Appunti di Logica e Algebra 2

Pietro Pizzoccheri

2024

Indice

1 Introduzione

1.1 Insiemi

Un insieme è una collezione di oggetti, detti elementi dell'insieme.

$$\mathbb{N} := \{0, 1, 2, 3, ...\} \quad \text{insieme dei numeri naturali}$$

$$\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\} \quad \text{insieme degli interi}$$

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\} \quad \text{insieme dei numeri razionali}$$

$$\mathbb{R} := \text{insieme dei numeri reali}$$

$$\mathbb{C} := \text{insieme dei numeri complessi}$$

1.1.1 Operazioni tra insiemi

$$\subseteq \quad \text{inclusione tra insiemi}$$

$$\subsetneq \quad \text{inclusione propria tra insiemi}$$

$$X \subseteq Y \quad \text{si legge "}X \text{ è sottoinsieme di } Y\text{" o "}X \text{ è incluso in } Y\text{"}$$

Se X è un insieme finito, indico con $|X|$ il numero di elementi di X, detto anche la **cardinalità di** X.

$$\varnothing : \text{Insieme vuoto e } |\varnothing| = 0$$

Siano X e Y due insiemi. L'insieme $X \times Y := \{(x, y) : x \in X, y \in Y\}$ lo chiamiamo **prodotto cartesiano** di X e Y.

Sia $A \in \mathcal{P}(x)$, dove $\mathcal{P}(X) := \{A : A \subseteq X\}$ è detto **Insieme delle parti di** X. L'insieme $A^c := X \setminus A$ è detto **complementare** di A

1.2 Funzioni

Siano X e Y due insiemi. **Una funzione** f **da** X **a** Y è un sottoinsieme $F \subseteq X \times Y$ tale che:

- $(x, y_1) \in F$, $(x, y_2) \in F \implies y_1 = y_2$, $\forall x \in X$, $y_1, y_2 \in Y$.
- $x \in X \implies \exists y \in Y$ tale che $(x, y) \in F$

Una funzione $F \subseteq X \times Y$ la indichiamo con $f : X \to Y$. E scriviamo $f(x) = y$ se $(x, y) \in F$.

Definizione: *La funzione* $Id_x : X \to X$ *tale che* $Id_x(x) = x, \forall x \in X$ *la chiamiamo* ***funzione identità su*** X

Definizione: *Una funzione* $f : X \to Y$ *è* ***iniettiva*** *se* $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$

Definizione: *Una funzione* $f : X \to Y$ *è* ***suriettiva*** *se* $Im(f) = Y$*, dove* $Im(f) = \{y \in Y : \exists x \in X \text{ tale che } f(x) = y\}$ *è detta* ***immagine di*** f

Definizione: *Una funzione* $f : X \to Y$ *è* ***biunivoca*** *se è sia iniettiva che suriettiva.*

1.2.1 Composizione di funzioni

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. La **composizione di** f **e** g è la funzione $g \circ f : X \to Z$ tale che $(g \circ f)(x) = g(f(x))$, $\forall x \in X$.

Definizione: *una funzione* $f : X \to Y$ *è detta* ***invertibile*** *se esiste una funzione* $g : Y \to X$ *tale che*

- $g \circ f = Id_X$
- $f \circ g = Id_Y$

la funzione g *è detta* ***funzione inversa di*** f *e la indichiamo con* f^{-1}.

Una funzione $f : X \to Y$ è invertibile se e solo se è biunivoca.

1.2.2 Operazioni su insiemi

Definizione: *Una funzione* $f : X \times X \to X$ *è detta* ***operazione su*** X*. Invece di* $f(x, y)$ *scriveremo* $x \cdot y$.

Definizione: *Un'operazione* $\cdot$ *su* X *è detta* ***associativa*** *se* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall x, y, z \in X$.

Definizione: *Un'operazione* $\cdot$ *su* X *è detta* ***commutativa*** *se* $x \cdot y = y \cdot x$, $\forall x, y \in X$.

Esempio:

- $\mathcal{P}(X)$ *con l'operazione di unione* $\cup$ *è associativa e commutativa, così come lo è con l'intersezione* $\cap$.
- $A \backslash B := A \cup B^C$ ***(differenza insiemistica)*** *è un'operazione su* $\mathcal{P}(X)$.
  non è associativa: sia $A \neq \varnothing$*. Allora* $A \backslash (A \backslash A) = A \neq (A \backslash A) \backslash A = \varnothing$
  non è commutativa: $A \backslash \varnothing = A \neq \varnothing \backslash A = \varnothing$*, se* $A \neq \varnothing$
- $A \Delta B := (A \backslash B) \cup (B \backslash A)$ ***(differenza simmetrica)*** *è un'operazione su* $\mathcal{P}(X)$.
  è commutativa e anche associativa, facilmente verificabile coi diagrammi di Venn.
- *sia* $F(X) := \{f : X \to X\}$.
  La composizione " $\circ$ *" è un'operazione su* $F(X)$.
  è associativa, ma non è commutativa.
- $a \circ b = \frac{a+b}{2}$ *è un'operazione commutativa su* $\mathbb{Q}$*, ma non associativa.*

Definizione: *Sia* $\cdot$ *un'operazione su* X*. Un elemento* $e \in X$ *tale che* $e \cdot x = x \cdot e = x$, $\forall x \in X$ *è detto* ***elemento neutro*** *o* ***identità***.

L'identità è unica; se $e, e' \in X$ sono due identità, allora $e = e \cdot e' = e'$.

1.3 Monoidi

Definizione: *Un insieme X con un'operazione associativa e un'identità è detto* ***monoide****.*

Esempio:

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *con l'addizione e identità 0 sono monoidi.*
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *con la moltiplicazione e identità 1 sono monoidi.*
- $\mathcal{P}(X)$ *con* $\cup$ *e come identità l'insieme X è un monoide.*
- $\mathcal{P}(X)$ *con* $\cap$ *e come identità l'insieme vuoto è un monoide.*
- $F(X) := \{f : X \to X\}$ *con la composizione "* $\circ$ *" e come identità la funzione identità (Id_X) è un monoide.*

Definizione: *Sia X un monoide. Un elemento $x \in X$ è detto* ***invertibile*** *se esiste $y \in X$ tale che $x \cdot y = y \cdot x = e$, dove e è l'identità di X. L'elemento y è detto* ***inverso*** *di x.*

Se $x \in X$ è invertibile, il suo inverso è unico e lo indichiamo con x^{-1}.
L'identità del monoide è invertibile e il suo inverso è l'identità stessa.

Esempio:

- *L'insieme degli elementi invertibili di* $(\mathbb{N}, +)$ *è* $\{0\}$*.*
- *Linsieme degli elementi invertibili di* $(\mathbb{Z}, +)$ *è* $\mathbb{Z}$*, di* $(\mathbb{Q}, +)$ *è* $\mathbb{Q}$*, di* $(\mathbb{R}, +)$ *è* $\mathbb{R}$*, , di* $(\mathbb{C}, +)$ *è* $\mathbb{C}$*.*
- *L'insieme degli elementi invertibili di* $(\mathbb{N}, \cdot)$ *è* $\{1\}$*, di* $(\mathbb{Z}, \cdot)$ *è* $\{1, -1\}$*, di* $(\mathbb{Q}, \cdot)$ *è* $\mathbb{Q} \setminus \{0\}$*, di* $(\mathbb{R}, \cdot)$ *è* $\mathbb{R} \setminus \{0\}$*, di* $(\mathbb{C}, \cdot)$ *è* $\mathbb{C} \setminus \{0\}$*.*
- *L'insieme degli elementi invertibili di $F(X) = \{f : X \to X\}$ è l'insieme delle funzioni invertibili.*

1.4 Gruppi

Definizione: *Un monoide X è detto* ***gruppo*** *se ogni suo elemento è invertibile. Se l'operazione è commutativa, il gruppo è detto* ***gruppo abeliano****.*

Esempio:

-