetto come quello descritto esista e sia essenzialmente unico. Si può provare senza troppa difficoltá (ma non lo faremo) che l'insieme $\mathbb{R}$ descritto dagli assiomi è unico (ossia che tra due insiemi che soddisfano gli assiomi elencati esiste una corrispondenza biunivoca che conserva operazioni e ordinamento).

Cercheremo invece di dare un'idea della sua costruzione.

Un modo per definire i numeri reali (spesso usato nelle superiori) è quello di partire dalla scrittura posizionale dei numeri razionali e di togliere la condizione sulla finitezza o periodicità delle cifre dopo la virgola. Un numero reale x è allora una scrittura su k cifre $c_r \dots c_0, q_1 q_2 \dots q_i \dots$ costituita da una sequenza finita di cifre prima della virgola $c_r \dots c_0$ e da una sequenza infinita qualsiasi di cifre dopo la virgola $q_1 q_2 \dots q_i \dots$ $(i \in \mathbb{N}^*)$.

Questa definizione, apparentemente molto intuitiva, presenta però vari inconvenienti, tra cui ad esempio i seguenti:

- è complicato stabilire se due scritture, una in base k e una in base h rappresentano o meno lo stesso numero reale;
- è complicato definire le operazioni, in particolare il prodotto.

Un approccio, in apparenza più complicato, ma in realtà molto concreto e maneggevole, è quello puramente insiemistico delle **sezioni di Dedekind**. L'idea da cui si parte è che la misura di un segmento, anche se non è esprimibile con un unico numero razionale, è perfettamente individuata se si conoscono tutte le sue approssimazioni razionali per eccesso e per difetto.

Definizione 9.1.2. *Una semiretta sinistra aperta di $\mathbb{Q}$ è un suo sottoinsieme A non vuoto, privo di massimo, che soddisfa la seguente condizione:*

$$\forall a \in A \text{ e } \forall q \in \mathbb{Q} : \quad q \leq a \Longrightarrow q \in A.$$

Analogamente una semiretta destra aperta di $\mathbb{Q}$ è un suo sottoinsieme B non vuoto, privo di minimo, che soddisfa la seguente condizione:

$$\forall b \in B \text{ e } \forall q \in \mathbb{Q} : \quad q \geq b \Longrightarrow q \in B.$$

Definizione 9.1.3. *Si dice* **numero reale** *x una coppia (A, B) di sottoinsiemi di $\mathbb{Q}$ con A semiretta sinistra, B semiretta destra, tali che $A \cap B = \emptyset$ e $A \cup B = \mathbb{Q}$ oppure $A \cup B = \mathbb{Q} \setminus \{q\}$. $\mathbb{R}$ è l'insieme di tutti i numeri reali.*

Esempio 9.1.4. *I numeri razionali possono essere pensati come numeri reali in modo del tutto naturale:*
se $q \in \mathbb{Q}$ allora $q = (A_q, B_q)$, dove $A_q = \{a \in \mathbb{Q} \mid a < q\}$ e $B_q = \{b \in \mathbb{Q} \mid b > q\}$.
In particolare $0 = (A_0, B_0) = (\mathbb{Q}^-, \mathbb{Q}^+)$.

Esempio 9.1.5. *Il numero $\sqrt{2}$, ossia la lunghezza della diagonale del quadrato di lato 1, è il numero reale (A, B), dove $B = \{q \in \mathbb{Q}^+ \mid q^2 > 2\}$ e $A = \mathcal{C}_{\mathbb{Q}}(B)$.*

Osservazione 9.1.6. *Le seguenti proprietà ci saranno utili per definire l'ordine, la somma e il prodotto in $\mathbb{R}$. Lasciamo le verifiche per esercizio al lettore, poiché non richiedono altro che la definizione di semiretta e le nozioni elementari sugli insiemi.*

a) *Un numero reale $x = (A, B)$ è perfettamente individuato anche dalla sola semiretta sinistra A oppure dalla sola semiretta destra B; infatti B è il complementare in $\mathbb{Q}$ di A, eventualmente privato del minimo, e, viceversa, A è il complementare in $\mathbb{Q}$ di B, eventualmente privato del massimo. Potremo allora scrivere anche $x = (A, \dots)$ oppure $x = (\dots, B)$.*

b) *Se B e B' sono semirette destre di $\mathbb{Q}$, anche $B + B' = \{b + b' \mid b \in B,\, b' \in B'\}$ è una semiretta destra di $\mathbb{Q}$ e $-B = \{-b \mid b \in B\}$ è una semiretta sinistra.*

c) *Se $x = (A, B)$ è un numero reale, allora l'insieme $B - A = \{b - a \mid b \in B, a \in A\}$ coincide con $\mathbb{Q}^+$.*

d) *Se B e B' sono semirette destre contenute in $\mathbb{Q}^+$, anche $B \cdot B' = \{bb' \mid b \in B,\, b' \in B'\}$ è una semiretta destra contenuta in $\mathbb{Q}^+$.*

e) *Se B_α (α variabile in un insieme I qualsiasi) sono semirette destre di $\mathbb{Q}$, anche $\bigcup_{\alpha \in I} B_\alpha$ è una semiretta destra di $\mathbb{Q}$.*

Definizione 9.1.7. *Siano $x = (A, B)$ e $y = (A', B')$ due numeri reali. Allora:*

- *$x \leq y$ se $B \supseteq B'$ (o, equivalentemente, se $A \subseteq A'$)*

- $x + y = (\ldots, B + B')$
- *Se* $x, y \geq 0$*, allora* $xy = (\ldots, B \cdot B')$.

Proposizione 9.1.8. *L'insieme* $\mathbb{R}$ *dotato dell'ordinamento e delle operazioni sopra definite è un campo ordinato che estende* $\mathbb{Q}$.

Dim: La dimostrazione completa di questo enunciato richiede molte verifiche, complessivamente lunghe, anche se nessuna particolarmente complicata. Vediamone solo alcune.

Le proprietà associative, commutative, distributive di somma e prodotto discendono immediatamente da quelle di $\mathbb{Q}$.

Ad esempio vale $x + y = y + x$, poiché, per la proprietà commutativa della somma in $\mathbb{Q}$, si ha $B + B' = \{b + b' \mid b \in B,\, b' \in B'\} = \{b' + b \mid b \in B,\, b' \in B'\} = B' + B$.

Esistenza dell'opposto. Se $x = (A, B)$, allora il suo opposto è $-x = (-B, -A)$.

Dalla definizione di somma si ha infatti $x + (-x) = (\ldots, B - A)$; ma $B - A = \mathbb{Q}^+$ (cfr. Osservazione 9.1.6 c) e quindi $x + (-x) = (\ldots, \mathbb{Q}^+) = 0$.

L'esistenza dell'opposto permette di estendere a tutte le coppie di numeri reali la definizione di prodotto ponendo $x \cdot y = -(x \cdot (-y)) = -((-x) \cdot y) = (-x) \cdot (-y)$.

Esistenza dell'inverso. Se $x = (A, B)$ è un numero reale strettamente positivo, allora $A \cap \mathbb{Q}^+$ è non vuoto e l'insieme $C = \{a^{-1} \mid a \in A \cap \mathbb{Q}^+\}$ è una semiretta destra. Allora $x^{-1} = (\ldots, C)$ è l'inverso di x. $\diamond$

Proviamo infine in modo completo la proprietà fondamentale dei numeri reali.

Teorema 9.1.9. $\mathbb{R}$ *è un campo ordinato completo.*

Dim: Siano X e Y due sottoinsiemi non vuoti di $\mathbb{R}$ tali che $\forall x \in X$ e $\forall y \in Y$ si ha $x \leq y$. Proviamo che esiste (almeno) un elemento $z \in \mathbb{R}$ tale che $x \leq z \leq y$, $\forall x \in X$ e $\forall y \in Y$.

Indichiamo con $x = (A_x, B_x)$ e $y = (A_y, B_y)$ gli elementi di X e Y rispettivamente.

Poniamo $z = (\ldots, \bigcup_{y \in Y} B_y)$ e verifichiamo che si ha $\overline{x} \leq z \leq \overline{y}$ per due qualsiasi elementi $\overline{x} \in X$ e $\overline{y} \in Y$.

La diseguaglianza $z \leq \overline{y}$ è ovvia poiché per costruzione $B_{\overline{y}} \subseteq \bigcup_{y \in Y} B_y$.

Inoltre si ha anche $\overline{x} \leq z$, poiché per ipotesi $\overline{x} \leq y$, ossia $B_{\overline{x}} \supseteq B_y$, $\forall y \in Y$, e quindi $B_{\overline{x}} \supseteq \bigcup_{y \in Y} B_y$. $\diamond$

Dal punto di vista algebrico $\mathbb{R}$ non ha proprietà significativamente migliori di $\mathbb{Q}$, poiché le operazioni hanno in $\mathbb{R}$ le stesse proprietà che hanno in $\mathbb{Q}$. Riguardo alla risolubilità delle equazioni polinomiali, il campo $\mathbb{R}$ presenta vantaggi e svantaggi rispetto a $\mathbb{Q}$. Infatti, ci sono molte più equazioni risolubili in $\mathbb{R}$ che in $\mathbb{Q}$ (ad esempio tutti i polinomi di grado dispari ammettono in $\mathbb{R}$ almeno una radice: cfr. Esempio 9.1.11 e Corollario 10.2.5), ma non tutte le equazioni polinomiali sono risolubili in $\mathbb{R}$ (ad esempio $X^2 + 1 = 0$ non lo è). D'altra parte non esiste più un metodo generale che permetta di calcolare le soluzioni reali, analogo a quello visto per le soluzioni razionali. Rimandiamo ai paragrafi successivi la trattazione più dettagliata di questi argomenti.

La completezza di $\mathbb{R}$ ha, però, come conseguenza di estrema importanza la convergenza delle successioni di Cauchy, fondamento di tutta l'Analisi matematica.

I due esempi seguenti mostrano come, reciprocamente, risultati di analisi possano essere usati per provare proprietà algebriche dei polinomi.

Esempio 9.1.10. *Siano $\alpha \in \mathbb{R}$ e $F(X)$ un polinomio a coefficienti reali. Allora α è una radice multipla di $F(X)$ se e solo se α è una radice comune a $F(X)$ e al "polinomio derivato" $F'(X)$.*

Se infatti α è una radice multipla di $F(X)$, ossia $F(X) = (X-\alpha)^n G(X)$ con $n \geq 2$, allora $F'(X) = (X-\alpha)^{n-1}G(X) + (X-\alpha)^n G'(X)$ con $n-1 \geq 1$ e quindi $F'(\alpha) = 0$.

Viceversa se α è una radice semplice di $F(X)$, ossia $F(X) = (X-\alpha)G(X)$ con $G(\alpha) \neq 0$, allora $F'(\alpha) = G(\alpha) \neq 0$ e quindi α non è radice di $F'(X)$.

Mediante l'algoritmo euclideo possiamo calcolare $M(X) = MCD(F(X), F'(X))$: le radici multiple di $F(X)$ sono esattamente le radici di $M(X)$.

Esempio 9.1.11. *Sia $F(X)$ un polinomio a coefficienti reali (che possiamo supporre monico) di grado d dispari. Allora $F(X)$ ha almeno una radice α in $\mathbb{R}$.*

Infatti, la funzione polinomiale $y = F(x)$ è una funzione continua, definita su tutto $\mathbb{R}$ e tale che:

$$\lim_{x\to+\infty} F(x) = \lim_{x\to+\infty} X^d = +\infty \quad e \quad \lim_{x\to-\infty} F(x) = \lim_{x\to-\infty} X^d = -\infty.$$

Quindi $y = F(x)$ assume sia valori positivi sia valori negativi.

Per il teorema di Weierstrass la funzione $y = F(x)$ assume tutti i valori intermedi e quindi, in particolare, assume anche il valore 0 in corrispondenza di un qualche $\alpha \in \mathbb{R}$.

9.2 Scrittura dei numeri reali

La definizione astratta da noi data di numero reale permette di introdurre in modo naturale la sua scrittura posizionale. Per definire la scrittura posizionale del numero reale positivo $x = (A, B)$ (la scrittura posizionale di un numero negativo y si ottiene premettendo il segno "$-$" alla scrittura di $x = -y$) fissiamo, come già fatto per $\mathbb{Z}$ e $\mathbb{Q}$, la base k e l'insieme delle k cifre.

La scrittura posizionale di x è la sequenza di cifre $c_r \dots c_0, q_1 \dots q_i \dots$ $(i \in \mathbb{N}^*)$ definite induttivamente da:

$$\begin{aligned} c_r \dots c_0 &= \min\{\text{parte intera (scritta in forma posizionale) di } b \mid b \in B\} \\ q_1 &= \min\{\text{prima cifra dopo la virgola di } b \mid b \in B \text{ del tipo } c_r \dots c_0, \dots\} \\ q_i &= \min\{i-\text{esima cifra dopo la virgola di } b \mid b \in B \text{ del tipo } c_r \dots c_0, q_1 \dots q_{i-1} \dots\} \end{aligned}$$

In questo modo si ottengono tutte le possibili sequenze di cifre; se infatti $c_r \dots c_0, q_1 \dots q_i \dots$ è una sequenza qualsiasi, essa rappresenta il numero reale $x = (A, B)$, dove

$$B = \{b \in \mathbb{Q} \mid b \geq c_r \dots c_0, q_1 \dots q_k \text{ per un qualche } k \in \mathbb{N}\}.$$

Dal punto di vista operativo la scrittura posizionale dei numeri reali non razionali, cioè una scrittura non finita e non periodica, è quasi sempre inutilizzabile. Ci sono però numeri le cui cifre dopo la virgola, anche se non periodiche, sono comunque ottenibili in modo sufficientemente semplice mediante una qualche formula matematica.

Esempio 9.2.1. *Il seguente numero irrazionale α è noto come* **numero di Liouville**.

Fissata la base 10 *(ma una qualsiasi altra base andrebbe ugualmente bene), la parte intera di α è* 0 *e sono* 0 *anche tutte le cifre dopo la virgola tranne quelle di posto $n!$, al variare di n in $\mathbb{N}$, che sono degli* 1*: $\alpha = 0,1100010000\ldots$.*

Per alcuni numeri reali le cifre dopo la virgola possono essere calcolate una alla volta in modo ricorsivo, eseguendo conti che si fanno via via più lunghi: ad esempio, mediante l'utilizzo di potenti calcolatori, sono state calcolate migliaia di cifre decimali di π (ma non tutte!).

Solitamente però i numeri reali non razionali non vengono indicati mediante la loro scrittura posizionale, ma usando metodi diversi che forniscono descrizioni del numero stesso, descrizioni che possono essere di tipo vario: algebrico, geometrico, analitico, ...

Così il simbolo $\sqrt{2}$ significa "il numero reale positivo il cui quadrato è 2" (descrizione di tipo algebrico), π è il "nome" del rapporto tra la lunghezza della circonferenza e quella del diametro (descrizione geometrica), e indica il limite della successione $S_n = (1 + \frac{1}{n})^n$ (descrizione analitica).

A partire dai numeri razionali e da alcuni numeri reali importanti (quelli sopra introdotti e pochi altri) altri numeri reali possono essere individuati mediante scritture miste, in cui intervengono operazioni e/o funzioni, del tipo:

$$\pi + e \quad \frac{\pi}{2}, \quad \frac{1-\sqrt{15}}{2}, \quad e^2, \quad \sin(1), \quad \log(2), \quad \sqrt[7]{\pi} - 3^{\sqrt{2}}, \quad e^{\pi}, \quad \pi^e.$$

Potremmo continuare a lungo a fare esempi via via più complicati di scritture di numeri reali; ma nonostante i nostri sforzi la maggior parte dei numeri reali rimane totalmente al di fuori della nostra possibilità di scrittura esplicita o di descrizione mediante una qualche proprietà!

9.3 Numeri algebrici e numeri trascendenti

La scrittura posizionale dei numeri reali permette di dimostrare che la cardinalità di $\mathbb{R}$ è più che numerabile (cfr. Esempio 4.2.12)e quindi che **esistono molti numeri reali non razionali**. I numeri reali non razionali si dicono **numeri irrazionali** e formano un insieme $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ di cardinalità più che numerabile. Se, infatti, si avesse $Card(\mathbb{I}) \leq \aleph_0$, allora si avrebbe anche

$$Card(\mathbb{R}) = Card(\mathbb{Q} \cup \mathbb{I}) \leq Card(\mathbb{Z}^+ \cup \mathbb{Z}^-) = Card(\mathbb{Z}) = \aleph_0.$$

Per ulteriori approfondimenti consigliamo la lettura del libricino di Ivan Niven *Numeri razionali ed irrazionali* (Ed. Zanichelli), che contiene molte informazioni interessanti, pur trattando l'argomento in modo elementare.

Una differente suddivisione dell'insieme dei numeri reali si ottiene a partire dalla seguente definizione.

Definizione 9.3.1. *Un numero reale x si dice* **algebrico** *se è radice di un polinomio a* **coefficienti razionali** *(o, equivalentemente, di un polinomio a coefficienti interi). Indicheremo con* $\mathbf{A}$ *l'insieme dei numeri reali algebrici e con* $\mathbb{T}$ *il suo complementare in* $\mathbb{R}$*, i cui elementi si dicono* **numeri trascendenti**.

Tra i numeri algebrici ci sono tutti i numeri razionali (se $q \in \mathbb{Q}$, allora q è radice del polinomio a coefficienti razionali $X - q$) ed anche altri numeri ($\sqrt{2}$ è radice dell'equazione a coefficienti razionali $X^2 - 2$) e quindi $\mathbf{A}$ contiene strettamente $\mathbb{Q}$.

Più complicato è provare che $\mathbf{A}$ non coincide con tutto $\mathbb{R}$; in modo particolare è difficile verificare direttamente la trascendenza di un certo numero reale, anche di π oppure di e che sono i numeri trascendenti più famosi. Sul già citato Niven si può trovare una prova diretta, elementare anche se non breve, della trascendenza del numero di Liouville. Non è invece ancora nota la trascendenza o meno di alcuni numeri del tipo di quelli elencati alla fine del precedente paragrafo; ad esempio non è tuttora noto se $e + \pi$ oppure $e\pi$ oppure π^e siano algebrici o trascendenti.

L'esistenza dei numeri trascendenti può, d'altra parte, essere dimostrata in modo più semplice, anche se indiretto, facendo nuovamente ricorso alla teoria della cardinalità.

Proposizione 9.3.2. *i) L'insieme dei polinomi a coefficienti interi ha cadinalità numerabile.*

ii) L'insieme dei numeri reali algebrici ha cardinalità numerabile.

Dim: i) Sia $F(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$ un polinomio non nullo a coefficienti interi di grado d. Chiamiamo **altezza** di $F(X)$ il numero naturale $h(F) = d + |a_d| + |a_{d-1}| + \cdots + |a_0|$. Per ogni numero naturale n vi è solo un numero finito di polinomi di altezza n.

Gli unici polinomi di altezza 1 sono i polinomi costanti 1 e -1.

I polinomi di altezza 2 sono X, $-X$, 2, -2. E così via.

Si può allora costruire una applicazione biunivoca $f\colon \mathbb{N} \to \mathbb{Z}[X]$ nel modo seguente: $f(0) = 0_{\mathbb{Z}[X]}$; $f(1)$ e $f(2)$ sono i due polinomi di altezza 1; $f(3)$, $f(4)$, $f(5)$ e $f(6)$ sono i quattro polinomi di altezza 2, e così via. Allora $Card(\mathbb{Z}[X]) = Card(\mathbb{N}) = \aleph_0$.

ii) Intanto $Card(\mathbf{A}) \geq \aleph_0$, poiché tutti i numeri razionali sono algebrici. Proviamo che vale anche la diseguaglianza opposta.

Ricordiamo che i polinomi a coefficienti interi possono essere pensati anche come particolari polinomi a coefficienti reali ed hanno quindi un numero di radici reali minore od uguale al loro grado.

Fissato un numero naturale $h \neq 0$, ci sono solo un numero finito di polinomi a coefficienti interi di altezza h e quindi un numero finito $k(h)$ di numeri reali algebrici che sono radici di tali polinomi. Possiamo allora costruire una applicazione $g\colon \mathbb{N} \to \mathbf{A}$ facendo corrispondere i primi $k(1)$ naturali alle $k(1)$ radici reali dei polinomi di altezza 1; i successivi $k(2)$ naturali alle $k(2)$ radici reali dei polinomi di altezza 2, e così via.

Tale applicazione non è iniettiva (poiché uno stesso numero algebrico è radice di tanti polinomi, anche di altezze diverse), ma è suriettiva per costruzione. Se infatti x è radice di un certo polinomio a coefficienti interi $F(X)$ di altezza h, allora x è immagine di almeno un numero naturale $r \leq k(1) + k(2) + \cdots + k(h)$.

Allora si ha $Card(\mathbf{A}) \leq Card(\mathbb{N}) = \aleph_0$ e quindi $Card(\mathbf{A}) = \aleph_0$. $\diamond$

Corollario 9.3.3. *I numeri reali algebrici* $\mathbf{A}$ *formano un sottoinsieme proprio di* $\mathbb{R}$ *ed anzi esiste un'infinità più che numerabile di numeri reali trascendenti.*

Possiamo riepilogare quanto visto in questo paragrafo con le seguenti relazioni insiemistiche:

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} = \mathbf{A} \cup \mathbb{T} \text{ con } \mathbb{Q} \subset \mathbf{A} \subset \mathbb{R} \text{ e quindi } \mathbb{T} \subset \mathbb{I} \subset \mathbb{R}.$$

Osserviamo però che mentre $\mathbb{I}$ e $\mathbb{T}$ sono semplici sottoinsiemi, $\mathbf{A}$, così come $\mathbb{Q}$, è un sottocampo di $\mathbb{R}$, ossia ha la struttura di campo mediante le stesse operazioni di somma e prodotto di $\mathbb{R}$.

Proposizione 9.3.4. $\mathbf{A}$ *è un campo con le operazioni di somma e prodotto indotte da quelle di* $\mathbb{R}$.

Dim: In questa dimostrazione facciamo ricorso a proprietà degli spazi vettoriali che sono trattati nel corso di Geometria 2.

Proviamo che opposti, inversi, somme e prodotti di numeri algebrici sono ancora numeri algebrici.

Se x è radice del polinomio a coefficienti interi $a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$, allora $-x$ è radice di $a_dX^d + (-1)a_{d-1}X^{d-1} + \cdots + (-1)^{d-1}a_1X + (-1)^d a_0$ e analogamente x^{-1} è radice di $a_d + a_{d-1}X + \cdots + a_1X^{d-1} + a_0X^d$.

Siano ora x e y due numeri algebrici radici rispettivamente dei polinomi monici a coefficienti razionali $F(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0$ e $G(X) = X^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0$. Si ha allora $F(x) = 0$ da cui $x^d = -b_{d-1}x^{d-1} - \cdots - b_1x - b_0$ e analogamente $G(y) = 0$ da cui $y^r = -c_{r-1}y^{r-1} - \cdots - c_1y - c_0$.

L'insieme V delle combinazioni lineari a coefficienti in $\mathbb{Q}$ di elementi del tipo $x^\alpha y^\beta$, $\alpha, \beta \in \mathbb{N}$, è uno spazio vettoriale su $\mathbb{Q}$, che, grazie alle precedenti relazioni, risulta avere dimensione $\leq dr$.

Infatti, ogni potenza di x con esponente $\geq d$ (ogni potenza di y con esponente $\geq r$) può essere scritta come combinazione lineare di potenze di x (risp. di y) di grado inferiore e quindi $\{x^\alpha y^\beta \mid 0 \leq \alpha \leq d-1, 0 \leq \beta \leq r-1\}$ è un insieme di generatori di V con dr elementi.

Allora $dr + 1$ elementi qualsiasi di V sono linearmente dipendenti.

In particolare sono linearmente dipendenti gli elementi $(x+y)^{dr}, (x+y)^{dr-1}, \ldots, (x+y), 1$ ossia esiste una relazione con coefficienti razionali non tutti nulli

$$q_{dr}(x+y)^{dr} + q_{dr-1}(x+y)^{dr-1} + \cdots + q_1(x+y) + q_0 = 0$$

e quindi $x+y$ è algebrico.

Allo stesso modo si prova che è algebrico il prodotto xy. $\diamond$

9.4 Esercizi

9.1. Caratterizzare tutte le coppie di numeri razionali (a, b) tali che $X^2 + aX + b$ abbia una radice razionale.

9.2. Definire il numero reale $2^{\sqrt{2}}$.

9.3. Siano $q \in \mathbb{Q}$, $q \neq 0$ e $x, y \in \mathbb{I}$. Provare oppure confutare mediante un esempio le seguenti affermazioni:

- **a.** $q + x$ e qx sono irrazionali;
- **b.** $x + y$ e xy sono irrazionali;
- **c.** $x + y$ e xy sono trascendenti se e solo se x e y lo sono;
- **d.** x^2 è trascendente se e solo se x lo è.

9.4. Provare che i numeri reali sono densi, ossia che tra due numeri reali esiste sempre un altro numero reale. Più precisamente provare che:

- **a.** tra due numeri reali sono compresi infiniti numeri reali;
- **b.** tra due numeri reali sono compresi infiniti numeri razionali e infiniti numeri irrazionali;
- **c.** tra due numeri reali sono compresi infiniti numeri algebrici e infiniti numeri trascendenti.

9.5*. Siano X e Y due sottoinsiemi non vuoti di $\mathbb{R}$ tali che $\forall x \in X$ e $\forall y \in Y$ si ha $x \leq y$.

Siano $x = (A_x, B_x)$ e $y = (A_y, B_y)$ gli elementi di X e Y. Provare che il numero reale $z' = (\ldots, \bigcap_{x \in X} B_x)$ soddisfa le relazioni $x \leq z' \leq y$, $\forall x \in X$ e $\forall y \in Y$.

9.6. Sia α un numero algebrico, radice del polinomio $F(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Q}[X]$ Trovare una radice del polinomio $G(X) = F(X-1)$ e una radice di $H(X) = F(2X+3)$.

9.7. Alla luce dell'esercizio precedente provare che $\sqrt{3}+2$ è un numero algebrico, trovando esplicitamente un polinomio a coefficienti razionali di cui è radice.

9.8. Verificare che i seguenti numeri $-3\sqrt[3]{2}$, $\frac{\sqrt[3]{2}}{5}$, $\sqrt[3]{2} - 1$, $\sqrt{2} + \sqrt{7}$ sono algebrici trovando esplicitamente per ciascuno di essi un polinomio a coefficienti razionali di cui sono radice.

9.9*. Verificare che i seguenti numeri sono algebrici trovando esplicitamente per ciascuno di essi un polinomio a coefficienti razionali di cui sono radice :

$$\sqrt{2} + \sqrt{7}, \quad \frac{1}{\sqrt{2} + \sqrt{7}}, \quad \sqrt{2} + \sqrt[3]{2}, \quad \sqrt{2} + \sqrt{3} + \sqrt{5}.$$

9.10*. Sia X un sottoinsieme non vuoto di $\mathbb{R}$. Si dice **maggiorante** di X ogni numero reale a tale che $a \geq x$ per ogni $x \in X$. Indichiamo con M_X l'insieme dei maggioranti di X. Provare che $X = \emptyset$ oppure M_X è un sottoinsieme di $\mathbb{R}$ che ammette minimo s.

(Se $M_X \neq \emptyset$, si dice che X è **superiormente limitato** e l'elemento s si dice **estremo superiore di** X; in caso contrario si dice che X non è superiormente limitato e che l'estremo superiore di X è $+\infty$)

9.11*. Sia X un sottoinsieme non vuoto di $\mathbb{R}$. Definire per analogia a quanto visto nell'esercizio precedente i concetti di **minorante** e di **estremo inferiore** di X.

9.12*. Sia X un sottoinsieme non vuoto di $\mathbb{R}$. Provare che se esiste il massimo m di X allora m è anche l'estremo superiore di X.

9.13. Trovare esempi espliciti (oppure provare che non esistono) di sottoinsiemi X di $\mathbb{R}$ tali che:

i) X è superiormente limitato, ma non è inferiormente limitato;

ii) X è superiormente limitato, ma non ha massimo;

iii) M_X è un insieme numerabile;

iv) M_X è un intervallo limitato di $\mathbb{R}$.

9.14. Determinare oppure provare che non esistono, motivando comunque in modo completo la risposta, maggioranti, minoranti, estremo superiore e inferiore, massimo e minimo di $X = \{\frac{1}{n+1} \mid n \in \mathbb{N}\}$.

9.15. Determinare oppure provare che non esistono, motivando comunque in modo completo la risposta, maggioranti, minoranti, estremo superiore e inferiore, massimo e minimo di $X = \{\frac{n}{n^2+1} \mid n \in \mathbb{Z}\}$.

9.16. Determinare oppure provare che non esistono, motivando comunque in modo completo la risposta, maggioranti, minoranti, estremo superiore e inferiore, massimo e minimo di $X = \mathbb{Q}$.

9.17. Determinare oppure provare che non esistono, motivando comunque in modo completo la risposta, maggioranti, minoranti, estremo superiore e inferiore, massimo e minimo di $X = \{sen(x) \mid x \in \mathbb{R}\}$.

9.18. Determinare oppure provare che non esistono, motivando comunque in modo completo la risposta, maggioranti, minoranti, estremo superiore e inferiore, massimo e minimo di $X = \{(1 + \frac{1}{n})^n \mid n \in \mathbb{N},\ n \geq 1\}$.

Capitolo 10

Il campo $\mathbb{C}$ dei numeri complessi

Il campo dei numeri complessi è (per noi) il punto di arrivo della serie di ampliamenti successivi di $\mathbb{N}$, quello in cui, finalmente, tutte le equazioni polinomiali ammettono un numero di radici pari al loro grado.

10.1 La forma algebrica dei numeri complessi

Definizione 10.1.1. *Si dice* **insieme dei numeri complessi** *il prodotto cartesiano* $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ *ossia l'insieme delle coppie di numeri reali* (a, b)*. In* $\mathbb{C}$ *sono inoltre definite le seguenti operazioni di somma e prodotto in* $\mathbb{C}$ *a partire dalle operazioni di* $\mathbb{R}$*:*

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) \\ (a,b) \cdot (c,d) &= (ac - bd, ad + bc) \end{aligned}$$

Lasciamo come esercizio al lettore la dimostrazione del seguente semplice risultato.

Lemma 10.1.2. *L'applicazione* $i \colon \mathbb{R} \to \mathbb{C}$ *data da* $i(a) = (a, 0)$ *è iniettiva e rispetta le operazioni, ossia* $i(a + b) = i(a) + i(b)$ *e* $i(ab) = i(a) \cdot i(b)$*.*

Grazie a questo risultato, nel seguito potremo senza ambiguità identificare i numeri reali con particolari numeri complessi.

Proposizione 10.1.3. $\mathbb{C}$ *con le operazioni sopra definite è un campo che estende* $\mathbb{R}$*.*

Dim: Ci limitiamo soltanto ad elencare le tante verifiche necessarie a provare che $\mathbb{C}$ è un campo, poiché sono tutte molto semplici:

- la somma e il prodotto sono associative e commutative e vale la proprietà distributiva del prodotto rispetto alla somma;
- $0_{\mathbb{C}} = (0, 0)$;
- $-(a, b) = (-a, -b)$;

- $1_{\mathbb{C}} = (1, 0)$;
- se $(a, b) \neq (0, 0)$, allora $(a, b)^{-1} = (\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$.

Il fatto che il campo $\mathbb{C}$ sia un'estensione di $\mathbb{R}$ è, a questo punto, conseguenza immediata del lemma precedente. $\diamond$

Nel seguito identificheremo sempre il numero reale a col numero complesso $(a, 0)$.

Esempio 10.1.4. *Il polinomio $X^2 + 1$ ha le due radici complesse $(0, 1)$ e $(0, -1)$. Si ha infatti:*

$$(0,1)^2 + 1 = (0,1)^2 + (1,0) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) + (1,0) = (-1,0) + (1,0) = (0,0).$$

Analogamente si verifica che anche $(0, -1)$ è una radice di $X^2 + 1$.

Più in generale, tutti i polinomi di grado 2 a coefficienti reali del tipo $X^2 + bX + c$ hanno due radici complesse, eventualmente coincidenti.

Se il discriminante $\Delta = b^2 - 4c$ è positivo o nullo, ci sono le radici reali $\frac{-b+\sqrt{\Delta}}{2}$ e $\frac{-b-\sqrt{\Delta}}{2}$ (e quindi le radici complesse $(\frac{-b+\sqrt{\Delta}}{2}, 0)$ e $(\frac{-b-\sqrt{\Delta}}{2}, 0)$).

Se Δ è negativo, ci sono le radici complesse $(\frac{-b}{2}, \frac{\sqrt{-\Delta}}{2})$ e $(\frac{-b}{2}, -\frac{\sqrt{-\Delta}}{2})$.

Definizione 10.1.5. *Il numero complesso $(0, 1)$ si dice* **unità immaginaria** *e si denota abitualmente con i.*
Ogni numero complesso $z = (a, b)$ può essere scritto nella forma $z = (a, 0) + (0, 1)(b, 0)$ ossia $z = a + ib$ con $a, b \in \mathbb{R}$; a si dice **parte reale** *di z, denotata $\mathrm{Re}(z)$, e b si dice* **coefficiente dell'immaginario** *di z, denotato $\mathrm{Im}(z)$.*

A questo punto possiamo pensare a $\mathbb{C}$ come all'insieme delle espressioni del tipo $a + ib$ con $a, b \in \mathbb{R}$. Le operazioni di somma e prodotto si ottengono mediante le usuali regole del calcolo letterale dalle operazioni in $\mathbb{R}$, tenendo conto inoltre che $i^2 = -1$:

$$(a + ib) + (a' + ib') = (a + a') + i(b + b')$$

$$(a + ib) \cdot (a' + ib') = aa' + iab' + ia'b + i^2bb' = (aa' - bb') + i(ab' + a'b).$$

Il numero complesso $-i = (0, -1)$ ha in realtà le stesse proprietà di i e risulta essere perfettamente interscambiabile con i.

Definizione 10.1.6. *Si dice* **coniugio** *la funzione di $\mathbb{C}$ in $\mathbb{C}$ data da*

$$z = a + ib \quad \mapsto \quad \overline{z} = a - ib.$$

Si tratta di una funzione biunivoca, che coincide con la sua inversa e che rispetta le operazioni.
Il numero complesso $\overline{z} = a - ib$ si dice **coniugato** *di $z = a + ib$.*

Lasciamo come esercizio al lettore la verifica dei seguenti fatti di cui avremo bisogno in seguito:

- $\forall z \in \mathbb{C}$: $\quad z + \overline{z} \in \mathbb{R}$ e $z - \overline{z} \in i\mathbb{R}$ (insieme dei numeri immaginari puri);

- $\forall z \in \mathbb{C} \setminus \{0\}$: $\quad z \cdot \overline{z} \in \mathbb{R}^+$;

- $\forall z \in \mathbb{C}$: $\quad z = \overline{z} \iff z \in \mathbb{R}$.

Definizione 10.1.7. *Si dice* **modulo** *del numero complesso $z = a + ib$ il numero reale positivo o nullo $|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}$.*
Da quanto sopra risulta $|z| = 0$ se e solo se $z = 0$.

Osservazione 10.1.8. *Nell'insieme dei numeri complessi possono essere introdotti molti ordinamenti parziali o anche totali, ma nessuno di questi rende $\mathbb{C}$ un campo ordinato ossia nessuno di questi è compatibile con le operazioni.*

Supponiamo, infatti, che esista un ordine totale $\preceq$ in $\mathbb{C}$ compatibile con le operazioni. Presi due qualsiasi numeri ($\neq 0$) opposti x e y, necessariamente uno è maggiore di 0 e l'altro minore di 0: se $x \succeq 0$ allora $y = 0 + y \preceq x + y = 0$ e viceversa.

Consideriamo in particolare la coppia di opposti i e $-i$.

Se $i \succeq 0$ e $-i \preceq 0$, moltiplicando i due membri di $i \succeq 0$ due volte per il numero positivo i otteniamo la contraddizione $-i \succeq 0$.

Analogamente se $-i \succeq 0$ e $i \preceq 0$, moltiplicando i due membri di $i \preceq 0$ due volte per il numero positivo $-i$ otteniamo la contraddizione $-i \preceq 0$.

Definizione 10.1.9. *Un campo K si dice* **algebricamente chiuso** *se ogni polinomio di grado d a coefficienti in K ammette d radici in K (pur di contare ciascuna con la sua molteplicità).*

10.2 Il Teorema Fondamentale dell'Algebra

Ci limitiamo ad enunciare, senza dimostrarlo, il seguente importantissimo risultato. Esistono diverse dimostrazioni di questo risultato, ma tutte richiedono conoscenze superiori di algebra o di analisi.

Teorema 10.2.1. (Teorema fondamentale dell'algebra) *Ogni polinomio $F(X) \in \mathbb{C}[X]$ di grado $d \geq 1$ ammette almeno una radice complessa.*

Dal Teorema fondamentale dell'algebra discendono le seguenti conseguenze, che dimostreremo dando per noto tale teorema.

Corollario 10.2.2. *Il campo $\mathbb{C}$ dei numeri complessi è* **algebricamente chiuso**, *ossia: ogni polinomio $F(X) = c_dX^d + c_{d-1}X^{d-1} + \cdots + c_0$ a coefficienti complessi, di grado $d \geq 1$, ammette d radici complesse $\alpha_1, \ldots, \alpha_d$ (non necessariamente distinte) e si decompone quindi nel prodotto di d fattori lineari*

$$F(X) = c_d(X - \alpha_1) \cdot \cdots \cdot (X - \alpha_d).$$

Dim: Procediamo per induzione sul grado d. Se $d = 1$ l'asserto è ovvio.

Supponiamolo vero per tutti i polinomi di grado $< d$ e proviamolo per il polinomio $F(X)$ di grado d. In virtù del Teorema fondamentale dell'algebra $F(X)$ ammette una radice in $\mathbb{C}$ che indichiamo con $alpha_d$. Per il Teorema di Ruffini, $F(X) = (X - \alpha_d)G(X)$, dove $G(X)$ ha grado $d-1$. Applicando l'ipotesi induttiva, $G(X)$ si decompone nel prodotto di fattori lineari $G(X) = c_d(X - \alpha_1) \cdot \cdots \cdot (X - \alpha_{d-1})$ e la tesi si ottiene per sostituzione. $\diamond$

Questo risultato relativo a $\mathbb{C}$ fornisce importanti informazioni anche sulle radici reali dei polinomi a coefficienti reali.

Corollario 10.2.3. (Teorema fondamentale dell'algebra per $\mathbb{R}$) *Ogni polinomio $F(X)$ a coefficienti reali, di grado d, ammette $d-2r$ radici reali $\beta_1, \ldots, \beta_{d-2r}$ e $2r$ radici complesse non reali, a due a due coniugate, $\gamma_1, \overline{\gamma_1}, \ldots, \gamma_r, \overline{\gamma_r}$, per un certo intero r, $0 \leq 2r \leq d$.*

Allora $F(X)$ si decompone in $\mathbb{R}[X]$ nel prodotto di $d - 2r$ fattori lineari e di r fattori di grado 2 con discriminante negativo:

$$F(X) = a_d(X - \beta_1) \cdot \cdots \cdot (X - \beta_{d-2r}) \cdot (X^2 + b_1X + c_1) \cdot \cdots \cdot (X^2 + b_rX + c_r)$$

in cui $b_i = -(\gamma_i + \overline{\gamma_i}) \in \mathbb{R}$, $c_i = \gamma_i \cdot \overline{\gamma_i} \in \mathbb{R}$ e $\Delta_i = b_i^2 - 4c_i < 0$.

Dim: Il polinomio a coefficienti reali $F(X) = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ può essere anche considerato come polinomio a coefficienti complessi (poiché $\mathbb{R} \subseteq \mathbb{C}$) e quindi, per il Teorema fondamentale dell'algebra, $F(X)$ ha d radici complesse non necessariamente distinte $\alpha_1, \ldots, \alpha_d$.

Valutiamo il polinomio $F(X)$ in un qualsiasi numero complesso z e quindi applichiamo il coniugio, ricordando che rispetta somma e prodotto e che non modifica i numeri reali:

$$\overline{F(z)} = \overline{a_dz^d + a_{d-1}z^{d-1} + \cdots + a_1z + a_0} = \overline{a_d}\,\overline{z}^d + \overline{a_{d-1}}\,\overline{z}^{d-1} + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} =$$

$$= a_d\overline{z}^d + a_{d-1}\overline{z}^{d-1} + \cdots + a_1\overline{z} + a_0 = F(\overline{z}).$$

Se, in particolare, z è una radice complessa di $F(X)$, ossia se $F(z) = 0$, allora $F(\overline{z}) = \overline{F(z)} = \overline{0} = 0$ e quindi anche $\overline{z}$ è una radice complessa di $F(X)$, una diversa radice complessa nel caso in cui z non sia reale.

Possiamo allora riordinare le d radici complesse di $F(X)$ in modo da avere prima le radici reali $\beta_1, \ldots, \beta_t$ e poi le coppie coniugate di radici non reali $\gamma_1, \overline{\gamma_1}, \ldots, \gamma_r, \overline{\gamma_r}$, con $t + 2r = d$ ossia $t = d - 2r$.

Le radici reali danno luogo a fattori di $F(X)$ di grado 1 con coefficienti reali $(X - \beta_i)$.

Le coppie di radici complesse coniugate non reali danno luogo a coppie di fattori lineari $(X - \gamma_j)$ e $(X - \overline{\gamma_j})$ che, singolarmente, hanno coefficienti non reali, ma il cui prodotto è un polinomio di grado 2 a coefficienti in $\mathbb{R}$:

$$(X - \gamma_j)(X - \overline{\gamma_j}) = X^2 - (\gamma_j + \overline{\gamma_j})X + \gamma_j\overline{\gamma_j} = X^2 + b_jX + c_j.$$

Calcoliamo infine il discriminante:

$$\Delta = (\gamma_j + \overline{\gamma_j})^2 - 4\gamma_j\overline{\gamma_j} = (\gamma_j - \overline{\gamma_j})^2 = (2i\mathrm{Re}(\gamma_j))^2 = -4\mathrm{Re}(\gamma_j)^2$$

che è appunto un numero reale negativo. $\diamond$

Corollario 10.2.4. *Ogni polinomio a coefficienti reali di grado d ha un numero di radici reali che ha la stessa parità di d.*

In particolare ogni polinomio di grado dispari ha almeno una radice reale.

Corollario 10.2.5. *Gli unici polinomi irriducibili di $\mathbb{R}[X]$ sono quelli di grado 1, oppure di grado 2 con discriminante negativo.*

Ogni polinomio a coefficienti reali di grado $d \geq 3$ è riducibile, ossia si spezza nel prodotto di (almeno) due polinomi di $\mathbb{R}[X]$ non costanti.

NOTA BENE I risultati, veramente fondamentali, presentati in questo paragrafo hanno carattere esclusivamente esistenziale, ossia provano l'esistenza di radici reali e complesse di polinomi reali e complessi, ma non forniscono metodi operativi per calcolare tali radici.

Sul versante operativo, esistono formule risolutive per radicali delle equazioni polinomiali di grado 2 (ben note) ed anche di grado 3 e 4 (meno usate perchè più complicate).

L'equazione generale di grado superiore non ammette, invece, formule risolutive per radicali (**Teorema di Abel-Ruffini**) e le classi di equazioni risolubili di grado ≥ 5 sono caratterizzate dalla **Teoria di Galois**.

Un particolare tipo di polinomi di grado qualsiasi di cui siamo in grado di calcolare tutte le radici complesse sarà esaminato nel paragrafo successivo.

Possiamo estendere ai numeri complessi la definizione di numeri algebrici. Si dice insieme dei **numeri complessi algebrici** il seguente sottoinsieme di $\mathbb{C}$:

$$\mathbf{A}_{\mathbb{C}} = \{z \in \mathbb{C} \mid z \text{ è radice di un polinomio } F(X) \text{ a coefficienti razionali}\}.$$

Usando le tecniche dell'Algebra lineare si può provare che $\mathbf{A}_{\mathbb{C}}$ ha la struttura algebrica di un campo, in modo del tutto analogo a quanto fatto per $\mathbf{A}$.

Si può, inoltre, provare che $\mathbf{A}_{\mathbb{C}}$ è algebricamente chiuso, ossia che ogni polinomio a coefficienti in $\mathbf{A}_{\mathbb{C}}$ (e non soltanto a coefficienti in $\mathbb{Q}$) ammette radici in $\mathbf{A}_{\mathbb{C}}$. Il campo $\mathbf{A}_{\mathbb{C}}$ è dunque la minima estensione di $\mathbb{Q}$ in cui tutte le equazioni polinomiali ammettono soluzioni.

Vi sono molti altri sottoanelli o sottocampi notevoli di $\mathbb{C}$. Vediamone due esempi particolarmente significativi, anche se una trattazione approfondita di questo argomento esula dagli scopi del corso.

Esempio 10.2.6. L'anello degli interi di Gauss *è il sottoanello di* $\mathbb{C}$*:*

$$\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

È un anello che ha molte proprietà in comune con $\mathbb{Z}$*, in particolare l'esistenza di una divisione con resto con le relative conseguenze, tra cui la fattorizzazione degli elementi non nulli e non invertibili nel prodotto di fattori primi.*

Un anello in cui non vale la fattorizzazione in fattori primi *Consideriamo il seguente sottoanello di* $\mathbb{C}$*:*

$$\mathbb{Z} + i\sqrt{5}\mathbb{Z} = \{a + i\sqrt{5}b \mid a, b \in \mathbb{Z}\}.$$

Gli elementi invertibili di questo anello sono soltanto $1, -1$*, ossia gli elementi che hanno modulo* 1*. Più in generale gli elementi di* $\mathbb{Z} + i\sqrt{5}\mathbb{Z}$ *hanno modulo il cui quadrato è sempre un numero intero:* 0 *per* 0*,* 1 *per gli invertibili,* ≥ 4 *per tutti gli altri; quindi i numeri riducibili hanno quadrato del modulo* ≥ 16*.*
In questo particolare anello il numero 6 *possiede due fattorizzazioni essenzialmente diverse in fattori irriducibili:*

$$6 = 2 \cdot 3 \qquad e \qquad 6 = (1 + \sqrt{5}i) \cdot (1 - \sqrt{5}i).$$

I fattori 2*,* 3*,* $(1+\sqrt{5}i)$ *e* $(1-\sqrt{5}i)$ *hanno quadrato del modulo inferiore a* 16 *e sono quindi irriducibili; inoltre* 2 *e* 3 *non sono associati a* $(1 + \sqrt{5}i)$ *e* $(1 - \sqrt{5}i)$ *perchè hanno modulo differente da questi ultimi: le due fattorizzazioni sono quindi essenzialmente diverse.*
Inoltre il numero irriducibile 2 *divide il prodotto* $(1 + \sqrt{5}i) \cdot (1 - \sqrt{5}i)$*, ma non divide nessuno dei due fattori:* 2 *è irriducibile, ma non è primo.*
In conclusione, nell'anello $\mathbb{Z} + i\sqrt{5}\mathbb{Z}$ *irriducibile non è equivalente a primo e non tutti i numeri si fattorizzano in fattori primi.*

10.3 Forma polare o trigonometrica dei numeri complessi

Un numero complesso è dato da una coppia di numeri reali (a, b) e quindi, in modo del tutto naturale, corrisponde al punto del piano cartesiano $\mathbb{R}^2$ di coordinate (a, b).

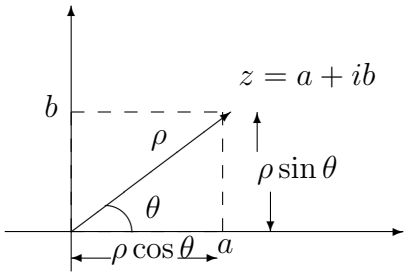
Definizione 10.3.1. *Col termine* **Piano di Gauss** *si intende appunto il piano cartesiano* $\mathbb{R}^2$ *identificato col campo dei numeri complessi* $\mathbb{C}$*. Lo zero di* $\mathbb{C}$ *corrisponde all'origine delle coordinate, i numeri reali corrispondono ai punti dell'asse* X*, i numeri immaginari puri corrispondono ai punti dell'asse* Y*.*

La somma di due numeri complessi, inoltre, corrisponde alla somma in $\mathbb{R}^2$ di vettori applicati nell'origine.

Se, infatti, i numeri complessi $z_1 = a_1 + ib_1$ e $z_2 = a_2 + ib_2$ corrispondono ai punti $P = (a_1, b_1)$ e $Q = (a_2, b_2)$, allora la loro somma $z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$ corrisponde al punto $R = (a_1 + a_2, b_1 + b_2)$ individuato dalla somma di vettori $\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{OR}$.

Per poter dare una buona interpretazione geometrica anche al prodotto, introduciamo la **rappresentazione trigonometrica** dei numeri complessi mediante le **coordinate polari**.

Ogni punto del $P = (a, b)$ del piano $\mathbb{R}^2$ (oppure, equivalentemente, ogni vettore $\overrightarrow{OP}$ applicato nell'origine, ogni numero complesso $z = a + ib$) può essere individuato mediante una coppia di coordinate polari (ρ, θ), dove ρ è la lunghezza del segmento $\overline{OP}$, ossia $\rho = \sqrt{a^2 + b^2}$, e θ è un qualsiasi angolo (misurato in radianti) tale che $a = \rho \cos\theta$ e $b = \rho \sin\theta$.



I numeri ρ e θ si dicono rispettivamente **il modulo** e **un argomento** di z.

Il modulo ρ può assumere qualsiasi valore reale positivo o nullo e si ha $\rho = 0$ se e soltanto se $z = 0$. In quest'ultimo caso (e solo in questo) non è definito alcun argomento, che, d'altra parte, risulta superfluo essendo il numero complesso già perfettamente determinato dall'informazione $\rho = 0$.

Se il modulo ρ di z è non nullo, allora vi sono infiniti possibili argomenti diversi per z.

L'unico argomento θ_0 di z tale che $0 \leq \theta_0 < 2\pi$ si dice **argomento principale** di z; ogni altro argomento di z differisce da θ_0 per multipli interi (positivi e negativi) di 2π: $\theta = \theta_0 + 2k\pi$, $k \in \mathbb{Z}$.

I passaggi da coordinate cartesiane a coordinate polari e viceversa si ottengono dalle relazioni già indicate in precedenza:

$$\text{da cartesiane a polari} \quad \begin{cases} \rho = \sqrt{a^2 + b^2} \\ \cos\theta = \frac{a}{\rho} \\ \sin\theta = \frac{b}{\rho} \end{cases} \quad ; \quad \text{da polari a cartesiane} \quad \begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases}$$

Proposizione 10.3.2. Formula del prodotto in coordinate polari. *Siano z_1 e z_2 numeri complessi con coordinate polari (ρ_1, θ_1) e (ρ_2, θ_2).*

Il loro prodotto ha come modulo i prodotti dei due moduli e come argomento la somma dei due argomenti: $z_1 \cdot z_2 = (\rho_1\rho_2, \theta_1 + \theta_2)$.

Dim: Calcoliamo il prodotto $z_1 \cdot z_2$ passando in coordinate cartesiane:

$$z_1 \cdot z_2 = (\rho_1 \cos\theta_1 + i\rho_1 \sin\theta_1) \cdot (\rho_2 \cos\theta_2 + i\rho_2 \sin\theta_2) =$$
$$= \rho_1\rho_2(\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + i\rho_1\rho_2(\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2).$$

Applicando infine la formula che dà seno e coseno dell'angolo somma otteniamo

$$z_1 \cdot z_2 = \rho_1\rho_2 \cos(\theta_1 + \theta_2) + i\rho_1\rho_2 \sin(\theta_1 + \theta_2)$$

che fornisce immediatamente modulo e argomento del prodotto dei due numeri complessi. ◇

Corollario 10.3.3. Potenze n-esime di un numero complesso *Sia $z = (\rho, \theta)$ un numero complesso espresso mediante coordinate polari e sia n un numero intero (positivo, negativo o nullo).*

Allora: $z^n = (\rho^n, n\theta)$.

Dim: Se $n = 0$, si ha $(\rho^0, 0 \cdot \theta) = (1, 0) = 1$ che è proprio, per convenzione, z^0.

Se $n = -1$, posto $z' = (\rho^{-1}, -\theta)$ si ha $z \cdot z' = (\rho\rho^{-1}, \theta - \theta) = (1, 0) = 1$ e quindi z' è proprio l'inverso z^{-1} di z.

Se $n \geq 2$ (oppure $n \leq -2$), è sufficiente moltiplicare n volte z per sè (rispettivamente $-n$ volte z^{-1} per sè) usando la formula del prodotto. ◇

Corollario 10.3.4. Radici n-esime di un numero complesso *Sia $z = (\rho, \theta)$ un numero complesso non nullo, espresso mediante coordinate polari, e sia n un numero intero positivo.*

Allora l'equazione $X^n = z$ ha esattamente n soluzioni distinte le cui espressioni in coordinate polari sono:

$$z_0 = (\sqrt[n]{\rho}\,, \frac{\theta}{n})\ ,\ z_1 = (\sqrt[n]{\rho}, \frac{\theta + 2\pi}{n}), \ldots, z_k = (\sqrt[n]{\rho}, \frac{\theta + 2k\pi}{n}), \ldots, z_{n-1} = (\sqrt[n]{\rho}, \frac{\theta + 2(n-1)\pi}{n}).$$

Dim: L'equazione polinomiale $X^n = z$ ha grado n e quindi non può avere più di n soluzioni distinte. Sarà allora sufficiente provare che quelle scritte sono sue soluzioni e che sono tutte diverse.

Presi due indici h, k diversi, $0 \leq h < k \leq n - 1$, i numeri complessi z_h e z_k hanno lo stesso modulo, ma argomenti $\frac{\theta+2h\pi}{n}$ e $\frac{\theta+2k\pi}{n}$ che differiscono per l'angolo $\frac{2(k-h)\pi}{n}$ maggiore di 0 e minore di 2π: z_h e z_k sono quindi numeri complessi diversi.

Infine, usando la formula delle potenze n-esime, troviamo:

$$z_k^n = ((\sqrt[n]{\rho})^n, n \cdot \frac{\theta + 2k\pi}{n}) = (\rho, \theta + 2k\pi) = (\rho, \theta) = z$$

e quindi i numeri complessi z_k sono soluzioni dell'equazione $X^n = z$. ◇

Geometricamente le radici $n-$esime del numero complesso z si dispongono ai vertici di un poligono regolare con n lati inscritto nella circonferenza di centro l'origine e raggio $\sqrt[n]{|z|}$. Calcolata una qualsiasi di tali radici, sarà allora possibile determinare in modo grafico tutte le altre costruendo il poligono regolare con n lati, con centro nell'origine e un vertice nel punto corrispondente alla radice trovata.

10.4 Esercizi

10.1. Eseguire le verifiche necessarie alla dimostrazione della Proposizione 10.1.3.

10.2. Verificare che se Δ è negativo, i numeri complessi $\frac{-b}{2}+i\frac{\sqrt{-\Delta}}{2}$ e $\frac{-b}{2}-i\frac{\sqrt{-\Delta}}{2}$ sono radici del polinomio X^2+bX+c a coefficienti reali, come affermato nell'Esempio 10.1.4.

10.3. Verificare che il coniugato di una somma è la somma dei coniugati e che il coniugato di un prodotto è il prodotto dei coniugati.

10.4. Sia z un qualsiasi numero complesso. Verificare che $z+\overline{z}$ e $z\cdot\overline{z}$ sono numeri reali e che $z-\overline{z}$ è immaginario puro.

10.5. Sia z un numero complesso.Verificare che $z=\overline{z}$ se e solo se $z\in\mathbb{R}$.

10.6. Calcolare la parte reale e la parte immaginaria dei seguenti numeri complessi:

$$(1+i)^5,\quad (2-i)^3-(1-3i)^2,\quad \frac{6+5i}{3-i},\quad \frac{(2+i)^3}{5i^{15}},\quad \frac{3-2i}{1+5i}+\frac{2-3i}{2-i}.$$

10.7. Determinare coordinate polari per i seguenti numeri complessi:

$$-3,\quad \pi,\quad \sin(2),\quad \cos(2),\quad \cos(2)+i\sin(2),\quad \cos(2)-i\sin(2),\quad \frac{1+i}{2},\quad 1-i\sqrt{3}.$$

10.8. Disegnare nel piano di Gauss i seguenti sottoinsiemi:

a. $A=\{z\in\mathbb{C}$ tali che $\mathrm{Re}(z)>\mathrm{Im}(z)\}$;

b. $B=\{z\in\mathbb{C}$ tali che $z+\overline{z}=i\}$; $B'=\{z\in\mathbb{C}$ tali che $z-\overline{z}=i\}$;

c. $C=\{z\in\mathbb{C}$ tali che $|z-2|\geq 2\}$; $C'=\{z\in\mathbb{C}$ tali che $|z+i|<|z-3|\}$;

d. $D=\{z=(\rho,\theta)\in\mathbb{C}$ tali che $\theta=\frac{\pi}{2}\}$; $D'=\{z=(\rho,\theta)\in\mathbb{C}$ tali che $\rho\geq 2\}$;

e. $E=\{z\in\mathbb{C}$ tali che $z-\overline{z}\in\mathbb{R}\}$; $E'=\{z\in\mathbb{C}$ tali che $\mathrm{Re}(z^4)=0\}$.

f. $F=\{z=(\rho,\theta)\in\mathbb{C}$ tali che $\theta=(2k+1)\pi$, $k\in\mathbb{Z}\}$;

g. $G=\{z=(\rho,\theta)\in\mathbb{C}$ tali che $\rho=1$ e $0\leq\theta\leq\pi\}$.

10.9. Consideriamo il polinomio $F(X)=2X^5-13X^4+37X^3-57X^2+48X-18$.

a. Verificare che $1-i$ è radice di $F(X)$.

b. Trovare tutte le radici razionali di $F(X)$.

c. Determinare la fattorizzazione di $F(X)$ in fattori primi in $\mathbb{R}[X]$.

d. Determinare la fattorizzazione di $F(X)$ in fattori primi in $\mathbb{C}[X]$.

10.10. Trovare tutte le radici complesse del polinomio X^6-8. Quali tra queste sono reali? Determinare la decomposizione di X^6-8 nel prodotto di fattori irriducibili in $\mathbb{C}[X]$ e poi in $\mathbb{R}[X]$.

10.11. Trovare tutte le radici complesse del polinomio $X^6 + 8$. Quali tra queste sono reali? Determinare la decomposizione di $X^6 + 8$ nel prodotto di fattori irriducibili in $\mathbb{C}[X]$ e poi in $\mathbb{R}[X]$.

10.12. Determinare le radici terze di i e le radici terze di $-i$.

10.13. Sia α una qualsiasi radice complessa del polinomio $X^8 + \sqrt{2}X^6 + 3$. È vero che α è un numero complesso algebrico? (Motivare la risposta).

10.14. Sia β una qualsiasi radice complessa del polinomio $X^3 - \pi X^2 + \pi + 1$. È vero che β è un numero complesso trascendente? (Motivare la risposta).

10.15. Verificare che $-2i$ è radice del polinomio $H(X) = X^3 + (2i - \pi)X^2 - (2i\pi - 3)X + 6i$. È vero che $-2i$ è algebrico? È vero che $H(X)$ è un polinomio a coefficienti razionali?

10.16. Dire se le seguenti affermazioni sono vere oppure false, motivando le risposte mediante dimostrazioni oppure controesempi, a seconda dei casi. Siano $\alpha \in \mathbb{C}$ e $F(X) \in \mathbb{C}[X]$:

- **a.** α algebrico e $F(\alpha) = 0 \Longrightarrow F(X) \in \mathbb{Q}[X]$;
- **b.** $F(X) \in \mathbb{Q}[X]$ e $F(\alpha) = 0 \Longrightarrow \alpha$ è algebrico;
- **c.** $F(X) \in \mathbb{Q}[X]$, α algebrico $\Longrightarrow F(\alpha) = 0$;
- **d.** $F(X) \notin \mathbb{Q}[X]$, α algebrico $\Longrightarrow F(\alpha) \neq 0$;
- **e.** α trascendente e $F(\alpha) = 0 \Longrightarrow F(X) \notin \mathbb{Q}[X]$.

10.17. Trovare la fattorizzazione in fattori irriducibili di $X^8 - 1$ in $\mathbb{R}[X]$ e in $\mathbb{C}[X]$.

10.18. Consideriamo il polinomio $G(X) = X^4 + 4X^2 + 8$.

- **a.** È vero che $G(X)$ è riducibile in $\mathbb{R}[X]$? In caso affermativo determinare la sua fattorizzazione in fattori irriducibili in $\mathbb{R}[X]$.
- **b.** È vero che $G(X)$ è riducibile in $\mathbb{C}[X]$? In caso affermativo determinare la sua fattorizzazione in fattori irriducibili in $\mathbb{C}[X]$.
- **c.** Trovare tutte le radici razionali di $G(X)$.
- **d.** Trovare tutte le radici algebriche di $G(X)$.

10.19. Calcolare parte reale e coefficiente dell'immaginario del numero complesso $(1 - i)^{53}$.

10.20. Disegnare nel piano di Gauss le radici quinte di i e le radici terze di $\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

10.21*. Verificare che i seguenti numeri complessi sono algebrici ossia sono radice di un polinomio a coefficienti razionali:

$$\cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right), \quad 2 + \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right), \quad 3 + i\sqrt{11}, \quad \sqrt[4]{2} - i, \quad \sqrt[3]{5} + i\sqrt{3}.$$

10.22. Per quali numeri $a \in \mathbb{C}$ l'equazione $X^6 - a = 0$ possiede almeno una radice immaginaria pura?

10.23. Determinare le radici (complesse) del polinomio $X^2 + 2X + i\sqrt{3}$.

10.24. Sia $F(X) = -3(X - 2)^3(X - 3i)(X - i + 5)(X^2 + X + 1)(3i + X)(5 + i + X)$.

a. Provare che $F(X) \in \mathbb{R}[X]$ senza eseguire i calcoli.

b. Determinare tutte le radici reali di $F(X)$ con la loro molteplicità.

c. Trovare la fattorizzazione di $F(X)$ in fattori primi in $\mathbb{R}[X]$.

10.25. Dimostrare direttamente senza usare il Teorema fondamentale dell'Algebra, che ogni polinomio di grado 2 a coefficienti complessi ammette due radici complesse.

10.26. Dire se il polinomio $G(X) = 3X^5 - X^4 + 6X^3 - 2X^2 + 3X - 1$ ha oppure non ha radici reali con molteplicità maggiore di 1. Ha radici complesse con molteplicità maggiore di 1?

10.27. Sia $\mathcal{G}$ l'insieme di tutti i numeri complessi del tipo $z = a + bi$ con a, $b \in \mathbf{Q}$. Mostrare che se x, $y \in \mathcal{G}$ allora $x + y$, $xy \in \mathcal{G}$, e che, inoltre, $x^{-1} \in \mathcal{G}$ se $x \neq 0$.

Posto $G = \{z = a+bi \in \mathcal{G} \mid a, b \in \mathbb{Z}\}$, quali delle proprietà precedenti resta valida in G? Determinare esplicitamente l'insieme degli $z \in G$ tali che $1/z \in G$.

10.28*. Sia $n > 1$ un un numero intero. Consideriamo gli n numeri complessi

$$\zeta_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \qquad k = 0, 1, \ldots, n-1.$$

Mostrare che:

a. $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ sono tutti distinti e $|\zeta_k| = 1$ per ogni k;

b. per ogni intero m si ha $\zeta_1^m = \zeta_r$, dove r è il resto della divisione di m per n;

c. $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ sono le n soluzioni complesse dell'equazione $X^n - 1 = 0$ (per questo motivo tali numeri sono detti *radici n-esime dell'unità*).

d. $\zeta_0 + \zeta_1 + \cdots + \zeta_{n-1} = 0$

10.29*. Sia $\mathcal{F}$ l'insieme di tutti i numeri reali della forma $a + b\sqrt{2}$ dove a, $b \in \mathbb{Q}$.

a. È vero che $\mathcal{F} = \mathbb{R}$?

b. Provare che $\mathcal{F}$ è un campo con le operazioni di somma e prodotto indotte da quelle di $\mathbb{C}$.

c. L'affermazione precedente rimarrebbe vera se ponessimo a, $b \in \mathbb{Z}$ nella definizione di $\mathcal{F}$?

d. Verificare che è una biezione l'applicazione

$$\sigma\colon \mathcal{F} \longrightarrow \mathcal{F}, \qquad \sigma(a + b\sqrt{2}) = a - b\sqrt{2}.$$

10.30*. Dimostrare che non esiste alcun ordinamento totale sul campo $\mathbb{Z}_3$ che renda $\mathbb{Z}_3$ un campo ordinato.

È vero anche per il campo $\mathbb{Z}_2$?

Capitolo 11

Esercizi di riepilogo

I seguenti esercizi sono presi da compiti d'esame.

11.1. Sia $\mathbb{R}^+$ l'insieme dei numeri reali strettamente positivi. Studiare le seguenti relazioni determinando, nel caso di equivalenze, la classe di $1 \in \mathbb{R}^+$.

a. $x \rho y \iff xy \geq y$ **b.** $x \rho y \iff x/y \in \mathbb{Q}$ **c.** $x \rho y \iff \log y - \log x \in \mathbb{Z}$.

11.2. Nell'anello $\mathbb{Z}_{36}$ delle classi di resto modulo 36:

a. determinare, se esiste, un numero minore di -1000 che rappresenta $[2]$;

b. provare che ogni classe ha un rappresentante multiplo di 5;

c. provare che $[13]$ è invertibile e determinare il suo inverso;

d. determinare il numero degli elementi non "cancellabili".

11.3. Nell'anello $\mathbb{Z}_{12}$ delle classi di resto modulo 12:

a. trovare tutte le classi $[x]$ tali che $[x]^2 + [x] = [2]$;

b. disegnare il grafico di $f\colon \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ data da $f([a]) = [a]^3 - [3a] + 1$.

11.4. Per ogni $n \in \mathbb{N}$, sia I_n l'intervallo aperto $(-\frac{1}{n+1},\ n)$ di $\mathbf{R}$. Determinare esplicitamente:

a. $\bigcap_{n\in\mathbb{N}} I_n$ **b.** $\bigcup_{n\in\mathbb{N}} I_n$ **c.** $\mathcal{C}_{\mathbb{R}}(I_n)$ **d.** $\mathcal{P}(I_3 \cap \mathbb{Z})$.

11.5. Sia A l'insieme dei numeri complessi che si possono scrivere nella forma $m + in$ con $m,\ n \in \mathbb{Q}$.

a. Verificare che A è un anello. A è un campo?

b. Determinare tutte le radici complesse del polinomio $X^3 - 8$. Quante sono le radici di $X^3 - 8$ in A?

c. Disegnare nel piano di Gauss l'insieme $\{(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)^n \mid n \in \mathbb{N}\}$.

11.6. Siano $f, g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ le funzioni così definite: $f(x) = x^2 + x, \quad g(x) = \overline{3}x^2 + \overline{5}$,

a. disegnare il grafico di f e il grafico di g;

b. determinare $\mathrm{Im}(f)$, $\mathrm{Im}(g)$, $f^{-1}(\overline{0})$, $g^{-1}(\overline{0})$;

c. risolvere in $\mathbb{Z}_7$ l'equazione $f(x) + g(x) = \overline{0}$;

d. calcolare $f \circ g$ e $g \circ f$. Provare che $f \circ g \neq g \circ f$ come funzioni.

11.7. In $\mathbb{Z}_6$ anello delle classi di resto modulo 6:

a. determinare gli elementi invertibili e gli zero-divisori;

b. quanto vale la funzione di Eulero $\phi(6)$?

c. dire se la funzione $f\colon \mathbb{Z}_6 \to \mathbb{Z}_6$ data da $f(\overline{a}) = \overline{a}^3$ è ben definita.

11.8. Siano $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ e $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ le applicazioni date rispettivamente da $f(n) = (2n-1,\ 3n)$ e da $g((a,b)) = b - a - 1$.

a. Dire se f è iniettiva, suriettiva, biunivoca.

b. Scrivere esplicitamente l'applicazione composta $g \circ f$. È vero che g è l'inversa di f?

c. Determinare gli insiemi $\mathrm{Im}(g)$ e $g^{-1}(2)$.

11.9. Si consideri nell'insieme di numeri A la relazione R_A così definita:
$n\ R_A\ m \iff n$ divide m in A (ossia $\iff \exists\ k \in A$ tale che $m = nk$).

a. Provare che se $A = \mathbb{Z}$ allora $R_{\mathbb{Z}}$ non è nè una relazione d'ordine, nè una relazione di equivalenza.
Posto $A = \mathbb{N}$:

b. Provare che $R_{\mathbb{N}}$ è una relazione d'ordine. $R_{\mathbb{N}}$ è un ordine totale?

c. Provare che 0 e 1 sono rispettivamente il massimo e il minimo di $(\mathbb{N},\ R_{\mathbb{N}})$.

11.10. Nel campo dei numeri complessi $\mathbb{C}$, calcolare:

a. la parte reale e il coefficiente dell'immaginario di $\frac{i-2}{1+3i}$;

b. le radici terze di i, ossia le soluzioni dell'equazione $X^3 = i$.

c. Dare la definizione di numero algebrico e provare che i numeri richiesti al punto **b.** sono numeri algebrici.

d. Disegnare nel piano di Gauss l'insieme dei numeri complessi le cui coordinate polari $(\rho,\ \theta)$ soddisfano le condizioni $1 \le \rho \le 2$ e $0 \le \theta \le \pi$.

11.11. Risolvere i seguenti problemi:

a. Provare mediante l'algoritmo euclideo che 149 è il MCD di 208153 e 189677.

b. Dire se è risolubile in $\mathbb{Z}$ l'equazione $208153\,x\ +\ 189677\,y = 1$.

c. Determinare tutte le soluzioni di

$$\begin{cases} 3x \equiv 7 \bmod 23 \\ 2x \equiv 6 \bmod 22 \end{cases} \quad \begin{cases} 14x \equiv 20 \bmod 12 \\ 12x \equiv 20 \bmod 14 \end{cases} \quad \begin{cases} 7x \equiv 15 \bmod 12 \\ 4x \equiv 12 \bmod 11 \end{cases} \quad \begin{cases} 3x \equiv 7 \bmod 10 \\ 3x \equiv 11 \bmod 7 \end{cases}$$

11.12. Sia X un insieme con 7 elementi, $X = \{x_1, \ldots, x_7\}$.

a. Quanti sono i sottoinsiemi di X? Quanti quelli che non contengono x_1?

b. Quante sono le applicazioni $f\colon X \to X$? Quante quelle che non contengono x_1 nell'immagine?

c. Quante sono le relazioni d'ordine totale che si possono definire in X?

11.13. In $\mathbb{Z} \times \mathbb{Z}$ si definisce la relazione: $(a,b)\ \rho\ (c,d)$ se e solo se $ab = cd$.

a. Provare che ρ è una relazione di equivalenza.

b. Determinare tutti gli elementi della classe di $(0,0)$ e quelli della classe di $(1,1)$.

c. Provare che $\phi(\overline{(a,1)}) = a$ definisce una applicazione biunivoca dal quoziente $\mathbb{Z} \times \mathbb{Z}/\rho$ in $\mathbb{Z}$.

11.14. Consideriamo l'anello $\mathbb{Z}_{25}$ delle classi di resto modulo 25.

a. Determinare tutte le soluzioni in $\mathbb{Z}_{25}$ dell'equazione $X^2 = \bar{0}$.

b. Per ogni elemento $\bar{n}$ determinato nel punto precedente, provare che $\overline{1+n}$ è una unità in $\mathbb{Z}_{25}$.

c. Calcolare il numero k tale che $0 \leq k < 25$, rappresentante della classe di 9999^{2221} in $\mathbb{Z}_{25}$.

11.15. Sia $f\colon A \to B$ una applicazione tra due insiemi non vuoti A e B.

a. Verificare che la relazione in A data da "$a\ R\ a'$ se e solo se $f(a) = f(a')$" è una relazione di equivalenza.

b. Siano b e b' due elementi distinti di B; verificare che $f^{-1}(b) \cap f^{-1}(b') = \emptyset$.

c. Se A ha n elementi e B ha m elementi, quante sono le possibili applicazioni iniettive $f\colon A \to B$?

d. Provare per induzione la formula $1^2 + 2^2 + \cdots + k^2 = \frac{2k^3+3k^2+k}{6}$.

11.16. Si consideri il polinomio $F(X) = X^3 - i$.

a. Calcolare e disegnare nel piano di Gauss le radici complesse del polinomio $F(X)$.

b. Dire, motivando la risposta, se esiste un polinomio a coefficienti reali che abbia esattamente le stesse radici di $F(X)$.

c. Sia α una radice di $F(X)$. Dire, motivando la risposta, se α è un numero algebrico.

11.17. Posto $R = \mathbb{Z}_{22}$, dimostrare o confutare le affermazioni seguenti:

a. Se n è un numero intero che è un quadrato in $\mathbb{Z}$, allora $\overline{n}$ è un quadrato in R.

b. Se n è un numero intero tale che $\overline{n}$ è un quadrato in R, allora n è un quadrato in $\mathbb{Z}$.

c. $\overline{13}$ è invertibile in R ed è l'inverso di se stesso.

d. Gli zero-divisori di R sono $\phi(22) = 10$.

11.18. Determinare la cifra finale della centesima potenza del numero 87697.

11.19. Siano $A = \{1,2,3\}$ e $B = \{1,3,9,27\}$. Scrivere esplicitamente tutti gli elementi di

a. $A \cup B$ **b.** $A \cap B$ **c.** $\mathcal{P}(A)$ **d.** $A \times B$.

11.20. Siano P l'insieme dei numeri interi pari e D l'insieme dei numeri interi dispari e sia $f\colon P \times D \to \mathbb{Z}$ la funzione definita da $f((a,b)) = a + 2b$.

a. Dire se f è iniettiva e/o suriettiva e determinare $f^{-1}(0)$ e $f^{-1}(1)$.

b. Dire se in $P \times D$ la relazione ρ data da: $(a,b)\rho(a',b') \Leftrightarrow 6$ divide $a - a'$ è una relazione di equivalenza e, in caso affermativo, determinare la classe rappresentata da $(0,1)$.

11.21. Siano A e B insiemi finiti disgiunti aventi rispettivamente 1 elemento e b elementi.

a. Quanti elementi ha $\mathcal{P}(A \cup B)$?

b. Quanti elementi ha il prodotto cartesiano $\mathcal{P}(A) \times \mathcal{P}(B)$?

c. Provare che l'applicazione $f\colon \mathcal{P}(A) \times \mathcal{P}(B) \to \mathcal{P}(A \cup B)$ definita ponendo $f((C,D)) = C \cup D$ è biunivoca.

d. Determinare esplicitamente l'inversa g di f (ossia dato $H \subset A \cup B$ dire chi è $g(H)$).

11.22. Risolvere i problemi seguenti:

a. Quanti sono i numeri interi positivi ≤ 10000 non divisibili nè per 3 nè per 7?

b. Dato il numero $k = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$, dire quanti sono i divisori di k in $\mathbb{N}$.

c. Dire quanti sono i divisori di k in $\mathbb{N}$ che hanno esattamente 3 fattori primi.

11.23. Siano A un insieme, B un suo sottoinsieme e X l'insieme delle parti $\mathcal{P}(A)$ di A.

a. Dire quali dei seguenti tre insiemi sono sempre coincidenti ed esibire un esempio esplicito in cui il rimanente è diverso dagli altri due:

$$\mathcal{C}_X(\mathcal{P}(B)), \qquad \{C \subseteq A \mid C \cap \mathcal{C}_A(B) \neq \emptyset\}, \qquad \mathcal{P}(\mathcal{C}_A(B)).$$

b. Siano $F(X)$, $G(X)$, $H(X)$ polinomi di $\mathbb{R}[X]$.
Posto $A = \{x \in \mathbb{R} \mid F(x) = 0\}$, $B = \{x \in \mathbb{R} \mid G(x) = 0\}$ e $C = \{x \in \mathbb{R} \mid H(x) = 0\}$, definire mediante equazioni gli insiemi: $A \cup B$, $B \cap C$ e $(A \cap B) \cup C$.

11.24. Consideriamo in $\mathbb{N}$ la relazione $x \rho y \iff x = y$ oppure $x - y \leq -4$.

a. Verificare che ρ è una relazione d'ordine in $\mathbb{N}$.

b. Mostrare mediante un esempio esplicito che ρ non è un ordine totale in $\mathbb{N}$. È vero che $4\mathbb{N}$ è un sottoinsieme di $\mathbb{N}$ totalmente ordinato da ρ?

c. Trovare il minimo di $\mathbb{N}$ rispetto all'ordinamento ρ oppure provare che il minimo non esiste.

11.25. Nell'anello $\mathbb{Z}_{34}$ delle classi di resto modulo 34:

a. provare che ogni classe ha un rappresentante multiplo di 5;

b. determinare, se esiste, un numero negativo pari che rappresenta $[5]$;

c. dire se $f\colon \mathbb{Z}_{34} \to \mathbb{Z}_{34}$ data da $f([x]) = [(-1)^x]$ è una funzione ben definita;

d. determinare il numero degli elementi non "cancellabili" in $\mathbb{Z}_{34}$.

11.26. Determinare tutte le soluzioni dei seguenti sistemi di congruenze:

$$\begin{cases} 4x \equiv 9 \bmod 5 \\ 4x \equiv 12 \bmod 16 \end{cases} \quad \begin{cases} x \equiv 5 \bmod 12 \\ 4x \equiv 10 \bmod 20 \end{cases} \quad \begin{cases} 5x \equiv 7 \bmod 12 \\ x \equiv 10 \bmod 14 \end{cases} \quad \begin{cases} 4x \equiv 12 \bmod 14 \\ 2x \equiv 4 \bmod 9 \end{cases}$$

11.27. Sia A l'insieme delle soluzioni complesse dell'equazione $F(X) = 0$ dove $F(X)$ è il polinomio $X^6 - X^5 - 2X^4 + 3X^3 + 3X^2$.

a. Verificare che -1 è una radice di $F(X)$ e determinare la sua molteplicità.

b. Quanti elementi ha A?

c. Quanti elementi hanno $A \cap \mathbb{R}$ e $A \cap \mathbb{Q}$?

d. Disegnare nel piano di Gauss l'insieme $\{x \in \mathbb{C} \mid |x - i| \leq 1\}$.

11.28. Dire se 2 può essere scritto come combinazione lineare $3744\,a + 8202\,b$ con $a, b \in \mathbb{Z}$ e in caso affermativo determinare dei valori per a e b.

11.29. Scrivere in base 3 il numero (che in base 10 è) 900, e in base 10 il numero che in base 11 si scrive 900.

11.30. Trovare tutte le soluzioni in $\mathbb{Z}$ dei seguenti sistemi di congruenze:

$$\begin{cases} 3x \equiv 7 \bmod 11 \\ 2x \equiv 22 \bmod 14 \end{cases} \quad \begin{cases} 6x \equiv 16 \bmod 12 \\ 2x \equiv 5 \bmod 9 \end{cases} \quad \begin{cases} 4x \equiv 16 \bmod 10 \\ 7x \equiv 5 \bmod 15 \end{cases} \quad \begin{cases} -x \equiv 3 \bmod 2 \\ 2x \equiv 5 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases}$$

11.31. Nell'anello $B = \mathbb{Z}_{21}$ delle classi di resto modulo 21:

- **a.** Dimostrare oppure confutare la seguente affermazione: ogni classe di equivalenza ha un rappresentante compreso tra -11 e 11.
- **b.** Provare che $[-2]$ è invertibile in B e determinare il suo inverso.
- **c.** Quanti sono gli elementi non invertibili di B?
- **d.** Trovare tutte le soluzioni in B dell'equazione $[x]^2 = [0]$.

11.32. Sia n un numero intero positivo. Sia $\phi\colon \mathbb{Z}_{15} \to \mathbb{Z}_n$ data da $\phi([x]_{15}) = [x]_n$.
Determinare tutti gli interi n per i quali ϕ è una applicazione ben definita.

11.33. Si considerino in $\mathbb{Z}$ le relazioni: ρ data da $a\rho b \iff a + 5b$ è un multiplo di 3 in $\mathbb{Z}$, σ data da $a\sigma b \iff a + 4b$ è un multiplo di 3 in $\mathbb{Z}$ e τ data da $a\tau b \iff a = b$ oppure $a \leq 4b$.

- **a.** Dire se ρ è una relazione di equivalenza e, in caso affermativo, determinare la classe di 0 e la classe di -2.
- **b.** Verificare che σ non è nè una relazione di equivalenza nè una relazione d'ordine.
- **c.** Dire se τ è un ordine in $\mathbb{Z}$ e, in caso affermativo, se è un ordine totale.

11.34. Sia $f\colon \mathbb{Z} \to \mathbb{Q}$ l'applicazione così definita $f(n) = n^2 - 4$ se $n \geq 0$ e $f(n) = \frac{3}{5}n$ se $n < 0$.
Dire se f è iniettiva, f è suriettiva, e calcolare $\mathrm{Im} f$, $f^{-1}(6)$ e $f^{-1}(1)$.
Provare per induzione che $f(1) + f(2) + \cdots + f(n) = \frac{2n^3+3n^2-23n}{6}$.

11.35. Si consideri l'insieme X delle parole di 5 lettere che si possono scrivere usando le lettere dell'alfabeto italiano (non importa se di senso compiuto o meno) e sia V il vocabolario che contiene esattamente queste parole.

- **a.** Quante sono le parole di X?
- **b.** Definire la relazione d'ordine "lessicografico" tra le parole di X (ossia la relazione d'ordine usata nel vocabolario V).
- **c.** Quante sono le parole di V che precedono la parola BARBA?

11.36. Per ogni numero naturale $n \geq 1$, indichiamo con A_n l'insieme dei numeri che si possono scrivere come prodotto di n fattori $a_1 a_2 \cdots a_n$, con $a_i \in \mathbb{N}$, $a_i \geq 2$.

- **a.** Provare che $A_2 \supset A_3$ e che $A_n \neq \emptyset$ per ogni $n \geq 1$.
- **b.** Verificare le relazioni: $A_{n+1} \subset A_n$ per ogni $n \geq 2$ e $\bigcap_{n\geq 1} A_n = \emptyset$.

11.37. Sia $f\colon \mathbb{Z} \to \mathbb{N}$ l'applicazione così definita $f(n) = 2^n$ se $n \geq 0$ e $f(n) = 3^{-n}$ se $n \leq 0$.

a. Provare o confutare le affermazioni: f è iniettiva, f è suriettiva.

b. Calcolare $\mathrm{Im}f$, $f^{-1}(6)$ e $f^{-1}(1)$.

c. Scrivere esplicitamente una applicazione $g\colon \mathbb{N} \to \mathbb{Z}$ tale che $g \circ f = id_{\mathbb{Z}}$.

11.38. Si considerino in $\mathbb{Z}$ le seguenti relazioni ρ e σ:

$$x\rho y \Leftrightarrow x - y \leq 100 \qquad \text{e} \qquad x\sigma y \Leftrightarrow x = y \text{ oppure } xy > 0.$$

a. Provare che σ è una relazione di equivalenza.

b. Calcolare le classi di equivalenza di 0, 2 e -3. Quanti elementi ha il quoziente $\mathbb{Z}/\sigma$?

c. Provare che $\phi\colon \mathbb{Z}/\sigma \to \mathbb{Z}/\sigma$ data da $[x] \mapsto [x^2]$ è una funzione ben definita e scrivere esplicitamente il suo grafico.

d. È vero che ρ è una relazione di ordine?

11.39. Provare mediante l'induzione le seguenti affermazioni:

a. Sapendo che tra i numeri vale la proprietà distributiva $a(b+c) = ab+ac$, provare la validità della proprietà distributiva generalizzata per somme di n addendi:

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n \quad (\text{ossia } a(\textstyle\sum_{i=1}^n b_i) = \sum_{i=1}^n (ab_i)\ ).$$

b. La successione di Fibonacci S_n è definita ricorsivamente da $S_0 = 1$, $S_1 = 1$, $S_{n+1} = S_n + S_{n-1}$ per ogni $n \geq 2$. Provare che per ogni $n \geq 4$ si ha $\frac{8}{5} \leq \frac{S_{n+1}}{S_n} \leq \frac{13}{8}$.

11.40. In un'aula con 100 posti (fissi e numerati) si presentano 60 studenti per sostenere uno scritto.

a. In quanti modi si possono sistemare gli studenti (se si mettono tutti seduti, uno al massimo per ogni posto)?

b. Quanti sono i possibili insiemi di posti vuoti?

c. Gli studenti usano complessivamente per lo scritto 100 fogli (i fogli sono tutti uguali e ogni studente usa almeno un foglio). Quante sono le possibili distribuzioni di fogli tra gli studenti?

11.41. Posto $F(X) = X^3 - 2X^2 - X - 6$ e $G(X) = X^4 + 2X^3 + 4X^2 + 3X + 2$:

a. dire se $F(X)$ e $G(X)$ sono irriducibili oppure riducibili in $\mathbb{R}[X]$;

b. determinare tutte le radici intere (ossia appartenenti a $\mathbb{Z}$) di $F(X)$ e di $G(X)$;

c. trovare un MCD di $F(X)$ e $G(X)$ in $\mathbb{R}[X]$;

d. dire se il MCD di $F(X)$ e $G(X)$ determinato nel punto precedente è anche MCD dei due polinomi in $\mathbb{C}[X]$.

11.42. Si consideri il polinomio $G(X) = X^4 + X^3 + X^2 + X + 1$ dell'anello $K[X]$.
Dire se $G(X)$ è irriducibile oppure riducibile nei casi seguenti: $K = \mathbb{R}$, $K = \mathbb{C}$, $K = \mathbb{Z}_5$.

11.43. Si consideri il polinomio $F(X) = X^4 + 4$.

a. Calcolare e disegnare nel piano di Gauss le radici complesse di $F(X)$.

b. Determinare in $\mathbb{R}[X]$ la decomposizione di $F(X)$ nel prodotto di polinomi irriducibili.

c. Disegnare nel piano di Gauss l'insieme A dei punti z tali che $2 \leq |z+1| \leq 5$. Vi sono radici di $F(X)$ contenute in A?

11.44. Si consideri il polinomio $F(X) = iX^3 + 1$.

a. Calcolare e disegnare nel piano di Gauss le radici complesse del polinomio $F(X)$.

b. Dire, motivando la risposta, se esiste un polinomio a coefficienti reali che abbia esattamente le stesse radici di $F(X)$.

c. Sia α una radice di $F(X)$. Dire, motivando la risposta, se α è un numero algebrico.

11.45. Nel campo dei numeri complessi $\mathbb{C}$:

a. determinare parte reale e coefficiente dell'immaginario di z, z^{-1} e z^2, dove $z = \frac{1-i}{2+i}$.

b. Calcolare tutte le radici complesse del polinomio $X^4 + 2$.

c. Disegnare nel piano di Gauss l'insieme: $\{z \in \mathbb{C} \mid i(z - \overline{z}) < 0\}$

11.46. Provare che un numero complesso α è algebrico se e solo se lo è il suo quadrato.

11.47. Calcolare in $\mathbb{C}$ tutte le radici terze del numero $1 + i$.

11.48. Siano A, B e C insiemi qualunque.

a. Dimostrare che $\mathcal{C}(A \cap B) = \mathcal{C}(A) \cup \mathcal{C}(B)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

b. Quale condizione deve soddisfare C per avere $A \cup (B \cap C) = (A \cup B) \cap C$?

c. Posto $A = \{x \in \mathbb{R} \mid x^2 + x - 2 = 0\}$, $B = \{1, -1, 2\}$ e $C = \{1, \{2, 3\}\}$, determinare in modo esplicito gli insiemi seguenti: $A \cup (B \cap C)$, $(A \cup B) \cap C$, l'insieme delle parti di B e l'insieme delle parti di C.

11.49. Si consideri la relazione ρ in $\mathbb{Z}$ data da: $x \rho y$ se e solo se $x = y$ oppure $x \leq y + 3$.

a. Verificare che ρ non è una relazione di equivalenza, ma è una relazione d'ordine.

c. Provare che ρ non è un ordine totale e determinare un sottoinsieme infinito di $\mathbb{Z}$ su cui ρ induce un ordine totale.

d. Dire quali delle seguenti applicazioni sono ben definite e, in caso affermativo, se sono iniettive e/o suriettive:

$$f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z} \text{ data da } f(\tfrac{n}{m}) = (n, m) \text{ se } n \neq 0, \qquad f(\tfrac{0}{m}) = 1$$

$$g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q} \text{ data da } g((n, m)) = \tfrac{n}{m} \text{ se } m \neq 0, \qquad g((n, 0)) = n$$

$$h : \mathbb{Q} \to \mathbb{R} \text{ data da } h(\tfrac{n}{m}) = \tfrac{n^2+m^2}{m^2}.$$

11.50. Provare per induzione che per ogni coppia di numeri naturali n, k tali che $n > k \geq 1$ si ha $\binom{n}{k} \geq k$.

11.51. Si consideri il polinomio $F(X) = 3X^5 + 7X^4 + 2X^3 - 4X^2 - X + 1$.

a. Verificare che -1 è una radice di $F(X)$ e determinare la sua molteplicità.

b. Trovare tutte le radici razionali di $F(X)$.

c. Dire se $F(X)$ ha anche radici reali non razionali.

d. Siano α un numero complesso e n un numero intero tali che $F(\alpha) = F(n)$. È vero che α è un numero algebrico?

11.52. Si consideri l'anello $\mathbb{Z}_{48}$ delle classi di resto modulo 48.

a. Determinare il numero complessivo dei divisori dello zero di $\mathbb{Z}_{48}$ e provare **esplicitamente** che $[15]$ è uno di essi.

b. Provare che per ogni numero primo $p > 3$ il numero $p^{16} - 1$ è divisibile per 48.

c. Risolvere i sistemi di congruenze

$$\begin{cases} 2x \equiv 1 \bmod 3 \\ 7x \equiv 5 \bmod 22 \end{cases} \qquad \begin{cases} 2x \equiv 10 \bmod 6 \\ 35x \equiv 25 \bmod 30 \end{cases}$$

11.53. a. Scrivere la formula dell'inverso di un numero complesso non nullo sia mediante le coordinate cartesiane sia mediante le coordinate polari.

b. Determinare parte reale e coefficiente dell'immaginario di $z = \frac{(1-3i)}{(-2+i)^2}$.

c. Determinare tutte le soluzioni dell'equazione $(X + 4)^3 = -8i$.

d. Disegnare nel piano di Gauss l'insieme B dei numeri complessi $z = a + ib$ tali che $-1 \leq b \leq 2$ e il cui argomento principale θ soddisfa le condizioni $\frac{\pi}{2} \leq \theta \leq \pi$.

11.54. Si considerino gli insiemi $A = \{1, 2, 3, 4, 5\}$ e $B = \{n \in \mathbb{N}$ tali che n è multiplo di $3\}$. Provare o confutare le seguenti affermazioni:

a. $X = \{(a, b) \in A \times B \;/\; b$ è multiplo di $3a\}$ è una corrispondenza tra A e B.

b. Il sottoinsieme X del punto precedente è il grafico di una funzione $f\colon A \to B$

c. $Y = \{(a, b) \in A \times B \;/\; b = 3a\}$ è il grafico di una funzione iniettiva $g\colon A \to B$.

d. Il numero di funzioni iniettive di A in A è uguale al numero di funzioni suriettive di A in A.

11.55. Risolvere i seguenti problemi:

a. Trovare il MCD di 3248 e 1421 ed esplicitare l'identità di Bézout.

b. Determinare tutti gli elementi dell'insieme $\{n \in \mathbb{Z} \mid n = 3248a + 1421b\,,\, a, b \in \mathbb{Z}\}$.

c. Determinare la fattorizzazione di 1421 in fattori primi. Quanti elementi ha l'insieme $\{n \in \mathbb{N}\,,\, 1 \leq n \leq 1421 \,/\, MCD(n, 1421) \neq 1\}$?

d. Determinare tutte le soluzioni in $\mathbb{Z}$ dei seguenti sistemi di congruenze:

$$\begin{cases} 5x \equiv 11 \bmod 13 \\ 2x \equiv -3 \bmod 9 \end{cases} \qquad \begin{cases} 2x \equiv 8 \bmod 12 \\ 6x \equiv 10 \bmod 16 \end{cases}$$

11.56. Nell'anello $\mathbb{Z}_{36}$ delle classi di resto modulo 36:

a. provare che $\overline{14}$ è uno zero-divisore e determinare $b \in \mathbb{Z}$ tale che $\overline{b} \neq \overline{0}$ e $\overline{14} \cdot \overline{b} = \overline{0}$;

b. dire se $\overline{12}$ è un quadrato perfetto in $\mathbb{Z}_{36}$.

c. Dire se le applicazioni $\phi, \psi \colon \mathbb{Z}_{36} \to \mathbb{Z}_8$ date da $\phi([a]) = \overline{a}$ e $\psi([a]) = \overline{a}^2$ sono ben definite.

11.57.
Nel campo dei numeri complessi $\mathbb{C}$:

a. Calcolare modulo e argomento dei numeri complessi $-1 - i$ e $\sqrt{3}i - 1$.

b. Verificare che $1 - i$ è radice del polinomio $F(X) = X^6 - 2X^5 + 2X^4 + 2X^2 - 4X + 4$.

c. Determinare la decomposizione di $F(X)$ in fattori irriducibili in $\mathbb{C}$ e in $\mathbb{R}$.

d. Disegnare nel piano di Gauss l'insieme $\{z \in \mathbb{C} \mid |z - 2i - 1| \leq 3\}$.

11.58. Si considerino gli insiemi $A = \{1, 2, 3, 4, 5\}$ e $B = \{n \in \mathbb{N}$ tali che n è multiplo di $3\}$. Provare o confutare le seguenti affermazioni:

a. $X = \{(a, b) \in A \times B \ / \ b$ è multiplo di $3a\}$ è una corrispondenza tra A e B.

b. Il sottoinsieme X del punto precedente è il grafico di una funzione $f \colon A \to B$

c. $Y = \{(a, b) \in A \times B \ / \ b = 3a\}$ è il grafico di una funzione iniettiva $g \colon A \to B$.

d. Il numero di funzioni iniettive di A in A è uguale al numero di funzioni suriettive di A in A.

11.59.
Risolvere i seguenti problemi:

a. Trovare il MCD di 3248 e 1421 ed esplicitare l'identità di Bézout.

b. Determinare tutti gli elementi dell'insieme $\{n \in \mathbb{Z} \mid n = 3248a + 1421b\,,\ a, b \in \mathbb{Z}\}$.

c. Determinare la fattorizzazione di 1421 in fattori primi. Quanti elementi ha l'insieme $\{n \in \mathbb{N}\,,\ 1 \leq n \leq 1421 \,/\, MCD(n, 1421) \neq 1\}$?

d. Determinare tutte le soluzioni in $\mathbb{Z}$ dei seguenti sistemi di congruenze:

$$\begin{cases} 5x \equiv 11 \bmod 13 \\ 2x \equiv -3 \bmod 9 \end{cases} \qquad \begin{cases} 2x \equiv 8 \bmod 12 \\ 6x \equiv 10 \bmod 16 \end{cases}$$

11.60. Nell'anello $\mathbb{Z}_{32}$ delle classi di resto modulo 32:

a. provare che $\overline{14}$ è uno zero-divisore e determinare $b \in \mathbb{Z}$ tale che $\overline{b} \neq \overline{0}$ e $\overline{14} \cdot \overline{b} = \overline{0}$;

b. dire se $\overline{13}$ è un quadrato perfetto in $\mathbb{Z}_{36}$.

c. Dire se le applicazioni $\phi, \psi \colon \mathbb{Z}_{12} \to \mathbb{Z}_8$ date da $\phi([a]) = \overline{a}^2$ e $\psi([a]) = \overline{a}^3$ sono ben definite.

11.61. Nel campo dei numeri complessi $\mathbb{C}$:

a. Calcolare modulo e argomento dei numeri complessi $-1 - i$ e $\sqrt{3}i - 1$.

b. Verificare che $1 - i$ è radice del polinomio $F(X) = X^6 - 2X^5 + 2X^4 + 2X^2 - 4X + 4$.

c. Determinare la decomposizione di $F(X)$ in fattori irriducibili in $\mathbb{C}$ e in $\mathbb{R}$.

d. Disegnare nel piano di Gauss l'insieme $\{z \in \mathbb{C} \mid |z - 2i - 1| \leq 3\}$.

11.62. In un teatro vi sono 400 persone.

a. Provare che ce ne sono almeno 2 che festeggiano il compleanno lo stesso giorno.

b. In quanti modi si possono sedere se nel teatro ci sono 350 posti?

c. La relazione $A\rho B$ se la data di nascita (GMA) di A precede la data di nascita di B, è una relazione d'ordine nell'insieme X delle presone presenti in teatro?

d. La relazione $A\sigma B$ se il giorno del compleanno (GM) di A coincide con quello di B, è una relazione di equivalenza nell'insieme X delle presone presenti in teatro? Se sì, quante classi di equivalenza ci sono?

11.63. Risolvere i seguenti problemi:

a. Trovare il MCD di 3248 e 5577 ed esplicitare l'identità di Bézout.

b. Determinare tutti gli elementi dell'insieme $\{n \in \mathbb{Z} \mid n = 3248a + 5577b\,,\ a, b \in \mathbb{Z}\}$.

c. Scrivere in base 5 il numero 3248.

d. Determinare tutte le soluzioni in $\mathbb{Z}$ dei seguenti sistemi di congruenze:

$$\begin{cases} 2x \equiv 11 \bmod 13 \\ 5x \equiv -3 \bmod 9 \end{cases} \qquad \begin{cases} 2x \equiv 8 \bmod 12 \\ 6x \equiv 10 \bmod 16 \end{cases}$$

11.64. Nell'anello $\mathbb{Z}_{17}$ delle classi di resto modulo 17:

a. determinare gli elementi invertibili e gli zero-divisori;

b. quanto vale la funzione di Eulero $\phi(17)$?

c. dire se l'applicazione $f\colon \mathbb{Z}_{17} \to \mathbb{Z}_{17}$ data da $f(\overline{a}) = \overline{min\{a, a^2\}}$ è ben definita.

11.65. Nel campo dei numeri complessi $\mathbb{C}$:

a. Calcolare modulo e argomento dei numeri complessi $-1 - i$ e $\sqrt{3}i - 1$.

b. Verificare che $1 - i$ è radice del polinomio $F(X) = X^6 - 2X^5 + 2X^4 + 2X^2 - 4X + 4$.

c. Determinare la decomposizione di $F(X)$ in fattori irriducibili in $\mathbb{C}$ e in $\mathbb{R}$.

d. Disegnare nel piano di Gauss l'insieme $\{z \in \mathbb{C} \mid |z - 2i - 1| \leq 3\}$.

11.66. Risolvere i seguenti problemi:

a. Trovare il MCD di 2010 e 507 ed esplicitare l'identità di Bézout.

b. Determinare la scrittura posizionale in base 7 del numero (che in base 10 si scrive) 4130.

c. Scrivere in base 10 il numero $(1210)_3$, dove l'indice indica la base usata.

d. Determinare tutte le soluzioni in $\mathbb{Z}$ dei seguenti sistemi di congruenze:

$$\begin{cases} 2x \equiv 3 \bmod 5 \\ x \equiv 7 \bmod 8 \end{cases} \qquad \begin{cases} 2x \equiv 6 \bmod 12 \\ 4x \equiv 3 \bmod 9 \end{cases}$$

11.67. Nell'anello $\mathbb{Z}_8$ delle classi di resto modulo 8:

- **a.** determinare gli elementi invertibili e gli zero-divisori;
- **b.** quanto vale la funzione di Eulero $\phi(8)$?
- **c.** dire se l'applicazione $f\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ data da $f(\overline{a}) = \overline{a}^2$ è ben definita;
- **d.** disegnare il grafico della funzione $g\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ data da $g(\overline{a}) = \overline{3a+1}$.

11.68. Nel campo dei numeri complessi $\mathbb{C}$:

- **a.** Calcolare parte reale e coefficiente dell'immaginario del numero complesso
$$\frac{1-2i}{1+i}.$$
- **b.** Determinare le radici quarte di 1, ossia le soluzioni dell'equazione $X^4 = 1$.
- **c.** Dare la definizione di numero algebrico e provare che i numeri complessi richiesti nel punto **b.** sono numeri algebrici.
- **d.** Disegnare nel piano di Gauss l'insieme $\{z \in \mathbb{C} \mid |z+i| \leq 1\}$.

11.69. Sia $X = \{x_1, \ldots, x_6\}$ un insieme con 6 elementi.

- **a.** Quanti sono i sottoinsiemi di X? E quanti sono i sottoinsiemi di X che non contengono x_6?
- **b.** Quanti sono i sottoinsiemi di X che contengono 2 elementi?
- **c.** Quante sono le applicazioni $f\colon X \to X$? Quante sono iniettive?
- **d.** Quante sono le possibili relazioni nell'insieme X?

Capitolo 12

Risposte ad alcuni esercizi

Capitolo 1

1.1 a. $\mathcal{P}(B) = \{\emptyset,\ \{1\},\ \{-1\},\ \{2\},\ \{1,-1\},\ \{1,2\},\ \{-1,2\},\ B\ \}$
$\mathcal{P}(C) = \{\emptyset,\ \{1\},\ \{\{2,3\}\},\ C\ \}$

1.1 b. Sono corrette soltanto le tre seguenti: $1 \in C$, $1 \in A$, $\{2,3\} \in C$.

1.2 $A \cap B = \{x \in \mathbb{N} \mid 10 \leq x \leq 19\}$, $A \cup B = \mathbb{N}$, $A \setminus B = \{x \in \mathbb{N} \mid x \leq 9\}$
$B \setminus A = \{x \in \mathbb{N} \mid x \geq 20\}$, $\mathcal{C}_X(A) = \{x \in \mathbb{N} \mid x \geq 20\}$, $\mathcal{C}_X(B) = \{x \in \mathbb{N} \mid x \leq 9\}$.

1.3 $\mathcal{C}_{\mathbb{R}}(Y \cup Z) = \{x \in \mathbb{R} \mid x \notin Y \text{ e } x \notin Z\} = (3,5) \cup [21,+\infty)$, $\mathcal{C}_{\mathbb{R}}(Y) = (3,+\infty)$, $\mathcal{C}_{\mathbb{R}}(Z) = (-\infty,5) \cup [21,+\infty)$.

1.4 i. Per esempio $A = \emptyset$, $B = \{1\}$, $C = \{2\}$, $A \cap B = A \cap C = \emptyset$.

ii. Per esempio $A = B = \{1\}$, $C = \emptyset$, $(B \cup A) \cap C = \emptyset$, $B \cup (A \cap C) = \{1\}$.

iii. Per esempio $X = A = \{1\}$, $B = \emptyset$, $A \setminus \mathcal{C}_X(B) = \emptyset$, $\mathcal{C}_X(\mathcal{C}_X(A) \setminus B) = X$.

1.7 $\mathcal{C}_{\mathbb{R}}(Y \cup Z)$ è
$(a,+\infty)$ se $c \leq b$ oppure se $b < c \leq a$
$[c,+\infty)$ se $b \leq a < c$
$(a,b) \cup [c,+\infty)$ se $a < b < c$.

1.8 $\bigcup A_n = \mathbb{N}$, $\bigcap A_n = \{0\}$.

1.9 $\bigcap B_n = \{x \in \mathbb{N} \mid x \text{ è dispari }\} = \{x \in \mathbb{N} \mid x = 2k+1,\ k \in \mathbb{N}\} = 2\mathbb{N}+1$, $\bigcup B_n = \mathbb{N}$.

1.10 $\bigcap C_n = 2\mathbb{N} \cup \{1\}$, $\bigcup C_n = \mathbb{N}$.

1.11 $\bigcap I_n = \emptyset$ perchè $\bigcap I_n \subseteq I_1 = (0,1)$ e per ogni $\forall x \in (0,1)$ esiste una cifra decimale di x non nulla: sia la k-esima; allora $x > \frac{1}{10^{k+1}}$ e quindi $x \notin I_n$ per $n = 10^{k+1}$.

1.12 Lo svolgimento è analogo al precedente.

1.13 Se $n \neq m$ allora $I_n \not\subseteq I_m$ poichè $\frac{1}{2^n} > \frac{1}{2^m}$quando $n < m$ e $-n < -m$ quando $n > m$.

1.14 Ad esempio $I_n = [-1+\frac{1}{n}, 1-\frac{1}{n}]$.

1.15 Intervalli siffatti non esistono: se $\bigcup I_n = \bigcup (a_n,b_n) \supseteq [0,1]$, allora per un qualche indice n_0 si avrà $1 \in (a_{n_0}, b_{n_0})$; preso allora $c = \frac{1}{2}(1+b_{n_0})$ si ha $1 < c < b_{n_0}$ ossia $c \in I_{n_0}$ e quindi $\bigcup I_n$ contiene strettamente $[0,1]$.

1.17 $A \cap B = \{2\}$ N.B. : non occorre determinare esplicitamente gli elementi di B, ma basta controllare quali degli elementi di A soddisfano l'equazione definente B.

$\mathcal{C}_{\mathbb{R}}(B) = \{x \in \mathbb{R} \mid x^4 - 2x^2 - 3x - 2 \neq 0\}$.

$A \cap \mathcal{C}_{\mathbb{R}}(B) = \{1,\ \sqrt{3},\ -2,\ 0\ \}$ N.B.: $\{-1\} \notin \mathbb{R}$.

1.19 Per esempio $A = \{0,\ 1\}$, $B = \{0,\ 2\}$, $C = \mathbb{N} \setminus \{0\}$.

1.20 Basta controllare che $D \neq \emptyset$, $P \neq \emptyset$, $P \cap D = \emptyset$ e $P \cup D = \mathbb{N}$.

1.23 Se $x,\ y,\ z$ sono tre elementi distinti, allora

$\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, A\}$.

A possiede esattamente 5 partizioni che sono:

la partizione banale $U_1 = \{A\}$;

la partizione data dai singleton $U_2 = \{\{x\}, \{y\}, \{z\}\}$;

$U_3 = \{\{x\}, \{y, z\}\}$, $U_4 = \{\{x, y\}, \{z\}\}$, $U_5 = \{\{x, z\}, \{y\}\}$.

1.24 La relazione $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B$ è vera .

Un controesempio alla relazione $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ è dato da ogni coppia di insiemi A, B non contenuti l'uno nell'altro, ad esempio $A = \{1\}$ e $B = \{2\}$. $\mathcal{P}(A) \cap \mathcal{P}(B)$ ha 3 elementi $\emptyset$, A e B mentre $\mathcal{P}(A \cap B)$ contiene oltre ai precedenti anche il quarto elemento $\{1, 2\}$.

1.25 Se $A = 6\mathbb{N}$ e $B = 3\mathbb{N} \setminus 6\mathbb{N}$, allora $U_1 = \{A, B\}$ è una partizione di $3\mathbb{N}$ costituita da due sottoinsiemi; se I_n è il singleton $\{3n\}$, allora $U_2 = \{I_n \mid n \in \mathbb{N}\}$ è una partizione di $3\mathbb{N}$ costituita da infiniti sottoinsiemi.

1.26 $\bigcup A_n = \mathbb{R}$, $\bigcap A_n = \emptyset$.

Gli A_n non formano una partizione perchè non sono due a due disgiunti; ad esempio $\sqrt{2}+1 \in I_0 \cap I_1$. Invece $A_n \cap \mathbb{Q}$ formano una partizione di $\mathbb{Q}$ poichè:

- $n + 2 \in A_n \cap \mathbb{Q}$ e quindi $A_n \cap \mathbb{Q} \neq \emptyset$;
- $(A_n \cap \mathbb{Q}) \cap (A_n \cap \mathbb{Q}) = (A_n \cap A_m) \cap \mathbb{Q} = \emptyset$ (infatti $A_n \cap A_m = \emptyset$ se $n \neq m \pm 1$ e $A_n \cap A_m$ è costituita da un unico numero irrazionale se $n = m \pm 1$;
- $\bigcup(A_n \cap \mathbb{Q}) = (\bigcup A_n) \cap \mathbb{Q} = \mathbb{R} \cap \mathbb{Q} = \mathbb{Q}$.

1.27 Falso, ad esempio se $A = \emptyset$.

1.28 Falso, ad esempio se $B = \emptyset$.

È vera in generale la sola implicazione $\{B,\ A \setminus B,\ \mathcal{C}_X(A)\}$ è una partizione di $A \Rightarrow B \subseteq A$; infatti B e $\mathcal{C}_X(A)$ sono disgiunti solo se $B \subseteq A$.

1.29 a. Falso. Si consideri ad esempio un sottoinsieme proprio B di A e la partizione di A data da $\{B, \mathcal{C}_A(B)\}$.

1.29 b. Falso. Si consideri ad esempio un sottoinsieme proprio B di A e sia $I = \{1\}$, $A_1 = B$.

1.30 $A \cap B$.

1.31 $\mathcal{C}_{\mathbb{R}}(A)$.

1.32 $A \cap (C \cup ((A \setminus C) \cap B)) = A \cap (C \cup B)$.

1.33 ii. No, perchè non sono due a due disgiunte, avendo appunto l'origine in comune.

1.33 iii. Sì, purchè si consideri tra le circonferenze anche quella degenere di raggio nullo, ridotta alla sola origine.

1.34 $A \times B = \{(-1,1),\ (-1,2),\ (0,1),\ (0,2),\ (1,1),\ (1,2)\ \}$;
$A \times A = \{(-1,-1),\ (-1,0),\ (-1,1),\ (0,-1),\ (0,0),\ (0,1),\ (1,-1),\ (1,0),\ (1,1)\ \}$;
$(A \times A) \cap (A \times B) = A \times (A \cap B) = \{(-1,1),\ (0,1),\ (1,1),\ \}$;
$(A \times A) \cup (A \times B) = A \times (A \cup B) = \{(-1,-1),\ (-1,0),\ (-1,1),\ (-1,2),\ (0,-1),\ (0,0),\ (0,1),\ (0,2),\ (1,-1),\ (1,0),\ (1,1),\ (1,2)\ \}$;
$\mathcal{P}(B \times B) = \{\emptyset, \{(1,1)\},\ \{(1,2)\},\ \{(2,1)\},\ \{(2,2)\},\ \{(1,1),\ (1,2)\},\ \{(1,1),\ (2,1)\},\ \{(1,1),\ (2,2)\},\ \{(1,2),\ (2,1)\},\ \{(1,2),\ (2,2)\},\ \{(2,1),\ (2,2)\},\ \{(1,1),\ (1,2),\ (2,1)\},\ \{(1,1),\ (1,2),\ (2,2)\},\ \{(1,1),\ (2,1),\ (2,2)\},\ \{(1,2),\ (2,1),\ (2,2)\},\ B \times B\}$;
$\mathcal{P}(B) \times \mathcal{P}(B) = \{(\emptyset,\emptyset),\ (\emptyset,\{1\}),\ (\emptyset,\{2\}),\ (\emptyset,B),\ (\{1\},\emptyset),\ (\{1\},\{1\}),\ (\{1\},\{2\}),\ (\{1\},B),\ (\{2\},\emptyset),\ (\{2\},\{1\}),\ (\{2\},\{2\}),\ (\{2\},B),\ (B,\emptyset),\ (B,\{1\}),\ (B,\{2\}),\ (B,B)\ \}$.

1.35 i. Presi degli elementi $a \in A_1$ e $b \in B_2$ (che esistono certamente perchè tali insiemi sono non vuoti), l'elemento (a,b) di $A \times B$ non è contenuto nè in $A_1 \times B_1$ nè in $A_2 \times B_2$.

1.35 ii. I quattro sottoinsiemi nella partizione sono tutti non vuoti perchè prodotto cartesiano di insiemi non vuoti.

Se $(i,j) \neq (i'j')$ allora $(A_i \times B_j) \cap (A_{i'} \times B_{j'}) = \emptyset$; se infatti $i \neq i'$ e $(a,b) \in (A_i \times B_j) \cap (A_{i'} \times B_{j'})$ allora $a \in A_i \cap A_{i'}$ contro l'ipotesi. Analogamente se $j \neq j'$.

Infine per ogni $(a,b) \in A \times B$ si ha $a \in A_i$ dove $i = 1$ oppure $i = 2$ e analogamente $b \in B_j$ dove $j = 1$ oppure $j = 2$; quindi $(a,b) \in A_i \times B_j$.

1.35 iii. La partizione data data al punto precedente è costituita da 4 sottoinsiemi ed è quindi diversa dalla partizione banale $\{A \times B\}$.

Capitolo 2

2.1 a. Proprietà R. $2x + 3x = 5x$ è multiplo di 5.

Proprietà S. Se $2x + 3y = 5k$ allora $2y + 3x = 5(x + y - k)$ è multiplo di 5.

Proprietà T. Se $2x + 3y = 5k$ e $2y + 3z = 5h$, allora $2x + 3z = 5(k + h - y)$ è multiplo di 5.

Le classi sono 5: $[1] = \{1,6\}$, $[2] = \{2\}$, $[3] = \{3\}$, $[4] = \{4\}$, $[5] = \{5\}$.

2.1 b. Non vale ad esempio la proprietà R. perchè $1 \not\rho 1$.

2.2 a. $\Delta_A = \{(-1,-1),\ (0,0),\ (1,1),\ \}$.

2.2 b. Soddisfa R. e A.

2.2 c. Non è una relazione d'ordine (e quindi neppure un ordine totale) perchè non è transitiva.

2.2 d. $R^{-1} = \{(1,-1),\ (0,1),\ (-1,-1),\ (0,0),\ (1,1),\ \}$.

2.4 iv. Sì: se C è un sottoinsieme di A, allora C come sottoinsieme di X ammette minimo c rispetto a R; poichè $c \in C \subseteq A$ e cRc' per ogni $c' \in C$ allora c è anche il minimo di C rispetto a ρ.

2.5 a. $\mathbb{Z}$ non ammette nè minimo nè massimo ed è sottoinsieme di $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

2.5 b. $\mathbb{Z}_-$ l'insieme dei numeri interi negativi non ha minimo, ma ha massimo -1.

2.5 c. e d. Il singleton $\{1\}$ ammette minimo e massimo 1.

2.6 b. Non si tratta di un ordine totale: ad esempio $2 \not\rho 3$ e $3 \not\rho 2$. Non essendo totale, non è neppure un buon ordine.

2.6 c. A ammette minimo 1 ma non ha massimo perchè non contiene alcun elemento M tale che $5\rho M$ e $6\rho M$; B ha massimo 12 ma non ha minimo perchè non contiene alcun elemento m tale che $m\rho 2$ e $m\rho 3$.

2.6 d. Il minimo di $\mathbb{N}$ è 1 e il massimo è 0 poichè per ogni naturale n si ha $n = n \cdot 1$ e $0 = 0 \cdot n$.

2.7 a. ρ non è una relazione di equivalenza perchè non è simmetrica: $2\rho 4$ ma $4 \not\rho 2$. ρ non è una relazione d'ordine perchè non è antisimmetrica: $2\rho(-2)$ e $(-2)\rho 2$ ma $-2 \neq 2$.

b. $S = \{(x, y) \in \mathbb{Z} \mid y = \pm x\}$. Le classi di equivalenza sono $[x] = \{x, -x\}$ se $x \neq 0$ e $[0] = \{0\}$.

2.8 a. e b. Come 6) a. e b. poichè $k \in \mathbb{N}$.

c. L'unico elemento confrontabile con tutti gli altri è 0 poichè per ogni $x \in \mathbb{Z}$ si ha $0 = 0 \cdot x$. Preso un qualsiasi altro elemento $x \neq 0$, allora non è confrontabile ad esempio con $-x$.

d. Sono 0, -1 e tutti i multipli negativi di 3 ossia i numeri del tipo $k \cdot (-3)$ con $k \in \mathbb{N}$.

e. $\{x \in \mathbb{Z} \mid x \geq 0\}$ ha minimo 1 e massimo 0;

$\{x \in \mathbb{Z} \mid x \leq 0\}$ ha minimo -1 e massimo 0;

$\{x \in \mathbb{Z} \mid x < 0\}$ ha minimo -1 e non ha massimo;

P non ha minimo e ha massimo 0;

D ha minimo 1 e non ha massimo.

2.9 Vogliamo provare che due elementi qualsiasi $a_1,\ a_2 \in A$sono confrontabili. Per ipotesi il sottoinsieme $\{a_1,\ a_2\}$ di A ammette minimo: sia a_1. Allora $a_1 \rho a_2$.

2.11 a. R. ovvia.

A. siano $x,\ y$ due elementi distinti di $\mathbb{N}$; se $x\rho y$ e $y\rho x$ allora per forza $2x$ divide y e $2y$ divide x ossia $y = k \cdot (2x) = (2k) \cdot x = (2k) \cdot h \cdot (2y)$. Quindi $y(4hk - 1) = 0$ e $y = 0$; in tal caso $x = 2hy = 0$ contro l'ipotesi $x \neq y$.

T. Sia $x\rho y$ e $y\rho z$. Se $x = y$ oppure $y = z$ allora ovviamente si ha anche $x\rho z$. Supponiamo ora $x \neq y$ e $y \neq z$; si ha allora $y = 2kx$ e $z = 2hy$ da cui $z = (2hk) \cdot 2x$ e quindi $x\rho z$.

Non è totale poichè ad esempio $1 \not\rho 3$ e $3 \not\rho 1$.

b. Consideriamo due elementi del tipo $m = 2^h,\ n = 2^k$. Se $h = k$, allora $m = n$ e quindi $n\rho m$. Se $h \neq k$, sia $h < k$ e quindi $h + 1 \leq k$; allora $n = 2^k = 2^{k-h-1} \cdot (2 \cdot 2^h) = 2^{k-h-1} \cdot 2m$ e ancora $m\rho n$.

c. Se $n,\ m$ sono naturali dispari, allora tra di essi la relazione $2m$ divide n non è mai verificata e quindi ρ si riduce a $n\rho m$ se $n = m$, la relazione di uguaglianza che è ovviamente una relazione di equivalenza le cui classi sono i singleton.

2.12 i. Verifichiamo solo la proprietà antisimmetrica e che l'ordine è totale.

A. Supponiamo che $(a, b)\rho(c, d)$ e $(c, d)\rho(a, b)$; allora $a + b \leq c + d$ e $c + d \leq a + b$ da cui $a + b = c + d$. Quindi $a \leq c$ e $c \leq a$ da cui $a = c$. Dalle due relazioni segue infine $b = (a + b) - a = (c + d) - c = d$ e le due coppie coincidono.

L'ordine è totale poichè date due coppie (a, b) e (c, d) vale sempre la relazione $a + b \leq c + d$ (oppure la relazione opposta $c + d \leq a + b$). Se la diseguaglianza è stretta allora $(a, b)\rho(c, d)$; se $a + b = c + d$ allora vale sempre la diseguaglianza $a \leq c$ (oppure la diseguaglianza opposta $c \leq a$) da cui ancora $(a, b)\rho(c, d)$.

ii. Per ogni coppia $(a, b) \in \mathbb{N} \times \mathbb{N}$ non nulla si ha $0 + 0 < a + b$ e quindi $(0, 0)\rho(a, b)$.

iii. Gli elementi che seguono immediatamente la coppia nulla sono nell'ordine $(0, 1)$, $(1, 0)$, $(0, 2)$, $(1, 1)$, $(2, 0)$, $(0, 3)$.

iv. Sia $k \in \mathbb{N}$; le coppie $(n, m) \in \mathbb{N} \times \mathbb{N}$ tali che $n + m = k$ sono esattamente $k + 1$ ossia $(i, k - i)$ con $i = 0, \ldots k$. Sia $(a, b) \in \mathbb{N} \times \mathbb{N}$; precedono tale coppia rispetto a ρ le coppie (n, m) tali che $n + m = k$ al variare di k da 0 ad $a + b$.

2.13 Il successore immediato di (a, b) è $(a, b+1)$; una coppia intermedia tra le due dovrebbe infatti avere primo elemento a e secondo elemento intermedio tra b e $b+1$. Invece presa una qualsiasi coppia (a, b) che precede $(3, 0)$ si avrà $a \leq 2$ e quindi la coppia $(2, b+1)$ è intermedia tra di loro.

2.14 Le relazioni sono tutte riflessive. Sono simmetriche solo b., c., e. e g. Sono transitive c., d., e., f. e g. Sono antisimmetriche solo a. ed f. L'unica relazione d'ordine è f., che non è totale. Sono relazioni di equivalenza c. ($[1] = \{-1, 1\}$), e. ($[1] = \{\frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z}$ entrambi dispari $\}$) e g. ($[0] = 3\mathbb{N}$).

2.15 $[1] = \mathbb{Z}$; $[\sqrt{2}] = \{n + \sqrt{2} \in \mathbb{R} \mid n \in \mathbb{Z}\}$; $[1.5] = \{n + 0.5 \mid n \in \mathbb{Z}\}$.
L'unico rappresentante x_0 di $[x]$ tale che $0 \leq x_0 < 1$ è $x - n$ dove n è la parte intera di x.

2.16 $[1] = \mathbb{Q} = [1.5]$; $[\sqrt{2}] = \{q + \sqrt{2} \mid q \in \mathbb{Q}\}$.
In $[x]$ vi sono infiniti rappresentanti y tali che $0 \leq y < 1$: sono tutti quelli del tipo $x + q - n$ tali che $q \in \mathbb{Q}$ e n è la parte intera di $x + q$.

2.18 b. $[(a, b, c)] = \{(a, b, c),\ (a, c, b),\ (b, a, c),\ (b, c, a),\ (c, a, b),\ (c, b, a)\ \}$;
$[(a, b, a)] = \{(a, b, a),\ (b, a, a),\ (a, a, b),\ (a, b, a),\ (b, a, a),\ (a, a, b)\ \}$;
$[(c, c, c)] = \{(c, c, c)\ \}$.

2.18 c. $X = \{(1,1,1),\ (1,1,2),\ (1,1,3),\ (1,2,1),\ (1,2,2),\ (1,2,3),\ (1,3,1),\ (1,3,2),\ (1,3,3),$
$(2,1,1),\ (2,1,2),\ (2,1,3),\ (2,2,1),\ (2,2,2),\ (2,2,3),\ (2,3,1),\ (2,3,2),\ (2,3,3),\ (3,1,1),$
$(3,1,2),\ (3,1,3),\ (3,2,1),\ (3,2,2),\ (3,2,3),\ (3,3,1),\ (3,3,2),\ (3,3,3)\ \}$
$[(1,1,1)] = \{(1,1,1)\}$;, $[(2,2,2)] = \{(2,2,2)\ \}$, $[(3,3,3)] = \{(3,3,3)\ \}$,
$[(1,1,2)] = \{(1,1,2),\ (1,2,1),\ (1,2,2),\ (2,1,1),\ (2,1,2),\ (2,2,1),\ \}$;
$[(1,1,3)] = \{(1,1,3),\ (1,3,1),\ (1,3,3),\ (3,1,1),\ (3,3,1),\ (3,1,3),\ \}$;
$[(1,2,3)] = \{(1,2,3),\ (1,3,2),\ (2,1,3),\ (2,3,1),\ (3,1,2),\ (3,2,1)\ \}$;
$[(2,2,3)] = \{(2,2,3),\ (2,3,2),\ (2,3,3),\ (3,2,2),\ (3,2,3),\ (3,3,2)\ \}$.

2.19 La classe di equivalenza dell'origine è costituita dalla sola origine; le altre classi sono circonferenze con centro l'origine.

2.20 b. La classe di equivalenza di un punto P è l'insieme dei punti della retta per P e per l'origine, privata dell'origine.

c. $C \cap [P] = \{P_1 = (\frac{a}{\sqrt{(a^2+b^2)}}, \frac{b}{\sqrt{(a^2+b^2)}}), P_2 = (\frac{-a}{\sqrt{(a^2+b^2)}}, \frac{-b}{\sqrt{(a^2+b^2))}})\}$.

d. L'intersezione contiene esattamente un punto per ogni P non appartenente alla retta r' parallela ad r e passante per l'origine; se $P \in r'$ l'intersezione è vuota.

e. Ad esempio l'insieme $\{P = (x, 1) \mid x \in \mathbb{R}\} \cup \{(1, 0)\}$.

Capitolo 3

3.1 La relazione $\{([n], n) \in \mathbb{Z}_2 \times \mathbb{Z} \mid n \in \mathbb{Z}\}$ non è il grafico di una funzione perchè contiene le due coppie $([0], 0)$ e $([2], 2)$ con $[0] = [2]$, ma $0 \neq 2$.
La corrispondenza inversa $\{(n, [n]) \in \mathbb{Z} \times \mathbb{Z}_2 \mid n \in \mathbb{Z}\}$ è invece il grafico di una funzione $\mathbb{Z} \to \mathbb{Z}_2$ poichè per ogni $n \in \mathbb{Z}$ esiste un'unica classe $[n]$.

3.2 f non è ben definita poichè $[0] = [2]$ ma $f([0]) = 0 \neq 2 = f([2])$. Invece è ben definita g; se $[n] = [m]$ allora $m = n + 2k$ e $g([m]) = [3m + 1] = [3n + 6k + 1] = [3n + 1] = g([n])$.

3.3 $f(7) = [7] = [1]$, $f(8) = [8] = [0]$, $Im(f) = f(\{-2,\ -1,\ 0\ 1\ \}) = \mathbb{Z}_2$,
$f^{-1}([7]) = f^{-1}(\{[7],\ [-1]\}) = \{2n + 1 \in \mathbb{Z} \mid n \in \mathbb{Z}\} = 2\mathbb{Z} + 1$.

3.4 Non sono ben definite soltanto d. ($[2] * [0] = [2^0] = [1] \neq [2] * [2] = [2^2] = [4]$ e inoltre $[0] * [0] = [0^0]$ non ha senso) ed e. ($[0] * [1] = [0]$ ma anche $[2] * [1] = [1]$).

3.5 a. è ben definita: se $[x] = [x']$ e $[y] = [y']$ ossia se $x' = x + h$ e $y' = y + k$ con $h, k \in \mathbb{Z}$, allora $[x'] * [y'] = [x + 2h] * [y + 2k] = [x + y + (2h + 2k)] = [x + y] = [x] * [y]$. Analogamente è ben definita c. Invece b. non è ben definita: $[0] * [\pi] = [0] \neq [\pi] = [1] * [\pi]$.

3.7 $f(0) = 5$, $f^{-1}(5) = \{n \in \mathbb{Z} \mid n^2 - 3n + 5 = 5\} = \{0,\ 3\ \}$, $f^{-1}(0) = \emptyset$. Non è nè suriettiva (poichè $f^{-1}(0) = \emptyset$) nè iniettiva (poichè $f^{-1}(5) = \{0,\ 3\ \}$.

3.8 $f(0) = 5$, $f^{-1}(5) = \{n \in \mathbb{Z} \mid 2n^2 - 3n + 5 = 5\} = \{0\}$ (N.B. $\frac{3}{2} \notin \mathbb{Z}$!), $f^{-1}(0) = \emptyset$. Non è suriettiva poichè $f^{-1}(0) = \emptyset$. Si tratta invece di una applicazione iniettiva: se ci fossero due interi a, b con la stessa immagine k, allora il polinomio $2x^2 - 3x + 5 - k$ dovrebbe avere le due radici intere a e b e quindi si avrebbe $2x^2 - 3x + (5 - k) = 2(x - a)(x - b)$ da cui $3 = 2(a + b)$ che è impossibile.

3.9 a. $f(\mathbb{N} \times \{0\}) = f(\{0\} \times \mathbb{N}) = \{0\}$.

b. $f^{-1}(n) = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m \geq n\} \cup \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m \geq n\}$.

c. f non è iniettiva (cfr. punto a.) e quindi non è biunivoca. È invece suriettiva: $\forall n \in \mathbb{N}$ si ha $f((n, n)) = n$.

3.10 a. $Im(f) = \mathbb{Z}$, $f(\mathbb{Z} \times \{0\}) = \mathbb{Z}$, $f(\{0\} \times \mathbb{Z}) = \{m^2 \mid m \in \mathbb{N}\}$.

b. $f^{-1}(4) = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n = 4 - m^2\}$, $f^{-1}(\mathbb{Z}_-) = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < -m^2\}$.

c. f non è iniettiva (cfr. punto a.) e quindi non è biunivoca. È invece suriettiva: per ogni $n \in \mathbb{Z}$ si ha $f((n, 0)) = n$.

3.11 a. f non è iniettiva e non è suriettiva: cfr. punto b.

b. $f^{-1}((1, 1)) = f^{-1}((4, 7)) = \emptyset$, $f^{-1}((1, 2)) = \{(2k + 1, 1) \mid k \in \mathbb{Z}\} \cup \{(2, 1)\}$, $f^{-1}((11, 12)) = \{(12, 11)\}$, $f^{-1}((4, 6)) = \{(6, 4)\}$.

c. $f(2\mathbb{Z} \times 2\mathbb{Z}) = 2\mathbb{Z} \times 2\mathbb{Z}$ e $f^{-1}(2\mathbb{Z} \times 2\mathbb{Z}) = \mathbb{Z} \times 2\mathbb{Z}$.

3.12 Le applicazioni sono 8 di cui 6 suriettive e nessuna iniettiva.

3.13 Non esiste alcuna applicazione f siffatta, poichè l'immagine di un insieme con due elementi contiene uno oppure due elementi e non più. Esistono invece infinite applicazione del tipo g, ad esempio $g(x) = 1$ per ogni $x \neq 1$ e $(1) = 2$.

3.14 $f(0) = 1$, $f(1) = 1$, $f(2) = 2$, $f(3) = 3$, $f(4) = 5$, $f(5) = 8$. Non è suriettiva poichè ad esempio $4 \notin Im(f)$: infatti f è crescente, ossia $f(n+1) \geq f(n)$ per ogni $n \in \mathbb{N}$, e $f(i) \neq 4$ se $i \leq 3$, $f(4) = 5 > 4$. Inoltre non è neppure iniettiva poichè $f(0) = f(1)$.

3.15 $Im(\phi) = \mathbb{N}$ poichè per ogni $n \in \mathbb{N}$ si ha $f((n, 1)) = n$. La controimmagine di ogni naturale $\neq 1$ contiene almeno due coppie, poichè: $f((n, 1)) = f((1, n)) = n$; nel caso in cui $n = p$ sia un numero primo, non ce ne sono altre. L'unica controimmagine che sia un singleton è $f^{-1}(1) = \{(1, 1)\}$.

3.16 Per provare che ϕ è biunivoca basta determinare la sua inversa, che è: $\phi^{-1}\colon \mathbb{R} \to \mathbb{R}$ data da $\phi^{-1}((a, b)) = (\frac{a+b}{2}, \frac{a-b}{2})$.

3.17 Le proprietà di ϕ dipendono dal sottoinsieme B scelto. Se $B = A$ allora ϕ è la funzione identità e quindi è biunivoca; se invece B è un sottoinsieme proprio di A, allora ϕ non è nè suriettiva nè iniettiva: infatti $A \notin Im(\phi)$ e inoltre se $a \in A \setminus B$, allora $\phi(\emptyset) = \phi(\{a\}) = \emptyset$.

3.18 a. $(g \circ f)(x) = x^4$, $(f \circ g)(x) = (x - 1)^4 + 1$;

b. $(g \circ f)(x) = |x|$, $(f \circ g)(x) = x$;

c. $(g \circ f)(x) = 2$ se $x > 0$ e $(g \circ f)(x) = 0$ se $x < 0$. La composizione $f \circ g$ non è definita poichè il codominio di g non coincide col dominio di f (e neppure è un suo sottoinsieme; ad esempio non ha senso $(f \circ g)(-1) = f(g(-1)) = f(0)$.

3.19 Per ogni g si ha $(f \circ g)(2) = f(g(2)) = (g(2))^2 \neq 2 = id(2)$. Definiamo $h_1(m) = h_2(m) = \sqrt{m}$ se m è il quadrato di un naturale e $h_1(m) = 1$ $h_2(m) = 2$ se m non è n quadrato.

3.20 Una applicazione g siffatta non esiste poichè $f(0) = f(1) = 0$ e quindi $g(0)$ dovrebbe essere sia 0 sia 1. Definiamo $h_1(m) = h_2(m) = -m + 1$ se $m \neq 2$ $h_1(2) = -1$ $h_2(2) = 2$

3.21 f non è iniettiva poichè ad esempio $f(6) = f(9) = 25$ e non è suriettiva poichè $Im(f) \subseteq 2\mathbb{Z}$. Non essendo nè iniettiva nè suriettiva ovviamente non è neppure biunivoca. $f^{-1}(0) = f^{-1}(-3) = \emptyset$ mentre $f^{-1}(1) = \{0,\ 1\}$.

3.23 $[n] = \{n,\ -n\}$ (caso particolare: se n=0, $[0] = \{0\}$). $\phi\colon \mathbb{Z}_{/\sim} \to Im(\phi)$ è data da $\phi([n]) = n^4$.

3.25 $A = \mathbb{R}$ e $f(x) = |x|$.

3.27 Sia $f\colon A = \mathbb{R} \to B = \mathbb{R}$.

1. Nè iniettiva, nè suriettiva. $g(f(-32)) = 32$. Modifiche $A = B = \mathbb{R}_{\geq 0}$.
2. Iniettiva, ma non suriettiva. $g(f(-32)) = -32$. Modifiche $B = \mathbb{R}_{>0}$.
3. Nè iniettiva, nè suriettiva. $g(f(-32)) = -32 + k\pi$ dove $k = [\frac{1}{2} + \frac{32}{\pi}]$ ($[x]$ indica la parte intera di x). Modifiche $A = [-\frac{\pi}{2}, \frac{\pi}{2}]$, $B = [-1, 1]$.
4. Nè iniettiva, nè suriettiva. $g(f(-32)) = -32 + h\pi$ dove $h = [1 + \frac{32}{\pi}]$. Modifiche $A = [0, \pi]$, $B = [-1, 1]$.
5. Iniettiva, ma non suriettiva. $g(f(-32)) = -32$. Modifiche $B = (-\frac{\pi}{2}, \frac{\pi}{2})$.

Capitolo 4

4.1 a. Base del'induzione $n = 1$: $\quad 1 = \frac{2\cdot 1^3 + 3\cdot 1^2 + 1}{6}$.

Passo induttivo: supposto l'asserto vero per un certo n_0 proviamo che vale anche per $n_0 + 1$:

$1 + 4 + \cdots + n_0^2 + (n_0+1)^2 =$ (per l'ipotesi induttivA) $\frac{2n_0^3 + 3n_0^2 + n_0}{6} + (n_0^2 + 2n_0 + 1) = \frac{2n_0^3 + 9n_0^2 + 13n_0 + 6}{6} = \frac{2(n_0+1)^3 + 3(n_0+1)^2 + (n_0+1)}{6}$

4.2 Il passo induttivo vale, ma $A = \emptyset$: non si tratta di una contraddizione poichè non vale il passo iniziale per alcun n_0.

4.4 Per induzione. Passo iniziale: per $k = 7$ si ha $(7-5)^4 = 16 > 7$.

Passo induttivo: se la formula vale per un qualche $k_0 \geq 7$ allora vale anche per $k_0 + 1$:

$((k_0+1)-5)^4 = (k_0-5)^4 + 4(k_0-5)^3 + 6(k_0-5)^2 + 4(k_0-5) + 1 >$ (ipotesi ind.) $k_0 + 4(k_0-5)^3 + 6(k_0-5)^2 + 4(k_0-5) + 1 > k_0 + 1$.

Infine $\{k \in \mathbb{N} \mid (k-5)^4 > k\} = \{k \in \mathbb{N} \mid k \neq 4,\ 5,\ 6\ \}$.

4.5 La formula è banalmente vera per $n = 1$. Supponiamola vera per un certo n_0 e proviamo che vale anche per $n_0 + 1$ rette. Osserviamo che si ha $\frac{(n_0+1)^2 + (n_0+1) + 2}{2} = \frac{n_0^2 + n_0 + 2}{2} + n_0 + 1$; basta allora considerare le parti corrispondenti a n_0 rette e notare che una ulteriore retta r attraversa (dividendoli in due) esattamente $n_0 + 1$ di tali parti: sono quelle corrispondenti alle $n_0 + 1$ parti della retta r individuate dai n_0 punti di intersezione di r con le altre rette.

4.7 Per induzione su n. Per $n = 0$ è definita per ogni $m \in \mathbb{N}$ da da $0 \cdot m = 0$.

Passo induttivo (avendo già definito la somma): $(n+1) \cdot m = n \cdot m + m$.

Sempre per induzione su m. Per $n = 2$ si ha $2 \cdot m = 1 \cdot m + m = m + m > m$ (cfr. esercizio precedente).

Passo induttivo : $(n+1) \cdot m = n \cdot m + m > m + m \geq m + 1$.

4.8 $f\colon \mathbb{N} \to \mathbb{N}$ data da $f(n) = n$ se $n \geq 2$, $f(0) = 1$ e $f(1) = 0$ è suriettiva e quindi ha la stessa immagine della funzione identità.

4.9 Indichiamo con $6\mathbb{Z}$ il sottoinsieme di $\mathbb{Z}$ dei multipli interi di 6. Provare che $Card(6\mathbb{Z}) = Card(\mathbb{Z})$.

4.10 L'applicazione $f\colon \mathbb{N} \to Q$ data $f(n) = n^2$ è biunivoca e quindi $card(Q) = card(\mathbb{N}) = \aleph_0$.

4.11 Se $A = \{1, \ldots, k\}$, l'applicazione $f\colon A \times \mathbb{N} \to \mathbb{N}$ data $f((i,n)) = i + kn$ è biunivoca e quindi $card(A \times \mathbb{N}) = card(\mathbb{N}) = \aleph_0$.

4.12 Le applicazion1 $f\colon (0,1) \to (3,+\infty)$ data $f(x) = \frac{3}{1-x}$ e $g\colon (0,1) \to \mathbb{R}$ data $g(x) = \frac{2x-1}{x(1-x)}$ sono biunivoche e quindi $card((0,1)) = card((3,+\infty)) = card(\mathbb{R})$.

4.13 L'applicazione $f : \gamma \to \Gamma$ data da $f((a,b)) = (\sqrt{2}a, \sqrt{2}b))$ è biunivoca e quindi $card(\gamma) = card(\Gamma)$. Le applicazioni $g, h : \mathbb{R} \to \gamma$ date da $g(t) = (\frac{t}{\sqrt{t^2+1}}, \frac{1}{\sqrt{t^2+1}})$ e $h(t) = (cos(t), sen(t))$ sono rispettivamente iniettiva e suriettiva e quindi $card(\mathbb{R}) = card(\gamma)$.

Infine γ contiene nel suo interno il segmento $(-1,1)$ dell'asse x e quindi gli infiniti punti a coordinate razionali $(a,0)$ con $a \in (-1,1) \cap \mathbb{Q}$.

4.14 Siano P l insieme dell 500 persone, $A = \{n \in \mathbb{N} \mid 1 \leq n \leq 366\}$ e $f\colon P \to A$ l'applicazione che associa ad ogni persona il il giorno dell'anno (bisestile) corrispondente al suo compleanno. Tale applicazione non può essere iniettiva perchè $500 > 366$.

Almeno $2 \cdot 366 + 1$.

4.15 Il numero degli abitanti in Italia supera la cifra di $366 \cdot 60 \cdot 250$, dove 366 sono i giorni dell'anno bisestile, 60 è una approssimazione per eccesso dei possibili (ragionevoli) numeri di scarpe e 250 è una approssimazione per eccesso delle possibili altezze espresse in centimetri. Per quanto riguarda Torino, la risposta è probabilmente no, poichè anche considerando valori più precisi delle maggiorazioni utilizzate prima, il risultato difficilmente sarà inferiore al numero di abitanti di Torino.

Capitolo 5

5.1 2, 6, 3, $\frac{6!}{2}$, $\frac{7!}{2\cdot 2}$, $\frac{9!}{4!\cdot 2!}$.

5.2 $\binom{20}{2}$, $\binom{n}{2}$.

5.3 $\binom{5}{2}$, NO , $\binom{n}{2}$.

5.4 3!, 3!.

5.5 $\frac{6!}{2!}$, 6^4, $6 \cdot 5 \cdot 5 \cdot 4$.

Nel primo caso si può solo se $m \geq n$; negli altri casi si può sempre, qualsiasi siano m ed n e i modi sono rispettivamente m^n e $\frac{m!}{(m-n)!}$.

Si può in ogni caso e i modi sono $m \cdot (m-1)^{n-2} \cdot (m-2)$.

5.6 Se per prodotto si intende il risultato (indipendente dall'ordine dei fattori) e si suppone di poter usare anche uno solo oppure due soli dei tre numeri a disposizione, allora i modi sono $C^r_{3,6} = \binom{8}{2} = 28$.

5.7 $D_{9,4} = 9 \cdot 8 \cdot 7 \cdot 6$.

5.8 $C^r_{4,30} = \binom{33}{3}$, $C^r_{4,26} = \binom{30}{3}$, $4 \cdot C^r_{4,14} = 4 \cdot \binom{17}{3}$, $4 \cdot C^r_{4,11} = 4 \cdot \binom{14}{3}$.

5.9 a. 4; $4^3 \cdot 4$.

5.9 b. Scegliamo l'applicazione $f\colon A \to B$ con grafico $\{(1,1),\ (2,2),\ (3,6),\ (4,4),\ (5,4)\}$; le possibili applicazioni g sono due con grafico rispettivamente $\Gamma_1 = \{(1,1),\ (2,2),\ (6,3),\ (4,4)\ \}$ e $\Gamma_2 = \{(1,1),\ (2,2),\ (6,3),\ (4,5)\ \}$.

5.9 c. Scegliamo l'applicazione $f\colon A \to C$ con grafico $\{(1,1),\ (2,1),\ (3,1),\ (4,1),\ (5,2)\}$. Le possibili applicazioni $g\colon C \to A$ sono 4 con grafico $\Gamma_i = \{(1,i),\ (2,5)\ \}$ dove $i \in \{1,\ 2,\ 3,\ 4\ \}$. Scelte differenti di f darebbero un numero diverso di applicazioni g.

5.9 d. Qualsiasi applicazione h si scelga il numero delle possibili applicazioni k è 4.

5.10 e. Qualsiasi applicazione h si scelga, il numero delle possibili applicazioni k è 8.

12.1 Qualche esercizio svolto

12.1. *Per ogni $n \in \mathbb{N}$, sia $A_n = \{k \in \mathbb{N} \mid k = n^2 + 2t + 3$ con $t \in \mathbb{N}\}$. Determinare in modo esplicito gli insiemi $X = \bigcup_{n\in\mathbb{N}} A_n$ e $Y = \bigcap_{n\in\mathbb{N}} A_n$.*

Un metodo per svolgere esercizi di questo tipo è quello di formulare ipotesi (possibilmente corrette) sugli insiemi X e Y e dimostrare quindi le uguaglianze tra insiemi ad esempio mediante la "doppia inclusione ".

Ragionevole ipotesi su X: $X = \mathbb{N} \setminus \{0, 1, 2\}$ ossia $X = \{x \in \mathbb{N} \mid x \geq 3\}$.

1) Proviamo l'inclusione $\bigcup_{n\in\mathbb{N}} A_n \subseteq \{x \in \mathbb{N} \mid x \geq 3\}$.
Si ha: $x \in \bigcup_{n\in\mathbb{N}} A_n \iff \exists\, n \in \mathbb{N}$: $x \in A_n \iff \exists\, n, t \in \mathbb{N}$: $x = n^2 + 2t + 3 \implies x \in \mathbb{N}$ e $x \geq 3$ ossia $x \in \{x \in \mathbb{N} \mid x \geq 3\}$.

2) Proviamo l'inclusione $\{x \in \mathbb{N} \mid x \geq 3\} \subseteq \bigcup_{n\in\mathbb{N}} A_n$.
Sia x un numero naturale ≥ 3; trattiamo separatamente il caso x pari e il caso x dispari. Se x è dispari, allora $x = 2s + 1$ con s numero naturale ≥ 1 e quindi $x = 0^2 + 2(s - 1) + 3$ ossia $x \in A_0$. Se x è pari allora $x = 2s$ con s numero naturale ≥ 2 e quindi $x = 1^2 + 2(s - 2) + 3$ ossia $x \in A_1$.

In conclusione $\{x \in \mathbb{N} \mid x \geq 3\} \subseteq A_0 \cup A_1 \subseteq \bigcup_{n\in\mathbb{N}} A_n$.

Ragionevole ipotesi su Y: $Y = \emptyset$.
Poichè Y è un sottoinsieme dei numeri naturali, per provare che Y è vuoto basterà verificare che nessun numero naturale gli appartiene. Più precisamente proviamo che $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ tale che $n \notin A_m$. Un intero m siffatto in genere dipenderà da n e comunque, fissato n, non è necessariamente unico; in questo caso ad esempio possiamo prendere $m = n$ poichè $n^2 + 3 > n$ e quindi $n^2 + 2t + 3 \neq n$ (ma anche $m = 1000n$ oppure $m = n + 37$ oppure .... sarebbero andati altrettanto bene).

Un modo alternativo (più sintetico) per provare che $\bigcap_{n\in\mathbb{N}} A_n = \emptyset$ è il seguente :
$\bigcap_{n\in\mathbb{N}} A_n \subseteq A_0 \cap A_1 = \emptyset$, dove l'inclusione ha validità generale e la seconda uguaglianza deriva immediatamente dall'osservazione che A_0 contiene solo numeri dispari mentre A_1 numeri pari. Notiamo esplicitamente che **non è necessario** dimostrare l'altra inclusione $\emptyset \subseteq Y$ poichè essa vale sempre per qualsiasi insieme.

12.2. *Per ogni $\alpha \in \mathbb{R}$, sia I_α l'intervallo aperto (senza gli estremi) $(\frac{\alpha^2}{\alpha^2+1}\,,\, \alpha^2+1)$. Determinare esplicitamente gli insiemi $A = \bigcup_{\alpha\in\mathbb{R}_+} I_\alpha$ e $B = \bigcap_{\alpha\in\mathbb{R}_+} I_\alpha$, dove $\mathbb{R}_+$ denota l'insieme dei numeri reali strettamente positivi.*

Proviamo che $A = (0\,,\, +\infty)$.
1) Per provare che $A \subseteq (0\,,\, +\infty)$ basta osservare che ogni intervallo I_α è costituito da numeri reali strettamente positivi.
2) Per provare che $(0\,,\, +\infty) \subseteq A$ esibiamo esplicitamente per ogni numero reale positivo x un intervallo I_α che lo contiene. Se $x = 1$, allora $x \in I_\alpha$ per ogni α; se $x > 1$, allora si ha $\frac{x^2}{x^2+1} < 1 < x < x^2 + 1$, ossia $x \in I_x$; se $0 < x < 1$, allora $x \in I_y$, dove $y = \sqrt{\frac{x}{2(1-x)}}$ poichè $\frac{y^2}{1+y^2} = \frac{x}{2-x} < x < 1 < 1 + y^2$. Osserviamo che ci sono molti intervalli I_α che contengono un certo numero x e che quindi quelli da noi esibiti non sono gli unici possibili e che quindi vi sono molte altre scelte diverse che sarebbero state altrettanto corrette.

Proviamo che $B = \{1\}$.
1) Per provare che $\{1\} \subseteq B$ basta osservare che $1 \in I_\alpha$ per ogni $\alpha \in \mathbb{R}_+$ poichè si ha sempre $\frac{\alpha^2}{\alpha^2+1} < 1$ ed anche $1 < \alpha^2 + 1$.
2) Per provare che $B \subseteq \{1\}$ proviamo che $\mathbb{R} \setminus \{1\} = \mathcal{C}_\mathbb{R}(\{1\} \subseteq \mathcal{C}_\mathbb{R}(B) = \bigcap \mathcal{C}_\mathbb{R}(I_\alpha)$. Se x è un numero reale negativo o nullo, allora $x \notin I_\alpha$ per ogni α; se $0 < x < 1$, allora $x \notin I_y$, dove $y = \sqrt{\frac{x}{1-x}}$ poichè $x = \frac{y^2}{1+y^2}$; se $x > 1$, allora $x \notin I_z$, dove $z = \sqrt{x - 1}$ poichè $x = z^2 + 1$

12.3. *È vero che per ogni coppia di insiemi $A, B \subset X$, la famiglia $\{A \cap B, A \setminus B, B \setminus A, \mathcal{C}_X(A \cup B)\}$ è una partizione di X?*

Per risolvere esercizi come questo può essere utile aiutarsi con un disegno tipo diagramma di Venn, tenendo però ben presente che ogni disegno è sempre un caso particolare (anche se noi cerchiamo di rappresentare il caso più generale possibile) e quindi non tiene conto di ogni possibile situazione. È opportuno quindi avere anche ben presenti le definizioni e le proprietà di tutti gli oggetti coinvolti.

In questo caso ad esempio un disegno potrebbe suggerire che la risposta sia positiva, mentre ricordando la definizione di partizione ci si accorge che la risposta è chiaramente negativa. La prima condizione affinchè una famiglia di sottoinsiemi sia una partizione è che ciascuno dei sottoinsiemi sia diverso da $\emptyset$, mentre si possono facilmente costruire degli insiemi A e B per i quali uno qualsiasi dei 4 sottoinsiemi elencati risulti vuoto. Allora:

La risposta è: NO. Per motivarla dobbiamo fornire un controesempio esplicito che può essere il seguente: $X = \mathbb{N}$, $A = \emptyset$, $B = \mathbb{N}$; si ha infatti addirittura $A \cap B = A \setminus B = \mathcal{C}_X(A \cup B) = \emptyset$.

In questo modo la risposta all'esercizio è corretta e completa. Volendo possiamo aggiungere che (come suggerito dal disegno di diagrammi di Venn) ogni volta che i 4 sottoinsieme sono tutti non vuoti, allora essi effettivamente costituiscono una partizione. Per verificare che ciò è proprio vero dobbiamo mostrare che la loro unione restituisce tutto X e che essi sono due a due disgiunti. Verifichiamo a mo' di esempio che $(A \setminus B) \cap \mathcal{C}_X(A \cup B) = \emptyset$.

Per questo osserviamo che $A \setminus B \subset A$ e che $\mathcal{C}_X(A \cup B) \subset \mathcal{C}_X(A)$. Poichè per definizione di complementare $A \cap \mathcal{C}_X(A) = \emptyset$ a maggior ragione sono disgiunti $A \setminus B$ e $\mathcal{C}_X(A \cup B)$.

12.4. *Dimostrare oppure confutare mediante controesempi le seguenti uguaglianze tra insiemi:*

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B), \qquad \mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B).$$

La prima uguaglianza è vera, poichè è vera per qualsiasi coppia di insiemi A e B, infatti:

$X \in \mathcal{P}(A) \cap \mathcal{P}(B) \iff X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$ (cioè X è un elemento sia dell'insieme delle parti di A sia dell'insieme delle parti di B) $\iff X \subseteq A$ e $X \subseteq B$ (cioè X è un sottoinsieme sia di A sia di B) $\iff X \subseteq A \cap B \iff X \in \mathcal{P}(A \cap B)$.

La seconda affermazione è falsa poichè è falsa per almeno una coppia di insiemi A e B. Per provarlo esibiamo un controesempio esplicito.

Sia $A = \{1, 2\}$ e $B = \{3, 4\}$. L'insieme $X = \{1, 3\}$ non è nè un sottoinsieme di A nè un sottoinsieme di B e quindi $X \notin \mathcal{P}(A) \cup \mathcal{P}(B)$, mentre $X \in \mathcal{P}(A \cap B)$ poichè $X \subset (A \cap B)$.

Attenzione: non abbiamo affatto provato la validità di $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$ perchè affermare che una certa relazione è falsa (ossia non è sempre vera) non significa affermare che è sempre falsa. Ad esempio per insiemi A e B tali che $A \subset B$, anche la seconda uguaglianza risulta verificata.

12.5. *In $\mathbb{Z}$ si consideri la relazione: $x \rho y$ se se $\exists k \in \mathbb{N}$ tale che $y = kx$.*

- ***a.*** *Verificare che ρ è una relazione d'ordine.*
- ***b.*** *È un ordine totale? È un buon ordinamento?*
- ***c.*** *Dire se $\mathbb{Z}$ e i sottoinsiemi $A = \mathbb{N}$ e $B = \{n \in \mathbb{Z} \colon n < 0\}$, $C = \{-2, -3, -4, -12\}$ di $\mathbb{Z}$ ammettono minimo e/o massimo rispetto alla relazione ρ.*

a. Verifichiamo che ρ è riflessiva, antisimmetrica e transitiva.

R) La proprietà riflessiva vale perché si ha $x = 1 \cdot x$ per ogni intero x e quindi $x \rho x$.

A) Osserviamo che due numeri di segno discorde non sono mai in relazione. Inoltre se x, y sono diversi e $x \rho y$, allora $y = kx$ per un certo $k \neq 1$. Se $k = 0$, allora $y = 0$ e non c'è nessun numero $x \neq 0$ tale che $0 \rho x$. Se $k \geq 2$, allora $|x| < |y|$. Quindi, se $x \neq y$ non possono valere sia $x \rho y$ sia $y \rho x$ perchè in tal caso si avrebbero le due diseguaglianze incompatibili $|x| < |y|$ e $|y| < |x|$.

T) Siano x, y, z interi tali $x \rho y$ e $y \rho z$ ossia $y = kx$ e $z = hy$ per certi $h, k \in \mathbb{N}$; allora $z = hkx$ dove $hk \in \mathbb{N}$ e quindi $x \rho z$.

b. Non si tratta di un ordine totale perchè due numeri di segno opposto, ad esempio 1 e -1, non sono confrontabili. Non essendo un ordine totale, non può essere neppure un buon ordine.

c. Poichè i numeri di segno opposto non sono confrontabili tra loro, mentre il minimo e il massimo (se esistono) devono essere confrontabili con tutti gli elementi dell'insieme, allora l'unico possibile candidato ad essere il minimo o il massimo di $\mathbb{Z}$ rispetto alla relazione ρ è 0. Come già osservato si ha $x\rho 0$ per ogni $x \in \mathbb{Z}$ poichè $0 = 0 \cdot x$ e $k = 0 \in \mathbb{N}$: 0 è allora il massimo di $\mathbb{Z}$ rispetto a ρ; inoltre essendo il massimo non può essere anche il minimo (il massimo e il minimo coincidono solo se l'insieme ha 1 elemento) e quindi $\mathbb{Z}$ non ha minimo. (Modo equivalente: 0 non è minimo perchè $0 \neq 2$ e $2\rho 0$.)

Il massimo di $\mathbb{N}$ è 0 perchè $0 \in \mathbb{N}$ e $x\rho 0$ per ogni $x \in \mathbb{Z}$ e quindi a maggior ragione anche per ogni $x \in \mathbb{N}$; il minimo di $\mathbb{N}$ è 1 poichè si ha $n = k \cdot 1$ con $k = n \in \mathbb{N}$.

L'insieme dei negativi B non ha massimo perchè per ogni $x \in B$ esiste $y \in B$, ad esempio $y = 2x$, tale che $x \neq y$ e $x\rho y$; il minimo di B è -1 perchè per ogni $x \in B$ si ha $x = k \cdot (-1)$ dove $k = -x \in \mathbb{N}$.

Il massimo di C è -12 poichè si ha $-12 = 6 \cdot (-2) = 4 \cdot (-3) = 3 \cdot (-4)$. Invece C non ha minimo; si ha infatti $(-2)\rho(-4)$ e $(-2)\rho(-12)$ ma -2 non è confrontabile con -3 e quindi non sono il minimo nè -4 nè -12 perchè -2 è più piccolo di loro (rispetto a ρ), nè -2 nè -3 perchè non sono confrontabili tra loro.

12.6. *In $\mathbb{N} \times \mathbb{N}$ si consideri la relazione $(a,b)\sigma(a',b')$ se $a < a'$ oppure $a = a'$ e $b \geq b'$.*

i) *Verificare che si tratta di una relazione d'ordine totale;*

ii) *provare che $\mathbb{N} \times \mathbb{N}$ non ammette nè minimo nè massimo rispetto a σ;*

i) R) Per ogni $(a,b) \in \mathbb{N} \times \mathbb{N}$ si ha $(a,b)\sigma(a,b)$ perchè $a = a$ e $b \geq b$.

A) Siano (a,b) e (a',b') due coppie tali che $(a,b)\sigma(a',b')$ e $(a',b')\sigma(a,b)$. Non è possibile che si abbia $a \neq a'$ perchè in tal caso dovremmo avere sia $a < a'$ sia $a' < a$. Allora $a = a'$ e inoltre $b \geq b'$ e $b' \geq b$; quindi $b = b'$ e le due coppie coincidono.

T) Supponiamo che si abbiano le due relazioni $(a,b)\sigma(a',b')$ e $(a',b')\sigma(a'',b'')$. Se $a = a' = a''$ allora $b \geq b' \geq b''$ e quindi si ha anche $(a,b)\sigma(a'',b'')$. Se $a \neq a'$ (oppure $a' \neq a''$) allora $a < a' \leq a''$ (risp. $a \leq a' < a''$) da cui $a < a''$ e, di nuovo, $(a,b)\sigma(a'',b'')$.

Infine, verifichiamo che si tratta di un ordine totale. Siano (a,b) e (c,d) due coppie in $\mathbb{N} \times \mathbb{N}$. Se $a \neq c$, allora uno dei due è minore dell'altro; supponiamo $a < c$: allora $(a,b)\sigma(c,d)$. Se $a = c$ allora uno tra b e d è minore o uguale all'altro; supponiamo $b \leq d$ supponiamo: allora di nuovo $(a,b)\sigma(c,d)$.

ii) Sia $(a,b) \in \mathbb{N} \times \mathbb{N}$; proviamo che non è né il minimo né il massimo rispetto alla relazione σ esibendo un elemento più grande e un elemento più piccolo: un elemento strettamente più grande è ad esempio $(a+1,b)$ mentre un elemento strettamente più piccolo è ad esempio $(a,b+1)$.

Capitolo 13

Appendice: Contributi degli studenti

Ho introdotto questo capitolo finale per raccogliere alcune delle numerose osservazioni significative scaturite dall'interesse e dalla partecipazione degli studenti alle lezioni del corso nell'anno accademico 2003/04.

È possibile (a volte fortemente probabile) che le cose presentate siano già comparse in precedenza in letteratura o siano addirittura ben note; non si tratta cioè di materiale originale nel senso che a questo termine si dà usualmente in matematica. L'originalità in questo caso consiste nel fatto che siano stati studenti (del primo anno!) a proporre loro congetture e a lavorare autonomamente per arrivare a provarle o confutarle, facendo così esperienza di un vero lavoro di ricerca senza rete, quale è in genere il lavoro del matematico.

Talvolta l'insegnate è intervenuta per correggere e ripulire l'esposizione o integrare con commenti e osservazioni.

13.1 Relazioni d'ordine

Elena Martinotti

In quanti modi diversi un insieme A con n elementi può essere dotato di una relazione d'ordine?

Si tratta probabilmente di un problema aperto di difficile soluzione.

Una possibile stima per eccesso è conseguenza della seguente osservazione:

Le relazioni d'ordine sono sottoinsiemi di $A \times A$ che contengono la diagonale Δ. Il numero dei possibili ordinamenti è allora maggiorato dalla cardinalità dell'insieme delle parti di $(A \times A) - \Delta$, ossia da 2^{n^2-n}.

13.2 Insiemi infiniti

Fulvio Di Sciullo - Andrea Mondino

La proposizione seguente fornisce una caratterizzazione degli insiemi infiniti mediante le relazioni d'ordine.

Sebbene ogni insieme, finito o infinito, possa essere dotato di una relazione d'ordine rispetto alla quale esso risulta ben ordinato, ossia rispetto alla quale ogni sottoinsieme non vuoto ha il minimo, tuttavia solo gli insiemi finiti possiedono un ordinamento rispetto al quale ogni sottoinsieme non vuoto ha sia il minimo sia il massimo.

Proposizione 13.2.1. *Le seguenti condizioni sono equivalenti per ogni insieme X:*

1) *X è un insieme finito;*

2) *X è dotato di un ordinamento $\preceq$ rispetto al quale ogni sottoinsieme non vuoto di X ammette minimo e massimo.*

Dim: Se X è un insieme finito, esiste una corrispondenza biunivoca φ tra X e l'insieme I_n dei numeri naturali compresi tra 1 e n, per un qualche $n \in \mathbb{N}$. L'ordinamento $\preceq$ su X indotto, tramite φ, dalla relazione d'ordine $\leq$ in $\mathbb{N}$ rispetta ovviamente la condizione 2).

Proviamo infine che per ogni insieme infinito X, non esiste alcun ordinamento che rispetti la condizione data in 2). Un tale ordinamento, se esistesse, dovrebbe essere in particolare un buon ordine; possiamo allora limitarci a provare che se $\preceq$ è un buon ordine in X, allora esiste un sottoinsieme non vuoto Y di X che non ammette massimo.

Costruiamo un tale sottoinsieme Y come l'immagine dell'applicazione $f\colon \mathbb{N} \to X$ definita per induzione nel modo seguente:

i) $f(0)$ è il minimo di X;

ii) avendo definito $f(i)$ per ogni $i = 0, \ldots, n$, $f(n+1)$ è il minimo di $X - \{f(0),\ f(1), \ldots, f(n)\}$.

(Notiamo che tale costruzione ha senso in quanto, essendo X infinito, l'insieme
$X - \{f(0),\ f(1), \ldots, f(n)\}$ non può essere vuoto.)

L'insieme Y così costruito non ha massimo, perchè per ogni suo elemento $f(k)$ si ha, per costruzione, $f(k) \prec f(k+1)$. $\diamond$

13.3 Binomiali

Raffaele Martucciello - Andrea Mondino

Proposizione 13.3.1. *Sia n un numero naturale ≥ 2. Sono fatti equivalenti:*

1) *n è primo;*

2) *n divide $\binom{n}{k}$ per ogni $1 \leq k \leq n-1$;*

Dim: $''1) \Rightarrow 2)''$ segue immediatamente dalla definizione di binomiale.

Per provare $''2) \Rightarrow 1)''$ supponiamo che n non sia primo e consideriamo un suo fattore primo p: allora n non divide $\binom{n}{p}$. Infatti:

$$\binom{n}{p} = \frac{n \cdot (n-1) \cdots (n-p+1)}{p!}.$$

L'unico fattore a numeratore divisibile per p è n e quindi nella fattorizzazione di $\binom{n}{p}$ il fattore primo p compare con esponente inferiore di una unità rispetto a quello con cui compare nella fattorizzazione di n.

$\diamond$

La proprietà 2) è il punto essenziale nella dimostrazione del Piccolo Teorema di Fermat. Si potrebbe quindi pensare che la non validità di questa proprietà per tutti i numeri non primi n abbia come conseguenza la non validità del Piccolo Teorema di Fermat per ogni numero non primo. In realtà, sebbene ciò sia corretto per molti numero interi (ad esempio per i prodotti di due primi o per i numeri che possiedono un fattore primo ripetuto) tale risultato può valere anche per qualche numero non primo, il più piccolo dei quali è 561.

Esempio 13.3.2. *Dalla fattorizzazione* $561 = 3 \cdot 11 \cdot 17$ *segue, grazie al Teorema Cinese, l'isomorfismo di anelli* $\mathbb{Z}_{561} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{17}$ *e quindi sarà sufficiente provare che per ogni intero* m *si ha* $m^{561} \equiv m$ *modulo* 3*, modulo* 11 *e anche modulo* 17*.*

Grazie al Teorema di Eulero si ha:

$$m^{561} = m^{560} \cdot m \equiv 1 \cdot m = m$$

sia modulo 3*, sia* 11*, sia modulo* 17 *in quanto* 560 *è divisibile per* $2 = \phi(3)$*, per* $10 = \phi(11)$ *e per* $16 = \phi(17)$*.*

Si noti che $X^{561} - X$ *è un polinomio monico di grado* 561 *che ha in* $\mathbb{Z}_{561}$ 561 *radici distinte, ma non coincide col polinomio* $X \cdot (X - \overline{1}) \cdot (X - \overline{2}) \cdots (X - \overline{560})$ *in quanto, ad esempio, in quest'ultimo il termine di grado* 1 *ha coefficiente nullo poichè* $1 \cdot 2 \cdots 560$ *è divisibile per* 3*, per* 11 *e per* 17 *e quindi è divisibile per* 561*.*

I numeri simili a 561, ossia i numeri n per i quali $x^n \equiv x$ modulo n per ogni intero x si chiamano **numeri di Carmichael** o anche **numeri pseudo primi** in quanto, pur non essendo numeri primi, superano tutti i test di primalità di Fermat.

Per maggiori dettagli sui numeri di Carmichael si veda:
http://en.wikipedia.org/wiki/Carmichael_number
oppure
http://mathworld.wolfram.com/CarmichaelNumber.html.

13.4 Sistemi di Congruenze

Andrea Mondino

Enunciamo e dimostriamo due risultati che, insieme, forniscono un criterio necessario e sufficiente per la risolubilità di ogni sistema di congruenze, criterio che ha come caso particolare il Teorema Cinese e risulta molto comodo nelle applicazioni.

Lemma 13.4.1. *Un sistema di* 2 *congruenze lineari*

$$\begin{cases} X \equiv a \bmod m \\ X \equiv b \bmod n \end{cases} \tag{13.1}$$

è risolubile se e solo se $mcd(m, n)$ *divide* $b - a$*.*

Dim: Una soluzione del sistema (13.1) è un numero intero x_0 della forma $x_0 = a + ms$ ed anche $x_0 = b + nt$ per opportuni coefficienti interi s, t. Un numero di questo tipo esiste se e solo se $b - a$ si può scrivere come combinazione lineare $ms - nt$ per opportuni coefficienti $s, t \in \mathbb{Z}$ e quindi, come già dimostrato, se e solo se $b - a$ è un multiplo di $mcd(m, n)$. $\diamond$

Teorema 13.4.2. *Un sistema di congruenze lineari*

$$\begin{cases} a_1 X \equiv b_1 \bmod n_1 \\ a_2 X \equiv b_2 \bmod n_2 \\ \cdots\cdots\cdots\cdots\cdots \\ a_k X \equiv b_k \bmod n_k \end{cases} \tag{13.2}$$

è risolubile se e solo se per ogni i, j*,* $(1 \leq i < j \leq k)$ *sono risolubili i sistemi di due congruenze:*

$$\begin{cases} a_i X \equiv b_i \bmod n_i \\ a_j X \equiv b_j \bmod n_j \end{cases} \tag{13.3}$$

.

Dim: È intanto evidente che la risolubilità due a due è una condizione necessaria alla risolubilità del sistema complessivo. Proviamo che è anche sufficiente.

Procediamo per induzione su k.

Se $k = 2$ l'asserto è ovviamente vero.

Supponiamo ora l'asserto vero per i sistemi con meno di k congruenze e proviamolo per il sistema (13.2), supponendo che soddisfi l'ipotesi di risolubilità due a due.

Naturalmente, in tali ipotesi, le congruenze sono risolubili anche singolarmente e quindi possiamo trasformare il sistema in uno equivalente della forma:

$$\begin{cases} X \equiv c_1 \bmod m_1 \\ X \equiv c_2 \bmod m_2 \\ \dots\dots\dots\dots\dots \\ X \equiv c_k \bmod m_k. \end{cases} \tag{13.4}$$

Proviamo che, sostituendo alle prime due congruenze un'unica congruenza che esprime le loro soluzioni comuni (che esiste per ipotesi), otteniamo un sistema di $k-1$ congruenze equivalente al precedente e che soddisfa a sua volta la condizione di risolubilità due a due.

Consideriamo, oltre alle prime due, anche una qualsiasi delle $k-2$ congruenze rimanenti:

$$\begin{cases} X \equiv c_1 \bmod m_1 \\ X \equiv c_2 \bmod m_2 \\ X \equiv c \bmod m. \end{cases} \tag{13.5}$$

Possiamo supporre che $mcd(m_1, m_2, m) = 1$ (in caso contrario possiamo dividere ogni termine delle congruenze per tale mcd) e indicare con d il $mcd(m_1, m_2)$.

A meno di un cambiamento di variabile del tipo $X' = X - c$ possiamo supporre $c = 0$; possiamo inoltre sostituire c_1 (rispettivamente: c_2) con una soluzione del sistema formato dalla prima (rispettivamente: seconda) e dalla terza congruenza (che esiste per ipotesi), ossia con un numero del tipo $q_1 m$ (risp.: $q_2 m$). Si ottiene così un sistema equivalente a (13.5) del tipo:

$$\begin{cases} X' \equiv q_1 m \bmod m_1 \\ X' \equiv q_2 m \bmod m_2 \\ X' \equiv 0 \bmod m. \end{cases} \tag{13.6}$$

Ancora in virtù delle ipotesi, sappiamo che esistono soluzioni del sistema formato dalle prime due congruenze; una tale soluzione Q è un numero della forma $Q = q_1 m + m_1 s = q_2 m + m_2 t$ (dove s, t sono opportuni interi) e il sistema (13.6) è equivalente a:

$$\begin{cases} X' \equiv Q \bmod \frac{m_1 m_2}{d} \\ X' \equiv 0 \bmod m. \end{cases} \tag{13.7}$$

Non ci resta che provare che il sistema (13.7) soddisfa la condizione di risolubilità data dal Lemma 13.4.1, ossia che $mcd(\frac{m_1 m_2}{d}, m)$ divide Q.

Per costruzione $mcd(d, m) = mcd(m_1, m_2, m) = 1$ e quindi si ha $mcd(\frac{m_1 m_2}{d}, m) = mcd(m_1 m_2, m) = mcd(m_1, m) \cdot mcd(m_2, m)$, dove i due numeri $mcd(m_1, m)$ e $mcd(m_2, m)$ sono coprimi. Possiamo allora dire che Q è multiplo del loro prodotto poichè è multiplo di ciascuno dei due in quanto $Q = q_1 m + m_1 s$ e $Q = q_2 m + m_2 t$. $\diamond$

Osservazione 13.4.3. *Per sapere se un sistema di congruenze ammette soluzioni senza risolverlo, è sufficiente scriverlo nella forma (13.4) e controllare la risolubilità due a due mediante il comodo criterio fornito dal Lemma 13.4.1.*