Algebra per Informatica

Alessio Caminata

Università di Genova
Anno accademico 2021–22

Indice

Notazioni

In queste note utilizzeremo le seguenti notazioni.

- Con il simbolo := intendiamo "uguale per definizione".
- Con il simbolo $\mathbb{N}$ denotiamo l'insieme dei numeri naturali incluso 0, cioè $\mathbb{N} := \{0, 1, 2, 3, \dots\}$.
- Con il simbolo $\mathbb{N}^*$ denotiamo l'insieme dei numeri naturali escluso 0, cioè $\mathbb{N}^* := \{1, 2, 3, \dots\}$.
- Con il simbolo $\mathbb{Z}$ denotiamo l'insieme dei numeri interi, cioè $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- Con il simbolo $\mathbb{Q}$ denotiamo l'insieme dei numeri razionali, cioè

$$\mathbb{Q} := \left\{ \frac{m}{n} : \ m \in \mathbb{Z}, \ n \in \mathbb{N}^*, \ \mathrm{MCD}(m, n) = 1 \right\}.$$

- Con il simbolo $\mathbb{R}$ denotiamo l'insieme dei numeri reali.

Supponiamo note le definizioni e le elementari proprietà degli insiemi numerici precedenti. I numeri complessi $\mathbb{C}$ verranno introdotti nel Capitolo 3.

1 Insiemi e funzioni

1.1 Insiemi

I concetti di insieme e appartenenza sono primitivi e non verranno definiti in questa sede; rimandiamo al corso di Logica per una discussione più approfondita.

Se A è un insieme e x è un elemento di A scriveremo $x \in A$. Se l'elemento x non appartiene ad A scriveremo $x \notin A$. Se tutti e soli gli elementi di A sono $x_1, \dots, x_n$ scriveremo $A = \{x_1, \dots, x_n\}$. Useremo anche la scrittura $A = \{x : \mathcal{P}(x)\}$, dove $\mathcal{P}$ è una qualche proprietà che descrive gli elementi di A. In altre parole, gli elementi di A sono tutti e soli quelli per cui vale la proprietà $\mathcal{P}$. Affinché l'insieme sia ben definito, la proprietà $\mathcal{P}$ dev'essere un criterio oggettivo e non soggettivo. Vediamo qualche esempio.

Esempio 1.1. (i) $A = \{x : x \text{ è un numero intero pari}\}$ è un insieme.
(ii) $B = \{x : x \text{ è un libro interessante}\}$ non è un insieme.
(iii) $C = \{x : x \text{ è una città in Italia}\}$ è un insieme.
(iv) $2 \in A$, $3 \notin A$, Taranto $\in C$, Parigi $\notin C$.
(v) L'insieme A si può scrivere anche così $A = \{x \in \mathbb{Z} : x = 2n,\ n \in \mathbb{Z}\}$.

Un insieme che contiene soltanto un elemento $\{*\}$ viene chiamato **singoletto**. L'insieme privo di elementi viene detto **insieme vuoto** e si denota con $\emptyset$ o $\{\ \}$.

Faremo uso dei connettivi logici per relazionare le proprietà che definiscono gli insiemi e dei quantificatori. Li ricapitoliamo brevemente ora, e rimandiamo nuovamente al corso di Logica per una discussione più approfondita delle loro proprietà. Siano $\mathcal{P}$ e $\mathcal{D}$ due proprietà e A un insieme.

- $\mathcal{P} \wedge \mathcal{D}$, si legge "$\mathcal{P}$ e $\mathcal{D}$", è la **congiunzione**;
- $\mathcal{P} \vee \mathcal{D}$, si legge "$\mathcal{P}$ o $\mathcal{D}$", è la **disgiunzione**;
- $\neg\mathcal{P}$, si legge "non $\mathcal{P}$", è la **negazione**;
- $\mathcal{P} \Rightarrow \mathcal{D}$ si legge "$\mathcal{P}$ implica $\mathcal{D}$", è l'**implicazione**;
- $\mathcal{P} \Leftrightarrow \mathcal{D}$ si legge "$\mathcal{P}$ se e solo se $\mathcal{D}$", è l'**equivalenza**;
- $\forall x \in A.\mathcal{P}(x)$ si legge "per ogni x in A $\mathcal{P}(x)$", vuol dire che per tutti gli elementi di A vale la proprietà $\mathcal{P}$. È il **quantificatore universale**.
- $\exists x \in A.\mathcal{P}(x)$ si legge "esiste x in A tale che $\mathcal{P}(x)$", vuol dire che esiste almeno un elemento di A per cui vale la proprietà $\mathcal{P}$. È il **quantificatore esistenziale**.
- $\nexists x \in A.\mathcal{P}(x)$ si legge "non esiste x in A tale che $\mathcal{P}(x)$", vuol dire che per nessun elemento di A vale la proprietà $\mathcal{P}$.
- $\exists! x \in A.\mathcal{P}(x)$ si legge "esiste unico x in A tale che $\mathcal{P}(x)$", vuol dire che esiste uno ed un solo elemento di A per cui vale la proprietà $\mathcal{P}$.

Si possono usare i quantificatori e i connettivi per definire le principali relazioni tra insiemi.

Definizione 1.2. Siano A e B due insiemi. Diremo che A è **contenuto** in B o che A è un **sottoinsieme** di B se $\forall x \in A. x \in B$, cioè se tutti gli elementi di A sono anche elementi di B. In simboli si scrive $A \subseteq B$ oppure $A \subset B$, o anche $B \supseteq A$ o $B \supset A$.

Gli insiemi A e B sono **uguali** se vale

$$x \in A \iff x \in B,$$

cioè se A e B hanno gli stessi elementi. In simboli scriviamo $A = B$.

Equivalentemente, il principio di estensionalità afferma che

$$A = B \iff \big((A \subseteq B) \wedge (B \subseteq A)\big),$$

cioè A e B coincidono se e soltanto se A è un sottoinsieme di B e B è un sottoinsieme di A.

Se A è un sottoinsieme di B ma non è uguale a B diciamo che A è **contenuto strettamente** in B o che A è un **sottoinsieme proprio** di B. A volte lo denotiamo con $A \subsetneq B$.

Dato un insieme A, l'**insieme delle parti** di A è l'insieme i cui elementi sono tutti e soli i sottoinsiemi di A. Si denota con $\mathcal{P}(A)$.

Esempio 1.3. (i) Sia $A = \{1, 2, 3\}$, l'insieme delle parti di A è

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

(ii) L'insieme delle parti dell'insieme vuoto è un singoletto $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Definizione 1.4. Siano A e B due insiemi.

- L'**unione** di A e B è l'insieme $A \cup B$ i cui elementi sono elementi di A o elementi di B, cioè
$$A \cup B := \{x : \ (x \in A) \vee (x \in B)\}.$$
- L'**intersezione** di A e B è l'insieme $A \cap B$ i cui elementi sono sia elementi di A che elementi di B, cioè
$$A \cap B := \{x : \ (x \in A) \wedge (x \in B)\}.$$
Gli insiemi A e B si dicono **disgiunti** se $A \cap B = \emptyset$.
- La **differenza** tra B e A (anche detta il **complementare** di A in B) è
$$B \setminus A := \{x \in B : \ x \notin A\}.$$

Si vede facilmente che

$$A \subseteq A \cup B \text{ e } B \subseteq A \cup B. \tag{1}$$

Inoltre, l'unione è il più piccolo insieme che soddisfa la proprietà (1). Infatti se C soddisfa (1), cioè se $A \subseteq C$ e $B \subseteq C$, allora anche $A \cup B \subseteq C$: dato $x \in A \cup B$ allora $x \in A$ o $x \in B$ ed in entrambi i casi segue $x \in C$.

Analogamente si ha che

$$A \cap B \subseteq A \text{ e } A \cap B \subseteq B. \tag{2}$$

E l'intersezione è il più grande insieme che soddisfa la proprietà (2). La verifica è lasciata per esercizio.

Le operazioni di intersezione e unione verificano le seguenti proprietà che seguono dalle corrispondenti proprietà dei connettivi logici $\vee$ e $\wedge$.

Proposizione 1.5. *Siano A, B, e C tre insiemi. Allora*
(i) $A \cup B = B \cup A$ *(proprietà commutativa dell'unione);*
(ii) $(A \cup B) \cup C = A \cup (B \cup C)$ *(proprietà associativa dell'unione);*
(iii) $A \cup A = A$ *(idempotenza dell'unione)*
(iv) $A \cap B = B \cap A$ *(proprietà commutativa dell'intersezione);*
(v) $(A \cap B) \cap C = A \cap (B \cap C)$ *(proprietà associativa dell'intersezione);*
(vi) $A \cap A = A$ *(idempotenza dell'intersezione).*

Dimostrazione. Dimostriamo soltanto la prima proprietà, a titolo esplicativo.
(i) $x \in A \cup B \iff (x \in A) \vee (x \in B) \iff (x \in B) \vee (x \in A) \iff x \in B \cup A$.

□

Esercizio 1.6. Dimostrare le seguenti proprietà:
(i) $A \cap B = A \iff A \subseteq B$;
(ii) $A \cup B = A \iff B \subseteq A$;
(iii) $(B \setminus A) = \emptyset \iff B \subseteq A$;
(iv) $(B \setminus A) = B \iff A \cap B = \emptyset$;
(v) $B = (B \setminus A) \cup (A \cap B)$;
(vi) $(B \setminus A) \cap (A \cap B) = \emptyset$.

Proposizione 1.7 (Proprietà distributiva)**.** *Siano A, B, e C tre insiemi. Allora*
(i) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;
(ii) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Dimostrazione. (i) Sia $x \in (A \cap B) \cup C$ allora $(x \in A \cap B) \vee (x \in C)$. Distinguiamo due casi:

- se $x \in A \cap B$ allora $x \in (A \cup C) \cap (B \cup C)$, perché $A \cap B \subseteq (A \cup C) \cap (B \cup C)$;
- se $x \in C$ allora $x \in (A \cup C) \cap (B \cup C)$, perché $C \subseteq (A \cup C) \cap (B \cup C)$.

In entrambi i casi abbiamo mostrato l'inclusione $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$. Viceversa, sia $x \in (A \cup C) \cap (B \cup C)$ allora $(x \in A \cup C) \wedge (x \in B \cup C)$:

- se $x \in C$ allora $x \in (A \cap B) \cup C$ poiché $C \subseteq (A \cap B) \cup C$;
- se $x \in A \cap B$ allora $x \in (A \cap B) \cup C$ poiché $A \cap B \subseteq (A \cap B) \cup C$;
- se $x \in A$, ma $x \notin B$ (o se $x \in B$, ma $x \notin A$) allora necessariamente $x \in C$ e ricadiamo nel caso precedente.

Questo dimostra l'altra inclusione $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

(ii) Se $x \in (A \cup B) \cap C$ allora $(x \in A \cup B) \wedge (x \in C)$, quindi $(x \in A \cap C) \vee (x \in B \cap C)$, cioè $x \in (A \cap C) \cup (B \cap C)$. Pertanto $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. Viceversa se $x \in (A \cap C) \cup (B \cap C)$ allora $(x \in A \cap C) \vee (x \in B \cap C)$, quindi $(x \in A \cup B) \wedge (x \in C)$, cioè $x \in (A \cup B) \cap C$. Quindi vale anche l'altra inclusione $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$ e pertanto l'uguaglianza.

□

Teorema 1.8 (Leggi di De Morgan)**.** *Siano A e B sottoinsiemi di un insieme X. Allora*
(i) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$*;*
(ii) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$*.*

Dimostrazione. (i) "$\subseteq$" Se $x \in X \setminus (A \cap B)$ allora $x \notin (A \cap B)$, ossia $(x \notin A) \vee (x \notin B)$ cioè $x \in (X \setminus A) \cup (X \setminus B)$.
"$\supseteq$" Se $x \in (X \setminus A) \cup (X \setminus B)$ allora $(x \notin A) \vee (x \notin B)$ cioè $x \notin (A \cap B)$, quindi $x \in X \setminus (A \cap B)$ come richiesto.

(ii) Dimostriamo la proprietà con una catena di equivalenze:

$$x \in X \setminus (A \cup B) \iff (x \notin A) \wedge (x \notin B) \iff (x \in X \setminus A) \wedge (x \in X \setminus B) \iff x \in (X \setminus A) \cap (X \setminus B).$$

□

Introduciamo ora il concetto di prodotto cartesiano di insiemi.

Definizione 1.9. Siano A e B due insiemi non vuoti, e siano $x \in A$ e $y \in B$ due elementi. L'insieme $\{\{x\}, \{x, y\}\}$ si chiama **coppia ordinata** con prima coordinata x e seconda coordinata y e si denota con (x, y). Il **prodotto cartesiano** $A \times B$ di A per B è l'insieme di tutte le coppie ordinate con prima coordinata un elemento di A e seconda coordinata un elemento di B, cioè

$$A \times B := \{(x, y) : \ x \in A, y \in B\}.$$

Nel caso in cui $A = \emptyset$ oppure $B = \emptyset$ si pone per definizione $A \times B = \emptyset$.

Osservazione 1.10. Si osserva che due coppie ordinate (x_1, y_1) e (x_2, y_2) sono uguali se e solo se sono uguali coordinata per coordinata, cioè vale

$$(x_1, y_1) = (x_2, y_2) \iff (x_1 = x_2) \wedge (y_1 = y_2).$$

Il prodotto cartesiano si può generalizzare in maniera naturale al prodotto di tre o più insiemi[1].

- Per tre insiemi A, B, C si pone

  $$A \times B \times C := \{(a, b, c) : \ (a \in A) \wedge (b \in B) \wedge (c \in C)\}.$$

  Con la condizione che due triple ordinate (a_1, b_1, c_1) e (a_2, b_2, c_2) sono uguali se e solo se $a_1 = a_2$, $b_1 = b_2$, e $c_1 = c_2$.

[1]Si può dare una definizione più formale di tripla (e n-upla) ordinata nello stile della Definizione 1.9, ma ci limiteremo a dare una definizione più intuitiva ed operativa.

- Per n insiemi $A_1, \ldots, A_n$ si definisce

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) : \ (a_1 \in A_1) \wedge \cdots \wedge (a_n \in A_n)\},$$

con l'uguaglianza tra n-uple ordinate $(a_1, \ldots, a_n)$ definita analogamente a prima. Useremo anche le notazioni $\prod_{i=1}^{n} A_i$ e $\bigtimes_{i=1}^{n} A_i$ per denotare $A_1 \times \cdots \times A_n$.

Nel caso gli insiemi siano tutti uguali, cioè $A_1 = A_2 = \cdots = A_n = X$ si usa la notazione delle potenze. Abbiamo quindi $X^2 = X \times X$, $X^3 = X \times X \times X$, e così via. Per comodità si pone anche $X^1 = X$ e $X^0 = \{\emptyset\}$, il singoletto che ha come elemento l'insieme vuoto.

Esempio 1.11. Il *piano cartesiano* o *piano euclideo* è il prodotto cartesiano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, costituito dalle coppie ordinate di numeri reali (x, y) con $x \in \mathbb{R}$ e $y \in \mathbb{R}$.

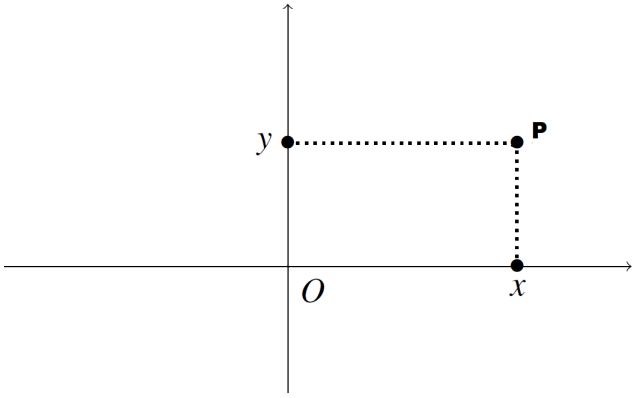


Figura 1: Il piano cartesiano $\mathbb{R}^2$ con il punto $P = (x, y)$.

1.1.1 Insiemi indiciati

Nel caso di unione, intersezione e prodotto cartesiano di più insiemi faremo spesso uso delle seguenti notazioni.

Definizione 1.12. Sia I un insieme, con **famiglia $\mathcal{F}$ di insiemi indiciati su** I si intendono degli insiemi A_i ($i \in I$) "etichettati" con gli elementi di I. Si denota la famiglia con $\mathcal{F} = \{A_i\}_{i \in I}$.

Data una famiglia di insiemi indiciati $\mathcal{F} = \{A_i\}_{i \in I}$, denotiamo poi

- $\bigcup_{i \in I} A_i = \{x \ : \ \exists i \in I \ \text{ per cui } x \in A_i\}$, unione di tutti gli insiemi di $\mathcal{F}$;
- $\bigcap_{i \in I} A_i = \{x \ : \ \forall i \in I \ \text{ si ha } x \in A_i\}$, intersezione di tutti gli insiemi di $\mathcal{F}$.

Casi tipici sono $I = \{1, \dots, n\}$ oppure $I = \mathbb{N}$.

Esempio 1.13. (i) Data la famiglia $A_i = \{i\}$ per $i \in \mathbb{N}$, si ha $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{N}$ e $\bigcap_{i\in\mathbb{N}} A_i = \emptyset$.
(ii) Sia $I = \{1, 2, \dots, 8\}$, e consideriamo la famiglia di intervalli reali $A_i = [0, i]$. Si ha quindi

$$\bigcup_{i\in I} A_i = [0, 8] \text{ e } \bigcap_{i\in I} A_i = [0, 1].$$

(iii) Scegliamo $I = \{k \in \mathbb{N} : \ k \geq 2\}$. Per ogni $k \in \mathbb{N}$, $k \geq 2$ prendiamo $A_k = \{n^k : \ n \in \mathbb{N}\}$, cioè A_2 è l'insieme dei quadrati dei numeri naturali, A_3 è l'insieme dei cubi e così via. Allora $\bigcup_{k\geq 2} A_k$ è un sottoinsieme proprio di $\mathbb{N}$ (per esempio non contiene 3) e $\bigcap_{k\geq 2} A_k = \{0, 1\}$.

1.2 Funzioni

Definizione 1.14. Siano X e Y due insiemi, una **relazione binaria** R tra X e Y è un sottoinsieme R del prodotto cartesiano $X \times Y$, cioè $R \subseteq X \times Y$. Useremo anche la notazione xRy per indicare che due elementi $x \in X$ e $y \in Y$ sono in relazione rispetto a R, cioè $(x, y) \in R$. La relazione $R = X \times Y$ viene detta **relazione totale o universale**, la relazione $R = \emptyset$ viene detta **relazione vuota**. Se $X = Y$, la **relazione diagonale**, denotata con Δ, è la relazione

$$\Delta := \{(x_1, x_2) \in X \times X : \ x_1 = x_2\}.$$

Data una relazione R, la relazione opposta, denotata con R°, è la relazione

$$R^\circ := \{(y, x) \in Y \times X : \ (x, y) \in R\}.$$

Definizione 1.15 (funzione)**.** Siano X e Y due insiemi, una **funzione** o **applicazione** o **mappa** da X a Y è una relazione $f \subseteq X \times Y$ tale che $\forall x \in X \ \exists! y \in Y$ tale che $(x, y) \in f$. Si denota con $f : X \to Y$. Inoltre per indicare che $(x, y) \in f$ si scrive $y = f(x)$. Si dice che y è il valore di f sull'argomento x o anche y è l'immagine di x mediante f. L'insieme X viene detto **dominio** di f e l'insieme Y **codominio** di f.

Intuitivamente un'applicazione $f : X \to Y$ è una "regola" che permette di assegnare ad *ogni* elemento x di X un *unico* elemento di Y denotato con $f(x)$. In quest'ottica talvolta utilizzeremo anche la seguente notazione per definire una funzione:

$$\begin{aligned} f : X &\to Y \\ x &\mapsto f(x). \end{aligned}$$

Tuttavia non bisogna dimenticare che anche il dominio X e il codominio Y fanno parte del "pacchetto di dati" che bisogna specificare per definire una funzione. Per esempio, la funzione $f : \mathbb{N} \to \mathbb{N}$ tale che $f(x) = x^2$ e la funzione $g : \mathbb{Z} \to \mathbb{N}$ tale che $g(x) = x^2$ sono due funzioni ben distinte.

Esempio 1.16. Consideriamo gli insiemi $X = \{1, 2, 3\}$ e $Y = \{a, b, c, d, e, f\}$ e le relazioni $\varphi, \psi \subseteq X \times Y$ date da:

$$\varphi = \{(1, a), (1, d), (2, e), (3, a)\}, \ \psi = \{(1, c), (2, c), (3, a)\}.$$

La relazione φ non è una funzione perchè all'elemento 1 di X corrispondono due elementi di Y. Invece la relazione ψ è una funzione $\psi : X \to Y$ perchè associa ad ogni elemento di X uno e un solo elemento di Y.

Definizione 1.17. Sia $f : X \to Y$ un'applicazione, se A è un sottoinsieme di X, si dice **immagine** di A mediante f l'insieme $f(A) = \{f(x) \mid x \in A\}$. Se $B \subseteq Y$, l'insieme $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$ si dice **controimmagine** (o **immagine inversa**) di B, se $B = \{y\} \subseteq Y$ è un singoletto, si scrive $f^{-1}(y)$ invece di $f^{-1}(\{y\})$.

Definizione 1.18. Sia $f : X \to Y$ una funzione. f si dice **iniettiva** se $\forall x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implica che $x_1 = x_2$. f si dice **surgettiva** (o **suriettiva**) se $f(X) = Y$. f si dice **bigettiva** o una **corrispondenza biunivoca** o una **bigezione** se è iniettiva e suriettiva.

Quindi f è iniettiva se e solo se elementi distinti di X hanno immagini distinte, ovvero se e solo se la controimmagine di ogni elemento di Y contiene al più un elemento di X. f è surgettiva se e solo se per ogni $y \in Y$ esiste almeno un $x \in X$ tale che $f(x) = y$, ovvero se e solo se la controimmagine di ogni elemento di Y è non vuota. Infine f è bigettiva se e solo se $\forall y \in Y$ $\exists! x \in X$ tale che $y = f(x)$.

Definizione 1.19. Sia $f : X \to Y$ una funzione, il **grafico** di f è l'insieme

$$\Gamma_f := \{(x, y) \in X \times Y : \ y = f(x)\},$$

cioè la definizione di f come relazione.

Alcuni esempi di funzioni importanti.

Definizione 1.20. Una funzione $f : X \to Y$ è **costante** se $f(X)$ è un singoletto, cioè $f(X) = \{y_0\}$ per un $y_0 \in Y$ fissato. La **funzione identità** su un insieme X è la funzione $\mathrm{id}_X : X \to X$ tale che $\mathrm{id}_X(x) = x$ $\forall x \in X$. Data una funzione $f : X \to Y$ e un sottoinsieme $A \subseteq X$, la **restrizione** di f ad A è la funzione $f|_A : A \to Y$ tale che $f|_A(x) = f(x)$ $\forall x \in A$. Dati due insiemi $A \subseteq X$, la funzione **inclusione** di A in X è la funzione $\iota_A(x) = x$ $\forall x \in A$.

La funzione identità è sempre una funzione bigettiva. Una funzione costante $f : X \to Y$ non è iniettiva se X ha almeno due elementi e non è surgettiva se X ha almeno due elementi. Data una funzione $f : X \to Y$ si può sempre ottenere una funzione surgettiva, restringendo il codominio all'immagine. Cioè la funzione $f : X \to f(X)$ è surgettiva.

Esempio 1.21. (i) La funzione $f : \mathbb{N} \to \mathbb{N}$ tale che $f(x) = x^2$ è iniettiva, ma non suriettiva.
(ii) La funzione $g : \mathbb{Z} \to \mathbb{N}$ tale che $g(x) = x^2$ non è iniettiva e non è suriettiva.
(iii) La funzione h : {regioni d'Italia} $\to$ {città d'Italia} che associa ad ogni regione il suo capoluogo di regione è iniettiva, ma non suriettiva.
(iv) La funzione φ : {parole della lingua italiana} $\to \{A, B, \ldots, Z\}$ che associa ad ogni parola la sua lettera iniziale è suriettiva, ma non iniettiva.

Esempio 1.22. La funzione *parte intera* $\mathrm{PI} : \mathbb{R} \to \mathbb{R}$ è definita da

$$\forall x \in \mathbb{R}. \forall n \in \mathbb{Z} \ n \leq x \Longrightarrow n \leq \mathrm{PI}(x).$$

Cioè $\mathrm{PI}(x)$ è il più grande intero $\leq x$. Ad esempio, $\mathrm{PI}(\frac{1}{2}) = 0$ e $\mathrm{PI}(-\frac{1}{2}) = -1$. Si ha che $\mathrm{PI}(\mathbb{R}) = \mathbb{Z}$, $\mathrm{PI}|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$. La funzione parte intera non è iniettiva e non è surgettiva. Useremo spesso la notazione $[-]$ oppure $\lfloor - \rfloor$per indicare la funzione parte intera $\mathrm{PI}(-)$.

La funzione *parte frazionaria* $\{-\} : \mathbb{R} \to [0, 1)$ è definita da $\{x\} = x - [x]$. É una funzione surgettiva, ma non iniettiva.

1.2.1 Composizione di funzioni

Salvo diversamente indicato, per il resto del capitolo tutti gli insiemi considerati sono non vuoti.

Definizione 1.23. Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni (tali che il dominio di g coincide con il codominio di f). La **composizione** (o **funzione composta**) di f e g è la funzione $g \circ f : X \to Z$ definita da $(g \circ f)(x) = g(f(x))\ \forall x \in X$. Con la notazione delle relazioni, la composta si scrive come

$$g \circ f = \{(x, z) \in X \times Z : \ \exists y \in Y.\ ((x, y) \in f) \wedge ((y, z) \in g)\}.$$

La composizione di applicazioni soddisfa la *proprietà associativa*. Date $f : X \to Y$, $g : Y \to Z$, e $h : Z \to W$ si ha

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

Inoltre, la funzione identità è *neutra* rispetto alla composizione $\mathrm{id}_Y \circ f = f$ e $f \circ \mathrm{id}_X = f$. Le verifiche sono facili ed sono lasciate per esercizio.

Osservazione 1.24. La composizione di applicazioni non verifica (in generale) la *proprietà commutativa*. Un primo problema è che date $f : X \to Y$ e $g : Y \to Z$ la composizione $f \circ g$ non è definita. Infatti la funzione f non si può applicare agli elementi della forma $g(x)$ perchè appartengono all'insieme Z, mentre il dominio di f è l'insieme X.

Anche nel caso in cui entrambe le composizioni $g \circ f$ e $f \circ g$ risultino definite (cioè se $X = Z$), si ha in generale

$$g \circ f \neq f \circ g.$$

A titolo di esempio si consideri $X = Y = Z = \mathbb{R}$ e le funzioni $f, g : \mathbb{R} \to \mathbb{R}$ tali che $f(x) = x^2$ e $g(x) = -x$. Le due composizioni sono $(g \circ f)(x) = -x^2$ e $(f \circ g)(x) = (-x)^2 = x^2$, che sono due funzioni distinte: ad esempio $(g \circ f)(2) = -4 \neq 4 = (f \circ g)(2)$.

Proviamo ora queste proprietà della composizione.

Proposizione 1.25. *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni. Allora*
(i) se f e g sono iniettive allora $g \circ f$ è iniettiva;
(ii) se f e g sono surgettive allora $g \circ f$ è surgettiva;
(iii) se f e g sono bigettive allora $g \circ f$ è bigettiva.

Dimostrazione. (i) Siano f e g iniettive, se x e $x' \in X$, e $(g \circ f)(x) = (g \circ f)(x')$ per l'iniettività di g , $g(f(x)) = g(f(x'))$ implica $f(x) = f(x')$ ed essendo f iniettiva si ha $x = x'$.

(ii) Se $z \in Z$ esiste $y \in Y$ tale che $g(y) = z$, ma, essendo anche f surgettiva, esiste $x \in X$ tale che $f(x) = y$, quindi $(g \circ f)(x) = g(f(x)) = z$, cioè $g \circ f$ è surgettiva.

(iii) Discende direttamente da i) e ii).

□

Proposizione 1.26. *Siano $f : X \to Y$ e $g : Y \to Z$ due applicazioni. Allora*
(i) se $g \circ f$ è iniettiva allora f è iniettiva;
(ii) se $g \circ f$ è surgettiva allora g è surgettiva;
(iii) se $g \circ f$ è bigettiva allora f è iniettiva e g è surgettiva.

Dimostrazione. (i) Siano x e $x' \in X$, se $f(x) = f(x')$ per l'iniettività di $g \circ f$, abbiamo che $(g \circ f)(x) = (g \circ f)(x')$ implica $x = x'$. Quindi f è iniettiva.
(ii) Se $z \in Z$ esiste $x \in X$ tale che $(g \circ f)(x) = z$, e, posto $y = f(x)$, si ha $g(y) = z$ quindi g è surgettiva.
(iii) Discende direttamente da i) e ii).

□

Definizione 1.27. Sia $f : X \to Y$ un'applicazione.
(i) f si dice **invertibile a sinistra** se esiste un'applicazione $g : Y \to X$ tale che $g \circ f = \mathrm{id}_X$. L'applicazione g viene detta **inversa sinistra** di f.
(ii) f si dice **invertibile a destra** se esiste un'applicazione $h : Y \to X$ tale che $f \circ h = \mathrm{id}_Y$. L'applicazione h viene detta **inversa destra** di f.
(iii) f si dice **invertibile** se esiste un'applicazione $t : Y \to X$ tale che $f \circ t = \mathrm{id}_Y$ e $t \circ f = \mathrm{id}_X$. L'applicazione t viene detta **inversa** di f e si denota con f^{-1}. Reciprocamente f è la funzione inversa di t.

Osservazione 1.28. Osserviamo per prima cosa che l'applicazione inversa (se esiste) è unica. Sia $f : X \to Y$ e siano $t_1, t_2 : Y \to X$ due inverse di f. Allora si ha

$$t_1 = t_1 \circ \mathrm{id}_Y = t_1 \circ (f \circ t_2) = (t_1 \circ f) \circ t_2 = \mathrm{id}_X \circ t_2 = t_2.$$

L'unicità invece non vale per inverse destre e sinistre. Una funzione può avere più inverse destre o più inverse sinistre.

Esempio 1.29. Consideriamo gli insiemi $X = \{1, 2, 3\}$ e $Y = \{a, b, c, d\}$.
(i) Sia $\varphi : X \to Y$ la funzione data da $\varphi(1) = a$, $\varphi(2) = b$, e $\varphi(3) = d$. Allora le funzioni $\psi_1, \psi_2 : Y \to X$ seguenti sono due inverse sinistre (distinte) di φ:

$$\psi_1(a) = 1,\ \psi_1(b) = 2,\ \psi_1(c) = 1,\ \psi_1(d) = 3;$$
$$\psi_2(a) = 1,\ \psi_2(b) = 2,\ \psi_2(c) = 2,\ \psi_2(d) = 3.$$

(ii) Sia $\eta : Y \to X$ la funzione data da $\eta(a) = 1$, $\eta(b) = 1$, $\eta(c) = 2$, $\eta(d) = 3$. Allora le funzioni $\mu_1, \mu_2 : X \to Y$ seguenti sono due inverse destre (distinte) di η:

$$\mu_1(1) = a,\ \mu_1(2) = c,\ \mu_1(3) = d,$$
$$\mu_2(1) = b,\ \mu_2(2) = c,\ \mu_2(3) = d.$$

Teorema 1.30. *Sia $f : X \to Y$ un'applicazione. Allora f è iniettiva se e solo se f è invertibile a sinistra.*

Dimostrazione. "$\Leftarrow$" Siccome f è invertibile a sinistra, esiste $g : Y \to X$ tale che $g \circ f = \mathrm{id}_X$. L'iniettività di f segue dalla Proposizione 1.26.
"$\Rightarrow$" Fissiamo un elemento arbitrario $x_0 \in X$ e definiamo una funzione $g : Y \to X$. Se $y \in f(X)$, poniamo $g(y) = x$, dove x è l'unico elemento di X tale che $f(x) = y$. Se $y \in Y \setminus f(X)$ poniamo $g(y) = x_0$. Si verifica facilmente che $g \circ f = \mathrm{id}_X$. □

Dalla Proposizione 1.26 segue anche facilmente che se f è invertibile a destra allora è surgettiva. Tuttavia il viceversa è più complicato e richiede l'uso del cosidetto *assioma della scelta*.

Assioma della scelta. *Sia $\{A_i\}_{i \in I}$ una famiglia di insiemi non vuoti con $I \neq \emptyset$. Allora esiste una funzione $\psi : I \to \bigcup_{i \in I} A_i$ con la proprietà $\psi(i) \in A_i$ per ogni $i \in I$. La funzione ψ è detta* funzione di scelta.

Nonostante la verità dell'assioma di scelta possa sembrare evidente, esso non è dimostrabile a partire dagli altri assiomi della teoria degli insiemi che sono comunemente assunti. Usiamo l'assioma di scelta per dimostrare la seguente proprietà (che di fatto è un'equivalente formulazione dell'assioma di scelta).

Teorema 1.31. *Sia $f : X \to Y$ un'applicazione. Allora f è surgettiva se e solo se f è invertibile a destra.*

Dimostrazione. "$\Leftarrow$" Siccome f è invertibile a destra, esiste $g : Y \to X$ tale che $f \circ g = \mathrm{id}_Y$. Abbiamo già osservato che la suriettività di f segue dalla Proposizione 1.26.
"$\Rightarrow$" Assumiamo che f sia surgettiva. Allora per ogni $y \in Y$ la controimmagine $f^{-1}(y)$ è un insieme non vuoto. Consideriamo quindi la famiglia di insiemi non vuoti $A_y = f^{-1}(y)$ indiciata sull'insieme $I = Y$. Per l'assioma della scelta, esiste una funzione $\psi : I \to \bigcup_{y \in Y} A_y$ tale che $\psi(y) \in f^{-1}(y)$ per ogni $y \in Y$. Definiamo $g(y) = \psi(y)$. Per costruzione si ha che $(f \circ g)(y) = f(g(y)) = y$ siccome $g(y) \in f^{-1}(y)$. Quindi $f \circ g = \mathrm{id}_Y$. □

Concludiamo con il seguente importante risultato.

Teorema 1.32. *Sia $f : X \to Y$ una funzione. Allora f è bigettiva se e solo se f è invertibile.*

Dimostrazione. "$\Leftarrow$" Se f è invertibile, ha sia inversa destra che inversa sinistra. La bigettività segue combinando i due teoremi precedenti.
"$\Rightarrow$" Sia f bigettiva. Allora per ogni $y \in Y$ esiste un unico $x \in X$ tale che $f(x) = y$. Definiamo $g(y) = x$. Allora g è una funzione $Y \to X$ e si ha che

$$\forall x \in X \ (g \circ f)(x) = g(f(x)) = x$$
$$\forall y \in Y \ (f \circ g)(y) = f(g(y)) = y.$$

Quindi g è l'inversa di f (che ricordiamo essere unica). □

Infine, menzioniamo che la composizione di funzioni non è l'unico modo per "produrre una nuova funzione a partire da due vecchie". Ad esempio, se $f : X \to Y$ e $g : Z \to W$ sono due funzioni, definiamo il **prodotto** $f \times g$ come la funzione

$$f \times g : X \times Z \to Y \times W, \quad (f \times g)(x, z) = (f(x), g(z)).$$

Lasciamo la verifica delle seguenti proprietà come esercizio per il lettore.

Esercizio 1.33. Siano $f : X \to Y$ e $g : Z \to W$ sono due funzioni. Allora

(i) se f e g sono iniettive allora $f \times g$ è iniettiva;
(ii) se f e g sono surgettive allora $f \times g$ è surgettiva;
(iii) se f e g sono bigettive allora $f \times g$ è bigettiva.

2 Numeri interi

In questo capitolo ci dedichiamo ad uno studio più approfondito delle proprietà e dei teoremi che riguardano i numeri naturali $\mathbb{N}$ e i numeri interi $\mathbb{Z}$.

2.1 Principio d'induzione

L'insieme dei **numeri naturali** $\mathbb{N} = \{0, 1, 2, 3 \dots\}$ è uno dei concetti primitivi della matematica, la cui esistenza diamo per buona. Esso può essere definito mediante gli *assiomi di Peano* stabiliti dal matematico italiano Peano. Tra di essi figura il **principio di induzione aritmetica** che è spesso utile in alcuni tipi di dimostrazioni.

Principio di induzione (prima forma). *Sia $\mathcal{P}$ una affermazione sui numeri naturali. Supponiamo siano soddisfatte le seguenti due condizioni:*
(i) *$\mathcal{P}(0)$ è vera;*
(ii) *per ogni naturale $n > 0$ se $\mathcal{P}(n-1)$ è vera allora $\mathcal{P}(n)$ è vera.*
Allora $\mathcal{P}(n)$ è vera per ogni numero naturale n.

La parte (i) viene detta *passo base*, mentre la parte (ii) viene detta *passo induttivo*. Il principio di induzione può essere anche riformulato nella maniera seguente (equivalente alla precedente) e applicato ai numeri interi $\mathbb{Z}$ maggiori o uguali di un intero fissato n_0.

Principio di induzione (seconda forma). *Sia $n_0 \in \mathbb{Z}$ fissato e sia $\mathcal{P}$ una affermazione sui numeri interi $n \geq n_0$. Supponiamo siano soddisfatte le seguenti due condizioni:*
(i) *$\mathcal{P}(n_0)$ è vera;*
(ii) *per ogni intero $n > n_0$ se $\mathcal{P}(n-1)$ è vera allora $\mathcal{P}(n)$ è vera.*
Allora $\mathcal{P}(n)$ è vera per ogni numero intero $n \geq n_0$.

Esempio 2.1. Proviamo usando il principio di induzione (prima forma) la formula per la somma dei primi n numeri interi: $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. L'affermazione $\mathcal{P}$ consiste nella formula stessa, cioè

$$\mathcal{P}(n) = \text{“ } 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}\text{”} .$$

Il passo base è $\mathcal{P}(0) =$ “$0 = 0$”, che è banalmente vero. Per il passo induttivo, supponiamo vera la formula $\mathcal{P}(n-1) =$ “ $0 + 1 + 2 + \cdots + (n-1) = \frac{(n-1)n}{2}$”. Aggiungendo n ad entrambi i membri dell'uguaglianza precedente, si ottiene ancora una uguaglianza vera, cioè

$$0 + 1 + 2 + \cdots + (n-1) + n = \frac{(n-1)n}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n(n+1)}{2},$$

che è l'affermazione $\mathcal{P}(n)$. Questo completa il passo induttivo e quindi la dimostrazione: $\mathcal{P}(n)$ è vera $\forall n \in \mathbb{N}$.

Nel seguito useremo il principio di induzione più liberamente, senza specificare ogni volta qual è l'affermazione $\mathcal{P}$, che quasi sempre sarà la formula che vogliamo dimostrare. A titolo esplicativo presentiamo alcuni esempi.

Esempio 2.2. (i) Proviamo che per ogni numero reale q, $q \neq 1$ la somma delle sue prime n potenze ($n = 0, 1 \dots$) è data dalla formula

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

L'affermazione è banalmente vera per $n = 0$, supponiamola vera per $n - 1$ cioè

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

e proviamola per n, ovvero aggiungiamo ai due membri dell'uguaglianza q^n, avremo che

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

da cui la tesi.

(ii) Proviamo che per ogni numero intero $n \geq 2$ si ha

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

L'affermazione è vera per $n = 2$, infatti $1 - \frac{1}{2} = \frac{1}{2}$, supponiamola vera per $n - 1$ cioè

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

Moltiplicando ambo i membri dell'uguaglianza per $1 - \frac{1}{n}$ si ottiene la tesi.

Vediamo una terza formulazione (equivalente) del principio di induzione.

Principio di induzione (terza forma). *Sia $n_0 \in \mathbb{Z}$ e sia $\mathcal{P}$ una affermazione sui numeri interi $n \geq n_0$. Supponiamo siano soddisfatte le seguenti due condizioni:*

(i) *$\mathcal{P}(n_0)$ è vera;*

(ii) per ogni intero $n > n_0$ se $\mathcal{P}(m)$ è vera per ogni intero m tale che $n_0 \leq m < n$, allora $\mathcal{P}(n)$ è vera.

Allora $\mathcal{P}(n)$ è vera per ogni numero intero $n \geq n_0$.

Si può provare che il principio di induzione è equivalente al **principio del minimo**.

Principio del minimo. *Sia $A \subseteq \mathbb{N}$ un sottoinsieme non vuoto. Allora $\exists k \in A$ tale che $\forall x \in A$ si ha $x \geq k$. L'elemento k viene detto* minimo *di A.*

2.2 Algoritmo euclideo

Definizione 2.3. Siano $a, b \in \mathbb{Z}$. Il numero a si dice **divisore** di b e b si dice **multiplo** di a (alternativamente si dice anche che a **divide** b) se esiste $k \in \mathbb{Z}$ tale che $b = ak$. In simboli, scriviamo $a \mid b$. Se a non è divisore di b scriviamo $a \nmid b$. In particolare, a si dice **pari** se $2 \mid a$, a si dice **dispari** se $2 \nmid b$.

Esempio 2.4. Abbiamo $2 \mid 4$, ma anche $-2 \mid 4$, $2 \mid -4$, e $-2 \mid -4$. Osserviamo che $3 \mid 0$, $1 \mid 3$ ma $0 \nmid 3$ e $3 \nmid 1$. In generale, dato $n \in \mathbb{Z} \setminus \{0\}$ valgono le seguenti

$$n \mid 0, \quad 0 \nmid n, \quad 1 \mid n, \quad 0 \mid 0.$$

Teorema 2.5 (Divisione Euclidea)**.** *Siano $a, b \in \mathbb{Z}$, $a > 0$ allora $\exists!$ $q, r \in \mathbb{Z}$ tali che $0 \leq r < a$ e*

$$b = a \cdot q + r.$$

Dimostrazione. "Esistenza". Consideriamo due casi.

- $b \geq 0$. Proviamo l'esistenza di q e r per induzione (terza forma) su b. Se $b = 0$, possiamo scrivere $b = a \cdot 0 + 0$ e quindi scegliamo $q = r = 0$. Per il passo induttivo, supponiamo adesso che per ogni $n \leq b$ la tesi sia verificata (cioè $\exists!$ $q, r \in \mathbb{Z}$ tali che $0 \leq r < a$ e $n = a \cdot q + r$) e proviamo che la tesi vale per $b + 1$. Se $b + 1 < a$ ci basta scegliere $q = 0$ e $r = b + 1$, infatti $b + 1 = a \cdot 0 + (n + 1)$. Se $b + 1 \geq a$, consideriamo il numero $b + 1 - a$. Si ha che $0 \leq b + 1 - a \leq b$ e quindi per ipotesi induttiva esistono $q_1, r_1 \in \mathbb{Z}$ con $r_1 < a$ tali che $b + 1 - a = a \cdot q_1 + r_1$. Possiamo quindi scrivere

  $$b + 1 = a \cdot q_1 + r_1 + a = a(q_1 + 1) + r_1$$

  e scegliamo pertanto $q = q_1 + 1$ e $r = r_1$ che soddisfano le richieste.

- $b < 0$. In questo caso $-b > 0$ e quindi per quanto provato al punto precedente esistono $q', r' \in \mathbb{Z}$ tali che $0 \leq r' < a$ e $-b = a \cdot q' + r'$. Se $r' = 0$ allora possiamo scrivere $b = a \cdot (-q') + 0$ e abbiamo finito (cioè scegliamo $q = -q'$ e $r = r' = 0$). Se invece $r' \neq 0$ scriviamo

  $$b = -a \cdot q' - r' = -q' \cdot a + a - a - r' = a(-q' - 1) + a - r'.$$

  Scegliamo quindi $q = -q' - 1$ e $r = a - r'$. Si ha per costruzione che $0 \leq r < a$ e $b = a \cdot q + r$.

"Unicità". Supponiamo che esistano $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tali che $0 \leq r_1, r_2 < a$, e

$$b = a \cdot q_1 + r_1 = a \cdot q_2 + r_2.$$

Proviamo che $q_1 = q_2$ e $r_1 = r_2$. Senza perdita di generalità possiamo supporre $r_2 \geq r_1$. Eguagliando entrambi i membri della doppia scrittura di b otteniamo

$$a(q_1 - q_2) = r_2 - r_1 \geq 0$$

Quindi $0 \leq a(q_1 - q_2) < a$ (siccome sia r_1 che r_2 sono minori di a). Questo implica che $q_1 - q_2 = 0$ e cioè $q_1 = q_2$. Infine otteniamo $r_2 - r_1 = a(q_1 - q_2) = 0$ e cioè $r_1 = r_2$. □

Osservazione 2.6. Dati $a, b \in \mathbb{Z}$ con $a > 0$, si ha che a divide b se e solo se il resto della divisione euclidea di b per a è nullo.

Esempio 2.7. (i) Dati $b = 24$ e $a = 13$ la divisione euclidea di b per a è $24 = 1 \cdot 13 + 11$ con $q = 1$ e $r = 11$. Si noti che $0 \leq 11 < 13$.

(ii) Dati $b = -11$ e $a = 5$ la divisione euclidea di b per a è $-11 = -3 \cdot 5 + 4$ con $q = -3$ e $r = 4$. La scrittura $-11 = -2 \cdot 5 - 1$ non è la divisione euclidea in quanto il resto -1 non soddisfa $0 \leq -1 < 5$.

Definizione 2.8. Siano $a, b \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$.

(i) Il **massimo comun divisore** $\mathrm{MCD}(a, b)$ di a e b è il più grande divisore positivo comune di a e b, cioè

$$\mathrm{MCD}(a, b) = \max\{n \in \mathbb{N} : \ n \mid a, \ n \mid b\}.$$

Se $\mathrm{MCD}(a, b) = 1$, a e b si dicono **primi tra loro** o **coprimi**.

(ii) Il **minimo comune multiplo** $\mathrm{mcm}(a, b)$ di a, b è il più piccolo multiplo positivo comune di a e b, cioè

$$\mathrm{mcm}(a, b) = \min\{n \in \mathbb{N} : \ a \mid n, \ b \mid n\}.$$

Osservazione 2.9. Diamo una definizione equivalente del massimo comun divisore[2]. Un numero $d \in \mathbb{N}$ è il massimo comun divisore di a e b se e solo se verifica le seguenti condizioni:

(i) $d \mid a$, $d \mid b$;

(ii) Se $c \in \mathbb{N}$ è tale che $c \mid a$, $c \mid b$ allora $c \mid d$.

Osservazione 2.10. Valgono le seguenti proprietà:

- $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$;
- $\mathrm{MCD}(a, b) = a \iff a \mid b$;
- $\mathrm{MCD}(a, 0) = a$

Osservazione 2.11. Osserviamo che il minimo comune multiplo si può calcolare facilmente a partire dal massimo comun divisore. Infatti abbiamo

$$\mathrm{mcm}(a, b) = \frac{ab}{\mathrm{MCD}(a, b)}.$$

Pertanto nel proseguo ci limiteremo a cercare un metodo efficace per determinare il massimo comun divisore.

La soluzione del problema di trovare il massimo comun divisore di due numeri è stata data da Euclide (300 a.c. circa) utilizzando la divisione euclidea. Supponiamo di avere due interi positivi a e b con $a \leq b$. Se a divide b allora a è il massimo comun divisore di a e b. Se a non divide b, sottraendo continuamente il minore dei due numeri dal maggiore resterà infine un numero che dividerà quello che lo precede, questo numero è il massimo comun divisore di a e b.

Esempio 2.12. Calcoliamo il massimo comun divisore di 78 e 32. Sottraiamo 32 da 78 e otteniamo 46 e 32, sottraendo 32 da 46 si ha 14 e 32, sottraiamo 14 da 32 e avremo 18 e 14, sottraendo 14 da 18 abbiamo 4 e 14, sottraiamo 4 da 14 otteniamo 10 e 4 sottraiamo 4 da 10,

[2]L'equivalenza delle due definizione dipende dal fatto che per un sottoinsieme finito e non vuoto $Y \subseteq \mathbb{N}$ si ha che $\max Y = \sup Y$

otteniamo 6 e 4, sottraiamo 4 da 6 e otteniamo 2 e 4, ora 2 divide 4 quindi 2 è il massimo comun divisore di 78 e 32.

Possiamo descrivere l'algoritmo in forma compatta usando il teorema di divisione:

$$\begin{aligned} 78 &= 32 \cdot 2 + 14; \\ 32 &= 14 \cdot 2 + 4; \\ 14 &= 4 \cdot 3 + 2; \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

E' facile vedere che 2 è il massimo comun divisore di 32 e 78 ma possiamo motivare in questo modo: 2 divide 4, quindi divide $4 \cdot 3 + 2 = 14$, quindi $14 \cdot 2 + 4 = 32$, quindi $32 \cdot 2 + 14 = 78$. Perciò 2 è divisore comune di 32 e 78. Inoltre, se c è divisore comune di 32 e 78 allora c divide 14 (per la prima equazione), quindi 14 e 32, quindi 4 (dalla seconda equazione), quindi 4 e 14, quindi 2 (dalla terza equazione). Quindi c divide 2.

Teorema 2.13 (Algoritmo Euclideo)**.** *Siano $a, b \in \mathbb{Z}$ con $a > 0$. Il massimo comun divisore di a e b si determina con la seguente serie di divisioni successive:*

$$\begin{aligned} b &= a \cdot q_1 + r_1, \\ a &= q_2 \cdot r_1 + r_2, \\ r_1 &= q_3 \cdot r_2 + r_3, \\ r_2 &= q_4 \cdot r_3 + r_4, \\ &\vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n, \end{aligned}$$

dove $q_i, r_i \in \mathbb{Z}$ sono tali che $0 < r_n < r_{n-1} < r_{n-2} < \cdots < r_3 < r_2 < r_1 < a$. In tal caso $\mathrm{MCD}(a, b) = r_n$.

Dimostrazione. Prima di tutto osserviamo che la procedura termina in quanto la successione di resti $r_1, r_2, \ldots$ è strettamente decrescente e per il principio del minimo (vedi pagina 16) ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette minimo. Pertanto $\exists n \in \mathbb{N}^*$ tale che $r_n \neq 0$ e $r_{n+1} = 0$. Mostriamo che $\mathrm{MCD}(a, b) = r_n$. Per fare ciò grazie all'Osservazione 2.9 è sufficiente provare che:

(i) $r_n \mid a$, $r_n \mid b$;
(ii) Se $c \in \mathbb{N}^*$ è tale che $c \mid a$, $c \mid b$ allora $c \mid r_n$.

Per la (i), basta osservare che partendo dal fondo delle divisioni successive si ottiene $r_n \mid r_{n-1}$, e siccome $r_{n-2} = q_n \cdot r_{n-1} + r_n$ si ha anche $r_n \mid r_{n-2}$ e così via. Fino ad ottenere che $r_n \mid a$ e $r_n \mid b$.

Per dimostrare la (ii), prendiamo $c \in \mathbb{N}$ tale che $c \mid a$ e $c \mid b$, cioè $a = c \cdot a'$ e $b = c \cdot b'$ per qualche $a', b' \in \mathbb{Z}$. Questa volta consideriamo le divisioni successive partendo dall'inizio e

otteniamo

$$\begin{aligned} r_1 &= b - a \cdot q_1 = c \cdot b' - c \cdot a' q_1 = c(b' - a' \cdot q_1) \implies c \mid r_1 \\ r_2 &= a - r_1 \cdot q_2 \implies c \mid r_2 \\ &\vdots \end{aligned}$$

Fino ad ottenere dall'ultima divisione che $c \mid r_n$. □

Esempio 2.14. Calcoliamo MCD$(235, 100)$ con l'algoritmo euclideo.

$$\begin{aligned} 235 &= 2 \cdot 100 + 35, \\ 100 &= 2 \cdot 35 + 30, \\ 35 &= 1 \cdot 30 + 5, \\ 30 &= 6 \cdot 5 + 0. \end{aligned}$$

L'ultimo resto non nullo è $r_3 = 5$, pertanto MCD$(235, 100) = 5$.

Esempio 2.15. Calcoliamo MCD$(963, 657)$ con l'algoritmo euclideo.

$$\begin{aligned} 963 &= 1 \cdot 657 + 306, \\ 657 &= 2 \cdot 306 + 45, \\ 306 &= 6 \cdot 45 + 36, \\ 45 &= 1 \cdot 36 + 9, \\ 36 &= 4 \cdot 9 + 0. \end{aligned}$$

L'ultimo resto non nullo è $r_4 = 9$, pertanto MCD$(963, 657) = 9$.

Teorema 2.16 (Identità di Bézout)**.** *Siano $a, b \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$ e sia $d = \text{MCD}(a, b)$. Allora $\exists x, y \in \mathbb{Z}$ tali che*

$$d = ax + by.$$

I numeri x e y dell'identità di Bézout si possono ricavare dall'algoritmo euclideo ripercorrendo i passaggi a ritroso. Vediamo come nei seguenti esempi.

Esempio 2.17. Siano $a = 100$ e $b = 235$. Ripercorriamo i passaggi dell'algoritmo euclideo a ritroso fino a ritrovare a e b:

$$\begin{aligned} 5 &= 35 - 1 \cdot 30 \\ &= 35 - 1 \cdot (100 - 2 \cdot 35) \\ &= 3 \cdot 35 - 1 \cdot 100 \\ &= 3 \cdot (235 - 2 \cdot 100) - 1 \cdot 100 \\ &= 3 \cdot 235 - 7 \cdot 100. \end{aligned}$$

Pertanto $x = -7$ e $y = 3$.

Esempio 2.18. Siano $a = 963$ e $b = 657$. Ripercorriamo i passaggi dell'algoritmo euclideo a ritroso fino a ritrovare a e b:

$$\begin{aligned} 9 &= 45 - 36 \\ &= 45 - (306 - 45 \cdot 6) \\ &= -306 + 45 \cdot 7 \\ &= -306 + (657 - 306 \cdot 2) \cdot 7 \\ &= 657 - 963 + (657 - (963 - 657) \cdot 2) \cdot 7 \\ &= -15 \cdot 963 + 22 \cdot 567. \end{aligned}$$

Pertanto $x = -15$ e $y = 22$.

2.3 Equazioni diofantee lineari

Ci occupiamo adesso del problema di trovare le soluzioni intere $x, y \in \mathbb{Z}$ di un'equazione di primo grado della forma $ax + by = c$. Trovare le soluzioni reali di una tale equazione è facile, per esempio se $b \neq 0$ basta considerare le coppie della forma $\left(x, \frac{c-ax}{b}\right)$ al variare di $x \in \mathbb{R}$. Per le soluzioni intere questo approccio non funziona, in quanto il numero $\frac{c-ax}{b}$ non è necessariamente un intero anche se $x \in \mathbb{Z}$. Vediamo come risolvere questo problema utilizzando l'algoritmo euclideo e gli strumenti introdotti finora.

Teorema 2.19. *Siano $a, b, c \in \mathbb{Z}$. Allora l'equazione*

$$ax + by = c$$

ammette soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ se e solo se $\mathrm{MCD}(a, b) \mid c$.

Dimostrazione. "$\Leftarrow$" Sia $d = \mathrm{MCD}(a, b)$. Siccome $d \mid c$ possiamo scrivere $c = \alpha \cdot d$ con $\alpha \in \mathbb{Z}$. Per il Teorema di Bézout esistono $x', y' \in \mathbb{Z}$ tali che $ax' + by' = d$. Moltiplicando per α si ottiene

$$a\alpha x' + b\alpha y' = \alpha d = c.$$

Pertanto scegliamo $x = \alpha x' \in \mathbb{Z}$ e $y = \alpha y' \in \mathbb{Z}$ e si ottiene $ax + by = c$.

"$\Rightarrow$" Sia $d = \mathrm{MCD}(a, b)$ e proviamo che $d \mid c$. Siccome $d \mid a$ e $d \mid b$, possiamo scrivere $a = d\alpha$ e $b = d\beta$ con $\alpha, \beta \in \mathbb{Z}$. Prendiamo $x, y \in \mathbb{Z}$ una soluzione dell'equazione, cioè tali che $c = ax + by$. Riscriviamo l'equazione come

$$c = d\alpha x + d\beta y = d(\alpha x + \beta y),$$

il che mostra che $d \mid c$. □

Il teorema precedente ci da una condizione necessaria e sufficiente affinché un'equazione diofantea della forma $ax + by = c$ abbia soluzioni. Il tal caso come facciamo a trovare le soluzioni? Facciamo prima un'osservazione.

Osservazione 2.20. Un'equazione diofantea $ax + by = c$ ammette soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ se e solo se $\text{MCD}(a, b) \mid c$. Supponiamo quindi che $d = \text{MCD}(a, b) \mid c$ e scriviamo $a = d \cdot \alpha$, $b = d \cdot \beta$, e $c = d \cdot \gamma$ con $\alpha, \beta, \gamma \in \mathbb{Z}$. Dati due interi $x, y \in \mathbb{Z}$ si ha

$$ax + by = c \iff d\alpha x + d\beta y = d\gamma \iff \alpha x + \beta y = \gamma.$$

Quindi le soluzioni dell'equazione $ax + by = c$ coincidono con le soluzioni di $\alpha x + \beta y = \gamma$, dove adesso $\text{MCD}(\alpha, \beta) = 1$.

Grazie all'osservazione precedente, possiamo ridurci a studiare le equazioni diofantee della forma $ax + by = c$ con $\text{MCD}(a, b) = 1$. Per trovare le soluzioni di queste equazioni possiamo utilizzare l'identità di Bézout. Vediamo un esempio.

Esempio 2.21. Troviamo una soluzione intera $x, y \in \mathbb{Z}$ dell'equazione $21x + 13y = 5$. Per garantire che una tale equazione abbia soluzioni, calcoliamo prima il massimo comun divisore di 21 e 13 con l'algoritmo euclideo.

$$\begin{aligned} 21 &= 1 \cdot 13 + 8, \\ 13 &= 1 \cdot 8 + 5, \\ 8 &= 1 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Quindi $\text{MCD}(21, 13) = 1$, e siccome $1 \mid 5$, l'equazione ha soluzioni. Per trovarle, risolviamo prima l'equazione associata in cui sostituiamo il termine noto con $\text{MCD}(21, 13)$:

$$21x + 13y = 1.$$

Le soluzioni di quest'ultima equazione si possono trovare grazie all'identità di Bézout, ripercorrendo i passaggi dell'algoritmo euclideo a ritroso. Otteniamo quindi $1 = -8 \cdot 13 + 5 \cdot 21$. Moltiplicando per 5 quest'ultima equazione otteniamo $5 = -40 \cdot 13 + 25 \cdot 21$. E quindi una soluzione è data da $x = 25$, $y = -40$.

Procedendo come nell'esempio precedente possiamo sempre trovare almeno una soluzione di $ax + by = c$, ma come trovare tutte le soluzioni? La risposta è nella proposizione seguente.

Proposizione 2.22. *Sia $(x_0, y_0) \in \mathbb{Z}^2$ una soluzione dell'equazione $ax + by = c$, dove $a, b, c \in \mathbb{Z}$ con $\text{MCD}(a, b) = 1$. Allora tutte le soluzioni di $ax + by = c$ sono della forma*

$$(x, y) = (x_0 + bk, y_0 - ak), \quad k \in \mathbb{Z}.$$

Ricapitolando, vediamo come trovare tutte le soluzioni intere dell'equazione diofantea

$$ax + by = c. \tag{3}$$

(i) Calcolare $d = \text{MCD}(a, b)$ e controllare che $d \mid c$.

(ii) Dividere (3) per d, $a = d\alpha$, $b = d\beta$, $c = d\gamma$, ottenendo

$$\alpha x + \beta y = \gamma \tag{4}$$

con $\mathrm{MCD}(\alpha, \beta) = 1$. L'equazione (3) e l'equazione (4) hanno le stesse soluzioni.

(iii) Trovare una soluzione particolare $(x_0, y_0) \in \mathbb{Z}^2$ dell'equazione (4) (per esempio utilizzando l'identità di Bézout).

(iv) Tutte le soluzioni di (4) (e quindi anche di (3)) si scrivono come

$$\begin{cases} x = x_0 + \beta k \\ y = y_0 - \alpha k \end{cases} \qquad \text{al variare di } k \in \mathbb{Z}.$$

Esempio 2.23. Troviamo tutte le soluzioni intere di $175x + 77y = 329$.

(i) Calcolo $\mathrm{MCD}(175, 77)$ con l'algoritmo euclideo.

$$\begin{aligned} 175 &= 2 \cdot 77 + 21, \\ 77 &= 3 \cdot 21 + 14, \\ 21 &= 1 \cdot 14 + 7, \\ 14 &= 2 \cdot 7 + 0. \end{aligned}$$

Si ha quindi che $d = \mathrm{MCD}(175, 77) = 7 \mid 329$. Pertanto l'equazione ha soluzioni.

(ii) Divido l'equazione $175x + 77y = 329$ per 7 e ottengo l'equazione

$$25x + 11y = 47$$

che ha le stesse soluzioni della precedente.

(iii) Troviamo una soluzione particolare $(x_0, y_0) \in \mathbb{Z}^2$. L'identità di Bézout mi dice che $1 = 4 \cdot 25 - 9 \cdot 11$. Pertanto moltiplicando per 47 ottengo la soluzione particolare $x_0 = 47 \cdot 4 = 188$ e $y_0 = 47 \cdot (-9) = -423$. Infatti $47 = 188 \cdot 25 - 423 \cdot 11$.

(iv) Tutte le soluzioni intere di $175x + 77y = 329$ sono quindi

$$\begin{cases} x = 188 + 11k \\ y = -423 - 25k \end{cases} \qquad \text{al variare di } k \in \mathbb{Z}.$$

2.4 Numeri primi e teorema di fattorizzazione unica

Definizione 2.24. Un numero intero $a > 1$ si dice **numero primo** se i suoi soli divisori sono 1 e a, altrimenti $a > 1$ si dice **numero composto**.

Osservazione 2.25. Per convenzione l'elemento $1 \in \mathbb{N}$ non si considera un numero primo. La motivazione principale è che 1 e -1 sono gli unici elementi *invertibili* di $\mathbb{Z}$ rispetto al prodotto.

Lemma 2.26. *Siano $a, b \in \mathbb{Z}$ e sia p un numero primo tale che $p \mid ab$. Allora $p \mid a$ o $p \mid b$.*

Dimostrazione. Supponiamo che $p \nmid a$ e proviamo che necessariamente $p \mid b$. Sappiamo che $p \mid ab$, quindi possiamo scrivere $ab = kp$ con $k \in \mathbb{Z}$. Siccome $p \nmid a$ si ha $\mathrm{MCD}(p, a) = 1$. Per l'identità di Bézout esistono $x, y \in \mathbb{Z}$ tali che $ax + py = 1$. Moltiplicando ambo i membri per b ottengo

$$b = bax + bpy = kpx + bpy = p(kx + by)$$

che mostra che $p \mid b$. □

Teorema 2.27 (Teorema fondamentale dell'aritmetica)**.** *Sia $a \in \mathbb{Z} \setminus \{0, -1, 1\}$ allora a si scrive in modo unico (a meno dell'ordine) come prodotto di un numero finito di numeri primi, cioè*

$$a = \pm p_1^{n_1} \cdots p_r^{n_r}$$

con $p_1, \ldots, p_r$ numeri primi e $n_1, \ldots, n_r \in \mathbb{N}$.

Dimostrazione. "Esistenza". Per prima cosa osserviamo che basta dimostrare la tesi per $a > 0$ (se $a < 0$ si prende la fattorizzazione di $-a > 0$ e si moltiplica per -1). Dimostriamo quindi l'esistenza di una fattorizzazione di $a \geq 2$ come prodotto di numeri primi per induzione. Nel passo base abbiamo $a = 2$ e la tesi è verificata perché 2 è un numero primo.

Per il passo induttivo, supponiamo che la tesi sia vera per ogni intero α tale che $0 < \alpha \leq a$ e mostriamo che vale anche per $a + 1$. Se $a + 1$ è primo, allora non c'è nulla da dimostrare. Se $a+1$ non è primo, allora esistono due interi $b, c \neq 1$ tali che $a+1 = b \cdot c$. In particolare, siccome $b \leq a$ e $c \leq a$ per ipotesi induttiva esistono due fattorizzazioni di b e c

$$b = p_1 \cdots p_s \quad \text{e} \quad c = q_1 \cdots q_r$$

con p_i e q_j numeri primi (non necessariamente distinti). Pertanto $a + 1$ si fattorizza come $a + 1 = p_1 \cdots p_s \cdot q_1 \cdots q_r$.

"Unicità". Siano $a = p_1 \cdots p_s$ e $a = q_1 \cdots q_r$ due fattorizzazioni di a. Mostriamo che le fattorizzazioni coincidono (a meno dell'ordine) e cioè $r = s$ e $p_i = q_i$ per ogni $i = 1, \ldots, s$. Supponiamo senza perdita di generalità che $r \geq s$. Siccome $p_1 \mid a = q_1 \cdots q_r$ per il Lemma 2.26 si ha che p_1 divide (almeno) uno tra $q_1, \ldots, q_r$. A meno di scambiare l'ordine dei q_i possiamo supporre che $p_1 \mid q_1$. Analogamente siccome $p_2 \mid a = q_1 \cdots q_r$, per il Lemma 2.26 si ha $p_2 \mid q_2$. Procedendo in questo modo si conclude che necessariamente $r = s$ e $p_i = q_i$ per ogni $i = 1, \ldots, s$. □

Teorema 2.28 (Euclide)**.** *Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo per assurdo che $p_1, \ldots, p_s$ siano tutti e soli i numeri primi. Consideriamo il numero $N = p_1 \cdots p_s + 1$. Per il Teorema fondamentale dell'aritmetica N dev'essere divisibile per un qualche numero primo. D'altra parte, si vede facilmente che per ogni $i = 1, \ldots, s$ la divisione euclidea di N per p_i da resto 1. Pertanto $p_i \nmid N \ \forall i = 1, \ldots, s$. Contraddizione[3]. □

[3]Si noti che non si può concludere che N sia un numero primo, ma soltanto che nella sua fattorizzazione N contiene un primo diverso da $p_1, \ldots, p_s$.

2.5 Appendice: rappresentazione di un intero in base b

Teorema 2.29 (Teorema di rappresentazione degli interi in base b)**.** *Siano $a, b \in \mathbb{Z}$, $a > 0$ e $b > 1$. Allora esistono $n, c_0, c_1, \ldots, c_n \in \mathbb{N}$ tali che $0 \leq c_i < b$ per ogni $0 \leq i \leq n$ e $c_n > 0$ tali che*

$$a = c_n b^n + \cdots + c_1 b + c_0.$$

Inoltre tale rappresentazione è unica. Diremo quindi che a in base b ha la rappresentazione

$$(a)_b = c_n c_{n-1} \ldots c_1 c_0$$

e che gli interi $c_n, c_{n-1}, \ldots c_1, c_0$ sono le cifre di a in base b.

Esempio 2.30. Vediamo alcune rappresentazioni del numero 2301 (in base 10):

- Poiché $2301 = 2 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0$ si ha $(2301)_{10} = 2301$.
- Poiché $2301 = 1 \cdot 2^{11} + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1$ si ha $(2301)_2 = 100011111101$.
- Poiché $2301 = 3 \cdot 5^4 + 3 \cdot 5^3 + 2 \cdot 5^2 + 1$ si ha $(2301)_5 = 33201$.
- Introduciamo 6 nuove cifre per utilizzare la base 16 *esadecimale*: a per 10, b per 11, c per 12, d per 13, e per 14, f per 15. Poiché $2301 = 8 \cdot 16^2 + 15 \cdot 16 + 13$ si ha $(2301)_{16} = 8fd$.

Osservazione 2.31 (Numero delle cifre di a in base $b > 1$)**.** Siano $a, b \in \mathbb{N}$ con $a > 0$ e $b > 1$. Se a ha n cifre in base b allora $b^{n-1} \leq a < b^n$. Prendendo il logaritmo in base b si ottiene $n - 1 \leq \log_b(a) < n$, pertanto $\lfloor \log_b(a) \rfloor = n - 1$ e quindi

$$n = \lfloor \log_b(a) \rfloor + 1.$$

3 Numeri complessi

Abbiamo visto e vedremo alcune proprietà dei numeri naturali $\mathbb{N}$ e dei numeri interi $\mathbb{Z}$. Nel Capitolo 4 daremo anche una definizione formale dei numeri razionali $\mathbb{Q}$. Diamo invece per buoni i numeri reali $\mathbb{R}$ per le cui proprietà ci rifacciamo al corso di Analisi (o Calculus 1). In questo capitolo, costruiamo un nuovo importante insieme di numeri: i numeri complessi $\mathbb{C}$.

3.1 Rappresentazione dei numeri complessi

Definizione 3.1. Definiamo l'insieme dei **numeri complessi** come $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ denotando ogni coppia ordinata $(x, y) \in \mathbb{R}^2$ come il numero complesso $x + iy$ (o alternativamente $x + yi$), dove l'*unità immaginaria* i corrisponde alla coppia $(0, 1)$. Dotiamo l'insieme $\mathbb{C}$ delle seguenti operazioni:

- la somma $(x + iy) + (u + iv) := x + u + i(y + v)$;
- il prodotto $(x + iy) \cdot (u + iv) := xu - yv + i(xv + yu)$.

Se $z = x + iy$ con $x, y \in \mathbb{R}$, chiamiamo x la **parte reale** di z e la indichiamo con $\Re(z)$ e chiamiamo y la **parte immaginaria** di z e la indichiamo con $\Im(z)$.

Osserviamo che due numeri complessi z e w sono uguali se e solo se hanno la stessa parte reale e la stessa parte immaginaria, ossia

$$z = w \iff ((\Re(z) = \Re(w)) \wedge (\Im(z) = \Im(w))) .$$

È facile verificare che la somma e il prodotto così definite sono operazioni associative e commutative, che l'elemento $0 := 0 + i0$, corrispondente alla coppia $(0, 0)$, è l'elemento neutro rispetto alla somma, cioè $\forall\, z \in \mathbb{C}$ si ha $z+(0+i0) = z$, e che l'elemento $1 := 1+i0$, corrispondente alla coppia $(1, 0)$ è l'elemento neutro rispetto al prodotto, cioè $\forall\, z \in \mathbb{C}$ si ha $z \cdot 1 + i0 = z$. Ogni elemento di $\mathbb{C}$ ammette opposto, dato $z = x + iy$ definiamo

$$-z := -x + i(-y).$$

Verifichiamo che $z+(-z) = x+iy+(-x-iy) = (x-x)+i(y-y) = 0$, e cioè $-z$ è l'opposto di z. Infine, ogni elemento non nullo di $\mathbb{C}$ ammette inverso moltiplicativo. Dato $z = x + iy \neq 0$ definiamo

$$z^{-1} := \frac{1}{z} := \left(\frac{x}{x^2 + y^2}\right) + i\left(\frac{-y}{x^2 + y^2}\right).$$

Si verifica che

$$(z + iy) \cdot \left(\left(\frac{x}{x^2 + y^2}\right) + i\left(\frac{-y}{x^2 + y^2}\right)\right) = 1,$$

e cioè z^{-1} è l'inverso di z.

Alla luce di quanto visto prima, possiamo identificare i numeri reali con i numeri complessi di parte immaginaria nulla, ottenendo un'inclusione

$$\begin{aligned} \mathbb{R} &\hookrightarrow \mathbb{C} \\ x &\mapsto x + i0 \end{aligned}$$

Invece i numeri complessi di parte reale nulla sono detti *numeri immaginari puri.*

Osservazione 3.2. Osserviamo la seguente importante proprietà dell'unità immaginaria i:

$$i^2 = i \cdot i = (1 + i0) \cdot (1 + i0) := 0 \cdot 0 - 1 \cdot 1 + i(0 \cdot 1 + 0 \cdot 1) = -1.$$

Segue quindi facilmente che $i^3 = i^2 \cdot i = -1 \cdot i = -i$ e $i^4 = i^2 \cdot i^2 = (-1)(-1) = 1$. Le potenze più alte di i si ripetono ciclicamente: $i^5 = i$, $i^6 = i^2 = -1$, e così via.

Definizione 3.3. Dato il numero complesso $z = x + iy$, il **complesso coniugato** di z che si indica con $\overline{z}$ è il numero $\overline{z} = x - iy$.

Lasciamo come esercizio per il lettore, la verifica delle seguenti proprietà dell'operazione di coniugazione.

Proposizione 3.4. *Siano $z, w \in \mathbb{C}$. Allora*

(i) $\overline{zw} = \overline{z} \cdot \overline{w}$;
(ii) $\overline{z + w} = \overline{z} + \overline{w}$;
(iii) $\overline{z} = z \iff z \in \mathbb{R}$;
(iv) $z + \overline{z} = 2\Re(z)$;
(v) $z - \overline{z} = 2\Im(z)$.

Definizione 3.5. Dato il numero complesso $z = x+iy$ il **modulo** di z è il numero reale definito come

$$|z| = \sqrt{\Re(z)^2 + \Im(z)^2} = \sqrt{x^2 + y^2}.$$

Il modulo di z rappresenta la distanza del punto (x, y) dall'origine.

Osserviamo che la definizione di modulo di un numero complesso coincide con quella di valore assoluto se il numero complesso è un numero reale. Cioè se $z = x \in \mathbb{R}$ abbiamo

$$|x| = \sqrt{x^2} = \begin{cases} x \text{ se } x \geq 0 \\ -x \text{ se } x < 0. \end{cases}$$

Proposizione 3.6. *Siano $z, w \in \mathbb{C}$. Allora*

(i) $z \cdot \overline{z} = |z|^2$;
(ii) $|zw| = |z||w|$;
(iii) $|z + w| \leq |z| + |w|$ (disuguaglianza triangolare);
(iv) se $z \neq 0$, $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$.

Dimostrazione. (i) Sia $z = x + iy$ con $x, y \in \mathbb{R}$.

$$z \cdot \overline{z} = (x + iy)(x - iy) = x^2 + xyi - xyi - i^2y^2 = x^2 + y^2 = |z|^2.$$

(ii) Siccome il modulo di un numero complesso è sempre ≥ 0 ci basta verificare l'uguaglianza tra i quadrati, e cioè $|zw|^2 = |z|^2|w|^2$. Siano $z = x + iy$ e $w = u + iv$ con $x, y, u, v \in \mathbb{R}$. Abbiamo

$$\begin{aligned} |zw|^2 &= |xu - yv + i(xv + yu)|^2 \\ &= (xu - yv)^2 + (xv + yu)^2 \\ &= u^2x^2 + v^2y^2 + v^2x^2 + u^2y^2 \\ &= (x^2 + y^2)(u^2 + v^2) \\ &= |z|^2|w|^2. \end{aligned}$$

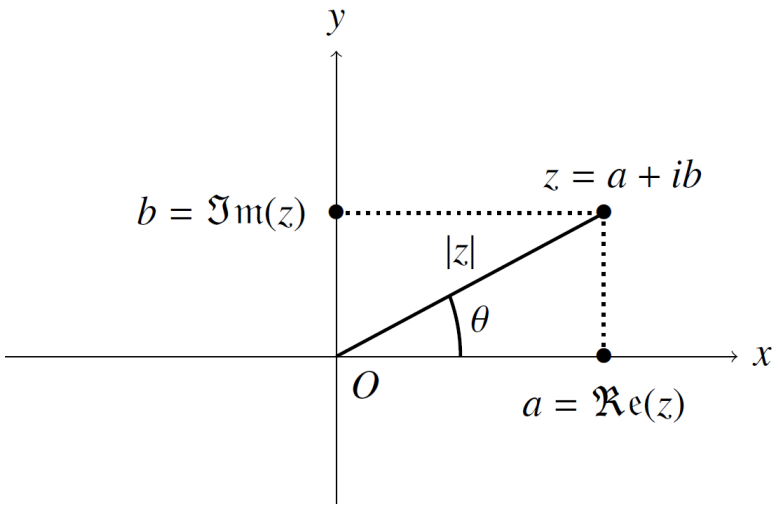


Figura 2: Il piano complesso

(iii) Questa proprietà si può verificare con una serie di tediosi conti (che omettiamo), oppure geometricamente rappresentando sul piano un parallelogramma di vertici 0, w, z e $z+w$. Si vede che la diagonale del parallelogramma ha lunghezza $|z+w|$ e deve quindi essere minore o uguale delle somma delle lunghezze di altri due lati del corrispondente triangolo e cioè $|z|+|w|$.

(iv) Abbiamo definito $\frac{1}{z}$ come

$$\frac{1}{z} = \left(\frac{x}{x^2+y^2}\right) + i\left(\frac{-y}{x^2+y^2}\right) = \frac{x-iy}{x^2+y^2} = \frac{\overline{z}}{|z|^2}.$$

□

3.2 Forma trigonometrica ed esponenziale di un numero complesso

Per come abbiamo definito inizialmente $\mathbb{C}$ vi è una corrispondenza biunivoca tra i punti del piano cartesiano $\mathbb{R}^2$ e i numeri complessi associando a ciascun numero $z = a + ib$ il punto P di coordinate (a, b) del piano . La distanza ρ di P dall'origine O (che è $\sqrt{a^2+b^2}$) coincide con il modulo $|z|$ di z.

Definizione 3.7. L'angolo θ formato[4] dal segmento OP con il semiasse positivo delle ascisse, si dice **argomento** di z e viene denotato con $\arg(z)$. Non si attribuisce argomento al numero complesso 0.

Osserviamo che se $z \neq 0$ l'argomento di z è definito a meno di multipli di 2π. Per evitare ambiguità, spesso prediligeremo due intervalli principali di variazione per l'argomento:

$$0 \leq \arg(z) < 2\pi \quad \text{oppure} \quad -\pi < \arg(z) \leq \pi.$$

[4] l'angolo θ si intende sempre misurato in radianti!

Inoltre, si vede facilmente che se $0 \neq z = a + ib$ ha modulo $|z| = \rho$ e argomento $\theta = \arg(z)$ allora

$$a = \rho\cos\theta,\ b = \rho\sin\theta, \quad \text{e} \quad \frac{b}{a} = \tan\theta.$$

Definizione 3.8. La **forma trigonometrica** di un numero complesso $z \neq 0$ è

$$z = |z|\big(\cos(\arg(z)) + i\sin(\arg(z))\big).$$

Utilizzando le formule di addizione per le funzioni trigonometriche si dimostra facilmente il seguente teorema.

Teorema 3.9. *Il prodotto di due numeri complessi non nulli ha per modulo il prodotto dei loro moduli e per argomento la somma degli argomenti. In formule, se $z, w \in \mathbb{C} \setminus \{0\}$ abbiamo*

$$z \cdot w = |z||w|\big(\cos\left(\arg(z) + \arg(w)\right) + i\sin\left(\arg(z) + \arg(w)\right)\big).$$

Questo ci porta ad introdurre la seguente notazione.

Definizione 3.10. La **forma esponenziale** di un numero complesso $z \neq 0$ è

$$z = |z|e^{i\arg(z)}.$$

Dove se $\theta \in \mathbb{R}$ si definisce $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

La forma esponenziale assume un significato profondo in analisi complessa dove costituisce un naturale prolungamento della funzione esponenziale reale. Per i nostri scopi è sufficiente considerare la forma esponenziale a livello formale e trattare le operazioni tra numeri complessi in forma esponenziale seguendo le usuali regole delle operazioni tra potenze. Ad esempio, grazie al Teorema 3.9 abbiamo che se $z, w \in \mathbb{C} \setminus \{0\}$ allora

$$z \cdot w = \left(|z|e^{i\arg(z)}\right)\left(|w|e^{i\arg(w)}\right) = |z||w|\left(e^{i(\arg(z)+\arg(w))}\right).$$

Analogamente, dato $z \in \mathbb{C}$, $z \neq 0$ e $n \in \mathbb{N}$ abbiamo la seguente, detta **formula di De Moivre**:

$$z^n = |z|^n e^{in(\arg(z))}.$$

3.3 Radici n-esime di un numero complesso

Sia n un numero intero positivo, ci occupiamo adesso del problema di trovare le "radici" di un dato numero x, cioè la ricerca di un numero (o più numeri) y che risolvano l'equazione $y^n = x$. La risposta è differente se cerchiamo tali radici tra i numeri reali $\mathbb{R}$ o tra i numeri complessi $\mathbb{C}$. Ricordiamo prima il caso reale.

Definizione 3.11. Sia $n \in \mathbb{N}$, $n \geq 1$ fissato. La **radice reale n-esima** di un numero reale $x \neq 0$ è data da:

(i) l'unico numero reale y tale che $y^n = x$, se n è dispari;

(ii) l'unico numero reale $y > 0$ tale che $y^n = x$, se n è pari e $x > 0$;

(iii) non esiste, se n è pari e $x < 0$.
Denotiamo con $\sqrt[n]{x}$ tale radice. Poniamo anche $\sqrt[n]{0} = 0$.

La radice reale n-esima fornisce la risposta alle ricerca delle radici reali di un numero reale. Infatti se n è dispari, esiste soltanto un numero reale y tale che $y^n = x$ e cioè $\sqrt[n]{x}$. Se invece n è pari e $x > 0$ esistono due numeri reali che soddisfano $y^n = x$, cioè $\sqrt[n]{x}$ e $-\sqrt[n]{x}$.

Nel caso complesso, una risposta al problema può essere data utilizzando la formula di De Moivre.

Teorema 3.12. *Siano $z \in \mathbb{C}$ e $n \in \mathbb{N}$, $n > 0$ due numeri fissati. Se $z \neq 0$ le soluzioni (in $\mathbb{C}$) dell'equazione $x^n = z$ sono n numeri complessi $z_0, \ldots, z_{n-1}$ tutti distinti tra loro e dati dalla seguente formula*

$$z_k = \sqrt[n]{|z|}\left(\cos\left(\frac{\arg(z) + 2k\pi}{n}\right) + i\sin\left(\frac{\arg(z) + 2k\pi}{n}\right)\right) \quad k = 0, 1, \ldots, n-1.$$

I numeri $z_0, \ldots, z_{n-1}$ vengono detti **radici n-esime complesse** *di z. Se $z = 0$ allora l'equazione $x^n = 0$ ha la sola soluzione 0 (di molteplicità n).*

Osservazione 3.13. Nella rappresentazione geometrica sul piano cartesiano le radici n-esime complesse di $z \in \mathbb{C}$ sono disposte sui vertici di un poligono regolare di n lati iscritto in una circonferenza di centro l'origine e raggio $\sqrt[n]{|z|}$. In particolare, le radici n-esime dell'unità sono disposte sui vertici di un poligono regolare di n lati iscritto in una circonferenza di centro l'origine e raggio 1 e avente uno dei suoi vertici nel punto $(1, 0)$ che corrisponde a $x = 1$. Esse sono date dalla formula

$$z_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \; k = 0, 1 \ldots, n-1.$$

Esempio 3.14. Calcoliamo le radici cubiche di $z = -8$. Si ha che $|z| = \sqrt{(-8)^2} = 8$ e $\arg(z) = \pi$. Pertanto le radici cubiche z_k di z sono date dalla formula

$$z_k = \sqrt[3]{8}\left(\cos\left(\frac{\pi + 2k\pi}{3}\right) + i\sin\left(\frac{\pi + 2k\pi}{3}\right)\right), \quad k = 0, 1, 2.$$

Abbiamo quindi

$$z_0 = \sqrt[3]{8}\left(\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right) = 2\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 1 + i\sqrt{3},$$
$$z_1 = 2\left(\cos\left(\frac{\pi + 2\pi}{3}\right) + i\sin\left(\frac{\pi + 2\pi}{3}\right)\right) = 2(\cos(\pi) + i\sin(\pi)) = -2,$$
$$z_2 = 2\left(\cos\left(\frac{\pi + 4\pi}{3}\right) + i\sin\left(\frac{\pi + 4\pi}{3}\right)\right) = 2\left(\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right)\right) = 1 - i\sqrt{3}.$$

Esempio 3.15. Calcoliamo le radici quinte di $z = \frac{3}{2} + \frac{3\sqrt{3}}{2}i$. Si ha che

$$|z| = \sqrt{\left(\frac{3}{2}\right)^2 + \left(\frac{3\sqrt{3}}{2}\right)^2} = \sqrt{\frac{9}{4} + \frac{27}{4}} = \sqrt{\frac{36}{4}} = \sqrt{9} = 3.$$

Quindi $z = 3\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ e se chiamiamo $\theta = \arg(z)$ allora $\cos(\theta) = \frac{1}{2}$ e $\sin(\theta) = \frac{\sqrt{3}}{2}$, pertanto $\theta = \frac{\pi}{3}$. Quindi le radici quinte z_k di z sono date dalla formula

$$z_k = \sqrt[5]{3}\left(\cos\left(\frac{\frac{\pi}{3} + 2k\pi}{5}\right) + i\sin\left(\frac{\frac{\pi}{3} + 2k\pi}{5}\right)\right), \quad k = 0, 1, \ldots, 4.$$

Abbiamo pertanto

$$z_0 = \sqrt[5]{3}\left(\cos\left(\frac{\pi}{15}\right) + i\sin\left(\frac{\pi}{15}\right)\right), \quad z_1 = \sqrt[5]{3}\left(\cos\left(\frac{7\pi}{15}\right) + i\sin\left(\frac{7\pi}{15}\right)\right),$$
$$z_2 = \sqrt[5]{3}\left(\cos\left(\frac{13\pi}{15}\right) + i\sin\left(\frac{13\pi}{15}\right)\right), \quad z_3 = \sqrt[5]{3}\left(\cos\left(\frac{19\pi}{15}\right) + i\sin\left(\frac{19\pi}{15}\right)\right),$$
$$z_4 = \sqrt[5]{3}\left(\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right)\right).$$

Una conseguenza del Teorema 3.12 è la seguente.

Proposizione 3.16. *Ogni equazione algebrica di secondo grado $ax^2 + bx + c = 0$ a coefficienti in $\mathbb{C}$ ammette sempre soluzioni in $\mathbb{C}$.*

Dimostrazione. Consideriamo l'equazione di secondo grado $ax^2+bx+c = 0$ dove $a, b, c \in \mathbb{C}$, $a \neq 0$. Questa equazione è equivalente all'equazione $(2ax + b)^2 = \Delta$ ponendo $\Delta = b^2 - 4ac$. Le soluzioni di questa seconda equazioni saranno quindi le radici quadrate (in senso complesso) di Δ. Per il Teorema 3.12 ci saranno allora due numeri complessi δ_1 e δ_2 (distinti se $\Delta \neq 0$, entrambi nulli se $\Delta = 0$) tali che $\delta_1^2 = \delta_2^2 = \Delta$. In definitiva quindi le soluzioni saranno:

$$w_1 = \frac{-b + \delta_1}{2a}, \quad w_2 = \frac{-b + \delta_2}{2a}.$$

□

Esempio 3.17. Consideriamo l'equazione di secondo grado $x^2 + 4x + 5 = 0$. Abbiamo $\Delta = 16 - 20 = -4$. Utilizzando la formula del Teorema 3.12 si possono trovare le due radici $\delta_1 = 2i$ e $\delta_2 = -2i$ che sono tali che $\delta_1^2 = \delta_2^2 = -4$. Le soluzioni dell'equazione $x^2 + 4x + 5 = 0$ sono pertanto

$$w_1 = \frac{-4 + 2i}{2} = -2 + i, \quad w_2 = \frac{-4 - 2i}{2} = -2 - i.$$

In generale, utilizzando tecniche matematiche più avanzate si può dimostrare il seguente risultato.

Teorema 3.18 (Teorema fondamentale dell'algebra)**.** *Sia*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

un polinomio a coefficienti $a_j \in \mathbb{C}$ di grado $n \in \mathbb{N}^*$ (cioè $a_n \neq 0$). Allora $p(x) = 0$ ha n soluzioni in $\mathbb{C}$ contate con la loro molteplicità. Più precisamente, $p(x)$ si può decomporre come

$$p(x) = a_n(x - w_1)^{m_1} \cdot (x - w_2)^{m_2} \cdots (x - w_r)^{m_r},$$

dove $m_1, \ldots, m_r \in \mathbb{N}^*$ e $w_1, \ldots, w_r \in \mathbb{C}$. I numeri $w_1, \ldots, w_r$ vengono detti **radici** *di $p(x)$. L'intero m_j è detto* **molteplicità** *della radice w_j. E si ha che $m_1 + m_2 + \cdots + m_r = n$.*

Esempio 3.19. Il polinomio $p(x) = x^2 + 4x + 5$ si può decomporre come

$$p(x) = (x - w_1)(x - w_2) = (x + 2 - i)(x + 2 + i).$$

Abbiamo quindi due radici $w_1 = -2 + i$ e $w_2 = -2 - i$ entrambe con molteplicità $m_1 = m_2 = 1$.

4 Relazioni d'equivalenza

Definizione 4.1. Sia A un insieme, una relazione $R \subseteq A \times A$ si dice **relazione d'equivalenza** se è:

(i) *riflessiva*, cioè $\forall a \in A$ si ha $(a, a) \in R$;
(ii) *simmetrica*, cioè vale $(a, b) \in R \Rightarrow (b, a) \in R$;
(iii) *transitiva*, cioè vale $((a, b) \in R) \wedge ((b, c) \in R) \Rightarrow (a, c) \in R$.

Generalmente le relazioni d'equivalenza si indicano con il simbolo $\sim$ o con il simbolo $\equiv$. Scriviamo quindi $x \sim y$ o $x \equiv y$ al posto di $(x, y) \in R$ o xRy. Se $x \sim y$ si dice che x e y sono **equivalenti** (rispetto a R).

Esempio 4.2.
1. La relazione totale ($R = A \times A$) e la relazione diagonale ($R = \Delta$) sono relazioni d'equivalenza.
2. La relazione $x \sim y \Leftrightarrow x = y$ è una relazione d'equivalenza detta *relazione d'uguaglianza*.
3. Sia $f : A \to B$ un'applicazione, definiamo su A la seguente relazione: $x \sim_f y$ se $f(x) = f(y)$. Si verifica facilmente che $\sim_f$ è una relazione di equivalenza che si dice *relazione di equivalenza associata a* f.

Definizione 4.3. Sia $\sim$ una relazione d'equivalenza su un insieme A. La **classe di equivalenza** di un elemento $a \in A$ è l'insieme

$$[a] := \{b \in A : \ b \sim a\}.$$

La classe di equivalenza di a si denota talvolta anche $\overline{a}$. Ogni elemento di una classe di equivalenza è detto **rappresentante** della classe.

Per la proprietà transitiva due classi di equivalenza o coincidono o sono disgiunte. Pertanto le classi di equivalenza di una relazione di equivalenza su un insieme A costituiscono una *partizione* di A, cioè

$$A = \bigcup_{a \in A} [a]$$

e le classi distinte sono tra di loro disgiunte.

Definizione 4.4. Sia $\sim$ una relazione d'equivalenza su un insieme A. L'insieme

$$A/\sim := \{[a] : \ a \in A\}$$

i cui elementi sono le classi di equivalenza è detto **insieme quoziente**. La mappa $\pi : A \to A/\sim$, $\pi(a) = [a]$ è detta **mappa quoziente**. Si tratta di una mappa surgettiva.

Vediamo ora un esempio importante di relazione d'equivalenza.

Esempio 4.5. Sia $n > 1$ un intero fissato. Definiamo una relazione d'equivalenza $\sim_n$ su $\mathbb{Z}$ nella maniera seguente

$$x \sim_n y \iff \exists k \in \mathbb{Z} \text{ tale che } x - y = kn.$$

Se $x \sim_n y$ si dice che x *è congruo a* y *modulo* n e si scrive $x \equiv y \bmod n$. La verifica che $\sim_n$ è una relazione d'equivalenza è lasciata per esercizio. L'insieme $\mathbb{Z}$ è unione di n classi di equivalenza distinte

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$$

perché ogni intero x è equivalente al resto della divisione di x per n e ci sono n resti possibili. Le classi $[0], [1], \ldots, [n-1]$ vengono dette *classi di resto modulo* n. L'insieme quoziente $\mathbb{Z}/\sim_n$ viene più spesso denotato con $\mathbb{Z}_n$ (oppure[5] con $\mathbb{Z}/n\mathbb{Z}$), cioè

$$\mathbb{Z}_n := \{[0], [1], \ldots, [n-1]\}.$$

Per esempio, per $n = 2$ si ha $\mathbb{Z}_2 = \{[0], [1]\}$ dove $[0] = \{\text{numeri pari}\}$ e $[1] = \{\text{numeri dispari}\}$.

Osservazione 4.6. Ogni affermazione (come una proprietà o una funzione) relativa ad un insieme quoziente $A/\sim$ enunciata mediante gli elementi di A deve essere indipendente dalla scelta dei rappresentanti delle classi!

Esempio 4.7. 1. L'associazione

$$\begin{aligned} \varphi : \mathbb{Z}_6 &\to \mathbb{Z} \\ \overline{x} &\mapsto x + 1 \end{aligned}$$

non definisce una funzione! Infatti si ha $\overline{2} = \overline{8}$ in $\mathbb{Z}_6$, ma $\varphi(\overline{2}) = 2 + 1 = 3 \neq 9 = 8 + 1 = \varphi(\overline{8})$. Quindi alla classe $\overline{2} = \overline{8}$ non è associato un unico elemento di $\mathbb{Z}$.

2. Consideriamo l'associazione

$$\begin{aligned} \psi : \mathbb{Z}_6 &\to \mathbb{Z}_3 \\ \overline{x} &\mapsto [x] \end{aligned}$$

dove $\overline{x}$ denota la classe di equivalenza in $\mathbb{Z}_6$ e $[x]$ denota la classe di equivalenza in $\mathbb{Z}_3$. ψ è una funzione ben definita. Infatti si verifica facilmente che se $\overline{x} = \overline{y}$, cioè x e y danno lo stesso resto se divisi per 6, allora $[x] = [y]$, cioè x e y danno lo stesso resto anche quando sono divisi per 3 (notare che il viceversa non è vero!).

Si può usare la relazione d'equivalenza per dare una definizione formale dei numeri interi $\mathbb{Z}$ e dei numeri razionali $\mathbb{Q}$ a partire dai numeri naturali $\mathbb{N}$.

Esempio 4.8 (definizione formale di $\mathbb{Z}$)**.** Definiamo la seguente relazione $\sim$ sul prodotto cartesiano $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

Lasciamo per esercizio la verifica che $\sim$ soddisfa le proprietà riflessiva, simmetrica, e transitiva, ed è pertanto una relazione d'equivalenza. L'insieme quoziente $\mathbb{N} \times \mathbb{N}/\sim$ può essere identificato con l'insieme dei numeri interi $\mathbb{Z}$ tramite la bigezione

$$\begin{aligned} \phi : \mathbb{N} \times \mathbb{N}/\sim &\longrightarrow \mathbb{Z} \\ \overline{(a, b)} &\mapsto a - b. \end{aligned}$$

[5] L'uso della notazione $\mathbb{Z}/n\mathbb{Z}$ verrà motivato nell'Esempio 9.24

Tramite questa bigezione l'insieme dei numeri naturali $\mathbb{N}$ corrisponde al sottoinsieme del quoziente dato da $\{\overline{(n,0)} : n \in \mathbb{N}\}$. A livello formale, si può prendere direttamente $\mathbb{N} \times \mathbb{N}/\sim$ come definizione dell'insieme degli interi $\mathbb{Z}$.

Esempio 4.9 (definizione formale di $\mathbb{Q}$)**.** Sull'insieme $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ poniamo la relazione

$$(x,y) \sim (z,t) \iff xt = yz.$$

Mostriamo che si tratta di una relazione d'equivalenza.

(i) proprietà riflessiva: $(x,y) \sim (x,y)$ siccome $xy = yx$;

(ii) proprietà simmetrica: se $(x,y) \sim (z,t)$ allora $xt = yz$, e quindi anche $yz = xt$, cioè $(z,t) \sim (x,y)$;

(iii) proprietà transitiva: se $(x,y) \sim (z,t)$ e $(z,t) \sim (u,v)$ allora $xt = yz$ e $zv = tu$. Se $x \neq 0$ allora $z \neq 0$ e $u \neq 0$ (y, t, e v sono non nulli per ipotesi), pertanto moltiplicando ambo i membri dell'uguaglianza $xt = yz$ per uv (che è $\neq 0$) otteniamo $xtuv = yzuv$, che si può riscrivere come $(xv)(tu) = (yu)(zv)$. Poichè $tu = zv$ otteniamo l'uguaglianza $xv = yu$, cioè $(x,y) \sim (u,v)$. Se $x = 0$ allora $z = 0$ e $u = 0$, pertanto si ha ancora l'uguaglianza $xv = 0 = yu$, cioè $(x,y) \sim (u,v)$.

L'insieme quoziente $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$ può essere identificato con l'insieme dei numeri razionali $\mathbb{Q}$ tramite la bigezione

$$\begin{aligned} \mu : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim &\longrightarrow \mathbb{Q} \\ \overline{(x,y)} &\mapsto \frac{x}{y}. \end{aligned}$$

Di fatto si può prendere $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$ come definizione dell'insieme dei numeri razionali $\mathbb{Q}$.

5 Cardinalità

Definizione 5.1. Due insiemi A e B si dicono **equipotenti** se esiste una funzione $f : A \to B$ bigettiva. In tal caso scriviamo $|A| = |B|$ o $\#A = \#B$, senza specificare la funzione f.

Osserviamo che l'equipotenza soddisfa tutte le proprietà di una relazione d'equivalenza.

(i) proprietà riflessiva. Ogni insieme A è equipotente a se stesso tramite l'identità $\mathrm{id}_A : A \to A$.

(ii) proprietà simmetrica. Se A è equipotente a B allora $\exists f : A \to B$ bigettiva. Per il Teorema 1.32 esiste la funzione inversa $g : B \to A$, che è anch'essa bigettiva. Pertanto anche B è equipotente ad A.

(iii) proprietà transitiva. Se A è equipotente a B tramite una mappa bigettiva $f : A \to B$, e B è equipotente a C mediante una mappa bigettiva $g : A \to C$ allora A è equipotente a C mediante la mappa bigettiva $g \circ f : A \to C$.

Le proprietà precedenti ci potrebbero portare a dire che l'equipotenza è una relazione d'equivalenza sull'insieme di tutti gli insiemi. Attenzione però che un tale oggetto, l'insieme di tutti gli insiemi, non è un insieme per via del *paradosso di Russell*. Lasciamo ai logici il compito di risolvere questi problemi e ci limitiamo a ricordare che l'equipotenza soddisfa le proprietà riflessiva, simmetrica e transitiva.

Definizione 5.2. Sia X un insieme.

- X si dice **finito** se X è vuoto oppure se esiste un intero $n > 0$ tale che X è equipotente all'insieme $\{1, 2, \dots, n\}$. In tal caso poniamo $|X| = n$ e diciamo che X ha **cardinalità** n. Poniamo anche $|\emptyset| = 0$.

- X si dice **infinito** se X non è finito. In tal caso diciamo che X ha cardinalità infinita[6].

Esistono diverse caratterizzazioni equivalenti del concetto di insieme infinito, ne raccogliamo alcune nel seguente teorema.

Teorema 5.3. *Sia X un insieme non vuoto. Allora sono equivalenti:*

(i) X è infinito (cioè X non è finito);

(ii) esiste un sottoinsieme proprio $Y \subsetneq X$ equipotente a X;

(iii) esiste un'applicazione iniettiva, ma non suriettiva $f : X \to X$.

Grazie al teorema precedente, possiamo dimostrare che l'insieme $\mathbb{N}$ dei numeri naturali è infinito. Infatti, l'applicazione *successore* $s : \mathbb{N} \to \mathbb{N}$ tale che $s(n) = n + 1$ è iniettiva, ma non suriettiva (siccome $s^{-1}(0) = \emptyset$). Introduciamo quindi la seguente definizione.

Definizione 5.4. Un insieme X si dice **numerabile** o di **cardinalità numerabile** se $|X| = |\mathbb{N}|$. In tal caso, si scrive anche $|X| = \aleph_0$, si legge "aleph zero".

[6] Talvolta si scrive anche $|X| = \infty$, sebbene tale scrittura non sia precisa in quanto esistono diverse "tipologie" di cardinalità infinite, come vedremo.

Osserviamo che un insieme numerabile X è necessariamente infinito. Infatti, se $f : \mathbb{N} \to X$ è una bigezione, la composizione $f \circ s \circ f^{-1} : X \to X$, dove s è l'applicazione successore, fornisce un esempio di applicazione iniettiva, ma non suriettiva da X verso se stesso.

Vediamo adesso alcuni esempi di insiemi numerabili.

Esempio 5.5. L'insieme $\mathbb{N}^*$ è numerabile. L'applicazione $f : \mathbb{N} \to \mathbb{N}^*$ data da $f(n) = n + 1$ è bigettiva. L'inversa di f è l'applicazione $f^{-1} : \mathbb{N}^* \to \mathbb{N}$ data da $f^{-1}(n) = n - 1$.

Esempio 5.6. L'insieme dei numeri interi $\mathbb{Z}$ è numerabile. L'applicazione $f : \mathbb{N} \to \mathbb{Z}$ definita da

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases}$$

è bigettiva. L'applicazione inversa $f^{-1} : \mathbb{Z} \to \mathbb{N}$ è data da

$$f^{-1}(m) = \begin{cases} 2m & \text{se } m \geq 0 \\ -1 - 2m & \text{se } m < 0 \end{cases}$$

La verifica che $f \circ f^{-1} = \mathrm{id}_{\mathbb{Z}}$ e $f^{-1} \circ f = \mathrm{id}_{\mathbb{N}}$ è lasciata per esercizio. Pertanto $\mathbb{N}$ e $\mathbb{Z}$ sono equipotenti.

Proposizione 5.7. *L'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile.*

Dimostrazione. Consideriamo la seguente applicazione

$$\begin{aligned} f : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (m, n) &\mapsto 2^m(2n + 1) - 1 \end{aligned}$$

e dimostriamo che è bigettiva.

f è iniettiva. Siano $(m, n), (r, s) \in \mathbb{N} \times \mathbb{N}$ tali che $f(m, n) = f(r, s)$. Osserviamo che m e n vengono univocamente determinati da $f(m, n) + 1$. Infatti, grazie al Teorema fondamentale dell'aritmetica (vedi Teorema 2.27), ogni numero naturale $k > 0$ si può scrivere univocamente nella forma $k = 2^m(2n + 1)$ con $m, n \in \mathbb{N}$. Pertanto l'uguaglianza $f(m, n) = f(r, s)$ implica $f(m, n) + 1 = f(r, s) + 1$ e di conseguenza $(m, n) = (r, s)$.

f è surgettiva. Sia $a \in \mathbb{N}$. Analogamente a prima $a + 1$ individua univocamente (sempre grazie al Teorema fondamentale dell'aritmetica) due numeri naturali $m, n \in \mathbb{N}$ tali che $a + 1 = 2^m(2n + 1)$ e quindi $a = 2^m(2n + 1) - 1 = f(m, n)$. □

Introduciamo la seguente notazione tra numeri cardinali.

Definizione 5.8. Siano A e B due insiemi. Scriviamo che $|A| \leq |B|$ se esiste un'applicazione iniettiva $f : A \to B$. Inoltre scriviamo che $|A| < |B|$ se esiste un'applicazione iniettiva $f : A \to B$, ma A e B non sono equipotenti (cioè non esiste alcuna applicazione bigettiva $g : A \to B$).

Nel caso in cui A e B siano insiemi finiti, la nozione di "disuguaglianza" tra numeri cardinali precedentemente introdotta rispecchia l'usuale disuguaglianza tra numeri interi.

Proposizione 5.9. *Siano A e B insiemi finiti con $|A| = n \in \mathbb{N}$ e $|B| = m \in \mathbb{N}$. Allora*

$$\exists f : A \to B \text{ iniettiva} \iff n \leq m.$$

Dimostrazione. "$\Leftarrow$" Per definizione di cardinalità esistono $\varphi : A \to \{1, \dots, n\}$ e $\psi : B \to \{1, \dots, m\}$ bigettive. E possiamo prendere come f la composizione $f = \psi^{-1} \circ \iota \circ \varphi$, dove $\iota : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$ è l' inclusione.
"$\Rightarrow$" Considerando le bigezioni φ e ψ come al punto precedente, e assumendo che esista $f : A \to B$ iniettiva si ottiene mediante composizione un'applicazione iniettiva $\psi \circ f \circ \varphi^{-1} : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$. Il che mostra che necessariamente $n \leq m$. □

Analogamente, si vede facilmente che se A è un insieme finito e B è un insieme infinito, si ha sempre $|A| \leq |B|$, o più precisamente $|A| < |B|$. La situazione è più complessa nel caso in cui entrambi gli insiemi A e B sono infiniti. Infatti, non tutti gli insiemi infiniti sono equipotenti tra di loro. Tuttavia la nozione di "disuguaglianza" tra numeri cardinali si comporta bene anche per insiemi infiniti, grazie al seguente importante risultato.

Teorema 5.10 (Cantor–Bernstein)**.** *Siano A e B due insiemi. Se esistono due mappe iniettive $f : A \to B$ e $g : B \to A$, allora esiste una mappa bigettiva $h : A \to B$, cioè A e B sono equipotenti. In altre parole, vale la seguente implicazione*

$$\big(|A| \leq |B|\big) \wedge \big(|B| \leq |A|\big) \Longrightarrow |A| = |B|.$$

Si può dimostrare che gli insiemi numerabili sono gli insiemi infiniti di cardinalità "più piccola", cioè vale che un insieme A è infinito se e solo se $\aleph_0 \leq |A|$. Introduciamo pertanto le seguenti definizioni.

Definizione 5.11. Sia X un insieme.

- X si dice **al più numerabile** se $|X| \leq \aleph_0$.
- X si dice **più che numerabile** se $|X| > \aleph_0$.

Per quanto detto prima, si ha che un insieme X è al più numerabile se e solo se X è finito oppure X è equipotente ad $\mathbb{N}$ (cioè è numerabile).

Vediamo un esempio di insieme più che numerabile.

Proposizione 5.12. *Sia X un insieme non vuoto*[7]*. Allora non esiste alcuna mappa surgettiva $f : X \to \mathcal{P}(X)$. In particolare, X e $\mathcal{P}(X)$ non sono equipotenti.*

Dimostrazione. Supponiamo per assurdo che esista un'applicazione surgettiva $f : X \to \mathcal{P}(X)$. Consideriamo l'insieme

$$S = \{x \in X : \ x \notin f(x)\}.$$

Osserviamo che per definizione $S \subseteq X$, cioè $S \in \mathcal{P}(X)$ (eventualmente S può essere anche vuoto). Siccome f è surgettiva, esiste $s \in X$ tale che $f(s) = S$. Abbiamo due possibilità:

[7]La conclusione della proposizione vale anche nel caso dell'insieme vuoto in quanto $|\mathcal{P}(\emptyset)| = 1 > 0 = |\emptyset|$.

1. se $s \in S$, allora $s \notin f(s) = S$;
2. se $s \notin S$, allora $s \in f(s) = S$.

In entrambi i casi si ottiene una contraddizione. □

Osservazione 5.13. Dato X insieme non vuoto, si ha sempre una mappa iniettiva $\varphi : X \to \mathcal{P}(X)$ data da $\varphi(x) = \{x\}$, cioè l'elemento $x \in X$ è mandato nell'insieme singoletto $\{x\} \in \mathcal{P}(X)$. Pertanto $|X| \leq |\mathcal{P}(X)|$. La proposizione precedente ci dice che $|X| \neq |\mathcal{P}(X)|$, cioè si ha $|X| < |\mathcal{P}(X)|$. In particolare, prendendo $X = \mathbb{N}$ otteniamo la disuguguaglianza tra cardinalità:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|.$$

In altre parole l'insieme delle parti $\mathcal{P}(\mathbb{N})$ ha cardinalità strettamente maggiore di quella di $\mathbb{N}$, cioè è più che numerabile.

Si può dare un'altra interpretazione della cardinalità dell'insieme delle parti.

Definizione 5.14. Siano A e B due insiemi. Denotiamo l'insieme delle funzioni da A a B con B^A:

$$B^A := \{f : A \to B \text{ funzione}\}.$$

Sia $B = \{0, 1\}$ l'insieme con due elementi, consideriamo l'insieme[8] $\{0,1\}^X = \big\{f : X \to \{0,1\}\big\}$.

Proposizione 5.15. *Sia X un insieme non vuoto. Allora $\mathcal{P}(X)$ è equipotente a $\{0,1\}^X$. In particolare, se X è finito $|\mathcal{P}(X)| = 2^{|X|}$.*

Dimostrazione. Sia $\varphi : 2^X \to \mathcal{P}(X)$ definita da $\varphi(f) = f^{-1}(1)$. L'applicazione φ è surgettiva. Infatti, dato $A \subseteq X$ consideriamo la *funzione caratteristica* di A

$$\chi_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A. \end{cases}$$

Si vede facilmente che $\varphi(\chi_A) = A$. L'applicazione φ è iniettiva, infatti se $f \neq g$ allora esiste $x \in X$ tale che $f(x) \neq g(x)$. Pertanto x apparterrà solo ad uno dei due insiemi $f^{-1}(1)$, $g^{-1}(1)$. Nel caso in cui X è finito, abbiamo quindi

$$|\mathcal{P}(X)| = \big|\{0,1\}^X\big| = |\{0,1\}|^{|X|} = 2^{|X|}.$$

□

Nel caso di insiemi finiti abbiamo un'ulteriore interpretazione dell'insieme delle funzioni B^A.

Lemma 5.16. *Siano $A = \{a_1, \ldots, a_n\}$ un insieme con n elementi e B un insieme finito. Allora la funzione*

$$\varphi : B^A \to B^n, \quad \varphi(f) = (f(a_1), \ldots, f(a_n))$$

è bigettiva. In particolare, gli insiemi B^A e B^n sono equipotenti.

[8] L'insieme $\{0,1\}^X$ si denota talvolta con 2^X, ma cercheremo di evitare tale notazione.

Dimostrazione. Per esercizio. □

Corollario 5.17. *Se A e B sono insiemi finiti, allora $A \times B$ e B^A sono insiemi finiti e*

$$|A \times B| = |A| \cdot |B|, \quad \left|B^A\right| = |B|^{|A|}.$$

Osservazione 5.18. La conclusione del corollario precedente non vale se A e B sono insiemi infiniti. Abbiamo visto ad esempio che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ (vedi Proposizione 5.7).

5.1 Le cardinalità di $\mathbb{Q}$ e $\mathbb{R}$

Lemma 5.19. *Sia $\{X_n : n \in \mathbb{N}\}$ una famiglia numerabile di insiemi al più numerabili non vuoti tali che, se $|X_n| < \aleph_0$ per ogni $n \in \mathbb{N}$ si abbia $X_n \cap X_m = \emptyset$ se $n \neq m$. Allora $\bigcup_{n\in\mathbb{N}} X_n$ è numerabile.*

Dimostrazione. Per ogni $n \in \mathbb{N}$, l'insieme X_n è al più numerabile, cioè $|X_n| \leq |\mathbb{N}|$. In particolare, esiste almeno una mappa iniettiva da X_n a $\mathbb{N}$, ne scegliamo una $f_n : X_n \to \mathbb{N}$ (la scelta è possibile grazie all'assioma della scelta). Consideriamo adesso due funzioni

$$\mu : \bigcup_{n\in\mathbb{N}} X_n \to \mathbb{N}, \ \mu(x) = \min\{n \in \mathbb{N} : \ x \in X_n\}$$
$$\phi : \bigcup_{n\in\mathbb{N}} X_n \to \mathbb{N} \times \mathbb{N}, \ \phi(x) = \left(\mu(x), f_{\mu(x)}(x)\right).$$

La mappa ϕ è iniettiva. Siano infatti x e y due elementi distinti di $\bigcup_{n\in\mathbb{N}} X_n$. Se $\mu(x) = \mu(y)$, allora $f_{\mu(x)}(x) \neq f_{\mu(x)}(y)$ perché $f_{\mu(x)}(x)$ è iniettiva e quindi $\phi(x) = (\mu(x), f_{\mu(x)}(x)) \neq (\mu(x), f_{\mu(x)}(y)) = \phi(y)$. Se $\mu(x) \neq \mu(y)$, allora $\phi(x) = (\mu(x), f_{\mu(x)}(x)) \neq (\mu(y), f_{\mu(y)}(y)) = \phi(y)$. Quindi si ha

$$\left|\bigcup_{n\in\mathbb{N}} X_n\right| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0.$$

Distinguiamo due casi.

1. Se esiste $n_0 \in \mathbb{N}$ tale che $|X_{n_0}| = \aleph_0$, allora

   $$\aleph_0 = |X_{n_0}| \leq \left|\bigcup_{n\in\mathbb{N}} X_n\right|$$

   e per il Teorema di Cantor–Bernstein si ha $\left|\bigcup_{n\in\mathbb{N}} X_n\right| = \aleph_0$.
2. Se $|X_n| < \aleph_0$ per ogni $n \in \mathbb{N}$, cioè tutti gli X_n sono insiemi finiti, allora fissiamo in ogni X_n un elemento $y_n \in X_n$. Siccome per ipotesi abbiamo che $X_n \cap X_m = \emptyset$ se $n \neq m$, gli elementi y_n sono tutti distinti. Pertanto la mappa

   $$h : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} X_n, \quad h(n) = y_n$$

   è iniettiva. Quindi $\aleph_0 = |\mathbb{N}| \leq \left|\bigcup_{n\in\mathbb{N}} X_n\right|$ e si conclude sempre per il Teorema di Cantor–Bernstein.

□

Teorema 5.20. *L'insieme $\mathbb{Q}$ dei numeri razionali è numerabile.*

Dimostrazione. Consideriamo la funzione

$$\psi : \mathbb{Q}^* \to \mathbb{N}^*, \quad \varphi\left(\frac{p}{q}\right) = |p| + |q|,$$

dove $p, q \in \mathbb{Z}$, $p, q \neq 0$ e $\mathrm{MCD}(p, q) = 1$. La mappa ψ è surgettiva e le controimmagini $\psi^{-1}(n)$ degli elementi di $\mathbb{N}^*$ sono finite e non vuote per ogni $n \in \mathbb{N}^*$. Inoltre sono a due a due disgiunte. Pertanto possiamo scrivere l'insieme $\mathbb{Q}$ come

$$\mathbb{Q} = \{0\} \cup \bigcup_{n \in \mathbb{N}^*} \psi^{-1}(n).$$

Quindi $\mathbb{Q}$ è numerabile per il Lemma 5.19. □

Concludiamo con il seguente risultato che non dimostriamo.

Teorema 5.21. *L'insieme dei numeri reali $\mathbb{R}$ è equipotente a $\mathcal{P}(\mathbb{N})$, in particolare è più che numerabile.*

6 Calcolo combinatorico

In questa sezione ci dedicheremo ad alcuni conteggi classici di cardinalità di insiemi finiti

Definizione 6.1. Sia X un insieme finito, un'applicazione bigettiva $X \to X$ viene detta **permutazione** di X. L'insieme delle permutazioni dell'insieme $X = \{1, \dots, n\}$ si denota con S_n (talvolta anche con $\mathfrak{S}_n$) e viene chiamato **insieme delle permutazioni**.

Lemma 6.2. *Siano X e Y due insiemi finiti con $|X| = n \leq m = |Y|$. Il numero di tutte le applicazioni iniettive $X \to Y$ è uguale a*

$$m \cdot (m-1) \cdots (m-n+1).$$

Dimostrazione. Siccome X ha cardinalità n possiamo "numerare" i suoi elementi e scrivere $X_n = \{x_1, \dots, x_n\}$. Contiamo quali sono le possibili immagini di x_1 in Y tramite un'applicazione iniettiva. Abbiamo m possibili scelte, siccome possiamo selezionare uno qualunque degli m elementi di Y. Ora, l'immagine di x_2 può essere un qualsiasi elemento di Y eccetto l'elemento che è stato scelto come immagine di x_1, perché l'applicazione deve essere iniettiva. Abbiamo quindi $m-1$ scelte per l'immagine di x_2. Analogamente abbiamo $m-2$ scelte per l'immagine di x_3 e così via, fino alle $m-n+1$ scelte per l'elemento x_n. □

Osservazione 6.3. Ricordiamo che per la Proposizione 5.9, se $|X| = n > m = |Y|$ non ci sono funzioni iniettive $X \to Y$.

Definizione 6.4 (fattoriale)**.** Sia $n \in \mathbb{N}$, il **fattoriale** di n è il numero intero

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

Dal Lemma 6.2, otteniamo immediatamente il seguente corollario.

Corollario 6.5. *Sia X un insieme finito con n elementi. Allora il numero di tutte le permutazioni di X è $n!$. In particolare $|S_n| = n!$.*

Introduciamo adesso un'altro strumento combinatorico utile per contare.

Definizione 6.6 (coefficiente binomiale)**.** Siano $k, n \in \mathbb{N}$ tali che $n \geq 1$ e $0 \leq k \leq n$, il **coefficiente binomiale** $\binom{n}{k}$ (si legge "n su k") è il numero intero

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

É immediato verificare le seguenti proprietà del coefficiente binomiale:

- $\binom{n}{0} = 1$;
- $\binom{n}{k} = \dfrac{n(n-1)\cdots(n-k+1)}{k!}$ se $k > 1$;

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

Lemma 6.7. *Siano $k, n \in \mathbb{N}^*$ con $n \geq 2$ e $0 \leq k \leq n$, allora*

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

Dimostrazione. Per esercizio. □

Il coefficiente binomiale risponde alla domanda: quanti sono i sottoinsiemi di k elementi di un insieme con n elementi?

Proposizione 6.8. *Sia X un insieme finito non vuoto con $|X| = n$. Per ogni intero $0 \leq k \leq n$ il numero di sottoinsiemi di X con esattamente k elementi è $\binom{n}{k}$.*

Dimostrazione. Per $k = 0$, abbiamo soltanto un sottoinsieme di X con 0 elementi, l'insieme vuoto $\emptyset$. Analogamente per $k = n$ abbiamo soltanto un sottoinsieme di X con n elementi, l'insieme X stesso. Siccome $\binom{n}{0} = 1 = \binom{n}{n}$, in questi due casi la tesi è dimostrata.

Per $0 < k < n$, contiamo in quanti modi possiamo costruire un sottoinsieme $Y \subseteq X$ di k elementi. Posso scegliere il primo elemento di Y in n modi diversi, prendendo uno qualsiasi degli elementi di X. Per il secondo elemento di Y, ho $n-1$ scelte, per il terzo $n-2$ e così via fino al k-esimo elemento di Y per cui ho $n-k+1$ scelte possibili. Ottengo così il numero $n \cdot (n-1) \cdots (n-k+1)$. In questo modo ho selezionato l'insieme Y in maniera ordinata, pertanto ciascuna permutazione di questi k elementi mi fornisce ancora lo stesso insieme Y. Quindi il numero di sottoinsiemi di k elementi è dato da

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

□

Il nome coefficiente binomiale è giustificato dal seguente teorema.

Teorema 6.9 (Teorema binomiale)**.** *Siano $x, y \in \mathbb{C}$ e sia $n \in \mathbb{N}^*$, si ha*

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

Dimostrazione. Per dimostrare la formula si può calcolare $(x+y)^n = (x+y)\cdots(x+y)$ e determinare il coefficiente di ciascun termine $x^{n-k}y^k$. Questo coefficiente è dato dal numero di modi in cui si possono scegliere k fattori nel prodotto di n fattori precedente. Per la Proposizione 6.8 questo numero è $\binom{n}{k}$.

In alternativa, dimostriamo il teorema per induzione su n. Per il passo base, l'uguaglianza da verificare è

$$(x+y)^1 = \sum_{k=0}^{1} \binom{1}{k} x^{1-k} y^k.$$

Il membro di sinistra è $(x+y)^1 = x+y$, mentre quello di destra è $\sum_{k=0}^{1} \binom{1}{k} x^{1-k} y^k = \binom{1}{0} x^{1-0} y^0 + \binom{1}{1} x^{1-1} y^1 = x + y$. Pertanto l'uguaglianza sussiste. Per il passo induttivo, supponiamo vera la tesi per $n-1$, e cioè l'uguaglianza

$$(x+y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k,$$

e dimostriamola per n. Scriviamo

$$\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} \\
&= (x+y) \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k \right) \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k-1} y^{k+1} \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=1}^{n} \binom{n-1}{k-1} x^{n-k} y^k \\
&= x^n + \sum_{k=1}^{n-1} \binom{n-1}{k} x^{n-k} y^k + y^n + \sum_{k=1}^{n-1} \binom{n-1}{k-1} x^{n-k} y^k \\
&= x^n + y^n + \sum_{k=1}^{n-1} \left(\binom{n-1}{k} + \binom{n-1}{k-1} \right) x^{n-k} y^k \\
&= x^n + y^n + \sum_{k=1}^{n-1} \binom{n}{k} x^{n-k} y^k \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.
\end{aligned}$$

□

Osservazione 6.10. Ponendo $x = y = 1$ nel teorema precedente, si ottiene l'uguaglianza

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Analogamente, ponendo $x = 1$ e $y = -1$ si ottiene l'identità

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Si può usare il coefficiente binomiale per dare un'altra dimostrazione della Proposizione 5.15 nel caso di insiemi finiti.

Corollario 6.11. *Sia X un insieme finito di cardinalità $|X| = n$, allora*

$$|\mathcal{P}(X)| = 2^n.$$

Dimostrazione. Dalla Proposizione 6.8 abbiamo che per ogni $0 \leq k \leq n$, il numero di sottoinsiemi di X con esattamente k elementi è $\binom{n}{k}$. Pertanto il numero totale di sottoinsiemi di X, cioè la cardinalità di $\mathcal{P}(X)$, è

$$|\mathcal{P}(X)| = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n,$$

dove la penultima uguaglianza segue dal Teorema binomiale. □

7 Relazioni d'ordine

Definizione 7.1. Sia X un insieme. Una relazione R su X è detta **preordine** se è
(1) *riflessiva*, cioè $\forall x \in X$ si ha $(x, x) \in R$;
(2) *transitiva*, cioè vale $((x, y) \in R) \wedge ((y, z) \in R) \Rightarrow (x, z) \in R$.
Se in aggiunta R è anche
(3) *antisimmetrica*, cioè vale $((x, y) \in R) \wedge ((y, x) \in R) \Rightarrow x = y$
si dice che R è un **ordine parziale**.

Un insieme X è **parzialmente ordinato** (in inglese "**poset**") se è dotato di un ordine parziale R. In tal caso scriviamo $(X, \lhd)$ dove utilizziamo il simbolo $\lhd$ per denotare l'ordine parziale, cioè scriviamo $x \lhd y$ invece di $(x, y) \in R$.

Osservazione 7.2. Molto spesso utilizzeremo anche il simbolo $\leq$ invece di $\lhd$ per denotare un ordine parziale. Questo in quanto gli ordini parziali sono dotati di proprietà simili a quelle della disuguaglianza classica tra numeri reali. Tuttavia si possono definire ordini parziali anche su insiemi X molto astratti e non soltanto su insiemi di numeri.

Definizione 7.3. Sia $(X, \lhd)$ un insieme parzialmente ordinato. Due elementi $x, y \in X$ si dicono **confrontabili** se vale $(x \lhd y) \vee (y \lhd x)$. L'ordine parziale $\lhd$ viene detto **ordine totale** se tutti gli elementi sono confrontabili, cioè se

$$\forall x, y \in X \text{ si ha } (x \lhd y) \vee (y \lhd x).$$

Se $\lhd$ è un ordine totale su X, l'insieme X viene detto **totalmente ordinato**.

Esempio 7.4.
1. La relazione "minore o uguale" $x \leq y$ sui numeri reali è un ordine totale su $\mathbb{R}$. La relazione "minore stretto" $x < y$ sui numeri reali non è un preordine in quanto non riflessiva.
2. La relazione diagonale Δ su un insieme X è un ordine parziale, ma non totale.
3. La relazione su $\mathbb{C}$ data da $z \lhd w$ se e solo se $|z| \leq |w|$ è un preordine, ma non è un ordine parziale.
4. Sia X un insieme non vuoto. La relazione su $\mathcal{P}(X)$ data da $A \lhd B$ se e solo se $A \subseteq B$ è un ordine parziale, ma non totale (a meno che X non sia un singoletto).
5. La relazione su $\mathbb{N}^*$ data da $n \lhd m$ se e solo se $n|m$ (cioè $m = n \cdot k$ per un qualche $k \in \mathbb{N}$) è un ordine parziale, ma non totale.

Definizione 7.5. Siano dati n insiemi parzialmenti ordinati $(A_1, \lhd_1), \ldots, (A_n, \lhd_n)$. Definiamo due ordini parziali sul prodotto cartesiano $A_1 \times \cdots \times A_n$.
(i) L'**ordine lessicografico** (LEX)

$$(a_1, \ldots, a_n) \lhd_{\text{LEX}} (b_1, \ldots, b_n) \iff \begin{cases} a_1 \lhd_1 b_1 & \text{se } a_1 \neq b_1 \\ a_{k+1} \lhd_{k+1} b_{k+1} & \text{se } a_j = b_j \ \forall j = 1, \ldots, k. \end{cases}$$

(ii) L'**ordine prodotto** $\lhd_1 \times \cdots \times \lhd_n$

$$(a_1, \ldots, a_n) \lhd_1 \times \cdots \times \lhd_n (b_1, \ldots, b_n) \iff a_i \lhd_i b_i \ \forall i = 1, \ldots, n.$$

Osservazione 7.6. Non è difficile verificare che se tutti i poset $(A_1, \lhd_1), \ldots, (A_n, \lhd_n)$ sono totalmente ordinati, allora $(A_1 \times \cdots \times A_n, \mathrm{LEX})$ è totalmente ordinato. Invece anche se i poset $(A_1, \lhd_1), \ldots, (A_n, \lhd_n)$ sono totalmente ordinati, non è detto che $(A_1 \times \cdots \times A_n, \lhd_1 \times \cdots \times \lhd_n)$ sia totalmente ordinato. Ad esempio $(\mathbb{R}, \leq)$ è totalmente ordinato, ma $(\mathbb{R}^2, \leq \times \leq)$ non è totalmente ordinato perché gli elementi $(1, 0)$ e $(0, 1)$ non sono confrontabili.

Definizione 7.7. Sia $(X, \lhd)$ un poset e sia $Y \subseteq X$ un sottoinsieme. L'**ordine indotto** su Y è l'ordine $\lhd_Y$ dato da $x \lhd_Y y$ se e solo se $x \lhd y$. Diremo che Y è una **catena** se $\lhd_Y$ è un ordine totale su Y.

Esempio 7.8. Consideriamo il poset $(\mathbb{N}^*, |)$. Fissato $a \in \mathbb{N}^*$ l'insieme $Y_a = \{a^k : \ k \in \mathbb{N}\}$ è una catena.

Definizione 7.9. Sia $(X, \lhd)$ un poset, sia $Y \subseteq X$ un sottoinsieme non vuoto, e sia $y \in Y$.

- y è il **minimo** di Y se per ogni $x \in Y$ si ha $y \lhd x$. In tal caso scriviamo $y = \min Y$.
- y è il **massimo** di Y se per ogni $x \in Y$ si ha $x \lhd y$. In tal caso scriviamo $y = \max Y$.
- y è **elemento minimale** di Y se per ogni $x \in Y$ vale $x \lhd y \Rightarrow x = y$.
- y è **elemento massimale** di Y se per ogni $x \in Y$ vale $y \lhd x \Rightarrow x = y$.

Osservazione 7.10. Valgono i fatti seguenti.

- Gli elementi minimo e massimo, se esistono, sono unici.
- Se esiste il minimo ogni elemento minimale coincide con il minimo. Analogamente se esiste il massimo ogni elemento massimale coincide con il massimo.
- Se $\lhd$ è un ordine totale, esiste un elemento minimale se e solo se esiste il minimo ed esiste un elemento massimale se e solo se esiste il massimo.

Esempio 7.11.

1. Consideriamo il poset $(\mathbb{N}, \leq)$ e prendiamo $Y = \mathbb{N}$. L'elemento minimo è 0 ed è anche l'unico elemento minimale. Non esiste il massimo e non esistono elementi massimali.
2. Consideriamo il poset $(\mathbb{Z}_{<0}, \leq)$ e prendiamo $Y = \mathbb{Z}_{<0}$. L'elemento massimo è -1 e non esiste l'elemento minimo. Essendo $\leq$ un ordine totale non esistono elementi minimali.
3. Consideriamo il poset $(\mathbb{Z}, \leq)$ e prendiamo $Y = \mathbb{Z}$. Non esiste nè massimo nè minimo. Essendo $\leq$ un ordine totale non esistono nè elementi minimali nè elementi massimali.

4. Sia X un insieme, consideriamo il poset $(\mathcal{P}(X), \subseteq)$. L'insieme vuoto $\emptyset$ è il minimo di $\mathcal{P}(X)$ e X è il massimo di $\mathcal{P}(X)$. Sia Y il sottoinsieme di $\mathcal{P}(X)$ costituito dai singoletti, cioè
$$Y = \{\{x\} : \ x \in X\}.$$
Ogni elemento di Y è sia minimale che massimale per Y, ma Y non ammette nè massimo nè minimo.

5. Consideriamo la famiglia $X = \{n\mathbb{Z} : \ n \in \mathbb{N}, n \geq 2\}$ dei sottoinsiemi di $\mathbb{Z}$ definiti come
$$n\mathbb{Z} = \{m \in \mathbb{Z} : \ m = nk, \ \text{ per un qualche } k \in \mathbb{Z}\}.$$
In altre parole $n\mathbb{Z}$ è l'insieme dei multipli (interi) di n. Allora $(X, \subseteq)$ è un insieme parzialmente ordinato. Osserviamo che se $a, b \geq 2$ sono interi, allora si ha
$$a\mathbb{Z} \subseteq b\mathbb{Z} \iff b|a.$$
In particolare, gli elementi $p\mathbb{Z}$ con p numero primo sono massimali di X. Non vi sono elementi minimali. Non vi è l'elemento massimo, nè l'elemento minimo.

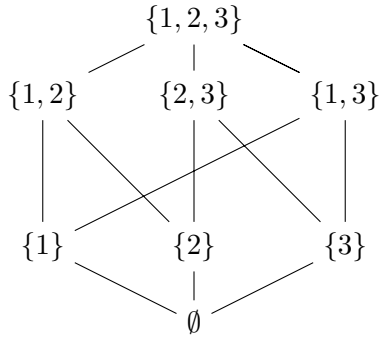
6. L'insieme
$$A = \{(n, n + (-1)^n) : \ n \in \mathbb{N}, n \geq 2\} = \{(2,3), (3,2), (4,5), (5,4), \dots\} \subseteq \mathbb{N} \times \mathbb{N}$$
con l'ordine indotto da $(\mathbb{N} \times \mathbb{N}, \leq \times \leq)$ ha due elementi minimali $(2,3)$ e $(3,2)$ ma non ha minimo.

7. Consideriamo $X = \{0, 1, 2, 3, \omega\}$ con il seguente ordine:
$$0 \lhd 1 \lhd 2 \lhd 3, \ 0 \lhd 0, \ 1 \lhd 1, \ 2 \lhd 2, \ 3 \lhd 3, \ \omega \lhd \omega.$$
Si verifica che $(X, \lhd)$ è un poset. Il sottoinsieme $Y = \{0, \omega\}$ non ha nè massimo nè minimo. L'elemento 0 è sia minimale che massimale per Y, l'elemento ω è sia minimale che massimale per Y.

Osservazione 7.12. Sia $(X, \lhd)$ un poset finito (cioè X è un insieme finito). Allora ogni sottoinsieme $Y \subseteq X$ ha elementi massimali e minimali. In tal caso può essere utile rappresentare gli elementi di X tramite un *diagramma di Hasse*. Si rappresenta ogni elemento di X come vertice e si traccia una linea che va da $x \in X$ a $y \in X$ se $x \lhd y$ e non esiste $z \in X$ tale che $x \lhd z \lhd y$. In questo caso si dice che y è un successore immediato di x. Inoltre si richiede che i vertici siano posizionati in modo che ogni segmento incontri esattamente due vertici: i due estremi.

Illustriamo la costruzione di un diagramma di Hasse in un esempio.

Esempio 7.13. Consideriamo $A = \{1, 2, 3\}$ e il poset dell'insieme delle parti $(\mathcal{P}(A), \subseteq)$. Il corrispondente diagramma di Hasse è il seguente.



Definizione 7.14. Sia $(X, \lhd)$ un poset. L'**ordine opposto** $\lhd^\circ$ su X è definito da

$$x \lhd^\circ y \iff y \lhd x.$$

Si verifica facilmente che l'ordine opposto è un ordine parziale. Gli eventuali elementi massimali (il massimo) per $\lhd$ diventano minimali (il minimo) per $\lhd^\circ$ e viceversa.

Definizione 7.15. Sia $(X, \lhd)$ un poset, sia $Y \subseteq X$ un suo sottoinsieme non vuoto, e sia $z \in X$.

- z è un **minorante** di Y se per ogni $x \in Y$ vale $z \lhd x$.
- z è un **maggiorante** di Y se per ogni $x \in Y$ vale $x \lhd z$.
- Se l'insieme dei minoranti di Y è non vuoto e ha massimo z, diciamo che z è l'**estremo inferiore** di Y. In tal caso scriviamo $z = \inf Y$.
- Se l'insieme dei maggioranti di Y è non vuoto e ha minimo z, diciamo che z è l'**estremo superiore** di Y. In tal caso scriviamo $z = \sup Y$.

Osservazione 7.16. Si verifica facilmente che se $\inf Y \in Y$ allora $\inf Y = \min Y$. Analogamente se $\sup Y \in Y$ allora $\sup Y = \max Y$. In altre parole, se il minimo di Y esiste allora coincide con l'estremo inferiore e se il massimo di Y esiste allora coincide con l'estremo superiore.

Esempio 7.17.

1. Consideriamo il poset $(\mathbb{R}, \leq)$ e l'intervallo $Y = (0, 1)$. L'insieme Y non ha nè massimo nè minimo. L'insieme dei minoranti di Y è l'intervallo $(-\infty, 0]$ e l'insieme dei maggioranti di Y è $[1, +\infty)$. Pertanto si ha $0 = \inf Y$, $1 = \sup Y$.

2. Consideriamo il poset $(\mathbb{R}, \leq)$ e l'intervallo $Y = [0, 1]$. L'insieme dei minoranti di Y è l'intervallo $(-\infty, 0]$, pertanto si ha $0 = \inf Y$. Siccome $\inf Y \in Y$ si ha anche $\min Y = \inf Y = 0$. Analogamente l'insieme dei maggioranti di Y è l'intervallo $[1, +\infty)$ e quindi $\max Y = \sup Y = 1$.

3. Consideriamo il poset dell'insieme delle parti $(\mathcal{P}(A), \subseteq)$, dove $A = \{1, 2, 3\}$ come nell'Esempio 7.13. Prendiamo il sottoinsieme $Y \subseteq \mathcal{P}(A)$ dato da $Y = \{\{2\}, \{3\}\}$. L'insieme dei maggioranti di Y è
$$\{\{2, 3\}, \{1, 2, 3\}\}$$
che ha come minimo $\{2, 3\}$. Pertanto $\sup Y = \{2, 3\}$. Analogamente l'insieme dei minoranti di Y è $\{\emptyset\}$ che ha come massimo $\emptyset$. Quindi $\inf Y = \emptyset$. D'altra parte, notiamo che Y non ammette nè massimo nè minimo (in quanto $\{2\}$ e $\{3\}$ non sono confrontabili).

7.1 Appendice: insiemi bene ordinati e ben fondati

Definizione 7.18. Sia $(X, \lhd)$ un poset. Diciamo che X è **bene ordinato** se ogni sottoinsieme non vuoto di X ha un elemento minimo.

Esempio 7.19.

1. Per il *principio del minimo* dei numeri naturali (vedi pagina 16), il poset $(\mathbb{N}, \leq)$ è bene ordinato. Cioè dato un qualunque sottoinsieme non vuoto Y di $\mathbb{N}$, l'insieme Y ha sempre un elemento minimo. Lo stesso vale per il poset $(\mathbb{N}^*, \leq)$.
2. Il poset $(\mathbb{Z}, \leq)$ non è bene ordinato, ad esempio il sottoinsieme $Y = \{n \in \mathbb{Z} : \ n < 0\}$ non ammette minimo.
3. Il poset $(\mathbb{N}^* \times \mathbb{N}^*, \leq \times \leq)$ non è bene ordinato. Ad esempio il sottoinsieme $Y = \{(2,3), (3,2)\}$ non ammette minimo.

Come mostra l'esempio precedente, il prodotto di insiemi bene ordinati con l'ordine prodotto non è, in generale, bene ordinato. Vale però la seguente proposizione.

Proposizione 7.20. *Siano $(X_1, \lhd_1)$ e $(X_2, \lhd_2)$ due poset bene ordinati. Allora $(X_1 \times X_2, \mathrm{LEX})$ è bene ordinato.*

Dimostrazione. Sia $A \subseteq X_1 \times X_2$ un insieme non vuoto. L'insieme

$$\mathrm{pr}_1(A) = \{x \in X_1 : \ \exists y \in X_2 \ (x, y) \in A\} \subseteq X_1$$

è un sottoinsieme non vuoto di X_1 che è bene ordinato, quindi ammette minimo. Sia $x_A = \min \mathrm{pr}_1(A)$. Consideriamo adesso l'insieme

$$B = \{y \in X_2 : \ (x_A, y) \in A\}.$$

Si tratta di un sottoinsieme di X_2 che è bene ordinato, pertanto $\exists y_B = \min B$. Per come sono stati costruiti x_A e y_B si ha che $(x_A, y_B) \leq_{\mathrm{LEX}} (x, y)$ per ogni $(x, y) \in A$. Pertanto $(x_A, y_B) = \min A$ e quindi il poset prodotto con l'ordine LEX è bene ordinato. □

Assioma del buon ordinamento. *Dato un insieme non vuoto X, esiste un ordine parziale $\lhd$ su X tale che $(X, \lhd)$ è un poset bene ordinato.*

L'assioma del buon ordinamento è equivalente all'assioma della scelta ed è anche equivalente al seguente assioma, detto Lemma di Zorn.

Lemma di Zorn. *Sia $(X, \lhd)$ un poset non vuoto tale che ogni catena in X possiede (almeno) un maggiorante, allora X possiede elementi massimali. Analogamente, se ogni catena in X possiede (almeno) un minorante, allora X possiede elementi minimali.*

Nonostante grazie all'assioma del buon ordinamento ogni insieme ammetta un ordine parziale che lo rende bene ordinato, spesso molti poset di interesse non risultano essere bene ordinati[9]. Per questo motivo, in alcuni contesti è utile introdurre la seguente nozione più debole.

[9] Questo può sembrare strano a prima vista, ma si tenga presente che la nozione di bene ordinato dipende dall'ordine scelto. Ad esempio $\mathbb{N} \times \mathbb{N}$ non è bene ordinato con l'ordine prodotto, ma è bene ordinato con l'ordine LEX.

Definizione 7.21. Sia $(X, \lhd)$ un poset. Diciamo che X è **ben fondato** se ogni sottoinsieme non vuoto di X ha un elemento minimale.

Siccome ogni elemento minimo è in particolare minimale, per un poset $(X, \lhd)$ vale

$$X \text{ bene ordinato} \implies X \text{ ben fondato.}$$

Il viceversa non vale in generale, come mostrano i seguenti esempi.

Esempio 7.22. Consideriamo il poset $(X, \lhd)$, dove $X = \{0, 1, 2, 3, \omega\}$ e l'ordine $\lhd$ è dato da $0 \lhd 1 \lhd 2 \lhd 3,\ \omega \lhd \omega$, come nell'Esempio 7.11. Allora $(X, \lhd)$ non è bene ordinato, ad esempio il sottoinsieme $Y = \{0, \omega\}$ non ha nè massimo nè minimo. D'altra parte si verifica che $(X, \lhd)$ è ben fondato, in quanto ogni sottoinsieme non vuoto di X ha elementi minimali.

Gli insiemi ben fondati permettono di utilizzare una generalizzazione del principio di induzione, chiamata **induzione strutturale**.

Principio di induzione strutturale. *Sia $(X, \lhd)$ un poset ben fondato. Sia $\mathcal{P}$ una affermazione sugli elementi di X. Supponiamo siano soddisfatte le seguenti due condizioni:*
(i) *$\mathcal{P}(x)$ è vera per ogni $x \in X$ elemento minimale;*
(ii) *per ogni $y, z \in X$ tali che $y \lhd z$ se $\mathcal{P}(y)$ è vera allora $\mathcal{P}(z)$ è vera.*
Allora $\mathcal{P}(x)$ è vera per ogni $x \in X$.

Concludiamo con la seguente proposizione, analogo della Proposizione 7.23 per insiemi ben fondati.

Proposizione 7.23. *Siano $(X_1, \lhd_1)$ e $(X_2, \lhd_2)$ due poset ben fondati. Allora $(X_1 \times X_2, \mathrm{LEX})$ e $(X_1 \times X_2, \lhd_1 \times \lhd_2)$ sono ben fondati.*

Dimostrazione. Per esercizio. □

8 Aritmetica modulare

8.1 Operazioni binarie

Definizione 8.1. Sia A un insieme, un'**operazione binaria** $*$ su A è una funzione

$$* : A \times A \to A$$

Useremo la notazione $x * y$ per indicare l'immagine $*(x, y)$.

Esempio 8.2. La somma $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ e il prodotto $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sono due operazioni su $\mathbb{Z}$. Allo stesso modo la somma e il prodotto su $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ sono operazioni binarie sui rispettivi insiemi.

Un'operazione $*$ su un insieme A può soddisfare diverse proprietà. Le più comuni ed importanti sono le seguenti.

- **Proprietà commutativa:** $\forall a, b \in A$ vale $a * b = b * a$.
- **Proprietà associativa:** $\forall a, b, c \in A$ vale $a * (b * c) = (a * b) * c$.
- **Elemento neutro:** $\exists e \in A$ tale che $\forall a \in A$ vale $e * a = a * e = a$.

Esempio 8.3.

1. La somma e il prodotto in $\mathbb{Z}$ sono associativi e commutativi. L'elemento neutro della somma è 0. L'elemento neutro del prodotto è 1.
2. Dato A insieme non vuoto, la composizione di funzioni

$$\begin{aligned} \circ : A^A \times A^A &\longrightarrow A^A \\ (f, g) &\mapsto g \circ f \end{aligned}$$

   è un'operazione associativa, ma non commutativa (a meno che A non sia un singoletto). L'elemento neutro è la funzione identità id_A.
3. L'operazione $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ tale che $x * y = \sqrt[3]{x + y}$ è commutativa, ma non associativa.
4. L'operazione $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tale che $a * b = 2a + 3b$ non è commutativa, non è associativa e non ha elemento neutro.

8.2 Le operazioni in $\mathbb{Z}_n$

Sia $n \geq 2$ e consideriamo l'insieme $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ delle classi di resto modulo n introdotto nell'Esempio 4.5 e dotiamolo di due operazioni.

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\overline{a}, \overline{b}) &\mapsto \overline{a + b} \end{aligned} \qquad \begin{aligned} \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\overline{a}, \overline{b}) &\mapsto \overline{a \cdot b} \end{aligned}$$

Verifichiamo che queste operazioni sono ben definite, cioè la corrispondente applicazione non dipende dalla scelta del rappresentante della classe in $\mathbb{Z}_n$, ma assume lo stesso valore su tutta

la classe. Siano $a, b, r, s \in \mathbb{Z}$ tali che $\overline{a} = \overline{r}$ e $\overline{b} = \overline{s}$ in $\mathbb{Z}_n$ allora $a - r = kn$ e $b - s = hn$ per qualche $h, k \in \mathbb{Z}$. Abbiamo quindi

$$a + b = r + kn + s + hn = r + s + (k + h)n \quad \text{ossia} \quad \overline{a + b} = \overline{r + s}.$$

Analogamente

$$ab = (r + kn)(s + hn) = rs + (rh + sk + khn)n \quad \text{ossia} \quad \overline{a \cdot b} = \overline{r \cdot s}.$$

Le operazioni + e $\cdot$ su $\mathbb{Z}_n$ verificano la proprietà commutativa e la proprietà associativa, si tratta di una conseguenza del fatto che la somma e il prodotto in $\mathbb{Z}$ verificano le stesse proprietà. Analogamente, vale anche la proprietà distributiva, cioè

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \qquad \forall a, b, c \in \mathbb{Z}.$$

Inoltre la classe $\overline{0}$ è elemento neutro della somma e la classe $\overline{1}$ è elemento neutro del prodotto.

Dato una qualunque classe $\overline{a} \in \mathbb{Z}_n$ esiste sempre un'altra classe $\overline{b} \in \mathbb{Z}_n$ tale che $\overline{a} + \overline{b} = \overline{0}$. Basta prendere $\overline{b} = \overline{-a}$, cioè la classe dell'opposto di a in $\mathbb{Z}$. Scriviamo quindi $-\overline{a}$ per indicare la classe $\overline{-a}$ che chiamiamo **opposto** di $\overline{a}$ (o anche *inverso rispetto alla somma*). Per il prodotto la situazione è più complicata, come illustra il seguente esempio.

Esempio 8.4. Consideriamo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. La classe $\overline{3}$ ammette un inverso rispetto al prodotto, infatti $\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$ che è l'elemento neutro del prodotto. Invece la classe $\overline{2}$ non ha un inverso rispetto al prodotto, infatti

$$\overline{2} \cdot \overline{2} = \overline{4} \neq \overline{1}, \quad \overline{2} \cdot \overline{3} = \overline{6} \neq \overline{1}, \quad \overline{2} \cdot \overline{4} = \overline{8} \neq \overline{1}.$$

Definizione 8.5. La classe $\overline{a} \in \mathbb{Z}_n$ si dice **invertibile in** $\mathbb{Z}_n$ (rispetto al prodotto) se $\exists \overline{b} \in \mathbb{Z}_n$ tale che $\overline{a} \cdot \overline{b} = \overline{1}$. In tal caso $\overline{b}$ si dice **inverso** di $\overline{a}$ e si denota con $\overline{a}^{-1}$. Altrimenti $\overline{a}$ si dice **non invertibile in** $\mathbb{Z}_n$. Denotiamo con $U(\mathbb{Z}_n)$ l'insieme degli elementi invertibili di $\mathbb{Z}_n$, cioè

$$U(\mathbb{Z}_n) := \{\overline{a} \in \mathbb{Z}_n : \ \overline{a} \text{ è invertibile}\}.$$

Esempio 8.6. Si verifica facilmente che $U(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$.

Possiamo dare una caratterizzazione degli elementi invertibili di $\mathbb{Z}_n$.

Teorema 8.7. *Sia $\overline{x} \in \mathbb{Z}_n$. Allora*

$$\overline{x} \text{ *è invertibile*} \iff \mathrm{MCD}(x, n) = 1.$$

Dimostrazione. Osserviamo innanzitutto che se $\overline{x} = \overline{y}$ allora si ha

$$\mathrm{MCD}(x, n) = 1 \iff \mathrm{MCD}(y, n) = 1.$$

Ciò segue subito dal fatto che $x = y + hn$ con $h \in \mathbb{Z}$. Pertanto la condizione $\mathrm{MCD}(x, n) = 1$ non dipende dalla scelta del rappresentante della classe $\overline{x}$.

"$\Rightarrow$" Se $\overline{x}$ è invertibile allora $\exists \overline{z} \in \mathbb{Z}_n$ tale che $\overline{x} \cdot \overline{z} = \overline{1}$. Pertanto $xz = 1 + kn$ per un qualche $k \in \mathbb{Z}$. Quindi otteniamo l'identità (di Bézout) $xz - kn = 1$ che mostra $\mathrm{MCD}(x, n) = 1$ (vedi Teorema 2.16).

"$\Leftarrow$" Viceversa se $\mathrm{MCD}(x, n) = 1$, per il Teorema 2.16 esistono $z, k \in \mathbb{Z}$ tali che $xz - kn = 1$. Pertanto $xz = 1 + kn$, cioè $\overline{x} \cdot \overline{z} = \overline{1}$ e quindi $\overline{x}$ è invertibile. □

Definizione 8.8. Dato un intero $m \in \mathbb{N}^*$ definiamo le potenze di una classe $\overline{a} \in \mathbb{Z}_n$ come

$$\overline{a}^m := \underbrace{\overline{a \cdots a}}_{m \text{ volte}}.$$

Se $m < 0$ e $\overline{a}$ è invertibile, definiamo $\overline{a}^m := (\overline{a}^{-1})^{-m}$. Poniamo infine $\overline{a}^0 := \overline{1}$ per ogni $\overline{a} \neq \overline{0}$.

8.3 I teoremi di Eulero e Fermat

Definizione 8.9. La funzione φ **di Eulero** è la funzione $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ definita da

$$\varphi(n) = \#\{m \in \mathbb{N}^* : \ m \leq n, \ \mathrm{MCD}(m, n) = 1\}.$$

ossia il numero dei naturali positivi $\leq n$ che sono coprimi con n.

Esempio 8.10. I primi valori della funzione φ sono i seguenti:

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Osservazione 8.11. Per il Teorema 8.7, la funzione di Eulero fornisce la cardinalità dell'insieme degli elementi invertibili di $\mathbb{Z}_n$:

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

Osservazione 8.12. Dato un intero $n \gg 0$ è un problema computazionalmente difficile determinare $\varphi(n)$. Diventa più semplice se si conosce la fattorizzazione di n. In tal caso si possono sfruttare le seguenti proprietà

$$\varphi(p) = p - 1 \ \forall p \ \text{ numero primo}$$
$$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{se } \mathrm{MCD}(m, n) = 1.$$

Più in generale, se n si fattorizza come $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ con $p_1, \ldots, p_s$ numeri primi, si ha

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Teorema 8.13 (Eulero)**.** *Siano $n, x \in \mathbb{Z}$ con $n \geq 2$ tali che* $\mathrm{MCD}(x, n) = 1$*. Allora*

$$x^{\varphi(n)} \equiv 1 \mod n.$$

Equivalentemente, $[x]^{\varphi(n)} = [1]$ in $\mathbb{Z}_n$.

Dimostrazione. Sappiamo dal Teorema 8.7 che gli elementi invertibili di $\mathbb{Z}_n$ sono le $\varphi(n)$ classi $[a]$ con $1 \leq a < n$ e $\mathrm{MCD}(a, n) = 1$. Indichiamo queste classi (distinte) con $[a_1], [a_2], \ldots, [a_{\varphi(n)}]$. Pertanto si ha

$$a_i \not\equiv a_j \mod n \ \text{ se } i \neq j.$$

Siccome x è coprimo con n e anche gli a_i lo sono, abbiamo $\mathrm{MCD}(a_i x, n) = 1$ per ogni $i = 1, \ldots, \varphi(n)$. Quindi anche la classe $[a_i x]$ è invertibile in $\mathbb{Z}_n$, abbiamo quindi

$$a_i x \equiv a_j$$

per un opportuno indice j che dipende da x e da a_i. Moltiplicando tra loro $[a_1x], \ldots, [a_{\varphi(n)}x]$ otteniamo tutte e sole le classi degli elementi invertibili in $\mathbb{Z}_n$, cioè

$$[a_1] \cdots [a_{\varphi(n)}] = [a_1x] \cdots [a_{\varphi(n)}x] = [a_1] \cdots [a_{\varphi(n)}][x]^{\varphi(n)}.$$

Moltiplicando ambi i membri per $[a_1]^{-1} \cdots [a_{\varphi(n)}]^{-1}$ otteniamo $[x]^{\varphi(n)} = [1]$ come richiesto. □

Se $n = p$ un numero primo, siccome $\varphi(p) = p - 1$ otteniamo come corollario il Teorema di Fermat.

Teorema 8.14 (Fermat)**.** *Sia p un numero primo e sia $x \in \mathbb{Z}$ tale che $p \nmid x$. Allora*

$$x^{p-1} \equiv 1 \mod p.$$

Equivalentemente, $[x]^{p-1} = [1]$ in $\mathbb{Z}_p$.

Osservazione 8.15. Il Teorema di Eulero–Fermat permette di determinare l'inverso di un elemento $[x] \in U(\mathbb{Z}_n)$ se si conosce $\varphi(n)$. Si ha infatti

$$[x]^{-1} = x^{\varphi(n)-1}.$$

In particolare, se $n = p$ primo si ha $[x]^{-1} = [x]^{p-2}$.

8.4 Appendice: il crittosistema RSA

Ci concentriamo adesso adesso su un'importante applicazione dell'aritmetica modulare. Vediamo come le nozioni introdotte finora si possono usare per costruire un crittosistema a chiave pubblica: il crittosistema RSA. Iniziamo con una formalizzazione matematica del concetto di crittosistema.

Definizione 8.16. Un **crittosistema** consiste di:

- un insieme finito A detto alfabeto (ad esempio $A = \mathbb{Z}_n$);
- l'insieme dei possibili messaggi in chiaro (*plaintexts*) $M \subseteq \bigcup_{m \in \mathbb{N}^*} A^m$;
- l'insieme dei possibili messaggi cifrati (*cyphertexts*) $C \subseteq \bigcup_{m \in \mathbb{N}^*} A^m$;
- l'insieme delle chiavi K;
- una funzione di cifratura (*encryption function*) $E : K \times M \to C$;
- una funzione di decifratura (*decryption function*) $D : K \times C \to M$;
- l'insieme delle chiavi ammissibili $S \subseteq K \times K$ tali che $\forall (k, k') \in S$ si ha

$$D(k', E(k, x)) = x \quad \forall x \in M.$$

Nella pratica, se due persone o enti, che per praticità chiameremo Alice e Bob, vogliono comunicare attraverso un canale di comunicazione insicuro, cioè nel quale ogni comunicazione viene intercettata e ascoltata, possono procedere nella maniera seguente. Alice e Bob si accordano su un crittosistema da usare e scelgono *preventivamente* una coppia di chiavi $(k, k') \in S$. Se Alice vuole inviare il messaggio $x \in M$ a Bob, calcola $y = D(k, x)$ e invia $y \in C$ attraverso il canale insicuro. Bob riceve $y \in C$ e calcola $x' = D(k', E(k, x))$. Grazie alle proprietà del crittosistema, si ha $x' = x$ e quindi Bob recupera il messaggio x di Alice.

Esempio 8.17 (Cifrario di Cesare)**.** Scegliamo[10] $A = M = C = \mathbb{Z}_n$. L'insieme delle chiavi è $K = \mathbb{Z}_n \setminus \{0\}$ e quello delle chiavi ammissibili è dato da $S = \{(k, k) : \ k \in K\}$, cioè la chiave di cifratura è la stessa della chiave di decifratura. Le funzioni di cifratura e decifratura sono

$$E(k, x) = x + k \qquad D(k, y) = y - k.$$

Ad esempio per $k = 3$ (la scelta usuale di Cesare), la parola

$$x = C|A|E|S|A|R = 3|1|5|19|1|18$$

viene cifrata in

$$y = 6|4|8|22|4|21 = F|D|H|V|D|U.$$

Questo cifrario è debole contro attacchi di "forza bruta". Se n è piccolo, ci sono soltanto $n - 1$ possibili chiavi.

Un'altro svantaggio del crittosistema di Cesare è che Alice e Bob devono accordarsi preventivamente su una chiave per poter comunicare, e devono potersi scambiare questa chiave attraverso un canale sicuro. Questo è un difetto comune a tutti i sistemi crittografici di tipo simmetrico.

Definizione 8.18. Un crittosistema è detto **simmetrico** o **a chiave segreta** se $S = \{(k, k) : k \in K\}$. Un crittosistema è detto **asimmetrico** o **a chiave pubblica** se non è possibile ottenere (in tempo ragionevole) la chiave di decifratura conoscendo la chiave di cifratura.

Il cifrario di Cesare è un crittosistema a chiave segreta. Uno dei primi crittosistemi a chiave pubblica ad essere stati proposti ed utilizzati è il **crittosistema RSA**, inventato nel 1977 da Rivest, Shamir, e Adleman. Lo descriviamo.

Bob sceglie $p, q \in \mathbb{N}$ due numeri primi "grandi" (e.g. $p, q \cong 2^{512} \cong 10^{154}$) e calcola $n = p \cdot q$. Calcola anche $\varphi(n) = (p - 1)(q - 1)$. Sceglie un intero $e \in \mathbb{Z}$ in modo che sia invertibile mod $\varphi(n)$ e calcola il suo inverso d. Cioè $e \cdot d = 1 \bmod \varphi(n)$. Gli insiemi del crittosistema sono $C = M = \mathbb{Z}_n$ e $K = \mathbb{Z}$ e le funzioni di cifratura e decifratura sono

$$\begin{aligned} E : \mathbb{Z} \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (e, \overline{x}) &\mapsto \overline{x}^e \end{aligned} \qquad \begin{aligned} D : \mathbb{Z} \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (d, \overline{y}) &\mapsto \overline{y}^d \end{aligned}$$

[10] Spesso si usa $n = 26$ facendo corrispondere $A \longleftrightarrow \overline{1}$, $B \longleftrightarrow \overline{2}$ e così via. Inoltre per facilitare la lettura in questo esempio omettiamo i simboli di classe $\overline{x}$ o $[x]$ per denotare le classi in $\mathbb{Z}_n$.

L'insieme delle chiavi ammissibili è

$$S = \{(e, d) \in \mathbb{Z} \times \mathbb{Z} : \ e \cdot d = 1 \bmod \varphi(n)\}.$$

Bob comunica l'intero e ad Alice, mentre mantiene segreto d. Se Alice vuole mandare un messaggio $\overline{x} \in \mathbb{Z}_n$ a Bob, calcola $\overline{y} = \overline{x}^e \in \mathbb{Z}_n$ e lo invia a Bob. Bob calcola $\overline{x'} = \overline{y}^d \in \mathbb{Z}_n$. Verifichiamo che $\overline{x'} = \overline{x}$, e cioè che Bob recupera il messaggio originale.

$$D(d, E(e, \overline{x})) = D(d, \overline{x}^e) = \overline{x}^{ed} = \overline{x}^{1+h\varphi(n)} = \overline{x} \cdot (\overline{x}^{\varphi})^h = \overline{x} \cdot \overline{1}^h = \overline{x}.$$

Abbiamo usato che se $ed = 1 \bmod \varphi(n)$ allora $ed = 1 + h\varphi(n)$ per un qualche intero $h \in \mathbb{Z}$. Mentre l'uguaglianza $\overline{x}^{\varphi(n)} = \overline{1}$ in $\mathbb{Z}_n$ segue dal Teorema di Eulero[11].

Ricapitolando, i dati del sistema sono:

(i) n, e *pubblici*;

(ii) p, q, $\varphi(n)$, d *privati* (cioè noti solo a Bob).

Esempio 8.19. 1) Bob sceglie $p = 101$, $q = 113$. Calcola $n = p \cdot q = 11413$ e $\varphi(n) = (p-1)(q-1) = 100 \cdot 112 = 11200$.

2) Bob sceglie $e = 3533$ che è coprimo con $\varphi(n)$ e quindi invertibile in $\mathbb{Z}_{\varphi(n)}$ e calcola il suo inverso $d = e^{-1} = 6597 \bmod \varphi(n)$.

3) Bob pubblica la sua chiave pubblica data dalla coppia $(n, e) = (11413, 3533)$. Il resto rimane segreto.

4) Alice vuole mandare il messaggio $\overline{x} = \overline{9726} \in \mathbb{Z}_n$ a Bob.

5) Alice calcola $\overline{y} = \overline{x}^e = \overline{9726}^{3533} = \overline{5761} \in \mathbb{Z}_n$ e lo manda a Bob.

6) Bob calcola $\overline{y}^d = \overline{5761}^{6597} = \overline{9726} \in \mathbb{Z}_n$ e recupera il messaggio originale di Alice.

Osservazione 8.20. Un osservatore esterno, che per praticità chiameremo Eve, in grado di ascoltare i messaggi inviati attraverso il canale vuole trovare $\overline{x}$ (o d) conoscendo soltanto $n, e, \overline{y}$.

- Il sistema è rotto se Eve è in grado di fattorizzare $n = p \cdot q$ perché così può calcolare $\varphi(n) = (p-1)(q-1)$ e di conseguenza anche $d = e^{-1} \bmod \varphi(n)$.
- Il sistema è rotto anche se Eve riesce a scoprire $\varphi(n)$, perché può calcolare d come prima. Tuttavia conoscere $\varphi(n)$ in questo caso è equivalente a fattorizzare n. Infatti, conoscendo $\varphi(n)$ Eve può calcolare $p+q = n+1-\varphi(n)$ e poi ottenere p e q come radici del polinomio di secondo grado $X^2 - (p+q)X + n$.

In generale, senza conoscere la fattorizzazione di n può essere computazionalmente molto costoso (e in molti casi infattibile) calcolare $\varphi(n)$ se n è prodotto di primi sufficientemente grandi.

[11] Nel caso $\mathrm{MCD}(x, n) = 1$ segue direttamente dal Teorema di Eulero in $\mathbb{Z}_n$, altrimenti bisogna ragionare modulo p e modulo q separatamente, ma omettiamo i dettagli.

9 Monoidi e gruppi

9.1 Definizioni e esempi

Definizione 9.1. Un **semigruppo** è una coppia $(M, *)$, dove M è un insieme e $* : M \times M \to M$ è un'operazione associativa su M. Un **monoide** è una tripla $(M, *, \lambda)$, dove $(M, *)$ è un semigruppo e λ è un *elemento neutro* per $*$, cioè verifica $\lambda * x = x * \lambda = x \ \forall x \in M$.

Chiaramente ogni monoide è un semigruppo, ma non vale il viceversa. Ad esempio $(\mathbb{N}^*, +)$ è un semigruppo, ma non un monoide. Mentre $(\mathbb{N}, +, 0)$ è un monoide[12].

Lemma 9.2. *L'elemento neutro di un monoide è unico.*

Dimostrazione. Sia $(M, *, \lambda)$ un monoide e sia $\mu \in M$ un altro elemento neutro, cioè μ verifica la condizione $\mu * x = x * \mu = x \ \forall x \in M$. Scegliendo $x = \lambda$ otteniamo

$$\lambda = \mu * \lambda = \mu,$$

dove la seconda uguaglianza segue dal fatto che λ è un elemento neutro. □

Definizione 9.3. Sia $(M, *, \lambda)$ un monoide, se l'operazione $*$ è commutativa, cioè verifica $x * y = y * x \ \forall x \in M$, il monoide si dice **monoide abeliano** o **monoide commutativo**.

Esempio 9.4.

- $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$ e $(\mathbb{N}^*, \cdot, 1)$ sono monoidi commutativi.
- $(\mathbb{Z}, +, 0)$ e $(\mathbb{Z}, \cdot, 1)$ sono monoidi commutativi.
- $(\Bbbk, +, 0)$ e $(\Bbbk, \cdot, 1)$ sono monoidi commutativi, dove $\Bbbk$ indica $\mathbb{Q}$, $\mathbb{R}$, oppure $\mathbb{C}$.
- $(\mathbb{Z}_n, +, \overline{0})$ e $(\mathbb{Z}_n, \cdot, \overline{1})$ sono monoidi commutativi.
- Sia X un insieme non vuoto. Allora $(\mathcal{P}(X), \cap, \emptyset)$ e $(\mathcal{P}(X), \cup, X)$ sono monoidi commutativi.
- Sia X un insieme non vuoto. Allora $(X^X, \circ, \mathrm{id}_X)$ è un monoide. Non è commutativo a meno che X non sia un singoletto.
- L'insieme dei numeri irrazionali $\mathbb{R} \setminus \mathbb{Q}$ non è un semigruppo nè rispetto alla somma nè rispetto al prodotto.

Definizione 9.5. Sia $(M, *, \lambda)$ un monoide e sia $a \in M$.

(i) a si dice **invertibile a sinistra** se esiste $b \in M$ tale che $b * a = \lambda$. L'elemento b viene detto **inverso sinistro** di a.

(ii) a si dice **invertibile a destra** se esiste $c \in M$ tale che $a * c = \lambda$. L'elemento c viene detto **inverso destro** di a.

(iii) a si dice **invertibile** se esiste $d \in M$ tale che $a * d = d * a = \lambda$. L'elemento d viene detto **inverso** di a e si denota con a^{-1}. Reciprocamente a è l'inverso di d.

[12] Facciamo presente però che in alcuni testi si può trovare la parola *semigruppo* usata semplicemente come sinonimo di *monoide*.

Proposizione 9.6. *Sia $(M, *, \lambda)$ un monoide. Allora valgono i seguenti fatti.*

(i) *λ è inverso sinistro e destro di se stesso.*

(ii) *Dato $a \in M$. Se $b \in M$ è inverso sinistro di a e $c \in M$ è inverso destro di a allora $b = c$. In particolare, se un elemento ha un inverso allora l'inverso è unico.*

(iii) *Se $(M, *, \lambda)$ è commutativo un elemento ha inverso destro se e solo se ha inverso sinistro.*

Dimostrazione. (i) Immediato siccome $\lambda * \lambda = \lambda$.

(ii) Siccome $b * a = \lambda$ e $a * c = \lambda$ abbiamo

$$b = b * \lambda = b * (a * c) = (b * a) * c = \lambda * c = c.$$

(iii) Immediata in quanto per la commutatività si ha che $b * a = \lambda$ se e solo se $a * b = \lambda$.

□

Esempio 9.7.

- In $(\mathbb{Z}, +, 0)$ e in $(\Bbbk, +, 0)$, dove $\Bbbk$ indica $\mathbb{Q}$, $\mathbb{R}$, oppure $\mathbb{C}$, ogni elemento ha inverso.
- In $(\mathbb{Z}, \cdot, 1)$ i soli elementi invertibili sono 1 e -1.
- In $(\Bbbk, \cdot, 1)$ tutti gli elementi $\neq 0$ sono invertibili ($\Bbbk = \mathbb{Q}, \mathbb{R}, \mathbb{C}$).
- In $(\mathcal{P}(X), \cap, \emptyset)$ e $(\mathcal{P}(X), \cup, X)$ i soli elementi invertibili sono $\emptyset$ e X rispettivamente.
- In $(\mathbb{Z}_n, \cdot, \overline{1})$ un elemento $\overline{x}$ è invertibile se e solo se $\mathrm{MCD}(x, n) = 1$ (vedi Teorema 8.7).

Sia X un insieme, abbiamo già visto una caratterizzazione degli elementi invertibili del monoide $(X^X, \circ, \mathrm{id}_X)$.

Proposizione 9.8. *Sia X un insieme non vuoto e sia f un elemento del monoide $(X^X, \circ, \mathrm{id}_X)$. Allora*

(i) *f è invertibile a sinistra se e solo se f è iniettiva.*

(ii) *f è invertibile a destra se e solo se f è surgettiva.*

(iii) *f è invertibile se e solo se f è bigettiva.*

Dimostrazione. Non si tratta altro che di una riformulazione dei teoremi 1.30, 1.31, e 1.32. □

Definizione 9.9. Un monoide $(M, *, \lambda)$ tale che ogni suo elemento ha inverso è detto **gruppo**. Se l'operazione è commutativa il gruppo si dice **abeliano** o **commutativo**.

Esempio 9.10.

- $(\mathbb{Z}, +, 0)$ e $(\Bbbk, +, 0)$, dove $\Bbbk$ indica $\mathbb{Q}$, $\mathbb{R}$, oppure $\mathbb{C}$, sono gruppi abeliani.
- Dato $\Bbbk = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, il monoide $(\Bbbk, \cdot, 1)$ non è un gruppo perché l'elemento 0 non è invertibile. Mentre $\big(\Bbbk \setminus \{0\}, \cdot, 1\big)$ è un gruppo abeliano.
- $(\mathbb{Z}_n, +, \overline{0})$ è un gruppo abeliano, mentre $(\mathbb{Z}_n, \cdot, \overline{1})$ non è un gruppo perché non tutti gli elementi sono invertibili. Ad esempio $\overline{0}$ non è mai invertibile. Invece $\big(U(\mathbb{Z}_n), \cdot, \overline{1}\big)$ è un gruppo abeliano.

- Sia X un insieme con almeno 2 elementi. Il monoide $(X^X, \circ, \mathrm{id}_X)$ non è un gruppo. Mentre se denotiamo con $\mathrm{Big}(X)$ l'insieme delle funzioni bigettive $X \to X$, allora $\big(\mathrm{Big}(X), \circ, \mathrm{id}_X\big)$ è un gruppo non abeliano. In particolare, l'insieme S_n delle permutazioni dell'insieme $\{1, 2, \ldots, n\}$ dotato dell'operazione di composizione di funzioni è un gruppo (vedi Definizione 6.1 per S_n).

Esempio 9.11. L'insieme S_3 è l'insieme delle permutazioni dell'insieme $X = \{1, 2, 3\}$. Per il Corollario 6.5 ha cardinalità $|S_3| = 3! = 6$. Vediamo più nel dettaglio quali sono gli elementi del gruppo $(S_3, \circ, \mathrm{id})$. Oltre all'elemento neutro che è la funzione identità $\mathrm{id} = \mathrm{id}_X$, abbiamo i seguenti due elementi

$$\begin{aligned} \phi : X &\to X \\ 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3 \end{aligned} \qquad\qquad \begin{aligned} \psi : X &\to X \\ 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \end{aligned}$$

L'elemento ϕ viene chiamato *trasposizione* di 1 e 2 e si denota con (1 2). Mentre l'elemento ψ viene chiamato 3-*ciclo* di 1, 2, 3 e si denota con (1 2 3). Componendo ϕ e ψ si possono ottenere altri elementi di S_3

$$\begin{aligned} \psi \circ \phi : X &\to X \\ 1 &\mapsto 3 \\ 2 &\mapsto 2 \\ 3 &\mapsto 1 \end{aligned} \qquad \begin{aligned} \phi \circ \psi : X &\to X \\ 1 &\mapsto 1 \\ 2 &\mapsto 3 \\ 3 &\mapsto 2 \end{aligned} \qquad \begin{aligned} \psi^2 : X &\to X \\ 1 &\mapsto 3 \\ 2 &\mapsto 1 \\ 3 &\mapsto 2 \end{aligned}$$

L'elemento $\psi \circ \phi$ è la trasposizione (1 3), l'elemento $\phi \circ \psi$ è la trasposizione (2 3), e l'elemento ψ^2 è il 3-ciclo (1 3 2). Si verifica inoltre che valgono le seguenti relazioni

$$\phi^2 = \mathrm{id}, \quad \psi^3 = \mathrm{id},$$

e che tutte le altre possibili composizioni delle funzioni ϕ e ψ restituiscono uno dei 6 elementi che abbiamo già trovato. Pertanto il gruppo S_3 è costituito da

$$S_3 = \{\mathrm{id}, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}.$$

Infine osserviamo che siccome $\phi \circ \psi \neq \psi \circ \phi$ il gruppo S_3 non è commutativo.

Definizione 9.12. Sia $(M, *, \lambda)$ un monoide. Dato un intero $m \in \mathbb{N}^*$ e un elemento $g \in M$ utilizzeremo a volte la seguente utile notazione

$$g^m := \underbrace{g * \cdots * g}_{m \text{ volte}}.$$

Se $m < 0$ e g è invertibile in M, definiamo $g^m := (g^{-1})^{-m}$. Poniamo infine $g^0 := \lambda$.

Definizione 9.13. Siano $(M_1, *_1, \lambda_1)$ e $(M_2, *_2, \lambda_2)$ due monoidi. Dotiamo il prodotto cartesiano $M_1 \times M_2$ della legge di composizione

$$*_1 \times *_2 : (M_1 \times M_2) \times (M_1 \times M_2) \longrightarrow M_1 \times M_2$$
$$((x, y), (z, t)) \mapsto (x *_1 z, y *_2 t).$$

Si verifica che $M_1 \times M_2$ con questa legge di composizione diventa un monoide avente come elemento neutro la coppia (λ_1, λ_2). Questo monoide viene chiamato **prodotto diretto** di M_1 e M_2.

Osservazione 9.14. Osserviamo che se $(x, y) \in M_1 \times M_2$ con x invertibile in M_1 e y invertibile in M_2, allora (x, y) è invertibile in $M_1 \times M_2$ e l'elemento inverso è dato da (x^{-1}, y^{-1}), dove l'inverso x^{-1} è calcolato in M_1 e l'inverso y^{-1} è calcolato in M_2. Infatti si verifica che

$$(x^{-1}, y^{-1}) *_1 \times *_2 (x, y) = (x^{-1} *_1 x, y^{-1} *_2 y) = (\lambda_1, \lambda_2).$$

In particolare, se G_1 e G_2 sono due gruppi, il loro prodotto diretto $G_1 \times G_2$ è un gruppo.

Esempio 9.15. Siano $n, m \in \mathbb{Z}$, $n, m > 1$ e consideriamo i gruppi $(\mathbb{Z}_n, +, \overline{0})$ e $(\mathbb{Z}_m, +, [0])$ dove usiamo $\overline{x}$ per denotare la classe di un elemento in $\mathbb{Z}_n$ e $[x]$ per denotare la classe di un elemento in $\mathbb{Z}_m$. Il gruppo prodotto

$$\mathbb{Z}_n \times \mathbb{Z}_m$$

ha cardinalità nm. La somma si effettua componente per componente, cioè $\big(\overline{x}, [y]\big) + \big(\overline{u}, [v]\big) = \big(\overline{x + u}, [y + v]\big)$, e l'elemento neutro è la coppia $\big(\overline{0}, [0]\big)$. L'inverso (rispetto alla somma) di un elemento $\big(\overline{x}, [y]\big)$ è l'elemento $\big(\overline{-x}, [-y]\big)$, dove l'inverso $\overline{-x}$ viene calcolato in $\mathbb{Z}_n$ e l'inverso $[-y]$ viene calcolato in $\mathbb{Z}_m$. Ad esempio, per $n = 3$, $m = 4$ abbiamo il gruppo $\mathbb{Z}_3 \times \mathbb{Z}_4$. L'inverso dell'elemento $\big(\overline{2}, [2]\big)$ è l'elemento $\big(\overline{1}, [2]\big)$. Infatti abbiamo

$$\big(\overline{2}, [2]\big) + \big(\overline{1}, [2]\big) = \big(\overline{2 + 1}, [2 + 2]\big) = \big(\overline{0}, [0]\big).$$

9.2 Sottogruppi e gruppi quoziente

Per il resto del capitolo ci restringiamo a studiare i gruppi e le loro proprietà. Tuttavia facciamo presente che molte delle definizioni che daremo, come quella di sottogruppo, possono essere estese facilmente al caso dei monoidi con le dovute accortezze.

Definizione 9.16. Sia $(G, *, \lambda)$ un gruppo. Un sottoinsieme $H \subseteq G$ è un **sottogruppo** di G se valgono:

(i) $\lambda \in H$;
(ii) $a, b \in H \implies a * b \in H$;
(iii) $a \in H \implies a^{-1} \in H$.

Le proprietà di sottogruppo garantiscono che la funzione $* : G \times G \to G$ che definisce l'operazione su G si restringa ad una funzione $*_H : H \times H \to H$ che definisce un analoga operazione su H. Pertanto $(H, *_H, \lambda)$ è a sua volta un gruppo.

Esempio 9.17.

- $(\mathbb{Z}, +.0)$ è un sottogruppo di $(\mathbb{Q}, +, 0)$, che a sua volta è un sottogruppo di $(\mathbb{R}, +, 0)$, il quale è un sottogruppo di $(\mathbb{C}, +, 0)$. Analogamente abbiamo la catena di sottogruppi
$$\big(\mathbb{Q} \setminus \{0\}, \cdot, 1\big) \ \subseteq \ \big(\mathbb{R} \setminus \{0\}, \cdot, 1\big) \ \subseteq \ \big(\mathbb{C} \setminus \{0\}, \cdot, 1\big).$$
- Sia $n \in \mathbb{Z}_+$. Definiamo il sottoinsieme delle **radici n-esime dell'unità** come
$$U_n := \{x \in \mathbb{C} : \ x^n = 1\}.$$
Si verifica che $(U_n, \cdot, 1)$ è un sottogruppo di $\big(\mathbb{C} \setminus \{0\}, \cdot, 1\big)$. Ad esempio
$$U_1 = \{1\}, \ \ U_2 = \{-1, 1\}, \ \ U_3 = \left\{1, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}\right\}, \ \ U_4 = \{1, -1, i, -i\}, \ \ldots.$$
- Sia $n \in \mathbb{Z}_+$. Consideriamo il sottoinsieme di $\mathbb{Z}$ costituito da tutti i multipli di n
$$n\mathbb{Z} = \{m \in \mathbb{Z} : \ m = nk, \ \text{per un qualche } k \in \mathbb{Z}\}.$$
Si verifica facilmente che $n\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +, 0)$. Inoltre si può dimostrare che tutti i sottogruppi di $(\mathbb{Z}, +, 0)$ sono necessariamente di questa forma.
- $(\mathbb{N}, +, 0)$ non è un sottogruppo di $(\mathbb{Z}, +.0)$, in quanto non verifica la condizione (iii). Infatti $2 \in \mathbb{N}$, ma il suo inverso (rispetto alla somma) -2 non appartiene a $\mathbb{N}$.

Esempio 9.18. Consideriamo il gruppo $S_3 = \{\mathrm{id}, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$ con le notazioni come nell'Esempio 9.11. Si verifica che
$$H = \{\mathrm{id}, \phi\} \quad \text{e} \quad N = \{\mathrm{id}, \psi, \psi^2\}$$
sono sottogruppi di S_3. Invece l'insieme $T = \{\mathrm{id}, \psi, \phi, \phi \circ \psi\}$ non è un sottogruppo in quanto $\psi \in T$, ma $\psi^{-1} = \psi^2 \notin T$.

Definizione 9.19. Sia $(G, *, \lambda)$ un gruppo e $\sim$ una relazione d'equivalenza su G. Diciamo che $\sim$ è **compatibile con l'operazione** $*$ se vale $\forall a, b, c, d \in G$
$$(a \sim b) \wedge (c \sim d) \implies (a * c) \sim (b * d).$$
In tal caso, definiamo un'operazione $[*]$ sull'insieme quoziente $G/\sim$ ponendo
$$[x][*][y] := [x * y] \ \ \forall x, y \in G.$$
L'operazione è ben definita e rende $(G/\sim, [*], \lambda)$ un gruppo che viene detto **gruppo quoziente**.

Esempio 9.20. Consideriamo il gruppo $(\mathbb{Z}, +, 0)$ e sia $n \in \mathbb{Z}_+$. La relazione d'equivalenza modulare, cioè $x \sim_n y \iff x \equiv y \ \mathrm{mod} n$, è compatibile con l'operazione di somma. Pertanto il quoziente $\mathbb{Z}/\sim_n = \mathbb{Z}_n$ è dotato di un'operazione $[+]$ che rende $(\mathbb{Z}_n, [+], [0])$ un gruppo . L'operazione $[+]$ è precisamente l'operazione di somma $+$ definita nella Sezione 8.2.

Un esempio importante di relazioni di equivalenza compatibili con la struttura di gruppo è dato dalla relazione indotta da un sottogruppo (normale). Siano $(G, *, \lambda)$ un gruppo e $H \subseteq G$ un sottogruppo. Il sottogruppo H induce la relazione

$$g \sim_S g' \iff g^{-1} * g' \in H.$$

Verifichiamo che $\sim_S$ è una relazione d'equivalenza.

1. (Proprietà riflessiva) Per ogni $g \in G$ si ha $g \sim_S g$ poiché $g^{-1} * g = \lambda \in H$.
2. (Proprietà simmetrica) Se $g \sim_S g'$ allora $g^{-1} * g' \in H$ e quindi $(g^{-1} * g')^{-1} = (g')^{-1} * g \in H$, ossia $g' \sim_S g$.
3. (Proprietà transitiva) Se $g \sim_S g'$ e $g' \sim_S g''$ allora $g^{-1} * g' \in H$ e $(g')^{-1} * g'' \in H$ per cui

$$g^{-1} * g'' = (g^{-1} * g') * ((g')^{-1} * g'') \in H.$$

   Quindi $g \sim_S g''$.

Dato $g \in G$ ricordiamo che la classe di equivalenza di g è il sottoinsieme di G dato da

$$[g] = \{x \in G : \ x \sim_S g\} = \{x = g * h : \ h \in H\}.$$

Denotiamo tale classe anche con $g * H$ e la chiamiamo **classe laterale sinistra** di G modulo H. L'insieme quoziente

$$G/\sim_S = \{g * H : \ g \in G\}$$

si denota con G/H. La sua cardinalità si denota con $[G : H] := \#(G/H)$ e si chiama **indice** di H in G.

Analogamente a prima definiamo su G la relazione d'equivalenza

$$g \sim_D g' \iff g * (g')^{-1} \in H.$$

Si verifica che $\sim_D$ è una relazione d'equivalenza, le cui classi vengono dette **classi laterali destre** di G modulo H. Esse sono

$$H * g := [g] = \{x \in G : \ x \sim_D g\} = \{x = h * g : \ h \in H\}.$$

L'insieme quoziente

$$G/\sim_D = \{H * g : \ g \in G\}$$

si denota[13] con $H\backslash G$.

I due insiemi quoziente G/H e $H\backslash G$ sono equipotenti. Una bigezione è data dalla seguente funzione

$$\begin{aligned} f : G/H &\longrightarrow H\backslash G \\ g * H &\mapsto H * g^{-1}. \end{aligned}$$

Si verifica che f è ben definita, infatti

$$g \sim_S g' \iff g^{-1} * g' \in H \iff g^{-1} * ((g')^{-1})^{-1} \in H \iff g^{-1} \sim_D (g')^{-1}.$$

[13] Il simbolo $\backslash$ è lo stesso che si usa per la differenza insiemistica tra due insiemi. Si capirà dal contesto di quale stiamo parlando.

Lasciamo per esercizio al lettore di mostrare che f è una bigezione. Pertanto i due insiemi G/H e $H\backslash G$ sono equipotenti e si ha $\#(H\backslash G) = [G : H] = \#(G/H)$. Attenzione che i due insiemi G/H e $H\backslash G$ sono in generale ben distinti, come mostra il seguente esempio.

Esempio 9.21. Consideriamo il gruppo $S_3 = \{\mathrm{id}, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$ con le notazioni come negli Esempi 9.11 e 9.18. Calcoliamo le classi laterali sinistre e destre del sottogruppo $H = \{\mathrm{id}, \phi\}$. Le classi laterali sinistre sono della forma $g \circ H$ al variare di $g \in S_3$. Otteniamo quindi tre classi distinte

$$\begin{aligned} H = \mathrm{id} \circ H = \phi \circ H = \{\mathrm{id}, \phi\} \\ \psi \circ H = (\psi \circ \phi) \circ H = \{\psi, \psi \circ \phi\} \\ \psi^2 \circ H = (\phi \circ \psi) \circ H = \{\psi^2, \phi \circ \psi\}. \end{aligned}$$

Analogamente le classi laterali destre sono della forma $H \circ g$ al variare di $g \in S_3$. Anche in questo caso otteniamo tre classi distinte

$$\begin{aligned} H = H \circ \mathrm{id} = H \circ \phi = \{\mathrm{id}, \phi\} \\ H \circ \psi = H \circ (\phi \circ \psi) = \{\psi, \phi \circ \psi\} \\ H \circ \psi^2 = H \circ (\psi \circ \phi) = \{\psi^2, \psi \circ \phi\}. \end{aligned}$$

Notiamo che le classi laterali sinistre e destre sono differenti dalle precedenti, inoltre abbiamo $\psi \circ H \neq H \circ \psi$.

Se G è un gruppo commutativo, allora per ogni $g \in G$ si ha che $g \sim_S g' \iff g \sim_D g'$. Quindi si ha che $g * H = H * g$, pertanto classi laterali sinistre e destre coincidono. Se G non è commutativo, classi laterali sinistre e destre possono essere differenti (come nel caso dell'Esempio 9.21). Per alcuni particolari sottogruppi però, questo non succede. Introduciamo quindi la seguente definizione.

Definizione 9.22. Sia $(G, *, \lambda)$ un gruppo e sia H un sottogruppo. Se per ogni $g \in G$ si ha

$$g * H = H * g$$

allora H si dice **sottogruppo normale**[14] di G. In tal caso si ha $G/H = H\backslash G$, e su di esso è indotta una struttura di gruppo definita da

$$[g] *_H [k] := [g * k] \ \forall g, k \in G.$$

Il gruppo $(G/H, *_H, [\lambda])$ viene detto **gruppo quoziente**.

Verifichiamo che l'operazione $*_H$ su G/H è ben definita. Siccome H è un sottogruppo normale, le due relazioni d'equivalenza $\sim_S$ e $\sim_D$ coincidono e le denotiamo entrambe con $\sim$. Dati $g, g', k, k' \in G$ tali che $g \sim g'$ e $k \sim k'$ si ha che $g' = g * u$ e $k' = k * v$ con $u, v \in H$.

[14] Attenzione che l'uguaglianza $g * H = H * g$ è un'uguaglianza tra insiemi e non vuol dire che $g * h = h * g$ per ogni $h \in H$!

Consideriamo l'elemento $u * k \in H * k$, siccome H è un sottogruppo normale si ha $H * k = k * H$ pertanto $\exists u' \in H$ tale che $u * k = k * u'$. Abbiamo quindi

$$g' * k' = g * u * k * v = g * k * u' * v$$

e siccome $u' * v \in H$, otteniamo $(g' * k)' \sim (g * k)$. Questo mostra che $*_H$ è un'operazione ben definita su G/H. Si verifica facilmente che l'elemento neutro dell'operazione $*_H$ è dato dalla classe $[\lambda]$ e cioè $[\lambda] = \lambda * H = H * \lambda = H$. Dato $g \in G$, l'inverso della classe $[g] \in G/H$ è la classe $[g]^{-1}$. Pertanto $(G/H, *_H, [\lambda])$ è un gruppo.

Osservazione 9.23. Se G è un gruppo abeliano, ogni sottogruppo $H \subseteq G$ è normale.

Esempio 9.24. Consideriamo il gruppo $(\mathbb{Z}, +, 0)$ e il sottogruppo $n\mathbb{Z} = \{nk : \ k \in \mathbb{Z}\}$ per $n \in \mathbb{Z}_+$. Siccome $(\mathbb{Z}, +, 0)$ è un gruppo abeliano, il sottogruppo $n\mathbb{Z}$ è normale. Infatti dati $a, b \in \mathbb{Z}$ le relazioni di equivalenza $\sim_S$ e $\sim_D$ si scrivono come

$$\begin{aligned} a \sim_S b &\iff -a + b \in n\mathbb{Z} \\ a \sim_D b &\iff a - b \in n\mathbb{Z} \end{aligned}$$

Abbiamo quindi $a \sim_S b \iff a \sim_D b \iff a \equiv b \bmod n$. Cioè le relazioni $\sim_S$ e $\sim_D$ coincidono con la relazione d'equivalenza modulare e il gruppo quoziente coincide con $\mathbb{Z}_n$, cioè

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Esercizio 9.25. Consideriamo il gruppo $S_3 = \{\mathrm{id}, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$ con le notazioni come negli Esempi 9.11, 9.18, e 9.21. Verificare che il sottogruppo $N = \{\mathrm{id}, \psi, \psi^2\}$ è un sottogruppo normale di S_3.

9.3 Ordine di un elemento

Iniziamo con il seguente importante teorema che lega la cardinalità di un gruppo e quella di un suo sottogruppo.

Teorema 9.26 (Lagrange)**.** *Sia G un gruppo finito e sia H un suo sottogruppo. Allora*

$$\#G = [G : H] \cdot \#H.$$

Dimostrazione. Se H ha m elementi, allora ciascuna classe laterale sinistra $g * H$ ha m elementi. Infatti gli elementi di $g * H$ sono della forma $g * h$ al variare di $h \in H$ e sono tutti distinti (se $g * h_1 = g * h_2$ moltiplicando per g^{-1} a sinistra entrambi i membri si ottiene $h_1 = h_2$). Essendo $[G : H]$ il numero delle classi laterali sinistre disgiunte, si ottiene immediatamente che $\#G = m[G : H]$ come richiesto. □

Una conseguenza interessante del teorema di Lagrange è che i sottogruppi H di un gruppo finito G devono necessariamente avere una cardinalità che divide la cardinalità di G.

Esempio 9.27. Consideriamo il gruppo $S_3 = \{\mathrm{id}, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$ con le notazioni come negli Esempi 9.11, 9.18, e 9.21. Abbiamo visto che il sottogruppo $H = \{\mathrm{id}, \phi\}$ ha tre classi laterali sinistre distinte: H, $\psi \circ H$, e $\psi^2 \circ H$. Pertanto $[G : H] = 3$. Siccome $|H| = 2$ e $|S_3| = 6$, l'uguaglianza del teorema di Lagrange è verificata.

Prendiamo ora $T = \{\mathrm{id}, \phi, \psi, \phi \circ \psi\}$. Siccome $|T| = 4 \nmid 6 = |S_3|$, per il teorema di Lagrange concludiamo immediatamente che T non è un sottogruppo di S_3. Attenzione che la condizione del teorema di Lagrange è necessaria per essere un sottogruppo, ma non è sufficiente. Ad esempio il sottoinsieme $P = \{\psi, \phi\}$ ha cardinalità $2 \mid 6$, ma non è un sottogruppo perché $\mathrm{id} \notin P$.

Definizione 9.28 (Ordine di un elemento in un gruppo)**.** Sia $(G, *, \lambda)$ un gruppo e sia $g \in G$. Chiamiamo **ordine** (o **periodo**) di g il più piccolo intero positivo n, se esiste, per cui

$$g^n = \underbrace{g * g * \cdots * g}_{n \text{ volte}} = \lambda.$$

Scriviamo $\mathrm{ord}_G(g) = n$. Se tale intero non esiste, diciamo che g ha ordine infinito e scriviamo $\mathrm{ord}_G(g) = \infty$. Inoltre chiamiamo **ordine** di G la cardinalità $|G|$.

Osservazione 9.29. Sia $(G, *, \lambda)$ un gruppo e sia $g \in G$,

$$\mathrm{ord}_G(g) = 1 \iff g = \lambda.$$

Proposizione 9.30. *Sia $(G, *, \lambda)$ un gruppo.*

(i) Sia $g \in G$. Se $g^m = \lambda$ per un qualche $m \in \mathbb{N}$ allora $\mathrm{ord}_G(g) \mid m$.

(ii) Se G è finito, allora $\mathrm{ord}_G(g) \mid \#G$ *per ogni $g \in G$. In parole: "*l'ordine di un elemento divide l'ordine del gruppo*".*

Dimostrazione. (i) Siccome $g^m = \lambda$, si ha $\mathrm{ord}_G(g) \leq m$. Consideriamo la divisione euclidea

$$m = k \cdot \mathrm{ord}_G(g) + r, \qquad k, r \in \mathbb{Z}, \quad 0 \leq r < \mathrm{ord}_G(g).$$

Proviamo che $r = 0$. Abbiamo

$$\lambda = g^m = g^{k \cdot \mathrm{ord}(g) + r} = g^{k \cdot \mathrm{ord}(g)} * g^r = (g^{\mathrm{ord}(g)})^k * g^r = \lambda^k * g^r = g^r.$$

Se per assurdo fosse $r > 0$ avremmo trovato un intero positivo e $< \mathrm{ord}_G(g)$ per cui $g^r = \lambda$, contraddicendo la minimalità di $\mathrm{ord}_G(g)$. Pertanto $r = 0$.

(ii) Consideriamo $H = \{\lambda, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$. Si verifica facilmente che H è un sottogruppo di G. Inoltre gli elementi di H sono tutti distinti, pertanto $|H| = \mathrm{ord}_G(g)$. Per il Teorema di Lagrange abbiamo quindi $\mathrm{ord}_G(g) = \#H \mid \#G$.

□

Esempio 9.31.

- Consideriamo il gruppo $(\mathbb{Z}_{12}, +, \overline{0})$. L'elemento $\overline{0}$ ha ordine 1, l'elemento $\overline{2}$ ha ordine 6, e l'elemento $\overline{1}$ ha ordine 12.

- Consideriamo il gruppo $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, prodotto diretto del gruppo $(\mathbb{Z}_2, +, \overline{0})$ con se stesso. L'ordine di G è 4, siccome $|\mathbb{Z}_2 \times \mathbb{Z}_2| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_2| = 2 \cdot 2 = 4$. Tuttavia osserviamo che G non contiene nessun elemento di ordine 4. Infatti, l'elemento neutro $(\overline{0}, \overline{0})$ ha ordine 1 e tutti gli altri elementi hanno ordine 2.

- Consideriamo il gruppo $(\mathbb{Z}, +, 0)$. L'elemento neutro 0 ha ordine 1, e tutti gli altri elementi $g \neq 0$ hanno ordine infinito. Infatti, dato $g \neq 0$, $\nexists n \in \mathbb{N}^*$ tale che $n \cdot g = 0$.

- Consideriamo il gruppo $(\mathbb{C}^*, \cdot, 1)$. Gli unici elementi di ordine finito sono le radici n-esime dell'unità
$$U_n = \{x \in \mathbb{C} : \ x^n = 1\}.$$
In particolare, si ha $\text{ord}(x) \mid n$ se e solo se $x \in U_n$. Ad esempio abbiamo $\text{ord}(-1) = 2$, $\text{ord}(i) = \text{ord}(-i) = 4$.

Nel caso del gruppo $U(\mathbb{Z}_n)$ degli elementi invertibili modulo n, la Proposizione 9.30 ci da il seguente corollario.

Corollario 9.32. *Sia $n \in \mathbb{N}$, $n > 1$ e sia $\overline{x} \in U(\mathbb{Z}_n)$. Allora*

$$\text{ord}(\overline{x}) \mid \varphi(n).$$

In particolare, se $n = p$ è un numero primo, l'ordine di ogni elemento di $U(\mathbb{Z}_p)$ divide $p - 1$.

Dimostrazione. Segue dalla Proposizione 9.30 tenendo conto che $|U(\mathbb{Z}_n)| = \varphi(n)$ per l'Osservazione 8.11. □

9.4 Sottogruppi ciclici

Sia $(G, *, \lambda)$ un gruppo e siano H_i (per $i \in I$) dei sottogruppi di G. Si verifica facilmente che l'intersezione
$$\bigcap_{i \in I} H_i$$
è un sottogruppo di G. Al contrario, l'unione di sottogruppi non è in generale un sottogruppo, come mostra il seguente esempio.

Esempio 9.33. Consideriamo il gruppo $(\mathbb{Z}, +, 0)$ e i sottogruppi $3\mathbb{Z}$ e $10\mathbb{Z}$. L'unione dei due sottogruppi $3\mathbb{Z} \cup 10\mathbb{Z}$ non è un sottogruppo. Infatti $3, 10 \in 3\mathbb{Z} \cup 10\mathbb{Z}$, ma $3 + 10 = 13 \notin 3\mathbb{Z} \cup 10\mathbb{Z}$.

Definizione 9.34. Sia $(G, *, \lambda)$ un gruppo e sia $A \subseteq G$ un sottoinsieme di G. Il **sottogruppo generato** da A è l'intersezione di tutti i sottogruppi di G che contengono A. Si denota con $\langle A \rangle$. In formule
$$\langle A \rangle := \bigcap_{\substack{A \subseteq H \subseteq G \\ H \text{ sottogruppo}}} H.$$

Se $A = \{x\}$ è un singoletto, scriviamo più brevemente $\langle x \rangle$ per indicare il sottogruppo generato da x. In tal caso, il sottogruppo $\langle x \rangle$ viene detto **sottogruppo ciclico** generato da x.

Osservazione 9.35. Il sottogruppo ciclico generato da un elemento x si può descrivere più esplicitamente nella maniera seguente

$$\langle x \rangle = \{x^m : \ m \in \mathbb{Z}\}.$$

Si tratta del sottoinsieme di G costituito da tutte le potenze di x, dove abbiamo utilizzato la notazione delle potenze introdotta nella Definizione 9.12.

Definizione 9.36. Un gruppo $(G, *, \lambda)$ si dice **ciclico** se è generato da un solo elemento, cioè se esiste $x \in G$ tale che $G = \langle x \rangle$.

Esempio 9.37. • Il gruppo $(\mathbb{Z}, +, 0)$ è ciclico generato dall'elemento 1. Infatti, posso scrivere ogni elemento $n > 0$ di $\mathbb{Z}$ come

$$n \cdot 1 = \underbrace{1 + 1 \cdots + 1}_{n \text{ volte}}.$$

E analogamente, se $n < 0$ abbiamo

$$(-n) \cdot (-1) = \underbrace{(-1) + (-1) \cdots + (-1)}_{-n \text{ volte}}.$$

Notare che con la notazione additiva per l'operazione di gruppo di $\mathbb{Z}$, l'*elevamento all'n-esima potenza* della Definizione 9.12 corrisponde semplicemente a moltiplicare per n. Inoltre dato $k \in \mathbb{Z}$, il sottogruppo $k\mathbb{Z}$ di ZZ è un sottogruppo ciclico. Si ha infatti

$$k\mathbb{Z} = \langle k \rangle.$$

- Sia $n \in \mathbb{Z}$, $n > 1$. Il gruppo $(\mathbb{Z}_n, +, \overline{0})$ è ciclico ed è generato dalla classe $\overline{1}$.
- Il gruppo $\big(U(\mathbb{Z}_5), \cdot, \overline{1}\big)$ è ciclico generato dalla classe $\overline{2}$. Abbiamo infatti

$$\overline{2}^2 = \overline{4}, \ \ \overline{2}^3 = \overline{8} = \overline{3}, \ \ \overline{2}^4 = \overline{16} = \overline{1}.$$

Cioè possiamo scrivere tutti gli elementi di $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ come potenze di $\overline{2}$.

Osservazione 9.38. Se G è un gruppo finito, allora

$$G = \langle x \rangle \iff \text{ord}_G(x) = |G|.$$

Esempio 9.39. • Il gruppo prodotto $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico. Infatti $|G| = 4$, ma G non contiene nessun elemento di ordine 4. Analogamente si può mostrare che i gruppi prodotto $\mathbb{Z}_n \times \mathbb{Z}_m$ con $n, m > 1$ non sono mai gruppi ciclici.

- Il gruppo $\big(U(\mathbb{Z}_8), \cdot, \overline{1}\big)$ non è ciclico. Abbiamo $U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ che ha ordine $4 = \varphi(8)$, ma non c'è nessun elemento di ordine 4 in $U(\mathbb{Z}_8)$. Infatti abbiamo

$$\overline{3}^2 = \overline{9} = \overline{1}, \qquad \overline{5}^2 = \overline{25} = \overline{1}, \qquad \overline{7}^2 = \overline{49} = \overline{1},$$

il che mostra che $\text{ord}(\overline{3}) = \text{ord}(\overline{5}) = \text{ord}(\overline{7}) = 2$.

9.5 Omomorfismi di gruppi

Definizione 9.40. Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi. Una funzione $\varphi : G_1 \to G_2$ è un **omomorfismo di gruppi** se verifica:

(i) $\varphi(\lambda_1) = \lambda_2$;

(ii) $\varphi(g *_1 h) = \varphi(g) *_2 \varphi(h)$ per ogni $g, h \in G_1$.

Detto in parole, un omomorfismo di gruppi è una funzione che "rispetta la struttura di gruppo", cioè manda l'identità di un gruppo nell'identità dell'altro e commuta con le operazioni dei due gruppi. Potrebbe sembrare naturale aspettarsi anche una terza condizione nella definizione di omomorfismo di gruppi, e cioè che un omomorfismo di gruppi commuti con l'inverso. In realtà, non è necessario aggiungere questa condizione tra le richieste perché è soddisfatta automaticamente se valgono le prime due (i) e (ii).

Lemma 9.41. *Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi e sia $\varphi : G_1 \to G_2$ un omomorfismo di gruppi. Allora per ogni $x \in G_1$ si ha*

$$\varphi(x^{-1}) = (\varphi(x))^{-1}.$$

Dimostrazione. L'elemento x^{-1} è l'inverso di x (in G_1), abbiamo quindi le uguaglianze

$$x^{-1} *_1 x = x *_1 x^{-1} = \lambda_1.$$

Applicando la funzione φ alle precedenti uguaglianze, otteniamo ancora uguaglianze vere (in G_2):

$$\varphi(x^{-1} *_1 x) = \varphi(x *_1 x^{-1}) = \varphi(\lambda_1).$$

Per le proprietà (i) e (ii) della definizione di omomorfismo di gruppi abbiamo $\varphi(x^{-1} *_1 x) = \varphi(x^{-1}) *_2 \varphi(x)$, $\varphi(x *_1 x^{-1}) = \varphi(x) *_2 \varphi(x^{-1})$, e $\varphi(\lambda_1) = \lambda_2$. Sostituendo nell'uguaglianza precedente queste tre, otteniamo

$$\varphi(x^{-1}) *_2 \varphi(x) = \varphi(x) *_2 \varphi(x^{-1}) = \lambda_2,$$

il che mostra che l'elemento $\varphi(x^{-1})$ è l'inverso di $\varphi(x)$ in G_2, e cioè $(\varphi(x))^{-1} = \varphi(x^{-1})$. □

Esempio 9.42.

- Sia $(G, *, \lambda)$ un gruppo. Si verifica facilmente che la funzione identità $\mathrm{id}_G : G \to G$ è un omomorfismo di gruppi.
- La funzione $f : \mathbb{Z} \to \mathbb{Z}$ tale che $f(x) = x + 2$ non è un omomorfismo di gruppi da $(\mathbb{Z}, +, 0)$ in se stesso, perchè $f(0) = 2 \neq 0$.
- La funzione $f : \mathbb{Z} \to \mathbb{Z}$ tale che $f(x) = 2 \cdot x$ è un omomorfismo di gruppi da $(\mathbb{Z}, +, 0)$ in se stesso. Infatti si ha

  $$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y) \quad \forall x, y \in \mathbb{Z}$$

  e $f(0) = 0$.

- La funzione $f : \mathbb{Z} \to \mathbb{Q} \setminus \{0\}$ tale che $f(n) = 2^n$ è un omomorfismo di gruppi dal gruppo $(\mathbb{Z}, +, 0)$ al gruppo $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$.

Osservazione 9.43. Sia $(G, *, \lambda)$ un gruppo, e sia $H \subseteq G$ un sottogruppo normale. Allora possiamo considerare la funzione di **proiezione sul quoziente**

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\mapsto [g] \end{aligned}$$

dove $[g]$ denota la classe di equivalenza di g modulo H, come descritta nella Sezione 9.2. Si può verificare che π è un omomorfismo surgettivo di gruppi.

Esempio 9.44. Consideriamo il gruppo $(\mathbb{Z}, +, 0)$ con il sottogruppo $n\mathbb{Z}$ e il quoziente $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. In questo caso, la proiezione sul quoziente è data da $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(x) = \overline{x}$. Possiamo invece chiederci se esistono omomorfismi di gruppo da $\mathbb{Z}_n$ a $\mathbb{Z}$. Supponiamo che $\varphi : \mathbb{Z}_n \to \mathbb{Z}$ sia un omomorfismo di gruppi e chiamiamo $a = \varphi(\overline{1}) \in \mathbb{Z}$, l'immagine del generatore $\overline{1}$ di $\mathbb{Z}_n$. Per le proprietà di omomorfismo di gruppi abbiamo

$$0 = \varphi(\overline{0}) = \varphi(\overline{n}) = \varphi(\underbrace{\overline{1} + \cdots + \overline{1}}_{n \text{ volte}}) = \varphi(\overline{1}) + \cdots + \varphi(\overline{1}) = a + \cdots + a = n \cdot a.$$

E siccome $n \neq 0$, e l'uguaglianza $0 = na$ è in $\mathbb{Z}$ concludiamo che $a = 0$. Pertanto $\varphi(\overline{1}) = 0$ da cui segue che φ è l'omomorfismo nullo, cioè $\varphi(\overline{x}) = 0$ per ogni $\overline{x} \in \mathbb{Z}_n$.

Proposizione 9.45. *Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi e sia $\varphi : G_1 \to G_2$ un omomorfismo di gruppi. Allora*

(i) L'immagine $\varphi(G_1)$ è un sottogruppo di G_2.

(ii) La controimmagine $\varphi^{-1}(\lambda_2)$ è un sottogruppo normale di G_1.

Definizione 9.46. Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi e sia $\varphi : G_1 \to G_2$ un omomorfismo di gruppi. La controimmagine $\varphi^{-1}(\lambda_2)$ viene detta **nucleo** dell'omomorfismo φ e si denota con $\ker \varphi$.

Proposizione 9.47. *Siano $(G_1, *_1, \lambda_1)$, $(G_2, *_2, \lambda_2)$, e $(G_3, *_3, \lambda_3)$ tre gruppi. Allora*

(i) Se $\varphi : G_1 \to G_2$ e $\psi : G_2 \to G_3$ sono omomorfismi di gruppi, allora la composizione $\psi \circ \varphi : G_1 \to G_3$ è un omomorfismo di gruppi.

(ii) Se $\varphi : G_1 \to G_2$ è un omomorfismo di gruppi bigettivo, allora la funzione inversa $\varphi^{-1} : G_2 \to G_1$ è un omomorfismo di gruppi.

Definizione 9.48. Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi e sia $\varphi : G_1 \to G_2$ un omomorfismo di gruppi. Se φ è bigettivo, viene detto **isomorfismo** di gruppi. Due gruppi si dicono **isomorfi** se esiste un isomorfismo di gruppi dal primo gruppo verso il secondo (e viceversa).

Osservazione 9.49. Siccome un isomorfismo di gruppi è in particolare una funzione bigettiva, se due gruppi G_1 e G_2 sono isomorfi allora sono anche equipotenti, cioè hanno la stessa cardinalità. Vale quindi

$$G_1, G_2 \text{ isomorfi} \implies G_1, G_2 \text{ equipotenti.}$$

La freccia $\not\Leftarrow$ non vale in generale.

Lemma 9.50. *Siano $(G_1, *_1, \lambda_1)$ e $(G_2, *_2, \lambda_2)$ due gruppi e sia $\varphi : G_1 \to G_2$ un isomorfismo di gruppi. Per ogni $g \in G_1$ abbiamo*

$$\mathrm{ord}_{G_2}(\varphi(g)) = \mathrm{ord}_{G_1}(g).$$

Dimostrazione. Sia $n = \mathrm{ord}_{G_1}(g) \in \mathbb{N}$ e sia $m = \mathrm{ord}_{G_2}(\varphi(g)) \in \mathbb{N}$. In particolare si ha $g^n = \lambda_1$. Applicando φ a questa uguaglianza otteniamo $\varphi(g^n) = \varphi(\lambda_1) = \lambda_2$. E siccome $\varphi(g^n) = \varphi(g)^n$, si ha che $\varphi(g)^n = \lambda_2$. Questo mostra che $\mathrm{ord}_{G_2}(\varphi(g)) \leq n$. Supponiamo per assurdo che valga $m = \mathrm{ord}_{G_2}(\varphi(g)) < n$. Abbiamo $\varphi(g)^m = \lambda_2$. Siccome φ è bigettiva, posso considerare la funzione inversa φ^{-1} che è anch'essa un omomorfismo di gruppi. Applicandola all'uguaglianza $\varphi(g)^m = \lambda_2$ otteniamo

$$g^m = \varphi^{-1}(\varphi(g^m)) = \varphi^{-1}(\varphi(g)^m) = \varphi^{-1}(\lambda_2) = \lambda_1.$$

Abbiamo quindi che $g^m = \lambda_1$ per un $m < n$ che contraddice la minimalità di $n = \mathrm{ord}_{G_1}(g)$. Pertanto vale $n = m$. □

Esempio 9.51. I gruppi $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ sono equipotenti (in quanto $|\mathbb{Z}_4| = |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$), ma non sono isomorfi. Supponiamo per assurdo che esista un isomorfismo di gruppi $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Siccome il generatore $\overline{1} \in \mathbb{Z}_4$ ha ordine 4, anche la sua immagine $\varphi(\overline{1}) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ deve avere ordine 4 per il Lemma 9.50. Però $\mathbb{Z}_2 \times \mathbb{Z}_2$ non ha elementi di ordine 4, contraddizione.

Esempio 9.52. Consideriamo i gruppi $(\mathbb{Z}_2, +, \overline{0})$ e $(U(\mathbb{Z}_6), \cdot, \overline{1})$. Sono equipotenti in quanto $|\mathbb{Z}_2| = 2$ e $|U(\mathbb{Z}_6)| = \varphi(6) = 2$. I due gruppi sono anche isomorfi, un isomorfismo di gruppi è dato da

$$\begin{aligned} \varphi : \mathbb{Z}_2 &\to U(\mathbb{Z}_6) \\ \overline{0} &\mapsto \overline{1} \\ \overline{1} &\mapsto \overline{5}. \end{aligned}$$

10 Anelli e campi

Consideriamo adesso degli insiemi su cui sono definite due operazioni.

Definizione 10.1. Un **anello** è una tripla $(A, +, \cdot)$ dove A è un insieme non vuoto e

$$+ : A \times A \longrightarrow A \quad \text{e} \quad \cdot : A \times A \longrightarrow A$$

sono due operazioni su A tali che:

(i) $(A, +)$ è un gruppo abeliano;
(ii) $\cdot$ è associativo, cioè $\forall a, b, c \in A$ vale $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(iii) vale la proprietà distributiva, cioè $\forall a, b, c \in A$ valgono

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Siccome $(A, +)$ è un gruppo abeliano, esiste un elemento di A, che denotiamo con 0_A o più semplicemente con 0, che è l'elemento neutro rispetto all'operazione $+$, cioè $a + 0 = 0 + a = a$ per ogni $a \in A$. L'operazione $\cdot$ non ha necessariamente un elemento neutro, quando questo succede si dice che A è un **anello con identità**. In tal caso, indichiamo l'elemento neutro rispetto al $\cdot$ con 1_A o più semplicemente con 1. Se l'operazione $\cdot$ è commutativa, diciamo che A è un **anello commutativo**.

Osservazione 10.2. Come abbiamo fatto nel caso di gruppi e monoidi sarebbe più corretto denotare un anello con identità come una quintupla $(A, +, \cdot, 0_A, 1_A)$ mettendo in evidenza anche gli elementi neutri rispetto alle due operazioni. Per non appesantire troppo le notazioni, ci limitiamo soltanto a indicare la tripla $(A, +, \cdot)$ o addirittura, quando le operazioni sono chiare dal contesto, indichiamo l'anello soltanto con l'insieme sottostante A. Infine, per analogia con le usuali operazioni tra numeri, chiameremo anche le operazioni $+$ e $\cdot$ su A somma e prodotto rispettivamente.

La proprietà distributiva lega le due operazioni $+$ e $\cdot$ presenti sull'anello. Questo ha delle interessanti conseguenze, come le seguenti.

Lemma 10.3. *Sia $(A, +, \cdot)$ un anello, e sia 0 l'elemento neutro rispetto al $+$. Allora per ogni $a \in A$ si ha*

$$0 \cdot a = a \cdot 0 = 0.$$

Dimostrazione. Per la proprietà distributiva abbiamo $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$, da cui otteniamo aggiungendo $-(0 \cdot a)$ ad entrambi i membri

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

Siccome $0 = (0 \cdot a) - (0 \cdot a)$, otteniamo $0 = 0 \cdot a$. Analogamente si verifica che $a \cdot 0 = 0$. □

Lemma 10.4. *Sia $(A, +, \cdot)$ un anello, e siano $a, b \in A$ allora*

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b).$$

Dimostrazione. Verifichiamo che $a \cdot (-b)$ è l'inverso dell'elemento $a \cdot b$ rispetto alla somma. Per la proprietà distributiva abbiamo

$$(a \cdot (-b)) + (a \cdot b) = a \cdot (-b + b) = a \cdot 0 = 0,$$

dove l'ultima uguaglianza vale per il Lemma 10.3. Pertanto $a \cdot (-b)$ coincide con $-(a \cdot b)$. Analogamente si verifica che $((-a) \cdot b) + (a \cdot b) = 0$. □

Siccome $(A, +)$ è un gruppo abeliano, tutti gli elementi di A hanno inverso rispetto alla somma. Per l'operazione $\cdot$, questo non è vero in generale. Ad esempio, una conseguenza del Lemma 10.3 è che 0 non può avere un inverso rispetto al prodotto.

Definizione 10.5. Sia $(A, +, \cdot)$ un anello con identità, se ogni elemento non nullo di A ha inverso rispetto al prodotto, cioè vale

$$\forall a \in A \setminus \{0\} \ \exists b \in A \text{ tale che } a \cdot b = b \cdot a = 1_A$$

allora A si dice **corpo** (in inglese *skew field*). Se in aggiunta l'operazione $\cdot$ è commutativa, A si dice **campo** (in inglese *field*).

Esempio 10.6.
1. $(\mathbb{Z}, +, \cdot)$ è un anello commutativo con identità. L'elemento neutro rispetto alla somma è 0, e rispetto al prodotto è 1. Gli unici elementi invertibili rispetto al prodotto sono 1 e -1, pertanto $\mathbb{Z}$ non è un campo.
2. Sia $\Bbbk = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, allora $(\Bbbk, +, \cdot)$ è un campo. L'elemento neutro rispetto alla somma è 0, e rispetto al prodotto è 1. Tutti gli elementi non nulli sono invertibili rispetto al prodotto.
3. Sia $n \in \mathbb{Z}$, $n > 1$, allora $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo con identità. L'elemento neutro rispetto alla somma è $\overline{0}$, e rispetto al prodotto è $\overline{1}$.

Proposizione 10.7. *Sia $n \in \mathbb{Z}$, $n > 1$, allora*

$$(\mathbb{Z}_n, +, \cdot) \ \textit{è un campo} \iff n \textit{ è primo.}$$

Dimostrazione. Sia $\overline{x} \in \mathbb{Z}_n$, $\overline{x} \neq \overline{0}$. Per il Teorema 8.7, abbiamo

$$\overline{x} \text{ è invertibile} \iff \mathrm{MCD}(x, n) = 1.$$

Per concludere, osserviamo che la condizione $\mathrm{MCD}(x, n) = 1$ è verificata per tutti gli $\overline{x} \neq \overline{0}$ se e soltanto se n è un numero primo. □