APPUNTI ED ESERCIZI

DI MATEMATICA DISCRETA

per il C.L. in Informatica

Cristina Bertone, Margherita Roggero

A.A. 2017/2018

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.

Useremo spesso 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. Gli elementi dell'insieme sono quelli presenti nell'elenco, non ha importanza se sono elencati più volte o in quale ordine.

Esempio 1.1. $A = \{0, 1\}$ è l'insieme costituito dai due numeri 0 e 1. Anche $\{1, 0\}$ e $\{0, 0, 1, 1, 1\}$ sono l'insieme A, perché l'ordine e le ripetizioni sono irrilevanti.

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 1.2. Non hanno alcun senso espressioni quali: $X = \{\text{multipli di } 2\}$, $Y = \{\text{numeri naturali grandi}\}$, $Z = \{\text{soluzioni dell'equazione } x^4 - 1 = 0\}$.

L'insieme $V = \{x \in \mathbb{R} \mid x^2 = -1\}$ è invece perfettamente definito. Poichè 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: $\{x \in \mathbb{R} \mid x^2 = -1\} = \emptyset = \{n \in \mathbb{N} \mid n > n\}$.

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, l'affermazione che a non appartiene all'insieme vuoto si scrive 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" oppure "se e solo 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. Per ogni insieme A, scriveremo $\#A = n$ oppure $|A| = n$ se A ha un numero finito n di elementi oppure $\#A = |A| = \infty$ se ne ha infiniti.

Esempio 1.3. (i) $\#\{x \in \mathbb{R} \mid x^2 - 3 = 0\} = \#\{-\sqrt{3},\ \sqrt{3}\} = 2$,

(ii) Se $A = \{1, 0, -3, 1, 7, 0, 0, 7\}$, si ha $|A| = 4$. Ricordiamo infatti che gli elementi di un insieme si contano una volta sola e quindi $A = \{1, 0, -3, 7\}$.

(iii) Indicando con $2\mathbb{Z}$ l'insieme dei numeri interi pari, ossia

$$2\mathbb{Z} = \{x \in \mathbb{Z} \mid \exists n \in \mathbb{N} :\ x = 2n,\ n \in \mathbb{Z}\}$$

si ha $\#2\mathbb{Z} = \infty$ ed anche $\#\mathbb{Z} = \infty$.

§ 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 1.4. L'implicazione $\forall n \in \mathbb{N}\ (n > 3 \Longrightarrow 2n$ è pari) è corretta. Invece $\forall n \in \mathbb{N}\ (n > 3 \Longrightarrow n^2 > 20)$ è falsa perché esiste almeno un caso in cui la prima affermazione è vera e la seconda no: $4 > 3$, ma $4^2 \leq 20$. Sono vere anche affermazioni piuttosto strane per il senso comune come: $\forall n \in \mathbb{N}\ (n < -3 \Longrightarrow 2n$ è pari)

$\forall n \in \mathbb{N}\ (n < -3 \Longrightarrow 2n$ è dispari)

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. Le strane affermazioni dell'esempio precedente sono considerate corrette poichè non ammettono controesempi: non vi sono infatti numeri naturali minori di -3 da poter usare come controesempi. Se A è un *sottoinsieme proprio* di B, ossia se è un sottoinsieme di B diverso da B stesso, si può anche scrivere $A \subset B$, oppure ancor pi'u chiaramente $A \subsetneq B$, invece di $A \subseteq B$. Quindi: $A \subsetneq B$ se ogni elemento di A è anche elemento di B, ma vi è almeno un elemento di B che non è elemento di A. Anche in questo caso una sbarra sul simbolo indica la sua negazione: $A \not\subset B$ significa che l'insieme A non è un sottoinsieme dell'insieme B, ossia che esiste almeno un elemento di A che non è elemento di B. In simboli:

$$A \not\subset B \Longleftrightarrow\ \exists\ a \in A,\ a \notin B.$$

Esempio 1.5. (i) $\{x \in \mathbb{N} \mid x^2 < 20\} \subseteq \mathbb{N}$; poichè siamo sicuri che vi sono dei numeri naturali che non appartengono al primo insieme (come per esempio $x = 100$) possiamo anche scrivere $\{x \in \mathbb{N} \mid x^2 < 20\} \subset \mathbb{N}$.

(ii) $\{x \in \mathbb{N} \mid x^7 - 3x^5 + 5x^2 - 3x + 1 > 0\} \subseteq \mathbb{N}$; in questo caso è difficile stabilire se i due insiemi sono diversi oppure no e quindi ci conviene evitare il simbolo $\subset$.

(iii) l'insieme dei numeri naturali $\mathbb{N}$ e l'insieme dei numeri interi pari $2\mathbb{Z}$ sono entrambi sottoinsiemi di $\mathbb{Z}$, ma nessuno dei due è sottoinsieme dell'altro:

$$\mathbb{N} \subset \mathbb{Z},\ 2\mathbb{Z} \subset \mathbb{Z}, \mathbb{N} \not\subset 2\mathbb{Z},\ 2\mathbb{Z} \not\subset \mathbb{N}.$$

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

La seguente proprietà viene usata molto spesso per provare l'uguaglianza tra due insiemi. **Doppia inclusione**

$$A = B \Longleftrightarrow A \subseteq B\ \wedge\ B \subseteq A$$

Il simbolo $\wedge$ abbrevia la congiunzione "e". Dunque, due insiemi sono diversi se differiscono almeno per un elemento, ossia se vi è almeno un elemento nel primo

che non appartiene al secondo oppure vi è almeno un elemento nel secondo che non appartinen al primo:

$$A \neq B \Longleftrightarrow \exists\, a \in A,\ a \notin B \ \vee\ \exists\, b \in B,\ b \notin A \Longleftrightarrow A \not\subseteq B \ \vee\ B \not\subseteq A$$

Il simbolo $\vee$ abbrevia la congiunzione "o", "oppure". Se A è un sottoinsieme proprio di B e B ha un numero finito n di elementi, ossia $\#B = n$, allora anche A ha un numero finito m di elementi, strettamente minore di n, ossia:

$$\#B \in \mathbb{N}\ e\ \ A \subset B \Longrightarrow \#A \in \mathbb{N}\ \ e\ \ \#A < \#B.$$

Invece se $\#B = \infty$, A può avere un numero finito di elementi o anche infiniti elementi come B. Ad esempio $2\mathbb{Z} \subset \mathbb{Z}$, ma $\#2\mathbb{Z} = \infty = \#\mathbb{Z}$.

§ 1.3 Intersezione, unione complementare

Definizione 1.6. *Siano A, B insiemi. 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:*

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

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

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

NOTA BENE: L'espressione $x \in A$ **oppure** $x \in B$ comprende anche il caso degli eventuali elementi che appartengono ad entrambi gli insiemi. Quindi:

$$A \cup B \supseteq A \cap B.$$

Talvolta useremo l'espressione "l'unione disgiunta di A e B" per indicare semplicemente l'unione $A \cup B$, ma sottolineando che i due insiemi A e B considerati sono disgiunti. Non è dunque un diverso tipo di unione, ma è solo un modo abbreviato per "l'unione dei due insiemi A e B (che sono insiemi disgiunti)". 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 1.7. 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 1.8. *Sia I un insieme non vuoto e, per ogni $i \in I$, sia A_i un insieme:*

$$a \in \bigcup_{i\in I} A_i \iff (\exists i \in I \quad a \in A_i), \qquad a \in \bigcap_{i\in I} A_i \iff (\forall i \in I \quad a \in A_i).$$

Esempio 1.9. 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 $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{Z}$. Dimostriamo l'ugualianza $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{Z}$ utilizzando il metodo della doppia inclusione. L'inclusione "$\bigcup_{n\in\mathbb{N}} A_n \subseteq \mathbb{Z}$" è ovvia perché tutti gli insiemi A_n sono contenuti in $\mathbb{Z}$ e quindi anche la loro unione lo è. Per dimostrare l'inclusione opposta "$\bigcup_{n\in\mathbb{N}} A_n \supseteq \mathbb{Z}$" proviamo che ogni numero intero x è contenuto in almeno uno degli insiemi A_n. Possiamo ad esempio scegliere $n = 1$ ed osservare che ogni numero intero è multiplo di 1. Oppure possiamo scegliere $n = |x|$ (dove $|x|$ è il valore assoluto di x). Allora $x = n$ se $x \geq 0$ e $x = -n$ se $x < 0$: in entrambi i casi x è un multiplo di n e quindi $x \in A_n$.

Esempio 1.10. Il dominio della funzione reale di variabile reale $y = \tan(x)$ è:

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

Un modo alternativo di scrivere il dominio della funzione tangente è quello di dire che è costituito da tutti i numeri reali **tranne** i multipli interi di π.

Definizione 1.11. *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:*

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

Quindi il dominio della funzione tangente è $\mathcal{C}_{\mathbb{R}}(\{n\pi \mid n \in \mathbb{Z}\})$.

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

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

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. Data una famiglia A_i, $i \in I$ di sottoinsiemi di un insieme X si ha:

$$\mathcal{C}_X\left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} \mathcal{C}_X(A_i) \quad e \quad \mathcal{C}_X\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} \mathcal{C}_X(A_i).$$

Definizione 1.12. *Dati gli insiemi A e B, si dice* **insieme differenza** *di B ed A, e si denota $B - A$, oppure $B \setminus A$, l'insieme formato da tutti gli elementi di B che non appartengono ad A, ossia:*

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

Talvolta si considera anche l'insieme costituito dagli elementi di due insiemi che non siano elementi comuni.

Definizione 1.13. *Dati gli insiemi A e B, si dice* **differenza simmetrica** *di A e B, e si denota $A \triangle B$, l'insieme formato da tutti gli elementi che appartengono ad uno solo tra A e B, ossia:*

$$x \in A \triangle B \Longleftrightarrow x \in A - B \textit{ oppure } x \in B - A$$

ovvero

$$B \triangle A = (A \cup B) - (A \cap B).$$

§ 1.4 Insieme delle parti

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

Esempio 1.14. 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 1.15. *Si dice* **insieme delle parti** *di un insieme X, l'insieme $\mathcal{P}(X)$ i cui elementi sono i sottoinsiemi di X:*

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

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

Esempio 1.16. 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 poichè 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. Dimostreremo in seguito questa affermazione.

§ 1.5 Partizioni

Vogliamo ora suddividere un insieme X in parti, ciascuna costituita da un suo sottoinsieme, in modo che riunendole tutte riotteniamo l'insieme di partenza. Se non poniamo altre condizioni che questa, otteniamo un **ricoprimento** di X. Ponendo alcune condizioni ulteriori otteniamo ricoprimenti speciali, che vengono utilizzati in numerose costruzioni matematiche.

Definizione 1.17. *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 1.18.

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:

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

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 $\mathbb{Z}$, poichè la loro unione non contiene il numero intero 1 (oppure perché non sono due a due disgiunti).

Solo per curiosità: il Paradosso di Russell. *Secondo la "definizione informale-intuitiva" per cui un insieme è dato semplicemente dai suoi elementi, 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 proprietà: $X \in X$.*

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?

$$Y \in Y \iff Y \text{ è un insieme del primo tipo} \iff Y \notin Y.$$

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.

§ 1.6 Prodotto cartesiano

Definizione 1.19. *Siano A, B 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:*

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

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.

Definizione 1.20. *Ogni sottoinsieme del prodotto cartesiano $A \times B$ si dice anche* **corrispondenza** *tra A e B. Se $D \subseteq A \times B$ e $(a, b) \in D$, diremo anche che gli elementi $a \in A$ e $b \in B$ sono in corrispondenza. Spesso le corrispondenze, come i sottoinsiemi in genere, vengono definite mediante una proprietà caratteristica. Se $A = B$ le corrispondenze in $A \times A$ si chiamano* **relazioni** *in A.*

Esempio 1.21.

a. Il sottoinsieme $D = 2\mathbb{Z} \times 2\mathbb{Z}$ è una corrispondenza in $\mathbb{Z} \times \mathbb{Z}$ (ed è una relazione in $\mathbb{Z}$). Due numeri interi n, m sono in corrispondenza se e soltanto se sono entrambi pari.

b. L'insieme delle coppie di numeri naturali (n, m) senza fattori in comune è una corrispondenza in $\mathbb{N} \times \mathbb{N}$.

c. L'insieme $\{(3, 2), (3, 1), (4, 1), (4, 4)\}$ è una corrispondenza in $\{1, 2, 3, 4\} \times \mathbb{N}$.

§ 1.7 Esercizi

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

1.1 Determinare $\#A$ nei seguenti casi:

a. $A = \{-1, 0, 3\} \cup \{-3, 3\}$

b. $A = \{x \in \mathbb{Z} \mid x^2 = x\}$

c. $A = \{x \in \mathbb{N} \mid x < 2\}$

d. $A = \{x \in \mathbb{Q} \mid x < 2\}$

e. $A = \{x \in \mathbb{N} \mid x \leq 5\} \cup \{x \in \mathbb{N} \mid x \geq 0\}$

f. $A = \{x \in \mathbb{Q} \mid x^2 = 2\}$.

1.2 Sia D un insieme con 3 elementi e F un insieme con 2 elementi. Quanti elementi ha $D \cap F$? Quanti elementi ha $D \cup F$? Per ogni caso possibile scrivere un esempio esplicito. **1.3** Sia C l'insieme dei numeri naturali dispari, D l'insieme dei numeri naturali multipli di 3 ed E l'insieme dei numeri naturali maggiori di 0. Scrivere in simboli i tre insiemi e stabilire se le seguenti affermazioni sono giuste o sbagliate (nel secondo caso esibire un controesempio):

a. $C \subset E$

b. $D = E$

c. $C \cup D = E$

d. $D - C = \{x \in \mathbb{N} \mid x \text{ è multiplo di } 6\ \}$.

e. $C \cap D = \{x \in \mathbb{N} \mid x \text{ non è multiplo di } 6\ \}$.

f. $D - E = \emptyset$.

1.4 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:

$$\{1\} \not\subseteq A \quad 1 \in C \quad \{1\} \in A \quad 2 \in C \quad 1 \subseteq A \quad 3 \in C$$
$$1 \in A \quad \{1\} \in C \quad A \subseteq B \quad \{2, 3\} \in C \quad B \subseteq A \quad \{2\} \in C$$

1.5 Siano $X = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid x^{26} + x^{16} - 2 = 0\}$ e $B = \{-1, 0, 1, 2\}$.

a. Volendo calcolare $A \cap B$ possiamo scegliere tra le due definizioni equivalenti:

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

Quale delle due è più semplice? Dare una motivazione e quindi calcolare $A \cap B$.

b. Determinare la lista degli elementi di $B - A$.

c. Scrivere $A \cup B$ come unione di due insiemi disgiunti.

1.6 Indichiamo con S e con T gli insiemi delle soluzioni reali delle equazioni $x^2 - 4x + 6 = 0$ e $3x^2 - 4x - 4 = 0$.

a. Determinare esplicitamente gli elementi dei due insiemi.

b. Esprimere mediante S e T ed elencare esplicitamente gli elementi dell'insieme delle soluzioni reali dell'equazione $(x^2 - 4x + 6)(3x^2 - 4x - 4) = 0$.

c. Esprimere mediante S e T ed elencare esplicitamente gli elementi dell'insieme delle soluzioni reali del sistema di equazioni $\begin{cases} x^2 - 4x + 6 = 0 \\ 3x^2 - 4x - 4 = 0 \end{cases}$.

1.7 Indichiamo con S l'insieme delle soluzioni dell'equazione $f(x) = 0$. Quale è l'insieme delle soluzioni dell'equazione $(x - 4) \cdot f(x) = 0$?

1.8 Siano $X = \mathbb{N}$, $A = \{x \in \mathbb{N} \mid x < 20\}$ e $B = \{x \in \mathbb{N} \mid x \geq 10\}$. Calcolare: $A \cap B$, $A \cup B$, $A - B$, $B - A$, $\mathcal{C}_X(A)$, $\mathcal{C}_X(B)$.

1.9 Sia $H = \{x \in \mathbb{Z} \mid -5 \leq x \leq 5\}$. Verificare che gli insiemi $H \cap 2\mathbb{Z}$, $\{x \in \mathbb{R} \mid (x^2 - 1)(x^2 - 9) = 0\}$ e $\{-5,\ 5\}$ costituiscono una partizione di H.

1.10 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 $\mathcal{C}_{\mathbb{R}}(Y \cup Z) = \mathcal{C}_{\mathbb{R}}(Y) \cap \mathcal{C}_{\mathbb{R}}(Z)$.

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

1.12 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) $A - \mathcal{C}_X(B) = \mathcal{C}_X(\mathcal{C}_X(A) - B)$.

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

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

1.15 Siano $X = \mathbb{Z}$, $C = \{x \in \mathbb{Z} \mid -2 < x \leq 3\}$, $D = \{x \in Z \mid x \; e \; pari\}$ e $E = C - D$. Determinare

a. $\#(X - D)$

b. $\#(C - D)$

c. $\#(C \cap D)$.

d. $\#(C - \mathcal{C}_X(D))$

e. $\#(C \cap \mathcal{C}_X(D))$

1.16 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 $\bigcup_{n\in\mathbb{N}} B_n$.

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

1.18 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 $A \cup B \cup C = \mathbb{N}$.

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

1.20 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 $\mathbb{N}$.

1.21 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.

1.22 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 $\mathcal{P}(B) \times \mathcal{P}(B)$.

Capitolo 2

Le funzioni

§ 2.1 Generalità sulle applicazioni o funzioni

Definizione 2.1. *Una* **applicazione o funzione** f *è una terna* $f = (A, B, G)$*, dove* A *e* B *sono insiemi non vuoti e* G *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:*

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

Notazioni e terminologia: A si dice **dominio** di f, B si dice **codominio** di f e G si dice **grafico** di f. Per indicare che f è una funzione da A in B invece che $f = (A, B, G)$ 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 $(a, b) \in G$ si scrive $b = f(a)$ e si dice che b è **l'immagine** di a.

Definizione 2.2. *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 G 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 una stessa funzione.

Esempio 2.3. 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 2.4. 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 $f = g$, poichè hanno lo stesso dominio A, lo stesso codominio $\mathbb{R}$ e lo stesso grafico: $G_f = G_g = \{(0, -7),\ (1, -6),\ (2, -5)\}$.

Esempio 2.5. Elenchiamo ora alcune funzioni particolarmente importanti e che capiterà spesso di usare.

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 di A.** 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 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 $a_1 * a_2$.

d. **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.

§ 2.2 Funzioni iniettive e suriettive

Definizione 2.6. *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 oppure corrispondenza 1–1**. Possiamo riformulare le precedenti definizioni usando il concetto di controimmagine.

Definizione 2.7. *Siano $f\colon A \longrightarrow B$ una funzione, b_0 un elemento di B e D un sottoinsieme di B. Si dice* **controimmagine di** b_0 *il sottoinsieme di A così definito:*

$$f^{-1}(b_0) = \{a \in A \mid f(a) = b_0\}.$$

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_0 del codominio non è altro che la controimmagine del sottoinsieme singleton $\{b_0\}$, ossia $f^{-1}(b_0) = f^{-1}(\{b_0\})$. 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 2.8. Siano $A = \{0, 1, 2, 3\}$, $B = \mathbb{R}$ e $g\colon A \longrightarrow \mathbb{R}$ l'applicazione definita da: $g(0) = 5$, $g(1) = \sqrt{5}$, $g(2) = -\pi$, $g(3) = -\pi$. Avremo allora $f^{-1}(-\pi) = \{2, 3\}$, $f^{-1}(\sqrt{5}) = \{1\}$, $f^{-1}(27) = \emptyset$. Consideriamo poi i seguenti sottoinsiemi di $\mathbb{R}$: $D_1 = [3, +\infty)$, $D_2 = (-\infty, 0)$, $D_3 = [-10, -8]$. Allora: $f^{-1}(D_1) = \{0\}$, $f^{-1}(D_2) = \{2, 3\}$, $f^{-1}(D_3) = \emptyset$.

Proposizione 2.9. *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.*

Dimostrazione. 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. □

Esempio 2.10.

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, poichè (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 $a_1 = a_2$.

§ 2.3 La composizione di funzioni

Definizione 2.11. *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 come "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 2.12. (Proprietà associativa della composizione)
Siano $f \colon A \longrightarrow B$, $g \colon B \longrightarrow C$ e $h \colon C \longrightarrow D$ funzioni. Allora: $(h \circ g) \circ f = h \circ (g \circ f)$.

Dimostrazione. 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 $h(g(f(a)))$. □

Grazie alla 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 la proprietà commutativa e la proprietà di cancellazione, come mostrano gli esempi che seguono.

Esempio 2.13. 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 $f \circ g$ poichè 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 2.14. 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 poichè ad esempio $(g \circ f)(0) = g(f(0)) = g(0) = 3$, mentre $(f \circ g)(0) = f(g(0)) = f(3) = 9$.

Esempio 2.15. Siano $f,\ g\colon \mathbb{N} \longrightarrow \mathbb{N}$ due funzioni e sia $c_7\colon \mathbb{N} \longrightarrow \mathbb{N}$ la funzione costante 7. Allora $c_7 \circ f = c_7 \circ g = c_7$ anche se $f \neq g$.

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

Esempio 2.16. 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 2.17. 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 $g \circ f_a = f_{g(a)}$.

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

Proposizione 2.18. *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.*

Dimostrazione. 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. □

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.

§ 2.4 Funzioni inverse

Definizione 2.19. *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 $f \circ g = id_B$.*

Non tutte le funzione hanno una funzione inversa. Infatti:

Proposizione 2.20. *Sia $f\colon A \longrightarrow B$ una funzione. Allora:*

$$f \text{ ha un'inversa } g \Longleftrightarrow f \text{ è biunivoca}$$

Dimostrazione. "$\Longrightarrow$" segue dalla Proposizione 2.18, ricordando che le funzioni identità sono iniettive e suriettive. "$\Longleftarrow$" Supponiamo f biunivoca e costruiamo esplicitamente la funzione inversa $g\colon B \longrightarrow A$ come corrispondenza inversa. Dunque $\forall b \in B$ poniamo $g(b) = a$ dove a è l'unico elemento di A tale che $f(a) = b$. Per costruizone, le due composizioni di f e g coincidono con l'identità di A e di B rispettivamente. □

Notiamo che è sempre possibile costruire la corrispondenza inversa di una funzione f, ma essa non è in generale una funzione a meno che, come prima dimostrato, f sia biunivoca. Se infatti f non è suriettiva, la corrispondenza inversa non risulta ovunque definita e se f non è iniettiva, la corrispondenza inversa non risulta funzionale. Proviamo ora che la funzione inversa, se esiste, è unica.

Proposizione 2.21. *Siano $f\colon A \longrightarrow B$ e $g, h\colon B \longrightarrow A$ delle funzioni. Se $g \circ f = id_A$ e $f \circ h = id_B$, allora $g = h$.*

Dimostrazione. Intanto g e h hanno lo stesso dominio e codominio. Ci basterebbe allora provare che hanno lo stesso grafo. Scegliamo invece un ragionamento di tipo più formale: calcoliamo la composizione "a tre" $g \circ f \circ h$ nei due modi diversi permessi dalla proprietà associativa:

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h.$$

□

Dunque non possono esistere due diverse funzioni inverse di una stessa funzione f. Di solito l'unica funzione inversa di f (naturalmente se esiste) viene denotata col simbolo f^{-1}. ATTENZIONE: le notazioni di funzione inversa e di controimmagine possono essere confuse una con l'altra.

§ 2.5 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 2.22. *Si dice che due insiemi A e B sono* **equipollenti** *oppure hanno la stessa* **cardinalità** *se esiste una funzione biunivoca $f\colon A \longrightarrow B$.*

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.

Definizione 2.23. *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 2.24. *Siano A e B insiemi. Allora:*

$$Card(A) = Card(B) \Longleftrightarrow Card(A) \leq Card(B) e Card(B) \leq Card(A).$$

Definizione 2.25. *Un insieme è* **infinito** *se è equipollente ad un suo sottoinsieme proprio ossia se ossia se esiste una funzione $f\colon A \longrightarrow A$ iniettiva ma non suriettiva, oppure suriettiva ma non iniettiva. Un insieme è* **finito** *se questo non capita.*

Esempio 2.26. L'insieme dei numeri naturali $\mathbb{N}$ è un insieme infinito poichè 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 $\mathbb{N}$.

Dalla definizione di insiem finito segue la seguente eproprietà,

Teorema 2.27. *Se A è un insieme* **finito** *e $f\colon A \longrightarrow A$ è una funzione, allora si ha:*

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

Nel seguito del capitolo indicheremo con I_n ($n \geq 1$) l'insieme dei numeri naturali $\{1, \ldots, n\}$. Diremo inoltre che l'insieme vuoto ha cardinalità 0.

Teorema 2.28. a. *Per ogni numero naturale 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 $Card(B) \geq Card(\mathbb{N}) > n$ per ogni $n \in \mathbb{N}$.*

La cardinalità dell'insieme infinito $\mathbb{N}$ 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**.

Esempio 2.29. $Card(\mathbb{Z}) = \aleph_0$. 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 $n < 0$. Anche $\mathbb{Q}$ ha cardinalità numerabile, ma non è semplice costruire esplicitamente una funzione biunivoca $\mathbb{N} \longrightarrow \mathbb{Q}$

Solo per curiosità: la cardinalità dei numeri reali. *$Card(\mathbb{R})$, detta anche* **cardinalità del continuo**, *è strettamente maggiore di $\aleph_0 = Card(\mathbb{N})$. 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 $y \notin \mathrm{Im}(f)$. Vi sono tuttavia insiemi che hanno cardinalità più grande di quella del di $\mathbb{R}$, ad esempio $\mathcal{P}(\mathbb{R})$, l'insieme delle parti di $\mathbb{R}$. Possiamo provare infatti, più in generale, che per ogni insieme A, finito o infinito, si ha $Card(A) < Card(\mathcal{P}(A))$. 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:*

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

§ 2.6 Il principio dei cassetti

Dalla definizione di insieme finito e dalle proprietà che abbiamo enunciato nella sezione precedente segue la proprietà conosciuta come **principio dei cassetti** o **principio della piccionaia**. *Se B è un insieme finito con n elementi e A è un suo sottoinsieme con m elementi, allora $m \leq n$ e inoltre A è strettamente più piccolo di B se e solo se $m < n$.* Questa proprietà appare meno evidente quando i numeri coinvolti sono grandi.

Esempio 2.30. In una grande città, come Milano Roma, vi sono sicuramente due persone con lo stesso numero di capelli in testa. Sappiamo infatti che il numero di capelli che un individuo può possedere non supera i 200˙000. Se tutti gli abitanti di Roma (o di Milano) avesso un diverso numero di capelli, l'insieme B costituito dai numeri di capelli di ciascun individuo avrebbe tanti elementi quanti sono gli abitanti (e quindi più di un milione di elementi), pur essendo un sottoinsieme dell'insieme A dei numeri interi da 0 a 200˙000 che ha solo 200˙001 elementi.

Possiamo enunciare il Prinipio dei cassetti anche coinvolgendo le nozioni di iniettività e suriettività delle funzioni: sia $f\colon A \to B$ una funzione tra gli insiemi A di cardinalità m e B di cardinalità k.

- Se f è iniettiva allora $m \leq k$, ossia
- se $m > k$, f non può essere iniettiva.
- Se f è suriettiva allora $m \geq k$, ossia
- se $m < k$, f non può essere suriettiva.

Si faccia attenzione al fatto che queste proprietà contengono delle implicazioni, non delle bi-implicazioni.

Esempio 2.31. Consideriamo una funzione $f\colon A \to B$ da un insieme A con 7 elementi ad un insieme B con 18 elementi. Possiamo affermare con totale sicurezza che f non è suriettiva in quanto $7 \not\geq 18$. Possiamo inoltre affermare che f potrebbe essere iniettiva, ma senza ulteriori informazioni non possiamo sapere se lo è oppure no.

§ 2.7 Esercizi

2.1 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?

2.2 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?

2.3 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.

2.4 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 $f^{-1}(\mathbb{Z}_{<0})$, dove $\mathbb{Z}_{<0}$ è l'insieme dei numeri interi strettamente negativi.

c. Dire se f è iniettiva, suriettiva, biunivoca.

2.5 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.

2.6 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?

2.7 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.)

2.8 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 è un singleton? Trovare tutti gli elementi di $\phi^{-1}(p)$, per ogni numero primo p.

2.9 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 $\psi(C) = C \cup B$.

2.10 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 $f \circ g = id_{\mathbb{N}}$.

2.11 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 $f \circ h = id_{\mathbb{N}}$.

2.12 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.

2.13 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.

2.14 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?

2.15 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?

2.16 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 3

Tecniche di enumerazione

§ 3.1 Il principio di inclusione-esclusione.

Vogliamo contare il numero di elementi dell'unione di due o più insiemi finiti. In questo capitolo pwer indicare il numero di elementi di un insieme A scriveremo $|A|$ invece $\#A$: si tratta di un altro modo di indicare la cardinalità che spesso si incontra sui libri. Iniziamo cl caso di 2 insiemi. Siano A e B due insiemi finiti di cardinalità finita n ed m rispettivamente, che siano disgiunti ossia privi di elementi comuni. Allora:

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

La formula si generalizza al caso di k insiemi finiti A_i , $i = 1, 2, \ldots, k$, con $|A_i = n_i$, disgiunti due a due:

$$| \cup A_i| = \sum_{i=1}^{k} |A_i| = n_1 + \cdots + n_k.$$

Se invece A e B hanno k elementi in comune (ossia $k = |A \cap B|$), allora la formula diventa:

$$|A \cup B| = |A| + |B| - |A \cap B| = n + m - k.$$

Il termine correttivo $-k$ si inserisce poichè i k elementi comuni ad A e B compaiono tra gli n del primo insieme e gli m del secondo e sarebbero pertanto contati due volte in $n + m$. Questa formula più generale è nota come **principio di inclusione-esclusione**. Tralasciamo la sua generalizzazione al caso di k insiemi poichè decisamente più complicata. La riportiamo solo per il caso $k = 3$, con un esempio di applicazione:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Esempio 3.1. Su 25 studenti, 15 hanno superato l'esame di Matematica, 12 quello di Chimica e 5 hanno superato entrambi gli esami. Quanti studenti hanno superato almeno un esame? Quanti studenti hanno fallito entrambi gli esami? Sia A l'insieme degli studenti che hanno superato l'esame di Matematica: $|A| = 15$.

Sia B l'insieme degli studenti che hanno superato l'esame di Chimica, $|B| = 12$.
$A \cap B$ è l'insieme degli studenti che hanno superato entrambi gli esami: $|A \cap B| = 5$.
La risposta alla prima domanda è l'ordine dell'insieme $A \cup B$, dato da $15+12-5 = 22$.
Non hanno superato nessuno dei due esami $25 - 22 = 3$ studenti.

Esempio 3.2. Sia $I = \{1, 2, \ldots, 20\}$. Quanti sono i numeri di I divisibili per 2 o per 3? Sia A l'insieme dei numeri pari di I: l'ordine di A è 10.
Sia B l'insieme dei multipli di 3 in I: $B = \{3, 6, 9, 12, 15, 18\}$ ha ordine 6.
$A \cap B$ è l'insieme dei multipli di 6 minori di 20: $A \cap B = \{6, 12, 18\}$ ha ordine 3.
I numeri di I divisibili per 2 o per 3 sono $10 + 6 - 3 = 13$.

Esempio 3.3. In un gruppo di amici tutti hanno visto almeno uno dei film x, y, z: 8 hanno visto il film x, 12 il film y e 9 il film z. Inoltre 6 hanno visto x e y, 4 hanno visto x e z, 7 hanno visto y e z e soltanto uno di essi ha assistito alle tre proiezioni. Da quante persone è formato il gruppo? Con ovvio significato delle notazioni si ha: $|X| = 8$, $|Y| = 12$, $|Z| = 9$, $|X \cap Y| = 6$, $|X \cap Z| = 4$, , $|Y \cap Z| = 7$, $|X \cap Y \cap Z| = 1$.
Quindi :

$$|X \cup Y \cup Z| = 8 + 12 + 9 - 6 - 4 - 7 + 1 = 13.$$

§ 3.2 Il metodo delle scelte successive

Consideriamo come primo caso quello del prodotto cartesiano.

Proposizione 3.4. *Siano A e B due insiemi finiti di cardinalità n e m rispettivamente. Allora:*

$$|A \times B| = |A| \cdot |B| = nm.$$

Dimostrazione. Se $A = \{a_1, \ldots, a_n\}$, consideriamo gli n sottoinsiemi B_i di $A \times B$ a due a due disgiunti formati ognuno dalle m coppie aventi a_i come prima componente. Per la formula della cardinalità dell'unione di insiemi disgiunti abbiamo

$$|A \times B| = |B_1| + \cdots + |B_n| = nm.$$

□

Osserviamo che disponendo in colonna e in riga gli n elementi di A e gli m elementi di B, il prodotto cartesiano $A \times B$ può essere visualizzato come una tabella di nm quadretti. Possiamo utilizzare il ragionamento precedente anche in situazioni più generali. *Se una scelta può essere compiuta in n modi diversi e, per ciascuno di essi, una seconda scelta può essere compiuta in m modi diversi, allora la successione delle due scelte può essere effettuata in nm modi distinti.* Nel caso del prodotto cartesiano la scelta del secondo elemento avviene sempre tra quelli di uno stesso

insieme. Come vedremo, in situazioni più generali si costruiscono coppie scegliendo il primo elemento in un insieme fisso con n elementi e il secondo elemento in un insieme di cardinalità m che però può dipendere dal primo elemento scelto. Mediante l'induzione quanto visto relativamente a due scelte si estende al caso di un numero finito di scelte consecutive.

Proposizione 3.5. *Supponiamo di dover eseguire k scelte consecutive e che la scelta i-esima possa avvenire in n_i modi diversi. Allora le sequenze di scelte possibili sono*

$$\prod_{i=1}^{k} n_i.$$

Dimostrazione. Procediamo per induzione su k. Per $k = 2$ la dimostrazione è quella presentata precedentemente. Supponiamo che l'asserto sia vero per un certo numero k_0 di scelte e proviamo che allora è vera per $k_0 + 1$ scelte. Per l'ipotesi induttiva possiamo eseguire le prime k_0 scelte in $N = \prod_{i=1}^{k_0} n_i$ modi. Possiamo pensare la nostra procedura di scelte come costituita da due momenti: in un primo momento eseguiamo le prime k_0 scelte in N modi e nel secondo momento eseguiamo l'ultima scelta in n_{k_0+1} modi possibili. Applicando il caso $k = 2$ in tutto avremo $N \cdot n_{k_0+1}$ modi. Possiamo quindi concludere che la formula vale anche nel caso $k_0 + 1$ scelte poichè

$$N \cdot n_{k_0+1} = (\prod_{i=1}^{k_0} n_i) \cdot n_{k_0+1} = (\prod_{i=1}^{k_0+1} n_i).$$

□

Il principio di moltiplicazione delle scelte (anche nella sua forma estesa a più di due scelte) ci permette di risolvere molti problemi combinatorici.

Esempio 3.6. Quante etichette si possono formare con un numero di due cifre (da 00 a 99) e una lettera (dell'alfabeto di 26 lettere)? Le etichette sono tanti gli elementi del prodotto cartesiano $C \times A$ dove C è l'insieme dei numeri da 0 a 99 (che ha 100 elementi) e A è l'insieme delle lettere dell'alfabeto, che ha quindi 26 elementi. Allora le etichette possibili sono $100 \cdot 26 = 2600$.

Esempio 3.7. Quanti oggetti possiamo differenziare con delle targhe costituite da 3 simboli di cui il primo è una lettera scelta tra α, β, γ, δ, il secondo è una cifra da 1 a 5 e il terzo è una lettera dell'alfabeto? Le lettere greche possono essere scelte in 4 modi, le cifre in 5 modi, la lettera finale in 26 modi: in tutto possiamo costruire $4 \cdot 5 \cdot 26 = 540$ targhe diverse.

Esempio 3.8. Supponiamo che il menù di un ristorante consista di 5 antipasti, 6 primi, 6 secondi e 4 dolci: quanti pasti completi (di quattro portate) possiamo ordinare? Le quaterne ordinate (e quindi le scelte possibili) sono $5 \cdot 6 \cdot 6 \cdot 4 = 720$.

Esempio 3.9. Scegliamo due persone in un gruppo di 7 come responsabile della cassa comune e addetto alle comunicazioni. In quanti modi può essere effettuata la scelta? La scelta di responsabile della cassa può essere effettuata in 7 modi diverse: scegliamo un elemento qualsiasi nell'insieme G costituito dalle 7 persone. La scelta dell'addetto alle comunicazioni può essere effettuata in 6 modi diversi: scegliamo un elemento qualsiasi nell'insieme $G - \{a\}$, dove a è la persona a cui è stata affidata la prima mansione; come si vede il secondo insieme, pur avendo in tutti i casi 6 elementi, cambia a seconda della prima scelta effettuata.

Il principio delle scelte successive può essere utilizzato per determinare alcune formule di calcolo combinatorico. Vediamone alcune.

§ 3.3 Disposizioni con ripetizione

Diciamo **disposizioni con ripetizione** di k elementi scelti in un insieme B di ordine m ogni ordinamento o disposizione di k elemnti scelti in B con la possibilità di usare più volte uno stesso elemento. In modo più formale:

Definizione 3.10. *Chiamiamo* ***disposizioni con ripetizione*** *di ordine k di elementi di un insieme B tutte le funzioni $f\colon I_k \to B$ oppure equivalentemente gli elementi del prodotto cartesiano $B \times \cdots \times B$ di B per se stesso k volte.*

Esempio 3.11. Le funzioni di I_3 in I_2 sono identificabili con le $2^3 = 8$ terne $(1,1,1)$, $(1,1,2)$, $(1,2,1)$, $(1,2,2)$, $(2,1,1)$, $(2,1,2)$, $(2,2,1)$, $(2,2,2)$. La prima è la funzione costante di valore 1, la seconda è la funzione tale che $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 2$, ..., l'ultima è la funzione costante di valore 2.

Il metodo delle scelte successive prova che il numero delle disposizioni con ripetizione di m elementi a k a k è

$$D^r_{k,m} = m^k.$$

Esempio 3.12. Vogliamo contare i sottoinsiemi di un insieme I di ordine n. Possiamo immaginare di costruire un sottoinsieme di I esaminando ciascun elemento di I e decidendo se vogliamo metterlo nel sottoinsieme oppure no. Dobbiamo cosıeseguire per n volte una scelta tra 2 possibilità. Quindi il numero di possibili sottoinsiemi è dato dal prodotto delle scelte e quindi, come già detto, è 2^n.

Esempio 3.13. Vogliamo calcolare il numero delle colonne tra loro diverse che si possono giocare al totocalcio. Come è noto, il gioco consiste nell'assegnare uno dei tre simboli 1, X, 2 ad ognuna delle 13 partite. Ogni colonna può essere identificata con una sequenza ordinata di elementi scelti tra 1, X, 2 e quindi con una funzione da I_{13} (i numeri da 1 a 13 corrispondono nell'ordine della schedina alle 13 partite) in un insieme con 3 elementi (i tre simboli citati). Le colonne possibili sono quindi $3^{13} = 1594323$. Giocando tutte queste colonne si ha la certezza del tredici (purtroppo con una spesa superiore alla vincita !!).

§ 3.4 Permutazioni

Si dice **permutazione** di n oggetti distinti un qualunque loro ordinamento o allineamento. Per contare il numero delle permutazioni è utile il simbolo di fattoriale. In modo più formale:

Definizione 3.14. *Chiamiamo* ***permutazioni*** *di un insieme B con m elementi tutte le funzioni biunivoche $f\colon I_m \to B$.*

Esempio 3.15. Se scriviamo le funzioni biunivoche f di $I_3 = \{1, 2, 3\}$ in sè elencando ordinatamente le immagini come terne $(f(1), f(2), f(3))$, otteniamo le 6 terne:

$$(1,2,3)\,,\ (1,3,2)\,,\ (2,1,3)\,,\ (2,3,1)\,,\ (3,1,2)\,,\ (3,2,1).$$

Osserviamo che in ogni terna compaiono i 3 numeri esattamente una volta sola e che ci'o nelle varie terne viene fatto in tutti gli ordini possibili: abbiamo ordinato (allineato) in tutti i modi possibili i nostri elementi.

Dato un numero naturale $n > 0$, chiamiamo **fattoriale** di n il numero:

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$$

Si pone inoltre $0! = 1$. E' una convenzione, ma come vedremo ha una motivazione ben precisa. Notiamo che $n!$ cresce rapidamente al crescere di n. Ne diamo i primi dieci valori: Il numero complessivo delle permutazioni di n oggetti è:

n	1	2	3	4	5	6	7	8	9	10
n!	1	2	6	24	120	720	5040	40320	362880	3628800

$$P_n = n!$$

Possiamo infatti scegliere in n modi diversi l'elemento da mettere al primo posto, in $n-1$ modi quello da mettere al secondo (tutti gli elementi vanno bene, tranne quello scelto per il primo posto), in $n-2$ modi quello da mettere al terzo posto e cosıvia. Per il principio delle scelte successive, complessivamente si possono dunque effettuare $n!$ scelte.

Esempio 3.16. Scriviamo tutte le $3! = 6$ permutazioni di 3 palline di colore B (bianco), R (rosso), V (verde). Abbiamo due allineamenti che mettono la pallina B al primo posto, altrettanti per R e V

$$B\,R\,V\ ,\ B\,V\,R\ ,\ R\,V\,B\ ,\ R\,B\,V\ ,\ V\,B\,R\ ,\ V\,R\,B.$$

Esempio 3.17. Scriviamo alcune delle $5! = 120$ permutazioni di 5 palline di colore B (bianco), R (rosso), V (verde), G (giallo) e N (nero). Possiamo iniziare scrivendo tutte quelle che hanno B al primo posto (che saranno 24, come le permutazioni dei 4 elementi R, V, G, N); tra queste possiamo iniziare da quelle che hanno R al secondo posto (che saranno 6 come le permutazioni di V, G, N):

$$B\,R\,V\,G\,N\ ,\ B\,R\,V\,N\,G\ ,\ B\,R\,G\,V\,N\ ,\ B\,R\,G\,N\,V\ ,\ B\,R\,N\,V\,G\ ,\ B\,R\,N\,G\,V.$$

Potremo poi cambiare l'elemento al secondo posto in tutti i modi possibili. Elencate tutte le permutazioni che iniziano con B, passeremo poi a quelle che iniziano con R, ecc. Procedere ordinatamente in questo modo ci permette di non dimenticarne nessuna e di non scrivere più volte una stessa permutazione.

§ 3.5 Disposizioni semplici

Si dice **disposizione semplice** di n oggetti a k a k (con $k \leq n$) ogni allineamento di k oggetti distinti scelti in un insieme di n. In modo più formale:

Definizione 3.18. *Chiamiamo **disposizioni semplici** di ordine k degli elementi di un insieme B tutte le funzioni iniettive $f\colon I_k \to B$.*

Osserviamo che se $|B| = n$, è necessario supporre $k \leq n$ poichè in caso contrario, per il principio dei cassetti, non ci sarebbero funzioni iniettive da I_k a B. Il numero totale di disposizioni semplici di n elementi a k a k è:

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

Possiamo infatti scegliere in n modi diversi l'oggetto da mettere al primo posto, in $n-1$ modi quello da mettere al secondo posto (vanno bene tutti, tranne quello messo al primo posto), in $n-2$ modi quello da mettere al terzo posto e cosıvia fino all'ultimo posto; poichè i posti sono k, all'ultimo posto potremo scegliere tra $n-(k-1)$ oggetti (tutti meno i $k-1$ già utilizzati).

Esempio 3.19. Sia I l'insieme formato da tre palline di colore verde (V), rosso (R), nero (N). Le disposizioni di queste tre palline a due a due sono $D_{3,2} = 3 \cdot 2 = 6$, e precisamente, sono gli allineamenti:

$$V\,R\ ,\ R\,V\ ,\ V\,N\ ,\ N\,V\ ,\ R\,N\ ,\ N\,R.$$

Possiamo vedere ogni disposizione anche come una funzione iniettiva dall'insieme $A = \{1, 2\}$ (o più generalmente da un insieme $A = \{a_1, a_2\}$ di ordine 2) in $B = \{V, R, N\}$ che associa ad 1 il primo elemento della disposizione e a 2 il secondo, ossia:

$$V\,R \ \textit{corrisponde a}\ f\colon 1 \mapsto V,\ 2 \mapsto R$$
$$f\colon 1 \mapsto B,\ 2 \mapsto V \ \textit{corrisponde a}\ B\,V.$$

Esempio 3.20. Consideriamo una funzione $f\colon A \to B$: come già osservato nel capitolo precedente, alcune sono iniettive e altre no. Contiamo quante sono quelle non iniettive. Ordiniamo in un modo qualsiasi gli elementi A, siano $a_1, a_2, \ldots, a_7$. Ogni funzione è individuata dalla lista ordinata delle 7 immagini $(f(a_1), f(a_2), \ldots, f(a_7))$, lista che in genere può contenere anche elementi ripetuti. Le funzioni sono quindi 18^7, come le disposizioni con ripetizione dei 18 elementi di B in liste di 7. Le funzioni iniettive sono quelle corrispondenti a liste senza ripetizioni: il loro numero è quindi $\frac{18!}{(18-7)!}$. Di conseguenza le funzioni non iniettive sono $18^7 - \frac{18!}{11!}$.

§ 3.6 Combinazioni semplici

Affrontiamo ora il problema quello da cui il calcolo combinatorio prende il nome. Vogliamo contare in quanti modi si possono scegliere k oggetti (diversi, ma senza un ordine precisato) in un insieme A di n oggetti diversi. Poichè non vogliamo precisare l'ordine con cui scegliamo i k elementi, ma solo quali sono, quello che vogliamo considerare è un sottoinsieme di A con k elementi.

Definizione 3.21. *Chiamiamo* ***combinazioni*** *di ordine k di elementi di un insieme A tutti i sottoinsiemi di A con k elementi.*

Anche in questo caso se $|A| = n$ è necessario supporre $k \leq n$. Per contare le combinazioni possiamo immaginare di costruire per prima cosa tutte le disposizioni di ordine k degli elementi di A (che sono $D_{n,k} = \frac{n!}{(n-k)!}$) e poi di raggruppare tra loro tutte quelle costituite dagli stessi elementi; ogni gruppetto contiene $k!$ disposizioni (le permutazioni dei k elementi che compaiono in ciascuna disposizione del gruppetto). I gruppetti corrispondono alle combinazioni (ossia ai sottoinsiemi con k elementi) e il loro numero è quindi $D_{n,k} : k!$.

Esempio 3.22. Se U è l'insieme formato da tre palline di colore verde (V), rosso (R), nero (N), le disposizioni di queste tre palline a due a due sono $D_{3,2} = 6$, e, precisamente, sono gli allineamenti: VR, RV, VN, NV, RN, NR. Le combinazioni di queste tre palline a 2 a 2 sono 3: $\{V, R\}$, $\{V, N\}$, $\{R, N\}$. Notiamo che ciascuno di essi corrisponde a $2! = 2$ diverse disposizioni.

§ 3.7 I binomiali

Per esprimere in modo generale la formula del numero di combinazioni utilizziamo il simbolo binomiale. Si dice **coefficiente binomiale** n su k, $(0 \leq k \leq n)$, il numero:

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

Potremo quindi scrivere sinteticamente:

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

Esempio 3.23. Aggiungiamo all'insieme U dell'esempio precedente una pallina gialla G e scriviamo tutte le combinazioni delle 4 palline a 2 a 2. Otteniamo $C_{4,2} = \binom{4}{2} = 6$ sottoinsiemi: $\{V, R\}, \{V, N\}, \{R, N\}, \{V, G\}, \{N, G\}, \{R, G\}$.

Esempio 3.24. In una lotteria vengono assegnati 3 premi uguali mediante 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 $C_{20,3} = \binom{20}{3} = 1140$.

Vediamo ora alcune proprietà dei binomiali. Siano k ed n numeri interi, $0 \leq k \leq n$.

i) Casi estremi: $\binom{n}{0} = \binom{n}{n} = 1$

ii) Simmetria: $\binom{n}{k} = \binom{n}{n-k}$

iii) Formula di Stiefel: $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.

Dimostrazione. Dimostriamo la formual di Stiefel in due modi diversi. La prima dimostrazione usa la definizione algebrica del simbolo binomiale. Vogliamo provare che è corretta l'uguaglianza

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

La correttezza o meno non si modifica se moltiplichiamo i due membri per il numero $k! \cdot (n-k)!$ e li dividiamo per il numero $(n-1)!$ (che sono entrambi $\neq 0$):

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

è evidente che l'uguaglianza è corretta. Proviamo ora la stessa uguaglianza ricordando che i binomiali contano le combinazioni semplici. Consideriamo un insieme A con n elementi, uno dei quali è l'elemento $\overline{a}$. Consideriamo i sottoinsiemi di A con k elementi. Possiamo suddividere tali sottoinsiemi in due tipi distinti: quelli che non contengono $\overline{a}$ e quelli che lo contengono. Quelli che non contengono $\overline{a}$ sono i sottoinsiemi di $A - \{\overline{a}\}$ (insieme con $n-1$ elelemnti) di cardinalità k: il loro numero è quindi $\binom{n-1}{k}$. Ogni sottoinsieme del secondo tipo può essere ottenuto considerando un sottoinsieme di $k-1$ elementi di $A - \{\overline{a}\}$ (a cui viene poi aggiunto $\overline{a}$): il

numero di tali sottoinsiemi è quindi $\binom{n-1}{k-1}$. Quindi il primo membro della formual di Stiefel fornisce il numero dei sottoinsiemi di A di cardinalità k sommando il numero di sottoinsiemi del primo tipo e il numero di sottoinsiemi del secondo tipo, mentre il secondo membro della formual $\binom{n}{k}$ fornisce direttamente numero di tutti i sottoinsiemi di A con k elementi. Quindi i due membri sono uguali □

Il nome dei coefficienti binomiali deriva dal fatto che essi sono appunto i coefficienti che compaiono nello sviluppo della potenza $n-$esima di un binomio mediante la **formula del binomio di Newton**.

Teorema 3.25. *Per ogni $n \in \mathbb{N}$, $n \geq 1$ si ha*

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

Dimostrazione. Dimostriamo questa formula in due modi diversi. Per la prima dimostrazione usiamo l'induzione su n. Per $n = 1$ abbiamo $(X+Y)^1 = 1 \cdot X + 1 \cdot Y$. Notiamo che il coefficiente 1 di X coincide proprio con $\binom{1}{0}$ e il coefficiente 1 di Y coincide con $\binom{1}{1}$. Supponiamo ora che la formula valga per un certo numero $n_0 \geq 1$ e proviamo che allora vale anche per il numero n_0+1. Possiamo scrivere $(X+Y)^{n_0+1}$ come prodotto $(X+Y)^{n_0} \cdot (X+Y)$. Usando l'ipotesi induttiva otteniamo

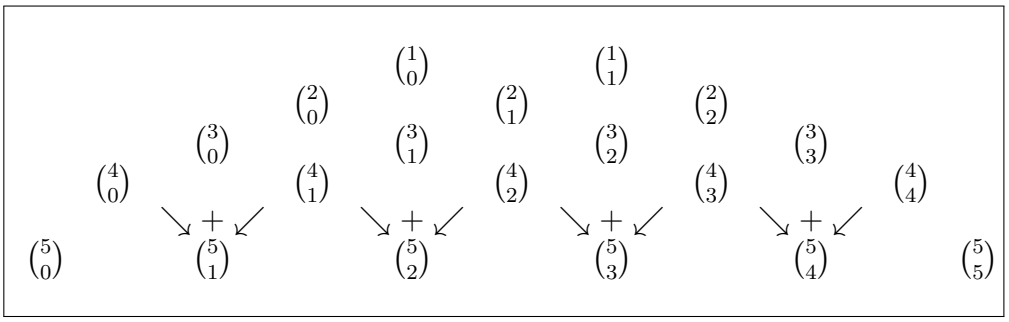
$$\left(\binom{n_0}{0}X^{n_0} + \binom{n_0}{1}X^{n_0-1}Y + \dots \binom{n_0}{k}X^{n_0-k}Y^k + \dots + \binom{n_0}{n_0}Y^{n_0}\right) \cdot (X+Y).$$

Eseguiamo quindi il prodotto e raccogliamo i monomi simili. Otteniamo una volta sola il monomio X^{n_0+1} moltiplicando X^{n_0} per X: dunque il suo coefficiente sarà $\binom{n_0}{0} \cdot 1 = \binom{n_0+1}{0}$. Lo stesso vale per il monomio Y^{n_0+1}. Otteniamo invece due volte ogni altro monomio $X^{n_0+1-k}Y^k$, con $1 \leq k \leq n_0$: una volta moltiplicando $X^{n_0-k}Y^k$ per X e una volta moltiplcando $X^{n_0+1-k}Y^{k-1}$ per Y. Dunque nel risultato il suo coefficiente sarà

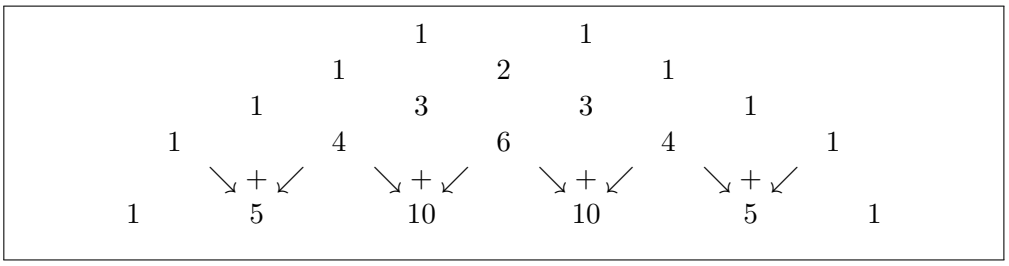
$$\binom{n_0}{k} \cdot 1 + \binom{n_0+1}{k-1} \cdot 1$$

che per la formula di Stiefel coincide proprio con $\binom{n_0+1}{k}$. Per seconda dimostrazione utilizzamo le combinazioni. Numeriamo da 1 a n gli n fattori $(X+Y)$ che corrispondono a $(X+Y)^n$. Eseguendo il prodotto mediante la proprietà distributiva otteniamo un monomio $X^{n-k}Y^n$ se scegliamo l'addendo Y in k fattori e nei rimanenti l'addendo X: i modi di scegliere k fattori tra gli n elencati è dato da $\binom{n}{k}$. Quindi nello sviluppo della potenza troveremo $\binom{n}{k}$ monomi simili $X^{n-k}Y^n$ tutti con coefficiente 1: raccogliendoli il coefficiente è pertanto $\binom{n}{k}$. □

Spesso i coefficienti binomiali si scrivono nel modo seguente detto **Triangolo di Tartaglia** (o Triangolo di Pascal):



Notiamo che il primo e l'ultimo coefficiente binomiale in ogni riga del triangolo sono uguali a 1 (per la prima proprietà vista), il triangolo è simmetrico rispetto alla retta verticale centrale (per la seconda propriet'a) e ogni coefficiente binomiale all'interno del triangolo è la somma dei due coefficienti binomiali alla sua destra e alla sua sinistra nella riga precedente (per la formula di Stiefel). Queste osservazioni ci permettono di riscrivere il triangolo di Tartaglia calcolando molto facilmente i numeri di ogni riga:



Solitamente ben noti sono gli sviluppi delle potenze fino al terzo grado:

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Se nei due membri della formula dello sviluppo della potenza del binomio sostituiamo $X = 1$ e $Y = 1$ otteniamo un'altra interessante proprietà dei binomiali: **iv)** la somma della riga n-esima del triangolo di Tartaglia è 2^n ossia:

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots \binom{n}{k} + \dots + \binom{n}{n}.$$

Le proprietà viste dei binomiali possono essere motivate osservando che:

i) c'è un solo un sottoinsieme con 0 elementi (l'insieme vuoto) e un solo sottoinsieme con $n = |A|$ elementi (tutto l'insieme A);

ii) scegliere k elementi tra n è come isolare i restanti $n-k$;

iii) fissato un certo elemento a_0 in un insieme A che ha n elementi, i sottoinsiemi di A con k elementi possono essere di due tipi: quelli che non contengono a_0 e quelli che lo contengono. Quelli del primo tipo sono tanti quanti i modi di scegliere k elementi nell'insieme $A \setminus \{a_0\}$ (che ha $n-1$ elementi); quelli del secondo tipo sono tanti quanti i modi di scegliere $k-1$ elementi in $A \setminus \{a_0\}$ (a cui aggiungere poi a_0 stesso);

iv) la somma di tutti i binomiali della riga n-esima del triangolo di Tartaglia è 2^n poichè, come abbiamo già visto, tutti i possibili sottoinsiemi di un insieme A con n elementi sono 2^n.

Esempio 3.26. Ad un appello d'esame si presentano 16 studenti, ma solo 10 possono essere interrogati il primo giorno. Ci sono più oppure meno di 1000 modi di scegliere i 6 che dovranno ritornare il giorno successivo? I modi di scegliere 6 elementi in un insieme di 16 sono:

$$\binom{16}{6} = \frac{16!}{10! \cdot 6!} = \frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 4 \cdot 14 \cdot 13 \cdot 11 > 1000.$$

Esempio 3.27. Dobbiamo scegliere 3 cavie maschio (tra le 10 a disposizione) e 4 cavie femmina (tra le 12 a disposizione) per un esperimento. In quanti modi può avvenire la scelta della coppia di cavie? La scelta è quella di 3 elementi in un insiem di 10 seguita dalla scelta di 4 elementi in un insieme di 12. Si ha quindi:

$$\binom{10}{3} \cdot \binom{12}{4} = \frac{10! \cdot 12!}{3! \cdot 7! \cdot 4! \cdot 8!} = \frac{10 \cdot 9 \cdot 8 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{3 \cdot 2 \cdot 4 \cdot 3 \cdot 2} = 5 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 59400.$$

§ 3.8 Multi-insiemi e combinazioni con ripetizione

Alcuni problemi che sembrano richiedere l'uso di un insieme in verità utilizzano qualcosa di diverso che sarà chiamato un **multi-insieme**.
Per esempio le lettere dell'alfabeto contenute nella parola *torino* sono, in ordine alfabetico, $\{i, n, o, o, r, t\}$. La notazione con le parentesi graffe ricorda quella di un insieme, ma un insieme non contiene elementi ripetuti. Siamo quindi in presenza di qualcosa di diverso.

Definizione 3.28. *Un* **multi-insieme** *scelto da un insieme S è una funzione $m : S \to \mathbb{N}$ da S all'insieme degli interi non negativi. Per ogni $x \in S$, $m(x)$ è detta la molteplicità di x nel multi-insieme. La cardinalità del multi-insieme è la somma delle molteplicità degli elementi di S.*

Esempio 3.29. Qual è la molteplicità di ciascuna lettera dell'alfabeto nella parola *torino*? Qual è la cardinalità del multi-insieme delle lettere di *torino*? La molteplicità di i, n, r, t è 1, la molteplicità di o è 2 mentre la molteplicità di ogni altra lettera dell'alfabeto è 0. In simboli la funzione di molteplicità è data da $m(i) = m(n) = m(r) = m(t) = 1$, $m(o) = 2$, $m(a) = m(b) = \cdots = 0$. La cardinalità del multi-insieme è $1 + 1 + 1 + 1 + 2 = 6$.

Esempio 3.30. Ad un gioco a premi partecipano 4 concorrenti. La prima prova consiste in 12 domande: per ogni domanda, il primo concorrente che dà la risposta giusta ottiene un punto. Supponendo vengano assegnati tutti i 12 punti, quanti sono i possibili esiti del primo gioco? Sappiamo che ogni concorrente ottiene un punteggio da 0 a 12, e che la somma dei punteggi dei concorrenti è 12. Possiamo immaginare di visualizzare l'esito come una lista di 1 (1 punto per ciascuna domanda) scrivendo prima quelli ottenuti dal primo concorrente, poi quelli del secondo e cosı via, inserendo un segno di separazione tra quelli di un concorrente e quelli del successivo. Ad esempio se il primo ha ottenuto 5 punti, il secondo 2, il terzo 4 e l'ultimo 1, avremo

$$1\ 1\ 1\ 1\ 1 \bullet\ 1\ 1\ \bullet\ 1\ 1\ 1\ 1\ \bullet\ 1$$

e se i punteggi sono stati 9, 0, 3, 0, avremo

$$1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \bullet\ \bullet\ 1\ 1\ 1\ \bullet$$

In tutti i casi ci saranno $12+3$ caselline (dove 3 è il numero di concorrenti meno uno) in cui sistemare i 3 separatori $\bullet$ e i 12 numeri 1: quindi i possibili esiti corrispondono a scegliere dove mettere i 3 separatori sceglinedo 3 posizioni tra $12 + 3$ (oppure a scegliere le 12 posizioni in cui sistemare gli 1). In formule:

$$\binom{12+4-1}{4-1} = \binom{12+4-1}{12}.$$

Teorema 3.31. *Il numero dei multi-insiemi di cardinalità k scelti da un insieme di n elementi è dato da*

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

Dimostrazione. (**Metodo dei separatori**). Indichiamo con $x_1, x_2, \ldots, x_n$ gli elementi di S. Per ogni multi-insieme su S di cardinalità k, cioè per ciascuna funzione m definita da S in $\mathbb{N}$ tale che $\sum_{x_i \in S} m(x_i) = k$, possiamo definire una sequenza di $k + n - 1$ numeri 1 e 0 come segue:

- si scrivono $m(x_1)$ numeri 1 seguiti da uno 0 (che funge da "separatore");
- successivamente si scrivono $m(x_2)$ numeri 1 seguiti da uno 0;

  ...

- si scrivono $m(x_{n-1})$ numeri 1 seguiti da uno 0;
- infine si scrivono $m(x_n)$ numeri 1, *senza* per'o mettere lo 0 finale.

Ora $m(x_1)+m(x_2)+\cdots+m(x_n)=k$ è la cardinalità del multi-insieme e quindi una sequenza come quella precedente contiene k volte il numero 1 e $n-1$ volte il numero 0, quindi in totale $k+n-1$ elementi. Inoltre, data una sequenza come sopra, si individua un multi-insieme scelto da S utilizzando gli 0 per suddividere la sequenza in n gruppi di numeri 1, dove per ogni gruppo il numero di 1 che compaiono rappresenta la molteplicità dell'elemento corrispondente. Quindi le sequenze del tipo precedente sono tante quanti i multi-insiemi scelti da S. Poichè il numero di tali sequenze è il numero di modi di scegliere gli $n-1$ elementi in cui posizionare i numeri 0, questo numero è dato da

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

cioè dal numero dei sottoinsiemi con k elementi di un insieme con $k+n-1$ elementi e quindi questo è anche il numero dei multi-insiemi di cardinalità k scelti in S. □

Esempio 3.32. Una pasticceria produce 5 tipi, a, b, c, d, e di paste ricoperte al cioccolato. In quanti modi diversi si può confezionare un vassoio con 8 di queste paste? Ogni confezione di 8 paste può essere pensata come un multi- insieme di cardinalità 8 scelto da un insieme di cardinalità 5. Quindi ci sono

$$\binom{5+8-1}{5-1}=\binom{12}{8}=\frac{12\cdot 11\cdot 10\cdot 9}{4\cdot 3\cdot 2}=11\cdot 5\cdot 9=495$$

confezioni diverse. Se ad ogni confezione associamo la sequenza di 12 numeri 1 e 0 con 4 numeri 0, la confezione 001110110111 contiene 0 paste di tipo a, 0 paste di tipo b, 3 paste di tipo c, 2 paste di tipo d e 3 paste di tipo e.

§ 3.9 Esercizi

3.1 Siano $H=\{1, 2, 3, 4\}$ e $K=\{a, b, c\}$; scrivere tutti gli elementi del prodotto cartesiano $H\times K$.

3.2 In una regione vi sono venti citt'a, collegate a coppie da una strada comunale. Quante strade comunali possiede la regione in questione?

3.3 Quante diagonali ha un poligono convesso di 6 lati?

3.4 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.

3.5 Quanti sono gli anagrammi della parola PADRE? E della parola MAMMA?

3.6 Scrivere tutti i numeri di due cifre (non necessariamente diverse) scelte tra 1, 2, 3, 4.

3.7 In quanti modi 3 oggetti possono essere colorati con 5 colori diversi?

3.8 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 $n \geq 2$?

3.9 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 $a < b < c$.

3.10 Calcolare il numero di modi distinti in cui può essere servito un giocatore di scala quaranta in una singola mano.

3.11 (a) Quanti insiemi di 5 carte si possono avere con un mazzo da poker di 52 carte? (b) Quanti poker di assi si possono formare ? (c) Quanti poker diversi si possono formare ?

3.12 Una classe è formata da 10 ragazzi e 10 ragazze. Dividiamo a caso la classe in due squadre composte da 10 persone ciascuna. In quanti modi questo può avvenire? Quanti sono i casi in cui le due squadre hanno lo stesso numero di ragazze e ragazzi? Quale è il rapporto tra tali due valori scritto in forma percentuale?

3.13 Dire quanti sono gli anagrammi della parola LOGICA e della parola ILLOGICA.

3.14 Scrivere tutti i numeri (di 3 cifre) formati dalle cifre 1 , 2 , 3 non ripetute.

3.15 Quattro giocatori di tennis vogliono giocare un doppio. Quante coppie distinte si possono formare?

3.16 Nel gioco del Super-enalotto bisogna indovinare 6 numeri scelti tra il numero 1 e il numero 90. Quanti insiemi di 6 numeri si possono formare ?

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

3.18 Uno studente deve seguire 3 corsi di lingue tra i seguenti: inglese, francese, tedesco, spagnolo, russo. Quante possibili scelte ha? quante se vuole includere il corso di inglese?

3.19 Verificare mediante le formule la validità della Formula di Stiefel.

3.20 (Da un compito d'esame) Quanti sono gli anagrammi della parola PROBLEMA che contengono almeno una tra le sequenze di lettere PR, RMAE, EP?

3.21 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 anzichè 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?

3.22 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 $f(a) = a$?

3.23 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, purchè non su pareti adiacenti? Generalizzare le risposte dei precedenti quesiti al caso di una stanza poligonale con n pareti.

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

3.25 Quanti sono i numeri naturali $1 \leq n \leq 500$ che sono multipli di almeno uno tra 2, 3, 5?

3.26 Quanti sono i numeri naturali $1 \leq n \leq 500$ che sono multipli di almeno uno tra 7, 17, 37?

3.27 Quanti sono i numeri naturali $1 \leq n \leq 12100$ che sono multipli di almeno uno tra 10, 55, 22?

3.28 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 4

Semigruppi, monoidi e gruppi

Iniziamo ora a studiare una alla volta alcune delle principali strutture algebriche, iniziando dalla struttura di monoide e di gruppo. Enunceremo e dimostreremo alcune delle loro principali proprietà e soprattutto impareremo a conoscere alcuni gruppi particolarmente significativi.

§ 4.1 Generalità sulle operazioni

Ricordiamo che una operazione binaria (ne esistono anche di più complicate) in un insieme A è una funzione $f\colon A \times A \to A$. Di solito non indicheremo una operazione con una lettera, come fatto ora, ma con un simbolo (ad esempio $+$, $\cdot$, $\circ$ o più in astratto $*$). Inoltre, se $*$ indica l'operazione, per l'immagine di una coppia (a, b) useremo la scrittura $a * b$ (come siamo abituati a fare con le operazioni tra numeri), invece della notazione tipica delle funzioni, ossia $*((a, b))$. Chiameremo tale immagine **risultato** dell'operazione tra a e b. Questa definizione di operazione racchiude una classe molto vasta di funzioni, alcune delle quali decisamente poco interessanti e altre ben note fino dai tempi della scuola elementare.

Esempio 4.1. La funzione costante $c_{14}\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ è una operazione in $\mathbb{R}$. Il risultato dell'operazione tra due qualsiasi numeri reali è sempre 14.

Esempio 4.2. L'addizione tra numeri naturali è una operazione in $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è una operazione in $\mathbb{N}$. Per ogni coppia di numeri naturali (n, m) l'immagine $f((n, m))$ è il numero naturale $n + m$.

Esempio 4.3. La funzione $\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\star(a, b) = a \star b = ab - a - b + 2$ è un'operazione su $\mathbb{Z}$.

Elenchiamo ora alcune proprietà interessanti relative alle operazioni (che possono essere soddisfatte oppure anche **non** soddisfatte) da una certa operazione). Sia $*$ una operazione nell'insieme A:

- Proprietà associativa: per ogni $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Proprietà commutativa: per ogni $a, b \in A$, $a * b = b * a$.

- Esistenza dell'elemento neutro: esiste $e \in A$ tale che $e * a = a * e = a$ per ogni $a \in A$.
- Esistenza dell'inverso (o opposto): per ogni $a \in A$, esiste $a^{-1} \in A$ (o $-a \in A$) tale che $a * a^{-1} = a^{-1} * a = e$ (o $a * (-a) = -a * a = e$).

§ 4.2 Semigruppi e monoidi

Definizione 4.4. *Sia A un insieme e $*$ un'operazione su A. $(A, *)$ è* **semigruppo** *se $*$ è associativa.*

Esempio 4.5. Gli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con l'usuale operazione somma sono tutti semigruppi. Analogamente se invece della somma consideriamo il prodotto.

Esempio 4.6. Sia A un insieme, sia A^A l'insieme delle funzioni $f : A \to A$ e sia $\circ$ la composizione di funzioni. Possiamo considerare $\circ$ come un'operazione su A^A:

$$\circ : A^A \times A^A \to A^A, \quad \circ(f, g) = f \circ g : A \to A$$

L'operazione $\circ$ è associativa:

$$\forall f, g, h \in A^A, f \circ (g \circ h) = (f \circ g) \circ h.$$

Si verifica osservando come agiscono $f \circ (g \circ h)$ e $(f \circ g) \circ h$ su un qualsiasi elemento di A:

$$\forall a \in A, (f \circ (g \circ h))(a) = f((g \circ h)(a)) = f(g(h(a)) = (f \circ g)(h(a)) = ((f \circ g) \circ h)(a).$$

Quindi $(A^A, \circ)$ è un semigruppo.

Esempio 4.7. Consideriamo $\mathbb{Z}$ e la funzione $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$: $(a, b) \mapsto a - b$. La funzione $-$ è un'operazione, ma non è associativa: infatti, è possibile trovare almeno una terna $a, b, c, \in \mathbb{Z}$ per cui $a-(b-c) \neq (a-b)-c$. Per esempio $a = 4, b = -2, c = 8$: $(4 - (-2)) - 8 = -2 \neq 10 = 4 - (-2 - 8)$. Quindi l'operazione $-$ non dà su $\mathbb{Z}$ la struttura di semigruppo.

Esempio 4.8. su $\mathbb{R} \times \mathbb{R}$ definiamo $(a, b) * (a', b') = (aa', ab' + b)$. Otteniamo un semigruppo.

Definizione 4.9. *Se $(A, *)$ è un semigruppo, possiamo definire le potenze di un elemento $a \in A$ mediante l'induzione:*

$$\begin{cases} a^1 = a \\ \forall n \geq 1 \quad a^{n+1} := a^n * a. \end{cases}$$

Proposizione 4.10. *Sia $(A, *)$ un semigruppo. Se $a \in A$ e m, n sono interi positivi, allora $a^n * a^m = a^{n+m}$ e $(a^n)^m = a^{nm}$.*

Dimostrazione. Dimostriamo per induzione su m che $a^n a^m = a^{n+m}$. Se $m = 1$, si ha $a^n * a^1 = a^n a = a^{n+1}$ per come abbiamo definito a^n. Supponiamo la proprietà sia vera per un certo m, ossia che valga $a^n * a^m = a^{n+m}$, e dimostriamo che allora vale la proprietà anche per l'intero successivo $m+1$, ossia che si ha $a^n * a^{m+1} = a^{n+m+1}$. Si hanno le uguaglianze:

$$a^n * a^{m+1} = a^n * (a^m * a) = (a^n * a^m) * a = a^{n+m} * a = a^{n+m+1}$$

dove

- la prima e la quarta uguaglianza valgono per la definizione di potenza
- la seconda uguaglianza vale perché l'operazione $*$ è associativa
- la terza uguaglianza vale per l'ipotesi induttiva fatta.

Dimostriamo ora per induzione su m che $(a^n)^m = a^{nm}$. Per $m = 1$, $(a^n)^1 = a^n = a^{n \cdot 1}$. Supponiamo ora che sia vero che $(a^n)^m = a^{nm}$ e otteniamo la catena di uguaglianze

$$(a^n)^{m+1} = (a^n)^m * (a^n)^1 = (a^n)^m * a^n = a^{nm} * a^n = a^{nm+n} = a^{n(m+1)}$$

dove

- la prima e la seconda uguaglianza valgono per la definizione di potenza
- la seconda uguaglianza vale per l'ipotesi induttiva
- la terza uguaglianza si ottiene applicando la prima proprietà delle potenze (che abbiamo già dimostrato).

□

Quando l'operazione che si considera è l'addizione tra numeri, oppure più in generale se usiamo il simbolo $+$ per indicare una operazione, le potenze di un elemento si denotano in modo diverso: l'operazione $\underbrace{a * a * \cdots * a}_{n \text{ volte}}$ con notazione additiva diventa $\underbrace{a + a + \cdots + a}_{n \text{ volte}}$ ed è quindi naturale indicarla con na dove $n \in \mathbb{N}$.

Esempio 4.11. Se sommiamo la matrice $M = \begin{pmatrix} 1 & 4 \\ -3 & 0 \end{pmatrix}$ con se stessa per 5 volte otteniamo la matrice $5M = M + M + M + M + M = \begin{pmatrix} 5 & 20 \\ -15 & 0 \end{pmatrix}$.

Proposizione 4.12. *Sia $(A, *)$ un semigruppo. Se esiste in A l'elemento neutro per $*$, allora esso è unico.*

Dimostrazione. Supponiamo che in A vi siano due elementi e, e' che soddisfano la proprietà che definisce l'elemento neutro. Eseguendo l'operazione $e * e'$ troviamo come risultato e', poichè e composto con ogni altro elemento di A lo lascia invariato; d'altra parte abbiamo anche $e * e' = e$, poichè la stessa proprietà vale per e'. Quindi $e = e * e' = e'$. □

Definizione 4.13. *Sia A un insieme e $*$ un'operazione su A. Si dice che $(A, *)$ è un* **monoide** *se $*$ è associativa ed esiste l'elemento neutro. In altre parole $(A, *)$ è un semigruppo dotato di elemento neutro.*

Esempio 4.14. Gli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con l'usuale operazione somma sono tutti monoidi, l'elemento neutro è sempre 0. Analogamente se invece della somma consideriamo il prodotto, abbiamo struttura di monoide per tutti gli insiemi sopra citati, con elemento neutro 1.

Esempio 4.15. Consideriamo $\mathbb{Z}$ e l'operazione $a * b := ab - a - b + 2$. Verifichiamo se $\mathbb{Z}, *$ è un semigruppo. Prendo a, b, c in $\mathbb{Z}$.

$$a*(b*c) = a*(bc-b-c+2) = (abc-ab-ac+2a)-a-(bc-b-c+2)+2 = abc-ab-ac-bc+a+b+c.$$

$$(a*b)*c = (ab-a-b+2)*c = (abc-ac-bc+2c)-(ab-a-b+2)-c+2 = abc-ab-ac-bc+a+b+c.$$

Quindi $(\mathbb{Z}, *)$ è un semigruppo. Verifichiamo se esiste un elemento neutro e rispetto all'operazione $*$. Cerchiamo $e \in \mathbb{Z}$ tale che $a * e = e * a = a$ per ogni $a \in \mathbb{Z}$.

$$a * e = ae - a - e + 2 = a \Rightarrow (e-2)a + (e-2) = 0 \Rightarrow e = 2.$$

L'elemento neutro esiste ed è 2. Quindi $(\mathbb{Z}, *)$ è un monoide.

Esempio 4.16. Definiamo su $\mathbb{R} \times \mathbb{R}$ l'operazione $(a, b) * (a', b') = (aa', ab' + b)$. L'operazione $*$ è associativa (si veda esercizio 5.1). $(\mathbb{R} \times \mathbb{R}, *)$ è un monoide perché esiste l'elemento neutro, $e = (1, 0)$.

Il monoide delle parole

Sia A un insieme, che chiamiamo **alfabeto**. Chiamiamo **parola nell'alfabeto** A una qualsiasi sequenza $a_1 a_2 \dots a_n$ di elementi $a_i \in A$ (ed anche la parola vuota, sequenza di 0 simboli).

Esempio 4.17. Sia $A = \{0, 1, 2, \dots, 15\}$. Alcune parole nell'alfabeto A sono ad esempio

$$1\ 5\ 15, \quad 4\ 4\ 4\ 3\ 4\ 5, \quad 6.$$

Per ogni $n \geq 0$, definiamo W_n come l'insieme delle parole w nell'alfabeto A formate da esattamente n elementi di A:

$$W_n := \{w = a_1 \dots a_n | a_i \in A\}.$$

Per $n = 0$, W_0 contiene un solo elemento, la **parola vuota** w_0 che non contiene nessun elemento di A. Invece $W_1 = A$.

Definizione 4.18. *L'insieme* $W_A = \bigcup_{n\in\mathbb{N}} W_n$ *è l'***insieme della parole** *nell'alfabeto* A*.*

Definiamo un'operazione su W_A: siano $w_1 = a_1 a_2 \dots a_n$ e $w_2 = b_1 b_2 \dots b_m$ due parole di W_A,

$$w_1 \circ w_2 = a_1 a_2 \dots a_n b_1 b_2 \dots b_m.$$

$w_1 \circ w_2$ è una parola di W_A e $\circ$ è un'operazione, quindi $(W_A, \circ)$ è una struttura algebrica. Chiamiamo $\circ$ la **concatenazione**.

Proposizione 4.19. $(W_A, \circ)$ *è un monoide.*

Dimostrazione. Dobbiamo verificare che la concatenazione sia un'operazione associativa e che esista l'elemento neutro. Per l'associatività è sufficiente osservare che se $w_1 = a_1 a_2 \dots a_n, w_2 = b_1 b_2 \dots b_m$ e $w_3 = c_1 c_2 \dots c_l$ allora

$$(w_1 \circ w_2) \circ w_3 = (a_1 a_2 \dots a_n b_1 b_2 \dots b_m) \circ w_3 = a_1 a_2 \dots a_n b_1 b_2 \dots b_m c_1 c_2 \dots c_l,$$

$$w_1 \circ (w_2 \circ w_3) = w_1 \circ (b_1 b_2 \dots b_m c_1 c_2 \dots c_l) = a_1 a_2 \dots a_n b_1 b_2 \dots b_m c_1 c_2 \dots c_l.$$

Inoltre l'elemento neutro rispetto a $\circ$ esiste, ed è la parola vuota w_0. □

§ 4.3 Gruppi

Definizione 4.20. *Siano* G *un insieme e* $*$ *un'operazione in* G*. Diremo che* $(G, *)$ *è un* **gruppo** *se:*

i) l'operazione $*$ *è associativa;*

ii) esiste un elemento $e \in G$*, detto* **identità** *o* **elemento neutro** *tale che* $\forall a \in G$ *si ha* $a * e = e * a = a$*;*

iii) ogni elemento ha l'inverso, ossia $\forall a \in G\ \exists b \in A$ *tale che* $a * b = b * a = e$*.*

Esempio 4.21. $\mathbb{Z}$ con la somma è un gruppo, mentre $\mathbb{N}$ con la somma non lo è (manca l'inverso degli elementi rispetto a $+$). Se consideriamo l'operazione prodotto usuale, nessun insieme tra $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ è un gruppo: infatti l'elemento 0 non possiede inverso rispetto al prodotto. Otteniamo invece un gruppo se consideriamo l'operazione prodotto negli insiemi $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, dove il simbolo di insieme numerico con stellina ad esponente indica l'insieme stesso privato dello zero. Quindi ad esempio $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Esempio 4.22. Sia A un insieme e sia A^A l'insieme di tutte le funzioni $f : A \to A$. Come già visto nell'Esempio 4.6, A^A con la composizione di funzioni $\circ$ è un semigruppo. Inoltre A^A è anche dotato di elemento neutro rispetto a $\circ$: la **funzione identità** Id_A e costituisce quindi un monomide.

$$\begin{array}{rcl} id_A : A & \to & A \\ a & \mapsto & a. \end{array}$$

Però, se $|A| \geq 2$, A^A non è un gruppo, poichè ad esempio le funzioni costanti non hanno inverso. Se infatti $a, b \in A$ sono due elementi diversi e indichiamo con c_a la funzione costante data da $c_a(x) = a \ \forall x \in A$, allora la composizione $c_a \circ g$ di una qualsiasi funzione $g \in A^A$ con c_a, coincide con c_a ed è quindi diversa da Id_A: si ha ad esempio $c_a(b) = a \neq Id_A(b) = b$.

Definizione 4.23. *Un gruppo $(G, *)$ si dice* **gruppo abeliano** *se l'operazione $*$ è anche commutativa, ossia $\forall a, b \in A$ si ha $a * b = b * a$.*

Da ora in poi indicheremo abitualmente l'operazione di un generico gruppo G mediante il simbolo $\cdot$ e chiameremo "prodotto" tale operazione, ossia adotteremo la **notazione moltiplicativa**. Per coerenza, l'unica identità di G sarà denotata con 1_G e l'unico inverso di un elemento $a \in G$ sarà denotato a^{-1}. Spesso il simbolo $\cdot$ di prodotto si sott'intende. Nel caso dei soli gruppi abeliani potremo indicare l'operazione di gruppo col simbolo $+$ e chiamarla somma, ossia useremo la **notazione additiva**; in tal caso indicheremo con 0_G l'identità del gruppo e con $-a$ l'inverso di un elemento $a \in G$ (che chiameremo opposto di a).

Proposizione 4.24. *Sia $(G, *)$ un gruppo. Allora:*

i) l'identità di G è unica;

ii) per ogni $a \in G$, l'inverso di a è unico.

iii) per ogni $a, b \in G$, l'inverso di ab è unico ed è dato da $b^{-1} * a^{-1}$ **prodotto degli inversi in ordine invertito**.

Dimostrazione. i) Abbiamo già dimostrato l'unicità dell'identità parlando dei semigruppi. *ii)* Supponiamo che per un dato elemento $a \in G$ esistano due elementi b e b' che si comportano come suoi inversi, ossia tali che $a * b = b * a = e$ ed anche $a * b' = b' * a = 1_G$. Eseguendo il prodotto a tre $b * a * b'$ ed utilizzando la proprietà associativa otteniamo:

$$b = b * 1_G = b * (a * b') = (b * a) * b' = 1_G * b' = b'.$$

Dal confronto del primo e dell'ultimo membro otteniamo allora $b = b'$ e quindi i due inversi sono in realtà lo stesso elemento. *ii)* Verifichiamo che quello scritto

è proprio l'inverso di $a * b$ applicando la definizione (tralasciamo ora il simbolo di operazione) :

$$(ab)(b^{-1}a^{-1}) = a(b\ b^{-1})a^{-1} = a\ 1_G\ a^{-1} = a\ a^{-1} = 1_G$$

ed anche

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

□

Proposizione 4.25. *Sia $(G, \cdot)$ un gruppo ed a, b, c tre suoi elementi. Allora:*

i) $ab = 1_G \iff ba = 1_G \iff b = a^{-1}$

ii) $ab = b \iff ba = b \iff a = 1_G$

iii) vale la cancellazione ossia: $ab = ac \iff ba = ca \iff b = c$.

Dimostrazione. i) Se $b = a^{-1}$ le altre due uguaglianze valgono per definizione. Supponiamo allora che $ab = 1_G$ e moltiplichiamo i due membri a sinistra per a^{-1} (che esiste poichè siamo in un gruppo). Otteniamo allora: $a^{-1}(ab) = a^{-1}1_G$. Per definizione di identità il secondo membro è a^{-1}, mentre per la proprietà associativa il primo membro diventa $(a^{-1}a)b = 1_G b = b$. Pertanto $b = a^{-1}$. La dimostrazione dell'altra implicazione è analoga: basterà moltiplicare a destra per a^{-1}. *ii)* Se $a = 1_G$, allora le altre due uguaglianze si ottengono per definizione di identit'a. Supponiamo allora $ab = b$ e moltiplichiamo i due membri a destra per b^{-1} (che esiste poichè siamo in un gruppo). Otteniamo cosı: $abb^{-1} = bb^{-1}$ ossia $a = 1_G$. L'altra implicazione si ottiene in modo analogo moltiplicando a sinistra per b^{-1}. *iii)* Anche la verifica della proprietà di cancellazione si ottiene come le precedenti, moltiplicando opportunamente (ossia a sinistra oppure a destra) per l'inverso di a, l'elemento che vogliamo "cancellare ". □

Esempio 4.26. Gli insiemi $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con l'operazione $\cdot$ sono gruppi

Esempio 4.27. Sia A un insieme e sia A^A l'insieme di tutte le funzioni $f : A \to A$. Come già visto negli Esempi 4.6 e 4.22, A^A con la composizione di funzioni $\circ$ è un monoide. $(A^A, \circ)$ non è in generale un gruppo: infatti le funzioni biunivoche da A in A sono tutte e sole quelle che possiedono inverso rispetto a $\circ$. Le funzioni non biunivoche invece non hanno inverso. Inoltre, per A^A non possono in generale valere le proprietà dei gruppi quali ad esempio la cancellazione. Per vederlo esplicitamente, possiamo pensare a $A = \mathbb{Z}$, e considerare la funzione $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = a^2$. Questa funzione non ha inversa rispetto a $\circ$. Per quel che riguarda la cancellazione, sia $h : \mathbb{Z} \to \mathbb{Z}$ la funzione definita come $h(a) = -a$. Allora

$$f \circ h = f \circ id_{\mathbb{Z}}, \quad \text{ma } h \neq id_{\mathbb{Z}}.$$

Esempio 4.28. Sia A un insieme e consideriamo $\widetilde{A^A} = \{f : A \to A | f \text{ è biunivoca}\}$. Osserviamo che possiamo considerare l'operazione di composizione di funzioni $\circ$ come un'operazione su $\widetilde{A^A}$: infatti, componendo funzioni biunivoche, otteniamo ancora una funzione biunivoca. $(\widetilde{A^A}, \circ)$ è un gruppo. Infatti

1. la composizione di funzioni $\circ$ è associativa in generale, in particolare in $\widetilde{A^A}$;
2. l'identità di A appartiene a $\widetilde{A^A}$, ed è l'elemento neutro rispetto a $\circ$;
3. se $f \in \widetilde{A^A}$, allora esiste l'inversa di f rispetto a $\circ$ (vedi Proposizione 2.20).

Definizione 4.29. *Sia $(G, \cdot)$ un gruppo e sia a un suo elemento. Definiamo le potenze di a con esponente intero (positivo, nullo o negativo) n nel modo seguente:*

- *se $n > 0$, a^n è la potenza di a che abbiamo già definito nei semigruppi*
- *se $n = 0$, poniamo $a^0 := 1_G$*
- *se $n < 0$ ossia se $n = -m$ con $m > 0$, poniamo $a^n := (a^{-1})^m$*

Le proprità delle potenze che abbiamo dimostrato nei semigruppi relativamente al caso degli esponenti positivi valgono nel caso dei gruppi anche per gli esponenti minori o uguali a 0 e si estendono a proprietà che riguardano gli inversi.

Corollario 4.30. *Se $(G, \cdot)$ è un gruppo e $a \in G$, allora valgono le proprietà seguenti per ogni $n, m \in \mathbb{Z}$:*

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{nm}$
- $(a^n)^{-1} = a^{-n}$

§ 4.4 Esercizi

4.1 Consideriamo su $\mathbb{R} \times \mathbb{R}$ l'operazione $(a, b) * (a', b') = (aa', ab' + b)$. Verificare che $*$ è associativa.

4.2 Sia A un insieme, $\mathcal{P}(A)$ il suo insieme delle parti e sia $\triangle$ la differenza simmetrica:

$$\triangle : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A), \quad (A, B) \mapsto (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

$\triangle$ è un'operazione? 'E commutativa? Esiste elemento neutro? Esiste inverso per ogni elemento di $\mathcal{P}(A)$?

4.3 Consideriamo su $\mathbb{R}$ l'operazione quoziente: per ogni $a, b \in \mathbb{R}$, $a : b$ è un numero reale. Verificare se l'operazione quoziente è commutativa, associativa, se esiste elemento neutro in $\mathbb{R}$ rispetto a tale

operazione e eventualmente se esiste inverso di ogni elemento in $\mathbb{R}$ rispetto all'operazione quoziente.

4.4 Si consideri su $\mathbb{N} \times \mathbb{N}$ l'operazione $(n, m) * (n', m') = (nn' + mm', nm' + n'm)$. Stabilire se $(\mathbb{N} \times \mathbb{N}, *)$ è un monoide.

4.5 Sia $A = \{a, b, c\}$ e consideriamo il monoide delle parole W_A. Quante sono le parole di W_4 che contengono solo a e b?

4.6 Si pone $G = \mathbb{R}^* \times \mathbb{R}$ e si definisce la seguente legge di composizione interna:

$$(a, b) * (c, d) = (ac, bc + d), \forall (a, b), (c, d) \in G.$$

1. Eseguire: $(1, 2) * (3, 5)$, $(1, 0) * (-1, 3)$;
2. verificare che $*$ è associativa;
3. trovare l'elemento neutro di $(G, *)$;
4. trovare l'inverso di $(1, 2)$, $(3, 5)$, $(-1, 4)$;
5. dimostrare che $(G, *)$ è un gruppo non abeliano.
6. Calcolare le potenze n-esime di $(1, 2)$ per ogni $n \in \mathbb{Z}$.

4.7 Considerati gli insiemi $G = \{a, b, c, d\}$ e $G' = \{1, 2, 3, 4\}$ con le operazioni definite dalle tabelle seguenti

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	d	a	b
d	d	c	b	a

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1. Trovare gli elementi neutri per cascuna delle strutture $(G, *)$ e $(G', \circ)$;
2. trovare l'inverso di cascun elmento di $(G, *)$ e $(G', \circ)$;
3. tralasciando l'associatività, dimostrare che $(G, *)$ e $(G', \circ)$ sono gruppi;
4. stabilire se $(G, *)$ e $(G', \circ)$ sono gruppi abeliani.

4.8 Si consideri la struttura algebrica $(\mathbb{Z}, *)$, dove l'operazione interna $*$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x * y = x + y - 3.$$

1. Stabilire se $*$ è una legge associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, *)$
3. se la struttura algebrica $(\mathbb{Z}, *)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto all'operazione $*$;
4. concludere se la struttura algebrica $(Z, *)$ è un monoide o un gruppo (abeliano?).

4.9 Si consideri la struttura algebrica $(\mathbb{Z}, \circ)$, dove l'operazione $\circ$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x \circ y = xy + x + y.$$

1. Stabilire se $\circ$ è un'operazione associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, \circ)$;
3. se la struttura algebrica $(\mathbb{Z}, \circ)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto alla legge $\circ$;
4. concludere se la struttura algebrica $(Z, \circ)$ è un monoide o un gruppo (abeliano?).

Capitolo 5

Il gruppo delle permutazioni

§ 5.1 Le permutazioni

Fissiamo un numero intero positivo n. Denotiamo con I_n l'insieme dei numeri naturali $\{1, \ldots, n\}$.

Definizione 5.1. *Sia σ una funzione che ha come dominio e codominio I_n. Se σ è biunivoca, allora σ è una* **permutazione**. *L'insieme di tutte le permutazioni definite su I_n si denota con S_n.*

NOTA BENE: se A è un insieme finito, per ogni funzione $f : A \to A$, si ha

$$f \text{ iniettiva} \Leftrightarrow f \text{ suriettiva} \Leftrightarrow f \text{ biunivoca.}$$

Esempio 5.2. Consideriamo in S_5 la permutazione σ data da:

$$\begin{array}{rcl} \sigma : I_5 & \to & I_5 \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 5 \\ 5 & \mapsto & 2 \end{array}$$

Per scrivere in modo veloce σ, utilizzeremo una tabella costituita da due righe: nella prima sono elencati ordinatamente gli elementi di I_5 e al di sotto di ciascuno di essi, la seconda riga contiene le loro immagini. Otteniamo cosı la seguente tabellina

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Possiamo utilizzare una tabellina analoga a quelle presentata nell'esempio per scrivere in modo sintetivo qualsiasi permutazione. Nella prima riga elenchiamo gli elementi di I_n e al di sotto di ciascuno scriviamo la sua immagine:

$$\begin{pmatrix} 1 & 2 & \ldots & n & n-1 \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Le permutazioni sono funzioni, possiamo quindi anche comporre due permutazioni.

Esempio 5.3. Consideriamo in S_5 la permutazione σ dell'esempio 5.2 e la seguente permutazione τ:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}.$$

Possiamo comporre (con l'usuale legge di composizione tra funzioni) σ e τ. Poiché la composizione di funzioni non è commutativa, eseguiamo entrambe le composizioni (ottenendo risultati diversi).

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 3, \quad (\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(3) = 1,$$

$$(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(4) = 5, \quad (\sigma \circ \tau)(4) = \sigma(\tau(4)) = \sigma(5) = 2,$$

$$(\sigma \circ \tau)(5) = \sigma(\tau(5)) = \sigma(2) = 4.$$

Riassumendo con la scrittura "a tabellina ":

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}.$$

Analogamente, possiamo calcolare $\tau \circ \sigma$, ottenendo:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

§ 5.2 Il gruppo delle permutazioni

Ricordiamo ora due proprietà della composizione tra funzioni Intanto, la composizione di funzioni gode della proprietà associativa. Inoltre, la composizione di due funzioni biunivoche è una funzione biunivoca. In particolare, se componiamo due permutazioni, otteniamo ancora una permutazione. Possiamo quindi affermare che S_n con l'operazione di composizione di funzioni è un semigruppo. Però se $n \geq 3$ l'operazione NON è commutativa (vedi Esempio 5.3). Nell'Esempio 4.28, abbiamo già verificato che l'insieme delle funzioni biunivoche da un insieme A nell'insieme A è un gruppo con la composizione $\circ$. Questo vale quindi anche per l'insieme delle permutazioni S_n con $\circ$. Vediamo esplicitamente come si scrivono nella nostra notazione l'identità e l'inverso in S_n. L'identità (o elemento neutro) è

$$e = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}.$$

cioè è la *funzione identit'a* definita come $e(i) = i$ per ogni $i \in I_n$. Si verifica facilmente che $e \circ \sigma = \sigma \circ e = \sigma$ per ogni $\sigma \in S_n$. Per poter affermare che S_n con l'operazione $\circ$ è un gruppo resta da dimostrare che per ogni $\sigma \in S_n$ esiste la permutazione inversa $\tau \in S_n$ tale che $\sigma \circ \tau = \tau \circ \sigma = e$. Possiamo costruire con facilità la funzione τ nel modo seguente:

- scriviamo σ mediante la tabellina
- scambiamo tra loro le due righe,
- riordiniamo le colonne in modo da avere nella prima riga i numeri in ordine crescente.

Esempio 5.4. Consideriamo la tabellina della permutazione $\sigma \in S_5$ di Esempio 5.2

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Per ottenere la permutazione inversa di σ, scambiamo le due righe della tabella precedente

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

e poi riordiniamo le colonne

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

Si verifica facilmente che la permutazione ottenuta col metodo illustrato è proprio la funzione inversa. Infatti, l'inversa di una funzione biunivoca $f\colon X \to Y$ è la funzione che associa ad un elemento $y \in Y$ l'unico elemento $x \in X$ tale che $f(x) = y$. Quindi l'immagine $\tau(r)$ di un elemento $r \in I_n$ è l'unico elemento $s \in I_n$ tale che $\sigma(s) = r$, ossia $\tau(r)$ è il numero che nella tabellina di σ si trova al di sopra di r.

Notazione 5.5. Per le permutazioni si usa sempre la notazione moltiplicativa. Quindi l'identità si denota con 1_{S_n} (oltre che con e e con Id) e la permutazione inversa di σ si denota con σ^{-1}. Infine, la composizione $\sigma \circ \tau$ si denota semplicemente con $\sigma\tau$, sottindendendo il simbolo $\circ$ di composizione

Riassumendo, abbiamo dimostrato che:

Teorema 5.6. *Sia S_n l'insieme delle permutazioni di I_n. Allora in S_n è definita un'operazione, la composizione di permutazioni, che ha le seguenti proprietà:*

1. *per ogni $\sigma, \tau, \rho \in S_n$ si ha $(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$, ovvero la composizione di permutazioni è associativa;*
2. *per ogni $\sigma \in S_n$, $\sigma \circ e = e \circ \sigma = \sigma$, dove e è la permutazione identità , ovvero esiste l'elemento neutro;*
3. *per ogni $\sigma \in S_n$, esiste una funzione denotata σ^{-1} tale che $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$, ovvero ogni elemento di S_n ha un inverso.*

Corollario 5.7. *L'insieme S_n delle permutazioni di I_n con l'operazione di composizione è un gruppo (non abeliano).*

§ 5.3 Cicli e scambi

Definizione 5.8. *Siano r un intero, $2 \leq r \leq n$, e siano $m_1,\ m_2,\ \ldots, m_r$ elementi distinti di I_n. Si dice r-**ciclo** di S_n e si indica con $(m_1 m_2 \ldots m_r)$ la permutazione $\sigma \in S_n$ tale che $\sigma(m_1) = m_2$, $\sigma(m_2) = m_3$, ..., $\sigma(m_{r-1}) = m_r$, $\sigma(m_r) = m_1$ e $\sigma(i) = i$ per ogni $i \in I_n - \{m_1,\ m_2,\ \ldots, m_r\}$. I 2-cicli si dicono anche* **scambi** *o* **trasposizioni**. *Due cicli $(m_1 m_2 \ldots m_r)$ e $(n_1 n_2 \ldots n_s)$ di S_n si dicono* **disgiunti** *se $\{m_1, m_2, \ldots, m_r\} \cap \{n_1, n_2, \ldots, n_s\} = \emptyset$. Dato un ciclo $\sigma = (m_1\ m_2\ \ldots\ m_r)$, diciamo che r è la* **lunghezza** *di σ.*

Esempio 5.9. In S_5 il simbolo $\begin{pmatrix} 2 & 4 & 1 \end{pmatrix}$ indica la permutazione $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$. Anche $\begin{pmatrix} 1 & 2 & 4 \end{pmatrix}$ e $\begin{pmatrix} 4 & 1 & 2 \end{pmatrix}$ indicano la stessa permutazione σ. Il termine ciclo si riferisce appunto alla natura circolare di questa permutazione. Infatti in un ciclo conta l'ordine in cui compaiono gli elementi, e non chi è il primo elemento. Invece il ciclo che si scrive invertendo l'ordine degli elementi della scrittura di σ ossia il ciclo $\tau = \begin{pmatrix} 4 & 2 & 1 \end{pmatrix}$ è la permutazione inversa di σ. Infatti $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$ e si ha $\sigma \circ \tau = \tau \circ \sigma = Id$. Il simbolo $\begin{pmatrix} 2 & 3 \end{pmatrix}$ indica la funzione che scambia tra loro 2 e 3 e lascia fissi 1, 4, e 5 ossia $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$.

Il risultato seguente raccoglie alcuni fatti importanti sulle permutazioni; per ciascuno di essi diamo una dimostrazione algoritmica, per mostrare come si può operare concretamente.

Teorema 5.10. *Sia n un intero positivo.*

i) Ogni permutazione di S_n, che non sia l'identità, si può scrivere in modo essenzialmente unico come composizione di cicli disgiunti.

ii) Due cicli disgiunti σ e τ commutano, ossia $\tau\sigma = \sigma\tau$.

iii) ogni ciclo di lunghezza r si può scrivere come prodotto di $r - 1$ scambi.

iv) ogni permutazione si può scrivere come composizione di scambi.

Dimostrazione. Dimostriamo innanzi tutto che due cicli disgiunti commutano tra loro. Dimostreremo poi le affermazioni i), iii) e iv) che riguardano l'esistenza di particolari decomposizioni in cicli, fornendo per ciascuna un algoritmo che costruisce tali decomposizioni. ii) Se $\sigma = (m_1 m_2 \ldots m_r)$ e $\tau = (n_1 n_2 \ldots n_s)$ sono disgiunti, la loro composizione, nei due modi, è la funzione f data da $f(m_i) = \sigma(m_i)$, $f(n_j) = \tau(n_j)$ e $f(t) = t$ se $t \in I_n - \{m_1, m_2, \ldots, m_r, n_1, n_2, \ldots, n_s\}$. i) Per costruire la decomposizione di una permutazione σ in cicli disgiunti consideriamo il piú piccolo

intero i tale che $\sigma(i) \neq i$ e iniziamo a costruire un ciclo $(i\ \sigma(i)\ \sigma(\sigma(i))\dots)$. Poichè gli elementi in I_n sono solo n, dopo al piú n applicazioni della funzione σ troveremo un elemento già insierito nel ciclo. Tale elemento non può essere che il primo, ossia i, poichè σ è iniettivo. Chiudiamo cosı il primo ciclo. Se abbiamo esaurito tutti gli elementi di I_n che non sono fissati da σ (ossia quelli tali che $\sigma(r) \neq r$), ci fermiamo. Altrimenti prendiamo uno degli elementi di I_n non ancora inseriti nel ciclo già costruito e non fissati da σ e iniziamo a costruire un secondo ciclo, fino a "chiuderlo". Ripetiamo la procedura fino ad esaurire gli elementi non fissati da σ. Il ciclo σ si scrive allora come composizione (in un ordine qualsiasi) dei cicli disgiunti costruiti. iii) Una decomposizione in scambi di una permutazione qualsiasi si otterrà componendo le decomposizioni in scambi dei cicli della sua decomposizione in cicli. Il ciclo $\sigma = (m_1 m_2 \dots m_r)$ si ottiene come composizione di scambi in tanti modi, ad esempio nel modo seguente:

$$(m_1 m_2 \dots m_r) = (m_1 m_r)(m_1 m_{r-1}) \dots (m_1 m_3)(m_1 m_2).$$

iv) si ottiene come conseguenza delle precedenti. □

Osservazione 5.11. La decomposizione di una permutazione in cicli disgiunti è essenzialmente unica, poiché l'unica variante possibile riguarda l'ordine con cui elenchiamo i cicli; si tratta di una variante poco significativa in quanto, come abbiamo provato, la composizione di cicli disgiunti gode della proprietà commutativa. Un'altra possibile variante riguarda la scrittura dei cicli; infatti possiamo elencare gli elementi che costituiscono un ciclo iniziando da uno qualsiasi di essi. Non si tratta di una diversa decomposizione in cicli, ma solo di simboli leggermente diversi per indicare uno stesso ciclo.

Esempio 5.12. Per decomporre $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}$ in cicli disgiunti cominciamo da 1, poichè $\sigma(1) \neq 1$. Costruiamo il primo ciclo applicando σ ripetutamente fino a ritrovare 1 stesso: $\sigma(1) = 2$, $\sigma(2) = 5$. $\sigma(5) = 1$. Otteniamo dunque il ciclo $\begin{pmatrix} 1 & 2 & 5 \end{pmatrix}$. Osserviamo ora che 3 non compare in questo ciclo e che $\sigma(3) \neq 3$. Costruiamo quindi un secondo ciclo partendo da 3, che si fermerà quando troveremo nuovamente 3: $\sigma(3) = 4$, $\sigma(4) = 3$. Otteniamo un secondo ciclo $\begin{pmatrix} 3 & 4 \end{pmatrix}$. Controlliamo ora che l'unico numero non considerato nei due cicli è 6, ma $\sigma(6) = 6$. Dunque la decomposizione è terminata: $\sigma = \begin{pmatrix} 1 & 2 & 5 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$. Le uniche varianti alla scrittura della decomposizione di σ sono l'odine dei cicli oppure il punto di inizio dei cicli stessi:

$$\sigma = \begin{pmatrix} 1 & 2 & 5 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 3 \end{pmatrix}\begin{pmatrix} 2 & 5 & 1 \end{pmatrix} = \dots$$

Una decomposizione di $\begin{pmatrix} 5 & 1 & 2 \end{pmatrix}$ in scambi è ad esempio $\begin{pmatrix} 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$ ma lo è anche $\begin{pmatrix} 5 & 1 \end{pmatrix}\begin{pmatrix} 5 & 2 \end{pmatrix}$. Quindi una decomposizione in scambi di σ è $\begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. Una diversa decomposizione in scambi di σ è $\begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$.

Raccogliamo nel corollario seguente alcuni fatti utili da ricordare, che sono conseguenza di quanto già detto ed in particolare del Teorema 5.10.

Corollario 5.13. *In S_n*

- *Se τ è l'r-ciclo $\begin{pmatrix} m_1 & \dots & m_r \end{pmatrix}$, allora τ^{-1} è l'r-ciclo $\begin{pmatrix} m_r & \dots & m_1 \end{pmatrix}$;*
- *se $\sigma = \tau_1 \cdots \tau_m$ è una decomposizione in cicli disgiunti di σ, allora $\sigma^{-1} = \tau_1^{-1} \cdots \tau_m^{-1}$.*
- *Se $\sigma = s_1 \dots s_r$ è una decomposizione in scambi, allora $\sigma^{-1} = s_r \cdots s_1$.*
- *se τ è un r-ciclo, allora $\tau^r = 1_{S_n}$ e $\tau^{-1} = \tau^{r-1}$;*
- *se σ si decompone come prodotto dei cicli disgiunti $\tau_1, \dots, \tau_m$ e r è im minimo comune multiplo della lunghezza di tali cicli, allora $\sigma^r = 1_{S_n}$ e $\sigma^{-1} = \sigma^{r-1}$.*

La prima affermazione si prova eseguendo direttamente il calcolo di τ^r. Per provare la seconda basta osservare che per la commutatività della composizione di cicli disgiunti abbiamo $\sigma^r = (\tau_1 \cdot \dots \cdot \tau_m)^r = \tau_1^r \dots \tau_m^r$ e che ciascuna potenza τ_i^r coincide con 1_{S_n} poichè r è un multiplo della lunghezza di τ_r.

Dimostrazione. □

Una stessa permutazione $\sigma \in I_n$ può essere decomposta in scambi in tanti modi diversi, anche costituiti da un diverso numero di scambi.

Definizione 5.14. *Una permutazione si dice* **pari** *se si può scrivere come composizione di un numero pari di scambi e si dice* **dispari** *se si può scrivere come composizione di un numero dispari di scambi.*

Una tale terminologia non avrebbe alcun senso se una stessa permutazione potesse essere contemporaneamente pari e dispari.

Teorema 5.15. *La parità di ogni permutazione è ben definita.*

Dimostrazione. Per ottenere la tesi è sufficiente provare che che ogni decomposizione in scambi della permutazione identica Id è costituita da un numero pari di scambi. Infatti se ci fosse una permutazione σ che può essere scritta mediante $r \in 2\mathbb{N}$ scambi ed anche mediante $r' \in 2\mathbb{N}+1$ scambi, allora anche σ^{-1} avrebbe la stessa proprietà e quindi $Id = \sigma\sigma^{-1}$ potrerbbe essere scritta mediante $r + r' \in 2\mathbb{N}+1$, scambi, componendo gli m scambi che danno σ con gli m' scambi che danno σ^{-1}. La nostra dimostrazione è un algoritmo che partendo da una qualsiasi decomposizione in m scambi di Id ne costruisce un'altra con $m-2$ scambi. Ripetendo la procedura arriveremo alla decomposizione con 0 scambi. Avremo cosı provato che $m - 2h = 0$,

ossia che m è pari. A questo scopo useremo le due formule seguenti, dove a, x, y sono elementi diversi di I_n:

$$\begin{pmatrix} a & x \end{pmatrix}\begin{pmatrix} a & y \end{pmatrix} = \begin{pmatrix} a & y \end{pmatrix}\begin{pmatrix} x & y \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} a & x \end{pmatrix}\begin{pmatrix} a & x \end{pmatrix} = Id$$

Fissiamo una decomposizione in scambi di Id ed osserviamo che ogni $i \in I_n$ che compare in uno di tali scambi deve comparire almeno in un altro. In caso contrario mediante tale composizione di scambi i non sarebbe immagine di se stesso, ma sarebbe immagine dell'altro elemento che fa coppia con lui nell'unico scambio che lo coinvolge. Supponiamo per semplicità che i sia 1 e procediamo nel modo seguente. Applicando ripetutamente la prima delle due formule precedenti possiamo "spostare" uno alla volta i cicli che coinvolgono 1 fino a farli diventare consecutivi. Ora consideriamo due di tali cicli consecutivi $\begin{pmatrix} 1 & x \end{pmatrix}\begin{pmatrix} 1 & y \end{pmatrix}$: se $x = y$ la seconda formula ci permette di cancellare i due cicli ottenendo una decomposizione di Id con 2 cicli in meno di prima. Se $x \neq y$, la prima formula ci permette di scrivere una decomposizione nello stesso numero di cicli, ma in cui 1 compare una volta in meno. Ripetendo la procedura riusciremo a ottenere una decomposizione in $m - 2k$ cicli, in cui 1 non compare più. Ora possiamo prendere in esame un altro numero che compare ed applicare a lui la stessa procedura, fino a farlo sparire. Al termine della procedura nessun numero comparirà negli scambi e quindi avremo 0 scambi. Durante ciascun passo della procedura il numero di scambi rimane invariato o diminuisce di 2: pertanto il numero iniziale m di scambi era pari. □

Abbiamo visto che la decomposizione di una permutazione in scambi non è univocamente determinata, ma lo è la decomposizione in cicli disgiunti, a meno dell'ordine in cui scriviamo i cicli stessi (Proposizione 5.10). Possiamo "catalogare" le permutazionidi S_n a seconda di quali sono le lunghezze delle permutazioni che costituiscono la sua decomposizione in cicli disgiunti. Piú precisamente, sia $\sigma \in S_n$ e sia $\sigma = \tau_1 \dots \tau_m$ la sua decomposizione in cicli disgiunti. Sia k_r il numero di cicli di lunghezza r presenti nella decomposizione di σ, con la convenzione di considerare gli elementi fissati da σ come 1-cicli. L'n-pla $(k_1, k_2, \dots, k_n)$ è detta il **tipo** della permutazione σ. Un altro modo di indicare il tipo di una permutazione è $[1^{k_1} 2^{k_2} \dots n^{k_n}]$.

Esempio 5.16. Usando la convenzione di non scrivere r^{k_r} quando $k_r = 0$ e di scrivere solo r quando $k_r = 1$, i possibili tipi di una permutazione di S_5 sono

$$[1^5], [1^3 2], [1^2 3], [12^2], [14], [23], [5].$$

Esempio 5.17. Calcoliamo il numero di permutazioni di S_{17} di tipo $[2^2 3^3 4]$. Si tratta di sistemare i numeri $1, 2, \dots, 17$ nella scrittura seguente al posto dei puntini:

$$(\cdot\cdot)(\cdot\cdot)(\cdot\cdot\cdot)(\cdot\cdot\cdot)(\cdot\cdot\cdot)(\cdot\cdot\cdot\cdot)$$

Ci sono 17! modi di fare ciò. Bisogna però tenere conto che la stessa permutazione σ può essere ottenuta con questa procedura in più modi differenti. Infatti si devono fare le due considerazioni seguenti:

1. Ci sono piú modi di scrivere lo stesso ciclo: un ciclo può essere individuato ponendo in prima posizione un suo qualsiasi elemento, mentre l'ordine degli altri elementi del ciclo è determinato da σ. Ci sono quindi 2 modi di scrivere lo stesso 2-ciclo, 3 modi di scrivere lo stesso 3-ciclo e, in generale, n modi di scrivere un n-ciclo. Nel nostro esempio il numero 17! va quindi diviso per $2^2 \cdot 3^3 \cdot 4$.

2. L'ordine di scrittura dei cicli di uguale lunghezza è arbitrario. Ci sono quindi 2! modi di ordinare due 2-cicli ottenendo la stessa permutazione, 3! modi di ordinare tre 3-cicli ottenendo la stessa permutazione, ecc. Quindi nel nostro esempio il numero 17! va ulteriormente diviso per $2! \cdot 3!$.

In totale il numero delle permutazioni del tipo assegnato è quindi:

$$\frac{17!}{2^2 \cdot 3^3 \cdot 4 \cdot 2! \cdot 3!}$$

Lo stesso risultato può essere ottenuto ragionando nel seguente modo.

- Ci sono $\binom{17}{2}$ modi differenti di individuare il primo 2-ciclo;
- ci sono $\binom{15}{2}$ modi differenti di individuare il secondo 2-ciclo;
- ci sono $\binom{13}{3} \cdot 2!$ modi differenti di individuare il primo 3-ciclo, dove $\binom{13}{3}$ sono i modi di scegliere 3 elementi dai 13 non ancora utilizzati e 2! i modi di posizionare i restanti due elementi dopo il primo che può essere scelto arbitrariamente;
- ci sono $\binom{10}{3} \cdot 2!$ modi differenti di individuare il secondo 3-ciclo;
- ci sono $\binom{7}{3} \cdot 2!$ modi differenti di individuare il terzo 3-ciclo;
- ci sono $\binom{4}{4} \cdot 3!$ modi differenti di individuare il 4-ciclo.

Infine, poichè l'ordine di scrittura dei cicli di uguale lunghezza nella decomposizione è arbitrario, il numero ottenuto va diviso per $2! \cdot 3!$. Quindi, in totale il numero delle permutazioni del tipo assegnato si può anche scrivere nella forma:

$$\frac{\binom{17}{2} \cdot \binom{15}{2} \cdot \binom{13}{3} \cdot 2! \cdot \binom{10}{3} \cdot 2! \cdot \binom{7}{3} \cdot 2! \cdot \binom{4}{4} \cdot 3!}{2! \cdot 3!}$$

Per calcolare la parità di una permutazione possiamo decomporla in scambi e poi contare il loro numero per stabilire se si tratta di un numero pari oppure dispari. Un metodo alternativo e più veloce è dato dalla seguente

Proposizione 5.18. *La parità di un r-ciclo è $r-1$. La parità di una permutazione di tipo $[1^{k_1}2^{k_2}\dots n^{k_n}]$ coincide con la parità di*

$$\sum_{r=1}^{n}(r-1)k_r$$

ossia dalla parità del numero di cicli di lunghezza pari.

Dimostrazione. La prima affermazione è conseguenza della Proposizione 5.10. Per quel che riguarda la seconda, basta ricordare che si può ottenere una decomposizione in scambi di una permutazione σ decomponendo prima σ nel prodotto di cicli disgiunti e poi sostituendo ad ogni ciclo una sua decomposizione in scambi. Decomponendo ogni r-ciclo in $r-1$ scambi, il numero complessivo di scambi in cui abbiamo decomposto σ è dato proprio dal numero presente nell'enunciato. Poichè a noi non interessa sapere quanti sono, ma solo se il numero è pari o dispari, ci basterà contare quanti sono i cicli disgiunti con lunghezza pari, poiché quelli di lunghezza dispari sono permutazioni pari e quindi non modificano la parità. □

§ 5.4 Esercizi

5.1 Considerate le seguenti permutazioni:

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&9&6&4&2&8&7&1&5\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&7&3&5&1&8&2&6&9\end{pmatrix}$$

$$\rho=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&5&4&2&6&1&3&9&8\end{pmatrix},\quad \pi=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&5&6&9&8&4&7\end{pmatrix},$$

calcolare i prodotti $\sigma\circ\tau$, $\tau\circ\sigma$, $\pi\circ\tau$, $\tau\circ\pi$, $\sigma\circ\tau\circ\pi$, $\sigma\circ\tau\circ\rho\circ\pi$.

5.2 Siano σ, τ, ρ, π le permutazioni dell'esercizio precedente. Scrivere le loro inverse rispetto alla composizione.

5.3 Siano σ, τ, ρ, π le permutazioni dell'esercizio 6.1. Scriverle come prodotto di cicli disgiunti. Scrivere inoltre come prodotto di cicli disgiunti anche $\sigma\circ\tau$, $\tau\circ\sigma$, $\pi\circ\tau$, $\tau\circ\pi$, $\sigma\circ\tau\circ\pi$, $\sigma\circ\tau\circ\rho\circ\pi$.

5.4 Scrivere tutti i possibili tipi di una permutazione di S_6.

5.5 Calcolare il numero di permutazioni di S_5 di tipo $[15]$ e il numero di quelle di tipo $[5]$.

5.6 Calcolare il numero di permutazioni di S_8 di tipo $[35]$ e il numero di quelle di tipo $[42]$.

5.7 Calcolare il numero di permutazioni di S_7 di tipo $[12^3]$.

5.8 Calcolare il numero di permutazioni di S_9 di tipo $[123^2]$. **5.9** Trovare l'inversa di ognuna delle seguenti permutazioni di S_9:

$$\sigma=(134265),\tau=(1352)(6847),\rho=(3269)(14)(587),\pi=(142)(637)(958)$$

5.10 Dimostrare che una permutazione σ e la sua inversa σ^{-1} hanno la stessa parit'a.

5.11 Dimostrare che, per ogni coppia di permutazioni σ e τ, le permutazioni $\sigma\tau$ e $\tau\sigma$ hanno la stessa parità.

5.12 Scrivere tutti i tipi di permutazioni in S_7 e in S_8.

5.13 Decomporre le permutazioni dell'esercizio 6.1 e dell'esercizio 6.9 in prodotto di trasposizioni.

5.14 Consideriamo le permutazioni $\sigma = (123)(456)(78)$, $\tau = (1357)(26)(4)(8)$. Trovare la parit'a di σ e τ, e scriverle come prodotto di trasposizioni.

5.15 Calcolare il numero di permutazioni di S_6 di tipo $[1^4 2]$ e il numero di quelle di tipo $[2^3]$.

5.16 Sia $\sigma = (12)$ permutazione di S_6. Determinare il numero di permutazioni τ di S_6 di tipo $[2^3]$ tali che $\sigma\tau = \tau\sigma$.

5.17 Siano σ e τ le seguenti permutazioni in S_9

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 5 & 3 & 9 & 6 & 8 & 1 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 2 & 8 & 7 & 6 & 9 & 4 & 3 \end{pmatrix}$$

e sia $\rho = \sigma \circ \tau$.

1. Determinare la decomposizione in cicli disgiunti e la parità di σ, τ e ρ;
2. Determinare il tipo di ρ e il numero di permutazioni di S_9 che hanno lo stesso tipo di ρ;
3. Si dica quanti sono gli 8-cicli di S_9 che contengono 2 ma non 7.

5.18 Siano σ, τ le permutazioni di S_{12} cosıdefinite:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 9 & 7 & 12 & 3 & 5 & 6 & 11 & 2 & 10 & 8 & 1 \end{pmatrix},$$

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 3 & 4 & 5 & 6 & 2 & 7 & 1 & 8 & 9 & 10 & 11 \end{pmatrix}.$$

1. Determinare la decomposizione in cicli disgiunti di σ e di τ.
2. Determinare il tipo di σ ed il numero di permutazioni di S_{12} che hanno lo stesso tipo di σ.
3. Determinare una permutazione ρ di S_{12} tale che $\sigma \circ \rho \circ \tau = \sigma \circ \tau$.

Capitolo 6

Ancora sui gruppi: sottogruppi e omomorfismi

Da ora in poi, nella trattazione generale useremo sempre (salvo diverso avviso esplicito) la notazione moltiplicativa per i gruppi.

§ 6.1 Sottogruppi di un gruppo

Definizione 6.1. *Siano $(G, \cdot)$ un gruppo e H un sottoinsieme di G. Si dice che H è un* **sottogruppo** *di G e si scrive $H < G$ se H è un gruppo con l'operazione indotta da quella di G. Più esplicitamente, H è un sottogruppo di G se*

- $1_G \in H$
- $\forall a, b \in H$, *si ha* $a \cdot b \in H$
- $\forall a \in H$, *si ha* $a^{-1} \in H$.

Spesso per verificare se un sottoinsieme di un gruppo è un suo sottogruppo è comodo utilizzare il seguente

Proposizione 6.2 (Criterio dei sottogruppi)**.** *Un sottoinsieme H di un gruppo $(G, \cdot)$ è un suo sottogruppo se e solo se soddisfa la seguente condizione:*

$$H \neq \emptyset \quad e \quad \forall a, b \in H \quad si\ ha \quad a \cdot b^{-1} \in H.$$

Dimostrazione. Supponiamo che H sia un sottogruppo di G. Poichè $1_G \in H$, allora $H \neq \emptyset$. Se inoltre $a, b \in H$, allora per definizione di sottogruppo anche $b^{-1} \in H$ e quindi $ab^{-1} \in H$. Quindi il sottogruppo H soddisfa il criterio. Supponiamo viceversa che H sia un sottoinsieme di G che soddisfa il criterio. Proviamo che soddisfa anche le tre condizioni per essere un sottogruppo. Prendiamo un qualsiasi elemento $a \in H$ (che esiste perché $H \neq \emptyset$), allora per il criterio $1_G = a \cdot a^{-1} \in H$. Applicando poi la condizione data dal criterio ai due elementi 1_H e a otteniamo $a^{-1} = 1_G \cdot a^{-1} \in H$. Se infine $a, b \in H$, per quanto abbiamo già provato sappiamo che $b^{-1} \in H$. Applicando il criterio alla coppia $a, b^{-1} \in H$, otteniamo $a \cdot b = a \cdot (b^{-1})^{-1} \in H$. □

Esempio 6.3. Il sottoinsieme $\mathbb{Z}$ di $\mathbb{Q}$ è un sottogruppo del gruppo $(\mathbb{Q}, +)$. Infatti $\mathbb{Z} \neq \emptyset$ e per ogni $x, y \in \mathbb{Z}$ la somma tra x e l'opposto di y sta in $\mathbb{Z}$. Invece $\mathbb{N}$ non è un sottogruppo di $(\mathbb{Q}, +)$. Infatti, $3, 7 \in \mathbb{N}$, ma $3 + (-7) \notin \mathbb{N}$.

Esempio 6.4. Il sottoinsieme $\mathbb{Q}_+$ dei numeri razionali positivi è un sottogruppo di $(\mathbb{Q} \setminus \{0\}, \cdot)$. Infatti l'identità 1 del gruppo appartiene a $\mathbb{Q}_+$, l'inverso di un numero razionale positivo è un numero razionale positivo e il prodotto di due numeri razionali positivi è ancora un numero razionale positivo. Invece $\mathbb{Q}_-$ dei razionali negativi non è un sottogruppo.

Esempio 6.5. Il sottoinsieme delle permutazioni pari di S_n è un sottogruppo di S_n. Infatti la permutazione identità è pari, componendo due permutazioni pari si ottiene una permutazione pari e l'inversa di una permutazione pari è pari. Questo sottogruppo si chiama **gruppo alterno** su n elementi e si denota A_n. Invece le permutazioni dispari di S_n non formano un suo sottogruppo, poiché ad esempio non contiene la funzione identità .

Esempio 6.6. Il sottoinsieme $5\mathbb{Z}$ dei multipli interi di 5 è un sottogruppo del gruppo $(\mathbb{Z}, +)$. Infatti $5\mathbb{Z} \neq \emptyset$ e la differenza tra due multipli interi di 5 è un multiplo intero di 5.

§ 6.2 Quanti elementi ha un sottogruppo: il Teorema di Lagrange

Fissiamo ora un gruppo $(G, \cdot)$, un suo sottgruppo H e un suo elemento g. L'insieme $\{gh \mid h \in H\}$ si denota con gH e si dice **laterale sinistro di H rappresentato da g**; in modo analogo potremmo definire il laterale destro.

Proposizione 6.7. *Con le notazioni precedenti:*

i) $|H| = |gH|$.

ii) $gH = g'H \iff g^{-1}g' \in H$.

iii) I laterali sinistri formano una partizione di G.

Dimostrazione. i) La funzione $\mu_g \colon H \to gH$ data da $\mu_g(h) = gh$ è biunivoca poiché ha come inversa la funzione $gH \to H$ che moltiplica ogni elemento gh a sinistra per g^{-1}. ii) "$\Longrightarrow$" Poiché $g' = g' \cdot 1_G \in g'H = gH$, allora esiste $h \in H$ tale che $g' = gh$ e quindi $g^{-1}g' = h \in H$. "$\Longleftarrow$" Sia $a := (g^{-1}g')^{-1} \in H$ e sia gk, un qualsiasi elemento di gH. Allora $gk = g(g^{-1}g'a)k = (gg^{-1})g'(ak) = g'(ak) \in g'H$. Di conseguenza $gH \subset g'H$. Per motivi di simmetria vale anche l'altra inclusione e quindi $gH = g'H$. iii) Nessun laterale gH è vuoto, poiché $1_G \in H$ e quindi $g = g \cdot 1_H \in gH$. Per lo

stesso motivo l'unione dei laterali è tutto G. Due laterali sinistri gH e $g'H$ hanno un elemento a in comune se e solo se esistono $h, m \in H$ tali che $a = gh = g'm$. Allora $g^{-1}g' = hm^{-1} \in H$ e quindi, grazie a ii), concludiamo che $gH = g'H$. □

Corollario 6.8 (Teorema di Lagrange)**.** *Se G è un gruppo finito ed H è un suo sottogruppo, allora il numero di elementi di H divide esattamente il numero di elementi di G.*

Dimostrazione. Abbiamo dimostrato che i laterali sinistri di H formano una partizione di G e che inoltre ciascuno di essi ha lo stesso numero di elementi di H. Dunque possiamo ottenere il numero di elementi di G moltiplicando il numero di elementi di H per il numero di laterali sinistri diversi. □

Esempio 6.9 (Il gruppo alterno)**.** è facile verificare che il sottoinsieme A_n delle permutazioni pari di S_n è un suo sottogruppo (detto **gruppo alterno**). Ogni laterale sinistro σA_n costituito da permutazioni con la stessa parità del rappresentante σ. Poiché la composizione di due permutazioni pari è pari e la composizione di due permutazioni dispari è pari, vi saranno due soli laterali A_n stesso e l'insieme formato dalle permutazioni dispari. Quindi il numero di elementi di A_n è $\frac{n!}{2}$.

Esempio 6.10. Il sottogruppo S_4 ha 24 elementi. Poiché 5 non divide 24 possiamo affermare che S_4 non ha sottogruppi di ordine 5. Infatti l'ordine di ogni suo sottogruppo deve appartenere all'insieme dei divisori di 24: $\{1, 2, 3, 4, 6, 12, 24\}$. Il teorema di Lagrange non afferma tuttavia che per ognuno di tali divisori esitono effettivamente sottogruppi con quell'ordine. Lasciamo come esercizio al lettore stabilire se in S_5 vi è un sottogruppo con 6 elementi.

§ 6.3 Omomorfismi strutture algebriche

Ora che consideriamo non solo insiemi, ma strutture algebriche (quindi un insieme dotato di un'operazione), ci interessa capire quando una funzione definita tra due strutture algebriche "rispetta" le operazioni.

Definizione 6.11. *Siano A, A' due insiemi e siano $*$ e $\star$ due operazioni definite su A e A' rispettivamente. Una funzione $f : A \to A'$ è un* **omomorfismo** *(detto anche* **morfismo***) rispetto alle operazioni $*$ e $\star$ se*

$$\forall a, b \in A, \quad f(a * b) = f(a) \star f(b).$$

Esempio 6.12. Si consideri la funzione $f : (\mathbb{Z}, +) \to (\mathbb{R}, \cdot)$ data da $f(a) = 2^a$. Possiamo verificare che f è un omomorfismo rispetto alle operazioni indicate. Infatti

$$\forall a, b \in \mathbb{Z}, \quad f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b).$$

Esempio 6.13. Si consideri la funzione $\varphi : (\mathbb{Z}, \cdot) \to (\mathbb{R}, +)$ data da $\varphi(a) = a^2$. Possiamo verificare che φ non è un omomorfismo rispetto alle operazioni indicate mostrando che in almeno un caso non rispetta le operazioni. Ad esempio

$$\varphi(3 \cdot 5) = \varphi(15) = 15^2 = 225 \neq \varphi(3) + \varphi(5) = 3^2 + 5^2 = 34$$

Se una struttura algebrica deve soddisfare anche altre condizioni, oltre a possedere una operazione, una funzione sarà un omomorfismo di quella struttura se oltre alle operazioni rispetterà anche le altre proprietà.

Definizione 6.14. *Siano $(A, *)$ e $(B, \star)$ due semigruppi. Diremo che una funzione $f : A \to B$ è un* **omomorfismo di semigruppi** *se è un omomorfismo rispetto alle operazioni. Se inoltre $(A, *)$ e $(B, \star)$ sono monoidi e 1_A, 1_B indicano rispettivamente l'elemento neutro di A rispetto all'operazione $*$ e l'elemento neutro di B rispetto all'operazione $\star$, diremo che $f : A \to B$ è un* **omomorfismo di monoidi** *se è un omomorfismo di semigruppi e inoltre $f(1_A) = 1_B$.*

Esempio 6.15. Consideriamo $\mathbb{Z} \times \mathbb{Z}$ con l'operazione di moltiplicazione componente per componente $(a, b) \cdot (a', b') = (aa', bb')$. Siverifica facilmente che si tratta di un monoide con identit'a $(1, 1)$, ma non di un gruppo: ad esempio $(0, 0)$ è un elemento privo di inverso. Consideriamo la funzione $f \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ data da $f((a, b)) = (a, 0)$. Questa funzione rispetta l'operazione del monoide, ma non è un omomorfismo di monoidi, in quanto $f((1, 1)) = (1, 0)$ che non è l'identità del codominio.

§ 6.4 Omomorfismi di gruppi

Definizione 6.16. *Siano $(G, \cdot)$, $(K, \cdot)$ due gruppi. Una funzione $f \colon G \longrightarrow K$ si dice* **omomorfimo di gruppi** *se rispetta le operazioni, ossia:*

$$\forall a, b \in G : \quad f(a \cdot b) = f(a) \cdot f(b).$$

L'idea di omomorfismo di struttura algebrica è quella di una funzione che rispetta tutte le proprietà della struttura algebrica. Nel caso dei gruppi ci si aspetterebbe che la definizione contenga anche la richiesta di mandare l'identità del dominio in quella del codominio e di mandare l'inverso di un elemento nell'inverso della sua immagine. Vediamo ora che queste condizioni sono solo apparentemente assenti dalla definizione; in realtà nel caso dei gruppi la condizione di essere compatibile con le operazioni ha come conseguenza anche quelle relative alle identità e agli inversi.

Lemma 6.17. *Per ogni omomorfismo di gruppi $f \colon (G, \cdot) \longrightarrow (K, \cdot)$, si ha:*

i) $f(1_G) = 1_K$

ii) $f(a^{-1}) = f(a)^{-1}$

iii) $f(a^n) = f(a)^n$

Dimostrazione. Preso un qualsiasi elemento $a \in G$, avremo per definizione di omomorfismo e di identità:

$$f(a) \cdot f(1_G) = f(a \cdot 1_G) = f(a) = f(a) \cdot 1_K.$$

Applicando la cancellazione a $f(a) \cdot f(1_G) = f(a) \cdot 1_K$ otteniamo $f(1_G) = 1_K$. □

Si faccia attenzione al fatto che la dimostrazione del lemma precedente funziona perché dominio e codominio sono gruppi, ma non vale ad esempio nel caso dei monomidi, come si vede nell'esempio seguente. Non tutte le funzioni tra due gruppi sono omomorfismi. La funzione considerata nel lemma seguente in genere non lo è , tuttavia si tratta di una funzione importante, con conseguenze interessanti.

Definizione 6.18. *Un omomorfismo di gruppi si dice:*

- **epimorfismo** *se è suriettivo*
- **monomorfismo** *se è iniettivo*
- **isomorfismo** *se è biunivoco.*

Se esiste un isomorfismo tra i gruppi G e K, allora si dice che G e K sono isomorfi e si scrive $G \simeq K$.

Esempio 6.19. Il gruppo delle simmetrie del triangolo equilatero è isomorfo al gruppo S_3 delle permutazioni di 3 elementi. Si ottiene un isomorfismo numerando da 1 a 3 i vertici del triangolo ed associado ad ogni simmetria del triangolo la corrispondente permutazione dei vertici. Il gruppo delle simmetrie del quadrato non è invece isomorfo al gruppo S_4. Possiamo costruire un monomorfismo in modo analogo a quanto fatto per il triangolo equilatero. Tuttavia nessuna simmetria del quadrato corrisponde alla permutazione che fissa due vertici adiacenti e scambia gli altri due.

Abbiamo visto che una funzione è suriettiva se la sua immagine insiemistica coincide col codominio. Ovviamente questo vale anche per i morfismi di gruppi. Tuttavia l'insieme immagine in questo caso ha proprietà più interessanti.

Lemma 6.20. *Se* $f\colon (G, \cdot) \longrightarrow (K, \cdot)$ *è un omomorfismo di gruppi, allora l'immagine di* f *è un sottogruppo di* K*, In simboli:* $Im(f) < K$.

Dimostrazione. Eseguiamo la verifica utilizzando il Criterio dei sottogruppi. Due qualsiasi elementi di $Im(f)$ sono del tipo $f(a)$, $f(b)$ con $a, b \in G$. Abbiamo allora, grazie alla Proposizione 6.17 e alla definizione di omomorfismo:

$$f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}).$$

Poiché G è un gruppo e $a, b \in G$, allora anche $a \cdot b^{-1} \in G$ e quindi $f(a \cdot b^{-1}) \in Im(f)$. □

Per verificare l'iniettività di una funzione dobbiamo controllare che ogni coppia di elementi diversi del dominio abbiano immagini diverse. Nel caso dei morfismi il controllo puè essere fattopiù velocemente usando la nozione seguente.

Definizione 6.21. *Dato un omomorfismo di gruppi $f\colon (G, \cdot) \longrightarrow (K, \cdot)$, si dice* **nucleo** *di f e si denota $Ker(f)$ l'insieme controimmagine di 1_K. In simboli:*

$$Ker(f) := \{a \in G \mid f(a) = 1_K\}.$$

Lemma 6.22. *Sia $f\colon (G, \cdot) \longrightarrow (K, \cdot)$ un omomorfismo di gruppi. Allora:*

i) il nucleo di f è un sottogruppo di G. In simboli $Ker(f) < G$.

ii) f è un monomorfismo $\iff Ker(f) = \{1_G\}$.

Dimostrazione. i) Usiamo il criterio. Siano a, b due elementi di $Ker(f)$, ossia due elementi di G tali che $f(a) = f(b) = 1_K$. Allora:

$$f(a \cdot b^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} = 1_K \cdot 1_K^{-1} = 1_K \cdot 1_K = 1_K.$$

Dunque $f(a \cdot b^{-1}) = 1_K$ ossia $a \cdot b^{-1} \in Ker(f)$. *ii)* "$\Longrightarrow$" Se f è iniettivo, la controimmagine di un elemento, in particolare la controimmagine di 1_K, contiene al massimo un elemento. D'altra parte $Ker(f)$ è un sottogruppo di G e quindi contiene almeno 1_G. Dunque $Ker(f) = \{1_G\}$. "$\Longleftarrow$" Supponiamo che f non sia iniettivo: esistono allora due elementi diversi a, b di G tali che $f(a) = f(b)$. Allora $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = f(a) \cdot f(a)^{-1} = 1_K$. Dunque $a \cdot b^{-1} \in Ker(f)$ e $a\, b^{-1} \neq 1_G$. □

Corollario 6.23. *Nelle ipotesi del Lemma precedente, se $f(a) = c$, allora l'insieme controimmagine di c è*

$$f^{-1}(c) = \{a \cdot d \mid d \in Ker(f)\} = \{d \cdot a \mid d \in Ker(f)\}.$$

Dimostrazione. Proviamo solo la prima uguaglianza; la seconda è del tutto analoga. Per "$\supseteq$"basta osservare che $f(a \cdot d) = f(a) \cdot f(d) = c \cdot 1_K = c$. "$\subseteq$"Sia $a' \in G$ tale che $f(a') = c$. Allora $f(a^{-1} \cdot a') = f(a)^{-1} \cdot f(a') = c^{-1} \cdot c = 1_K$. Dunque $a^{-1} \cdot a' \in Ker(f)$. Ponendo $d := a^{-1} \cdot a' \in Ker(f)$, otteniamo $a' = (a \cdot a^{-1}) \cdot a' = a \cdot (a^{-1} \cdot a') = a \cdot d$. □

§ 6.5 Gruppi ciclici

Lemma 6.24. *Sia $(G, \cdot)$ un gruppo ed a un suo elemento. Il sottoinsieme $H := \{a^n \mid n \in \mathbb{Z}\}$ di G è un suo sottogruppo.*

Dimostrazione. Usiamo il criterio dei sottogruppi. Se a^n e a^m sono due qualsiasi elementi di H, allora il prodotto del primo per l'inverso del secondo è $a^n \cdot (a^m)^{-1} = a^n \cdot a^{-m} = a^{n-m}$ (Corollario 4.30) e quindi appartiene ad H . □

Definizione 6.25. *Sia $(G, \cdot)$ un gruppo e a un suo elemento. Si dice* **sottogruppo ciclico generato da** *a e si denota con $\langle a \rangle$ il sottogruppo costituito dalle potenze di a con esponenti interi. Diremo che G è un* **gruppo ciclico** *se vi è un suo elemento a tale che $G = \langle a \rangle$.*

Attenzione: In notazione additiva, ossia se il gruppo è $(G, +)$, scriveremo

$$G =< g >= \{ng \mid n \in \mathbb{Z}\}.$$

Esempio 6.26. Il sottoinsieme $5\mathbb{Z}$ dei multipli interi di 5 è un sottogruppo ciclico di $(\mathbb{Z}, +)$. Infatti in notazione additiva elevare a potenza n-esima un elemento significa sommarlo con se stesso n volte se $n > 0$ e significa sommare con se stesso $(-n)$-volte il suo opposto se $n < 0$; infine se $n = 0$ la potenza con esponente 0 è per definizione l'identità del gruppo, ossia nel nostro caso è 0. Quindi in notazione additiva la potenza n-esima di x si scrive nx e in questo caso è proprio il prodotto di n per x. Dunque i multipli di 5 costituiscono il sottogruppo ciclico generato da 5 nel gruppo $\mathbb{Z}$ con l'operazione di addizione. Notiamo che $(\mathbb{Z}, +)$ stesso è un gruppo ciclico perché coincide col suo sottogruppo ciclico generato da 1.

Esempio 6.27. Nel gruppo delle permutazioni S_5 il sottogruppo ciclico generato dal ciclo $\sigma = (1 \;\; 4 \;\; 2)$ contiene 3 elementi, ed esattamente $\langle \sigma \rangle = \{1_{S_5} = \sigma^0, \sigma = \sigma^1, (1 \;\; 2 \;\; 4) = \sigma^2\}$. Infatti si può verificare che $\sigma^3 = 1_{S_5}$ e quindi tutte le potenze con esponenti interi positivi coincidono con uno dei 3 elementi scritti. Inoltre da $\sigma^3 = 1_{S_5}$ si deduce anche che $\sigma^2 = \sigma^{-1}$ e quindi anche le potenze di σ con esponenti negativi coincidono con una delle 3 potenze elencate.

Proposizione 6.28. *Sia σ un r-ciclo del gruppo simmetrico S_n. Il sottogruppo ciclico generato da σ ha esattamente r elementi:*

$$\langle \sigma \rangle = \{1_{S_n} = \sigma^0, \sigma = \sigma^1, \sigma^2, \ldots, \sigma^{r-1}\}.$$

Dimostrazione. Sia $\sigma = (c_1 \;\; c_2 \;\; \ldots \;\; c_r)$. Possiamo intanto osservare che $\sigma^r = 1_{S_n}$ e quindi, generalizzando il ragionamento fatto nell'esempio precedente, ogni potenza di σ coincide con una di quelle elencate. Inoltre tutte le potenze elencate sono diverse; infatti se $0 \leq n < m \leq r - 1$ abbiamo $\sigma^n(c_1) = c_n \neq \sigma^m(c_1) = c_m$. Quindi $\sigma^n \neq \sigma^m$. □

Esempio 6.29. Il gruppo $(\mathbb{Z}, +)$ contiene oltre ai sogruppi banali, ossia al sottogruppo nullo che contiene solo 0 e il sottogruppo che coincide con tutto $\mathbb{Z}$, anche tanti altri sottogruppi ciclici. Per ogni $n \geq 0$, il sottoinsieme di $\mathbb{Z}$ dei multipli interi di n:

$$n\mathbb{Z} := \{nt \mid t \in \mathbb{Z}\}$$

è un sottogruppo di $(\mathbb{Z}, +)$. Nei prossimi capitoli vedremo che questi sono tutti i possibili sottogruppi di $(\mathbb{Z}, +)$. Cosideriamo per ora un caso particolare. Il sottoinsieme $H := \{6h+9k \mid h, k \in \mathbb{Z}\} \subset \mathbb{Z}$ à un sottogruppo di $(\mathbb{Z}, +)$. Presi infatti due qualsiasi elementi $6h+9k$ e $6h'+9k'$ di H, avremo $(6h+9k)-(6h'+9k') = 6(h-h')+9(k-k') \in H$. Mostriamo ora che H coincide col sottogruppo ciclico $3\mathbb{Z}$. L'inclusione $H \subseteq 3\mathbb{Z}$ à evidente: tutti gli elementi di H sono multipli di 3: $6h + 9k = 3(2h + 3k)$. L'altra inclusione si ottiene osservando che $3 = 6 \cdot 2 + 9 \cdot (-1) \in H$ e quindi per ogni $t \in \mathbb{Z}$ si ha $3t = 6 \cdot 2t + 9 \cdot (-t) \in H$.

§ 6.6 Periodo di un elemento

Consideriamo ora un elemento g di un gruppo $(G, \cdot)$ e le sue potenze. Se vi sono due esponenti diversi $n \neq m$ tali che $g^n = g^m$, allora per la potenza con esponente la loro differenza si ha $g^{n-m} = g^n \cdot (g^m)^{-1} = g^n \cdot (g^n)^{-1} = 1_G$. In particolare supponendo $n > m$, avremo una potenza di g con esponente positivo che vale 1_G.

Definizione 6.30. *Diremo che g ha* **periodo infinito** *se tutte le potenze di g sono tutte diverse. In caso contrario si dice* **periodo di** *g il minimo intero positivo v tale che $g^v = 1_G$.*

In notazione additiva, ossia se $g \in (G, +)$, il periodo di g à il minimo intero positivo v tale che $vg = 0_G$ (oppure à infinito).

Esempio 6.31. Consideriamo il gruppo S_5 delle permutazioni di $\{1, 2, 3, 4, 5\}$ con l'usuale composizione. Componendo con sé stessa la permutazione $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$ otteniamo $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$ e $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = Id$. Dunque il peiodo di σ à 3.

Lemma 6.32. *L'identità 1_G di un gruppo $(G, \cdot)$ à l'unico elemento con periodo 1. Il periodo di un elemento $g \in G$, $g \neq 1_G$, coincide con l'ordine del sottogruppo ciclico generato da g, ossia:*

- *g ha ordine infinito $\iff < g > \simeq \mathbb{Z}$*
- *g ha ordine finito k allora $< g >$ ha k elementi.*

Dimostrazione. Consideriamo l'omomorfismo $\varphi\colon \mathbb{Z} \longrightarrow G$ definito da associando ad ogni $k \in \mathbb{Z}$ la potenza g^k. Se g ha ordine finito k allora $< g >$ è costituito dalle potenze di g con esponenti da 0 a $k-1$. □

Corollario 6.33. *Il periodo di un qualsiasi elemento di un gruppo finito G di ordine n è un divisore di n.*

§ 6.7 Alcuni gruppi importanti

I gruppi diedrali

Si dicono **gruppi diedrali** i gruppi di simmetrie di un dato poligono i Possiamo considerare ad esempio le simmetrie del triangolo isoscele, oppure quelle dell'esagono regolare o quelle di un rettangolo non quadrato e cosı via. Un modo semplice per individuare le simmetrie di un poligono è quello di etichettare i suoi vertici (ad esempio ordinatamente con i numeri da 1 a n) e di considerare quindi la permutazione dei vertici corrispondente a ciascuna simmetria. 'E facile verificare che in questo modo le simmetrie di un triangolo rettangolo corrispondono all'intero gruppo S_3. Invece per $n \geq 4$, e simmetrie di un poligono regolare con n lati corrispondono ad un sottogruppo proprio di S_n di cardinalità $2n$: ci sono n vertici in cui "spostare" il vertice etichettato con 1 e per ciascuno ci sono due vertici, quelli a lui adiacenti, in cui spostare il vertice 2.

Le classi di resto $\mathbb{Z}_n$

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:

$a \equiv b \bmod n$ se e solo se le divisioni di a e di b per n 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. Tratteremo più a fondo la divisione con resto in uno dei prossimi capitoli. 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 6.34. 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* $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Dimostrazione. 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 $0 \leq r < n$. □

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. Le classi di resto $\mathbb{Z}_n$ con l'operazione di somma prima definita è un gruppo abeliano. L'identità è $[0]$ e l'opposto di una classe $[a]_n$ é la classe che ha come rappresentante l'opposto, ossia $-[a]_n = [-a]_n$.

Esempio 6.35. Scriviamo esplicitamente le tabelline della somma nei casi $n = 3$ e $n = 2$. Per semplicità nelle tabelline scriviamo solo i numeri che sono rappresentanti speciali delle classi, sottointendendo il simbolo che indica la classe.

Tabellina di$\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabellina di$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Otteniamo due tabelline simmetriche rispetto alla diagonale principale poiché l'operazione è commutativa. Osserviamo anche che in ogni riga ed in ogni colonna compaiono tutti gli elementi, ma scritti ogni volta in un diverso ordine.

Il risultato delle operazioni + e $\cdot$ in $\mathbb{Z}_n$ non sempre è "intuitivo".

Esempio 6.36. Scriviamo la tabella delle operazioni + e $\cdot$ in $\mathbb{Z}_6$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Possiamo anche considerare $\mathbb{Z}_n$ con l'operazione di prodotto sui rappresentanti: $[a]_n \cdot [b]_n := [ab]_n$. Però $(\mathbb{Z}_n, \cdot)$ non è un gruppo. Infatti $[1]_n$ è l'identità rispetto al prodotto, ma $[0]_n$ non ha l'inverso.

§ 6.8 Esercizi

6.1 Consideriamo la funzione $f : \mathbb{R} \to \mathbb{R}$ definita come $f(x) := 2x$.
Consideriamo $\mathbb{R}$ con l'operazione $+$. La funzione f è un omomorfismo di $(\mathbb{R}, +)$ in sé stesso? 'E anche un omomorfismo di monoidi?
Consideriamo $\mathbb{R}$ con l'operazione $\cdot$. La funzione f è un omomorfismo di $(\mathbb{R}, \cdot)$ in sé stesso? 'E anche un omomorfismo di monoidi?

6.2 Consideriamo l'insieme $\{1, -1\}$ e l'usuale operazione prodotto $\cdot$. $(\{1, -1\}, \cdot)$ è un semigruppo? 'E anche un monoide?

6.3 Consideriamo i monoidi $(\mathbb{Z}, +)$ e $(\{1, -1\}, \cdot)$ e la funzione $f : \mathbb{Z} \to \{1, -1\}$,

$$f(a) = \begin{cases} 1 & \text{se } a \text{ è pari} \\ -1 & \text{se } a \text{ è dispari} \end{cases}$$

f è un omomorfismo di monoidi?

6.4 Consideriamo la funzione $f : \mathbb{R}^+ \setminus \{0\} \to \mathbb{R}$ definita come $f(x) := \log(x)$. Consideriamo $\mathbb{R}^+ \setminus \{0\}$ con l'operazione $+$ e $\mathbb{R}$ con l'operazione $\cdot$. La funzione f è un omomorfismo?

6.5 Sia A un insieme e sia $(W_A, \circ)$ il monoide libero delle parole su A. Definiamo la funzione **lunghezza di una parola**:

$$\begin{array}{rcl} \lambda : W_A & \to & \mathbb{N} \\ w = a_1 \dots a_n & \mapsto & n. \end{array}$$

Se consideriamo $\mathbb{N}$ con l'operazione $+$, λ è un omomorfismo di monoidi?

6.6 Si consideri la struttura algebrica $(\mathbb{Z}, \circ)$, dove l'operazione $\circ$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x \circ y = xy + x.$$

1. Stabilire se $\circ$ è un'operazione associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, \circ)$;

3. se la struttura algebrica $(\mathbb{Z}, \circ)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto alla legge $\circ$;
4. concludere se la struttura algebrica $(Z, \circ)$ è un monoide o un gruppo (abeliano?).

6.7 Sia S_4 il gruppo delle permutazioni di $\{1, 2, 3, 4\}$ con l'usuale composizione. Scrivere tutti gli elementi del gruppo ciclico H generato da $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

6.8 Nel gruppo S_5 delle permutazioni di $\{1, 2, 3, 4, 5\}$ con l'usuale composizione, determinare il peiodo di $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ e di $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$.

6.9 Sia $(G, \cdot)$ un gruppo abeliano e siano $a, b \in G$.

(a) Provare che se a e b hanno periodo finito anche ab ha periodo finito.

(b) Provare che l'insieme H degli elementi di G con periodo finito formano un sottogruppo.

6.10 Sia $(G, \cdot)$ un gruppo e siano $a, b, c \in G$.

(a) Provare che a e a^{-1} hanno lo stesso periodo.

(b) Provare che ab e ba hanno lo stesso periodo.

6.11 Si consideri in $\mathbb{Q}$ l'operazione $\triangle$ definita da $a \triangle b = ab + a + b$.

(a) perché $(\mathbb{Q}, \triangle)$ non è un gruppo?

(b) Verificare che $(\mathbb{Q}^*, \triangle)$ è un gruppo.

6.12 Si consideri in $\mathbb{Z}$ l'operazione $\bullet$ definita da $a \bullet b = a + b - 1$. È vero che $(\mathbb{Z}, \bullet)$ è un gruppo?

6.13 Si consideri in $\mathbb{Z}$ l'operazione $*$ definita da $a * b = ab + a + b$.

(a) Verificare che $*$ è associativa e commutativa e ammette elemento neutro.

(b) È vero che $(\mathbb{Z}, *)$ è un gruppo?

6.14 Sia $M = \{\frac{1+4m}{1+4n} \ / \ n, m \in \mathbb{Z}\}$ dotato dell'usuale operazione di prodotto. Verificare che M è un gruppo.

6.15 Sia $H = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$. Dimostrare che H è un sottogruppo di $(\mathbb{R}, +)$. È vero che $H - \{0\}$ è un sottogruppo del gruppo moltiplicativo $\mathbb{R}^*$?

6.16 Il gruppo prodotto Siano $(G, \cdot)$ e $(H, \cdot)$ due gruppi. Provare che l'operazione nell'insieme prodotto cartesiano $G \times K$ definita da $(a, b) \cdot (a', b') := (a \cdot a', b \cdot b')$ rende $G \times K$ un gruppo. Se non diversamente specificato, il prodotto cartesiano di due gruppi viene sempre considerato dotato di questa struttura di gruppo e viene chiamato *gruppo prodotto*. Verificare che le funzioni di proiezione π_1, π_2 dal prodotto cartesiano su uno dei fattori, nel caso di un gruppo prodotto sono degli epimorfismo di gruppi.

6.17 Consideriamo i gruppi additivi $\mathbb{Z}$, $\mathbb{Z}_6$ e $\mathbb{Z}_5$ e sia $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}_6 \times \mathbb{Z}_5, +)$ definita da $f(n) = ([2n]_6 \ , \ [3n]_5)$.

(a) Verificare che si tratta di un omomorfismo di gruppi.

(b) Determinarne nucleo e immagine.

(c) Determinare il numero di elementi e un rappresentante per ogni classe di $\mathbb{Z}/Ker(f)$.

6.18 Si consideri in $G = S_3 \times \mathbb{Z}_6$ l'operazione definita da $(\sigma, \overline{a}) * (\tau, \overline{b}) = (\sigma\tau, \overline{a+b})$.

(a) Verificare che G è un gruppo. E' abeliano?

(b) Dire se $H = S_3 \times \{\overline{0}\}$, $K = S_3 \times \{\overline{1}\}$, $M = \{1_{S_3}\} \times \mathbb{Z}_6$ sono sottogruppi ed in caso affermativo se sono abeliani.

6.19 Consideriiamo i gruppi additivi $\mathbb{Z}_9$ e $\mathbb{Z}_{12}$. Indichiamo con $[n]$ la classe di un numero intero n in $\mathbb{Z}_9$ e con $\overline{n}$ la sua classe in $\mathbb{Z}_{12}$.

(a) Provare che $f : \mathbb{Z}_9 \to \mathbb{Z}_{12}$ tale che $f([n]) = \overline{n^2}$ non è una funzione ben definita. Verificare che invece lo è $g : \mathbb{Z}_9 \to \mathbb{Z}_{12}$ data da $g([n]) = \overline{4n}$.

(b) Determinare $Im(g)$, $g^{-1}(\overline{0})$ e $g^{-1}(\overline{1})$. g è un omomorfismo di gruppi?

(c) Determinare tutti i possibili omomorfismi di gruppi da $\mathbb{Z}_9$ in $\mathbb{Z}_{12}$.

6.20 Consideriiamo i gruppi additivi $\mathbb{Z}_8$ e $\mathbb{Z}_{12}$. Indichiamo con $[n]$ la classe di un numero intero n in $\mathbb{Z}_8$ e con $\overline{n}$ la sua classe in $\mathbb{Z}_{12}$.

(a) Provare che $f : \mathbb{Z}_{12} \to \mathbb{Z}_8$ tale che $f(\overline{n}) = [4n^2]$ è una funzione ben definita e che è un omomorfismo di gruppi.

(b) Determinare $Im(f)$, $Ker(f)$ e gli insiemi controimmagine di ogni elemento del codominio.

6.21 Sia S_3 il gruppo delle permutazioni di 3 elementi e sia $g\colon S_3 \to S_3$ definito da $\sigma \mapsto \sigma^2$.

(a) Determinare $g^{-1}(1_{S_3})$.

(b) Verificare che g non è un omomorfismo di gruppi.

Capitolo 7

Gli anelli

§ 7.1 Generalità sugli anelli

Definizione 7.1. *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. $(A, +)$ *è un gruppo abeliano*

2. $(A, \cdot)$ *è un semigruppo*

3. *valgono le roprietà distributive del prodotto rispetto alla somma:*

$$\forall a,\ b,\ c \in A: \qquad (a+b)\cdot c = a\cdot c + b\cdot c, \qquad c\cdot(a+b) = c\cdot a + c\cdot b$$

Inoltre l'anello A si dice **commutativo con identità** *se soddisfa anche le due ulteriori condizioni:*

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

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

Esempio 7.2. L'insieme dei numeri interi $\mathbb{Z}$ dotato delle operazioni $+$ e $\cdot$ è un anello commutativo con identità, con $0_{\mathbb{Z}} = 0$ e $1_{\mathbb{Z}} = 1$.

Esempio 7.3. L'insieme $\mathbb{Z}_n$ delle classi di resto modulo n (Capitolo 9) dotato delle operazioni $+$ e $\cdot$ è un anello commutativo con identità. In particolare:

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

ii) $-[a] = [-a]$;

iii) $1_{\mathbb{Z}_n} = [1]$.

Molte proprietà dei numeri interi che usiamo abitualmente 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), incluso ad esempio $\mathbb{Z}_n$. L'enunciato seguente presenta alcune proprietà di questo tipo; alcune altre sono inserite tra gli esercizi.

Lemma 7.4. *Sia A un anello. Allora:*

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

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

iii) *vale la proprietà di cancellazione per la somma $a + c = b + c \Longrightarrow a = b$.*

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

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

v) *l'identità rispetto al prodotto è unico;*

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

Dimostrazione. Le proprietà i), ii), iii) derivano dal fatto che $(A, +)$ è un gruppo. iv) 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. v) L'unicità dell'identità moltiplicativa si prova in modo del tutto analogo a quello seguito per l'identità additiva. vi) Basta provare che $(-1_A) \cdot a$ soddisfa la definizione di l'opposto di a, ossia che sommato con lui dà 0_A:

$$a + (-1_A) \cdot a = 1_A \cdot a + (-1_A) \cdot a = (1_A + (-1_A)) \cdot a = 0_A \cdot a = 0_A.$$

□

Definizione 7.5. *Siano A e B due anelli. Nel prodotto cartesiano $A \times B$ si possono introdurre due operazioni di somma e prodotto ponendo $\forall (a, b), (a', b') \in A \times B$*

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

Si verifica che con tali **operazioni componente per componente***, il prodotto cartesiano $A \times B$ è un anello, detto* ***anello prodotto*** *di A e B. Se inoltre A e B sono anelli commutativi con identità, anche $A \times B$ lo 'e . Se infine esistono le identità 1_A e 1_B, allora anche l'anello prodotto ha identità $1_{A \times B} = (1_A, 1_B)$.*

§ 7.2 Divisori dello zero e unità

In questa sezione consideriamo sempre un anello commutativo con identità A. Spesso sottointenderemo 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 7.6. *Si dice che A è un* **dominio di integrità** *o semplicemente un* **dominio** *se in A vale la* **legge di annullamento del prodotto** *ossia se*

$$\forall\ a, b \in A: \quad ab = 0_A \Longrightarrow a = 0_A \text{ oppure } b = 0_A.$$

Lemma 7.7. *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 $ac = bc \Longrightarrow a = b$.*

Dimostrazione. 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) $a = b$. □

Definizione 7.8. *Un elemento $a \in A$ 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 7.9. 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.

Esempio 7.10. In $\mathbb{Z}_6$, l'anello delle classi di resto modulo 6 si ha $[2] \cdot [3] = [6] = [0]$, anche se $[2] \neq [0]$ e $[3] \neq [0]$. Quindi $\mathbb{Z}_6$ non è un dominio di integrit'a.

Esempio 7.11. L'anello prodotto $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrit'a. Infatti $(1, 0) \neq 0_{\mathbb{Z}\times\mathbb{Z}} = (0, 0)$ e $(0, 1) \neq 0_{\mathbb{Z}\times\mathbb{Z}} = (0, 0)$, ma il loro prodotto è nullo:

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0_{\mathbb{Z}\times\mathbb{Z}}.$$

Definizione 7.12. *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 7.13. In $\mathbb{Z}$ gli unici elementi invertibili sono 1 e -1. Due elementi sono allora associati se sono uguali oppure sono opposti.

Esempio 7.14. In $\mathbb{Z}_6$ gli unici elementi invertibili sono $[1]$ e $[5] = [-1] = -[1]$. Quindi in $\mathbb{Z}_6$, $[a]$ e $[b]$ sono associati se $[a] = [b]$ oppure se $[a] = [5][b] = [5b] = [-1][b] = [-b]$.

Esempio 7.15. Nell'anello prodotto $\mathbb{Q} \times \mathbb{Q}$ sono invertibili tutti gli elementi (a, b) tali che $a \neq 0$ e $b \neq 0$, mentre non lo sono tutti gli altri, ossia quelli in cui 0 compare al primo e/o al secondo posto.

Esempio 7.16. Le seguenti sono le tabelline del prodotto in $\mathbb{Z}_3$ e in $\mathbb{Z}_4$:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Escludendo $[0]_3$ da $\mathbb{Z}_3$ otteniamo un gruppo col prodotto. Infatti i due elementi diversi da $[0]_3$ sono inversi di se stessi. Invece, nel caso $n = 4$ non otteniamo un gruppo neanche escludendo $[0]_4$, ossia neppure $(\mathbb{Z}_4 - \{[0]_4\}, \cdot)$ è un gruppo. Infatti anche $[2]_4$ non ha l'inverso.

Definizione 7.17. *Si dice che un anello commutativo con identità A è un* **campo** *se ogni elemento non nullo di A è una unità.*

Esempio 7.18. L'anello $\mathbb{Z}_3$ è un campo. Anche nell'anello $\mathbb{Z}_7$, tutti gli elementi tranne $[0]$ sono invertibili, quindi anche $\mathbb{Z}_7$ è un campo. Invece $\mathbb{Z}_4$ non è un campo.

§ 7.3 Omomorfismi di anelli

Definizione 7.19. *Siano A e B due anelli. Una funzione $f\colon A \to B$ si dice* **omomorfismo di anelli** *se*

i) f è un omomorfismo dei gruppi additivi $(A, +)$ e $(B, +)$ (ossia rispetta la somma):

$$\forall a, a' \in A\colon \quad f(a + a') = f(a) + f(a')$$

ii) f è un omomorfismo dei semigruppi moltiplicativi $(A, \cdot)$ e $(B, \cdot)$ (ossia rispetta il prodotto):

$$\forall a, a' \in A\colon \quad f(a \cdot a') = f(a) \cdot f(a').$$

Se inoltre A e B hanno identit'a , si richiede che valga anche: $f(1_A) = 1_B$.

Definizione 7.20. *Un omomorfismo di anelli si dice:*

- **epimorfismo** *se è suriettivo*
- **monomorfismo** *se è iniettivo*
- **isomorfismo** *se è biunivoco.*

Possiamo caratterizzare la suriettività e l'iniettività di un omomorfismo di anelli mediante l'immagine e il nucleo, esattamente come abbiamo visto nel caso degli omomorfismi di gruppi.

Definizione 7.21. *L'immagine di un omomorfismo di anelli* $f\colon (A,+,\cdot) \to (B,+,\cdot)$ *è* $Im(f) := \{b \in B \mid \exists a \in A :\ f(a) = b\}$. *Il nucleo di* f *è* $Ker(f) := \{a \in A \mid f(a) = 0_B\}$.

Le definizioni date di nucleo e di immagine si riferiscono semlicemente alla struttura additiva degli anelli A e B. Ricordando che ogni omomorfismo di anelli è anche, per definizione, un omomorfismo di gruppi additivi, otteniamo il risultato seguente:

Proposizione 7.22. *Sia* $f\colon (A,+,\cdot) \to (B,+,\cdot)$ *un omomorfismo di anelli. Allora*

- f *è un epimorfismo di anelli, ossia è suriettivo* $\iff Im(f) = B$
- f *è un monomorfismo di anelli, ossia è iniettivo* $\iff Ker(f) = \{0_A\}$.

§ 7.4 Costruzione di $\mathbb{Z}$ (Facoltativa)

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 7.23. *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 7.24. *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:*

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

Mediante i ossiamo identificare i numeri naturali con i numeri interi positivi e considerare $\mathbb{N}$ come un sottoinsieme di $\mathbb{Z}$.

§ 7.5 Esercizi

7.1 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). **7.2** Si consideri l'anello $\mathbb{Z}_8$ con la somma e il prodotto usuali

a. Stabilire quali sono gli elementi invertibili di $\mathbb{Z}_8$.

b. Determinare gli eventuali zero-divisori di $\mathbb{Z}_8$.

c. è vero che $\mathbb{Z}_8$ è un dominio? è vero che $\mathbb{Z}_8$ è un campo?

7.3 Si consideri l'anello $\mathbb{Z}_{11}$ con la somma e il prodotto usuali

a. Stabilire quali sono gli elementi invertibili di $\mathbb{Z}_{11}$.

b. Determinare gli eventuali zero-divisori.

c. è vero che $\mathbb{Z}_{11}$ è un dominio? è vero che $\mathbb{Z}_{11}$ è un campo?

7.4 Si consideri l'anello $\mathbb{Z}$ con le operazioni usuali e l'anello prodotto $\mathbb{Z} \times \mathbb{Z}$.

a. Stabilire se la funzione $g \colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ data da $g(x) = (x, -x)$ è un omomorfismo di anelli.

b. La funzione g è iniettiva? è suriettiva?

7.5 Si considerino gli anelli $\mathbb{Z}$ e $\mathbb{Z}_6$ con le operazioni usuali e l'anello prodotto $\mathbb{Z} \times \mathbb{Z}_6$.

a. Provare che la funzione $h\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_6$ data da $h(x) = (x, [3x])$ è un omomorfismo di anelli.

b. Determinare nucleo e immagine di h.

c. h è un monomorfismo di anelli? è un epimorfismo di anelli?

7.6 Stablire se la funzione $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ data da $\varphi(x) = \frac{x}{2}$ è un omomorfismo di anelli. è anche un omorfismo di anelli commutativi con identità ?

7.7 Stablire se la funzione $\psi\colon \mathbb{Z} \to \mathbb{Q}$ data da $\psi(x) = \frac{1}{x}$ è un omomorfismo di anelli.

7.8 Determinare il nucleo e l'immagine dell'omomorfismo $f\colon \mathbb{Z} \to \mathbb{Z}_6 \times \mathbb{Z}_4$ data da $f(x) = ([x]_6, [x]_4)$.

7.9 Determinare il nucleo e l'immagine dell'applicazione $g\colon \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_8$ data da $f(x) = ([x]_3, [x]_8)$.

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

7.11 Sia A un anello commutativo con identità e siano u e v elementi invertibiie di A.

a. Provare che u è cancellabile ossia che $\forall a, b \in A : au = bu \Rightarrow a = b$.

b. Provare che uv è invertibile.

c. Provare per induzione che v^n è invertibile , per ogni $n \in \mathbb{Z}$.

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

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

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

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

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

Capitolo 8

L'anello degli interi $\mathbb{Z}$

In questo capitolo approfondiamo lo studio dell'anello $\mathbb{Z}$. In particolare ci concentreremo sull'algoritmo di divisione in $\mathbb{Z}$ e le sue applicazioni. Le proprietà di cui ci occuperemo riguardano la possibilità di dividere un elemento per un altro. Iniziamo introducendo alcune definizioni generali sugli anelli che riguardano appunto i fattori di un elemento.

§ 8.1 Elementi irriducibili ed elementi primi

Definizione 8.1. *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 $a \not| b$.*

Definizione 8.2. *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 8.3. 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.

Esempio 8.4. Si consideri in $\mathbb{Z}_6$ l'elemento $[2]$. $[2]$ è primo in $\mathbb{Z}_6$: infatti, se $[2]$ divide $[a] \cdot [b] = [a \cdot b]$, allora a è pari o altrimenti b è pari. Tuttavia, $[2]$ non è irriducibile in $\mathbb{Z}_6$: è sufficiente osservare che $[2] = [2] \cdot [4]$, è né $[2]$ né $[4]$ sono invertibili in $\mathbb{Z}_6$ (si veda la tabella della moltiplicazione di $\mathbb{Z}_6$ nel Capitolo 9).

Osservazione 8.5. 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 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 8.6. *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.*

§ 8.2 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 8.7. *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 $0 \leq r < |b|$.*

Dimostrazione. 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. □

Definizione 8.8. *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 8.9. *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.*

Dimostrazione. 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 $-$. □

Esempio 8.10. 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 8.11. *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 8.12. 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 8.13. *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.*

Dimostrazione. 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. □

Teorema 8.14. (Identità di Bézout) *Siano a, b due interi non entrambi nulli. Allora esistono dei numeri interi opportuni (ma non unici!) x, y tali che*

$$MCD(a, b) = ax + by.$$

Grazie al Lemma 8.13 possiamo calcolare il massimo comun divisore $MCM(a, b)$ e i numeri interi x, y che compaiono nell'identità di Bézout, col 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:

$$MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2) = MCD(r_2, r_3) = \cdots = MCD(r_k, 0) = r_k$$

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 8.15. Vogliamo calcolare $MCD(a = 3522, b = 321)$:

- $3522 = \mathbf{321} \cdot 10 + \mathbf{312}$
- $321 = \mathbf{312} \cdot 1 + \mathbf{9}$
- $312 = \mathbf{9} \cdot 34 + \mathbf{6}$
- $9 = \mathbf{6} \cdot 1 + \mathbf{3}$
- $6 = \mathbf{3} \cdot 2 + \mathbf{0}$.

Pertanto $MCD(3522, 321) = 3$.

Esempio 8.16. 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 8.17. *Siano $a, b, c \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Allora:*

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

Dimostrazione. 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 $x = x't$, $y = y't$. □

Le equazioni del tipo $ax + by = c$ con $a, b, c \in \mathbb{Z}$ nelle incognite x, y di cui si cercano suluzioni $(x = m, y = n)$ in $\mathbb{Z}^2$ si dicono **equazioni Diofanteee lineari in due incognite**. 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.

L'indovinello dei 4 galloni

John McLane è un poliziotto statunitense. Sta inseguendo un pazzo che lascia bombe in giro per New York. Di fianco ad una fontana trova una valigetta e due taniche da 3 e 5 galloni rispettivamente. Nella valigetta c'è una bomba controllata da una bilancia. Per disinnescare la bomba John deve appoggiare sopra la bilancia una tanica con esattamente 4 galloni d'acqua. Ha un minuto di tempo prima che la bomba esploda quindi per misurare i 4 galloni può usare solo le due taniche che ha a portata di mano. Come fa? (Indovinello tratto dal film "Die hard- Duri a morire") SOLUZIONE: dobbiamo cercare le soluzioni all'equazione diofantea

$$5x + 3y = 4. \tag{1}$$

Infatti, abbiamo a disposizione due contenitori della capacità di 3 e 5 galloni rispettivamente, con i quali dobbiamo ottenere (versando acqua in un contenitore o

svuotandola da uno all'altro) esattamente 4 galloni. Cerchiamo soluzioni intere per x e y perché i contenitori non sono graduati: cercare di riempire uno dei due contenitori "a metàrq', rischieremmo di far esplodere la bomba a causa di un'imprecisione! Le uniche mosse che ci garantiscono precisione, sono quelle di riempire completamente un contenitore (+1) o svuotarlo completamente (-1). Posso travasare acqua da un recipiente all'altro, ma per essere "precisi", posso travasare completamente un contenitore pieno nell'altro. Questo non "influisce"sulle variabili dell'equazione. L'equazione (1) ha soluzione se e solo se $MCD(5,3)|4$ (Corollario 8.17). In effetti $MCD(5,3) = 1$, quindi l'equazione (1) ha soluzione! Per trovarla (con certezza!), calcoliamo $MCD(5,3)$ con l'algoritmo euclideo per poi esplicitare l'identit'a di Bézout:

1) $5 = 1 \cdot 3 + 2$

2) $3 = 1 \cdot 2 + 1$

3) $2 = 2 \cdot 1 + 0$

Da queste equazioni troviamo $x', y' \in \mathbb{Z}$ tali che $5x' + 3y' = 1$:

2) $1 = 3 - 2$

1) $2 = 5 - 3$ da cui, sostituendo nella precedente, $1 = 3 - (5 - 3)$ ossia $1 = 2 \cdot 3 - 5$.

Quindi $x' = -1$, $y' = 2$. Una soluzione (non è l'unica!!!!) dell'equazione (1) è $x = -4, y = 8$. In pratica: John McLane deve riempire alla fontana la tanica da 3 galloni per 8 volte. Ogni volta che lo riempie, la svuota in quello da 5. Di volta in volta, il recipiente da 5 galloni si riempirà fino all'orlo, e John dovrà svuotarlo per 4 volte. Alla fine di questo procedimento, nella tanica da 5 galloni ci saranno esattamente 4 galloni di acqua! Non è l'unica soluzione!!!!! John può anche riempire 3 volte il recipiente da 3, travasare man mano in quello da 5 e poi svuotare quello da 5 solo 1 volta: $3 \cdot 3 - 5 = 4$.

§ 8.3 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 8.18. *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 8.19. *Sia a un numero intero $\neq 0, 1, -1$. Allora a può essere scritto come prodotto di numeri interi irriducibili $a = a_1 \cdot \cdots \cdot a_k$.*

Dimostrazione. 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 $k = i + j$, $a = b_1 \cdots b_i \cdot c_1 \cdots c_j$. □

Lemma 8.20. *Sia p un numero intero $\neq 0, 1, -1$. Allora :*

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

Dimostrazione. "$\Longrightarrow$" 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 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 8.14). 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. □

Teorema 8.21. (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.*

Dimostrazione. 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 $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_h$, 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 $q_1 q_2 \cdots q_h$, 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 $a = p_1 p_2 \cdots p_{k-1} p_k = q_1 q_2 \cdots q_{h-1} p_k$. Mediante la cancellazione otteniamo $p_1 p_2 \cdots p_{k-1} = q_1 q_2 \cdots q_{h-1}$, 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. □

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

Dimostrazione. 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. □

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.

§ 8.4 Esercizi

8.1 Calcolare MCD di 18779 e 4183 usando l'algoritmo euclideo.

8.2 Scrivere l'identità di Bézout per i numeri 45 e 51.

8.3 Calcolare il MCD e l'identità di Bézout dei numeri $a = 148131$ e $b = 36951$.

8.4 Determinare la scrittura posizionale in base 7, 2 e 13 del numero (che nella abituale base 10 si scrive) 4581.

8.5 Scrivere nella abituale base 10 i numeri $(110101)_7$, $(110101)_2$, $(110101)_{13}$, dove l'indice indica la base usata.

8.6 Si consideri il numero $(201)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 5.

8.7 Consideriamo $k = 16$, e adottiamo la notazione $a = 10, b = 11, c = 12, d = 13, e = 14, f = 15$. Si consideri il numero $(f41c)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 8.

8.8 Consideriamo $k = 16$, e adottiamo la notazione $a = 10, b = 11, c = 12, d = 13, e = 14, f = 15$. Si consideri il numero $(f41c)_{16}$, scritto in base 16, e si riscriva lo stesso numero in base 8.

8.9 Si scriva il numero intero 8000 in base 16.

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

8.11 Trovare il MCD di 8037 e di 13395 ed esplicitare l'identità di Bézout. Calcolare inoltre $mcm(8037, 13395)$.

8.12

1. Trovare il MCD di 3105 e 2277 ed esplicitare l'identità di Bézout.
2. Trovare tutti gli $x, y \in \mathbb{Z}$ che sono soluzione per l'equazione $3105x + 2277y = 2070$.
3. Trovare il mcm di 3105 e 2277.

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

8.14 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 $a\mathbb{Z} = \{at \mid t \in \mathbb{Z}\}$.

8.15 I produttori della serie di film Die Hard vogliono girare un ultimo film della serie, in cui l'eroe John McLane muore a causa dell'indovinello delle taniche: gli vengono fornite una tanica di capacità n galloni e una di capacità m galloni, e deve ottenere esattamente 3 galloni, solo riempiendo completamente e svuotando completamente le taniche, altrimenti scoppierà una bomba.
Quali tra le seguenti coppie di interi n, m porta di sicuro alla morte John McLane?

1. $n = 972, m = 504$;
2. $n = 1705, m = 1001$;
3. $n = 899, m = 1247$.

8.16 Determinare il MCD di 6120, 720 e 880.

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

8.18 Dire se le seguenti equazioni hanno soluzioni intere:

$$35\, x + 84\, y = 6 \qquad 49\, x + 168\, y = 14.$$

CAPITOLO 9

Gli anelli delle classi di resto

§ 9.1 Unità e zero-divisori in $\mathbb{Z}_n$

Il risultato seguente caratterizza le unità e gli zero-divisori degli anelli $\mathbb{Z}_n$.

Proposizione 9.1. *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 $\mathbb{Z}_n \iff MCD(a,n) > 1$.*

Dimostrazione. **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 8.17) $\iff MCD(a,n) = 1$. **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 $ab \in n\mathbb{Z} \iff mcm(a,n) \leq ab < an \iff MCD(a,n) > 1$. □

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 9.2. *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.*

Dimostrazione. 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. □

Corollario 9.3. *Sia n un intero ≥ 2. Allora:*

$$\mathbb{Z}_n \text{è un campo} \iff \mathbb{Z}_n \text{ è un dominio} \iff n \text{ è un numero primo.}$$

Dimostrazione. "$\mathbb{Z}_n$ 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 9.1). □

Esempio 9.4. 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 $35 : MCD(15, 35)$.

§ 9.2 Congruenze

Definizione 9.5. *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 9.6. *La congruenza lineare $aX \equiv b \bmod n$ ammette soluzioni se e solo se $MCD(a, n)$ divide b.*

Dimostrazione. L'asserto segue immediatamente dal Corollario 8.17. □

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 9.7. 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 9.8. 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 $m=n/MCD(a,n)$.

§ 9.3 La funzione di Eulero

Definizione 9.9. *Si chiama* **funzione di Eulero** *l'applicazione* $\phi\colon \mathbb{N}\setminus\{0,1\} \to \mathbb{N}$ *data da* $\phi(n)=Card\{k \in \mathbb{N} \mid 1 \le k < n,\ MCD(n,k)=1\}$*, 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 $p\cdot 0$, $p\cdot 1$, $p\cdot 2$, …, $p\cdot(p^{k-1}-1)$. 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 9.10. (Moltiplicatività della funzione di Eulero) *Siano* $p_1,\dots,p_k$ *primi distinti. Allora :*

$$\phi(p_1^{r_1}\cdots p_k^{r_k})=\phi(p_1^{r_1})\cdots\phi(p_k^{r_k})=p_1^{r_1-1}(p_1-1)\cdots p_k^{r_k-1}(p_k-1).$$

Teorema 9.11. (Teorema di Eulero) *Siano* a,n *interi positivi tali che* $MCD(a,n)=1$*. Allora* $a^{\phi(n)} \equiv 1 \bmod n$*.*

Dimostrazione. 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 $1 \le k \le p-1$.)

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.

□

Esempio 9.12. 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:

$$2^6 = 64 = 7 \cdot 9 + 1 \text{ quindi } 64 \equiv 1 \bmod 7 \text{ ossia } 2^{\phi(7)} \equiv 1 \bmod 7.$$

Esempio 9.13. Vogliamo calcolare la cifra x che indica le unità del numero 327^{82} 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 9.14. 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

$$\overline{3}^{925} = \overline{3}^{23 \cdot 40 + 5} = (\overline{3}^{40})^{23} \cdot \overline{3}^5 = \overline{1} \cdot (\overline{3}^5) = \overline{243} = \overline{43}.$$

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.

§ 9.4 Solo per curiosità : Crittografia e RSA

(da *10 lezioni di matematica* di G. Ferrarese, M. Roggero, G. Tamone, Aracne ed.)

La **crittografia**, dal greco $\chi\rho\upsilon\pi\tau o\sigma$ = 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 facilit'a. Nata come raccolta di tecniche e di sistemi per assicurare la riservatezza di messaggi tra regnanti, imperatori, amanti, etc, 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, poiché ne fanno uso tessere Bancomat, telefoni cellulari, trasmissioni televisive, internet e in genere ogni strumento di comunicazione elettronica.
Le sue origini sono antichissime; basti pensare che piú di 6000 anni fa si scrivevano geroglifici egizi in modo non standard e ancora oggi si lavora per la loro interpretazione e che nella Bibbia si trova un esempio di crittografia mediante sostituzione di ogni lettera dell'alfabeto con la lettera che occupa la stessa posizione nell' alfabeto scritto al contrario. 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 Leonard Adleman; essi realizzarono una procedura che, dalle loro iniziali, prende il nome di "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 maggiori di m: in questo modo m è sicuramente coprimo con $n = pq$. Inoltre sapendo che $n = pq$ egli può facilmente calcolare la funzione di Eulero $\phi(n) = (p-1)(q-1)$.

- 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 $hd = 1 + k\phi(n)$.

- Infine rende pubblici i due numeri n e h, mentre mantiene il piú 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 messagio 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. Si ha infatti:

$$\overline{c}^d = \overline{m}^{hd} = \overline{m}^{1+k\phi(n)} = \overline{m} \cdot (\overline{m}^k)^{\phi(n)} = \overline{m} \cdot \overline{1} = \overline{m}.$$

  Qualunque sia il numero m' che ottiene come rappresentante della classe $\overline{c}^d = \overline{m}$, egli può infine ricavare m come resto della divisione di m' per n; infatti m (essendo positivo e minore di n) è proprio il resto della divisione per n di ogni numero m' congruo a m modulo n.

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 $(\overline{m}^k)^{\phi(n)} = \overline{1}$. 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 9.15. 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. Perché questa simulazione con numeri cosı 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 $d = 27$ (poiché $3 \cdot 27 = 1 + 2 \cdot 40$). 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:

$$\overline{13}^{27} = (\overline{13}^3)^9 = \overline{52}^9 = \overline{-3}^9 = \overline{-19683} = \overline{-48} = \overline{7}.$$

§ 9.5 Esercizi

9.1 Determinare l'unico numero compreso tra 0 e 52 che stia nella classe di resto modulo 52 di $k = 427$ e poi di $h = -444$.

9.2 Come si fa ad ottenere esattamente 3 litri di acqua usando un recipiente da 5 litri e un altro da 7 litri?

9.3 Eseguire in $\mathbb{Z}_{12}$ i calcoli: $\overline{5}\cdot\overline{3} + \overline{21} - \overline{6}$.

9.4 Scrivere la tabellina del $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5\cdot 0}$, $\overline{5\cdot 1}$, $\overline{5\cdot 2}$ .... Quanto fa $\overline{5\cdot 8734}$?

9.5 Scrivere la lista delle potenze di $\overline{5}$ in $\mathbb{Z}_{12}$ ossia: $\overline{5}^0$, $\overline{5}$, $\overline{5}^2$ .... Quanto fa $\overline{5}^{8734}$?

9.6 Provare che in in $\mathbb{Z}_7$ tutte le classi tranne $\overline{0}$ sono invertibili determinando esplicitamente gli inversi.

9.7 Risolvere le seguenti equazioni in $\mathbb{Z}_7$ mediante sostituzione diretta di ciascun elemento di $\mathbb{Z}_{12}$:

$$\overline{5}x = \overline{1}\ ,\ \overline{2}x = \overline{6}\ ,\ x^2 = \overline{1}\ ,\ x^2 = \overline{0}.$$

9.8 Se $\overline{28} = \overline{2}$ in $\mathbb{Z}_n$, cosa possiamo dire di n?

9.9 Risolvere mediante sostituzione diretta l'equazione in $\mathbb{Z}_8$: $[6]\,[x] = [0]$.

9.10 Calcolare $\phi(100), \phi(528), \phi(121), \phi(297), \phi(700), \phi(215)$

9.11 Trovare la cifra finale di 17^{307} e 18^{75}.

9.12 Calcolare le ultime due cifre di 9^{201} e 302^{46}.

9.13 Fino dalle elementari si imparano alcuni espedienti pratici per riconoscere velocemente se un numero è divisibile per 2, 3, 4, 5 e 11. Ottenere in modo rigoroso questi criteri operando sulle classi di resto in modo analogo a quanto fatto per la prova del 9. Perch non si imparano anche criteri per la divisibilità per 7 o per 13?

9.14 Verificare se la relazione tra i punti del piano per cui due punti sono in relazione se e solo se hanno la stessa distanza dall'origine è una relazione di equivalenza.

9.15 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono parallele è una relazione di equivalenza.

9.16 Verificare se la relazione tra triangoli del piano per cui due triangoli sono in relazione se e solo se sono simili è una relazione di equivalenza.

9.17 Verificare se la relazione tra le rette del piano per cui due rette sono in relazione se e solo se sono perpendicolari è una relazione di equivalenza.

9.18 Verificare se la relazione tra numeri reali per cui due numeri sono in relazione se e solo se uno dei due divide l'altro è una relazione di equivalenza. **9.19** Sia $X = \mathbb{R}[x]/(x^2+1)$ l'insieme

delle classi di equivalenza di polinomi ottenuto mediante la relazione di equivalenza per cui due polinomi sono equivalenti se e solo se divisi per x^2+1 hanno lo stesso resto. Provare che X è in corrispondenza biunivoca con $\mathbb{C}$.

9.20 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 $[m] = [s]$.

9.21 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?

9.22 Si determini (se esiste) l'inverso di $[2]^{1432}$ in $\mathbb{Z}_{29}$.

9.23 L'equazione $[3522] \cdot [x] = [1]$ ha soluzioni in $\mathbb{Z}_{500}$?

9.24 Risolvere le congruenze:

$$3x \equiv 7 \bmod 11 \qquad 8x \equiv 18 \bmod 30 \qquad 9x \equiv 12 \bmod 20$$

$$2x \equiv 11 \bmod 13 \qquad 8x \equiv 4 \bmod 10 \qquad 4x \equiv 7 \bmod 15$$

9.25 Calcolare $\phi(36)$, $\phi(528)$ e $\phi(121)$, dove ϕ è la funzione di Eulero.

9.26 Determinare la cifra delle unità del numero 3477^{159}.

9.27 Determinare la cifra delle unità e quella delle centinaia del numero 17^{1609}.

9.28 Risolvere la congruenza $2x \equiv 10^{712} \mod 11$.

9.29 Determinare il generatore del sottogruppo $H =< 36, 30 >$ di $(\mathbb{Z}, +)$.

9.30 Nel gruppo $(\mathbb{Z}_{55}, +)$ delle classi di resto modulo 55:

(a) Determinare il numero di elementi del sottogruppo ciclico di generato da $[10]_{55}$.

(b) Verificare che il sottogruppo ciclico generato da $[12]_{55}$ coincide con tutto $\mathbb{Z}_{55}$.

(c) Scrivere tutti gli elementi del sottogruppo ciclico generato da $[10]_{55}$.

(d) Dimostrare che $(\mathbb{Z}_{55} - \{0\}, \cdot)$ non à un gruppo.

9.31 Determinare tutti gli elementi del gruppo $(\mathbb{Z}_{16}^*, \cdot)$ e il periodo di ciascuno. Dedurre da quanto ottenuto se $(\mathbb{Z}_{16}^*, \cdot)$ à un gruppo ciclico?

9.32 Determinare tutti gli elementi del gruppo $(\mathbb{Z}_{12}^*, \cdot)$ e il periodo di ciascuno. Dedurre da quanto ottenuto se $(\mathbb{Z}_{12}^*, \cdot)$ à un gruppo ciclico?