

CAPITOLO 1

Fondamenti

In questo capitolo presentiamo alcune nozioni necessarie per i successivi capitoli.

1. Assiomi, postulati, definizioni

La Matematica è la scienza ipotetico-deduttiva per eccellenza. A partire da premesse che vengono chiamate ipotesi deduce conseguenze chiamate tesi. L'insieme di ipotesi, tesi ed il ragionamento che permette di ricavare la tesi dall'ipotesi si chiama Teorema. Un Teorema si intende dimostrato nel caso in cui, assumendo che l'ipotesi sia vera, con ragionamento logico si prova che la tesi è vera. Nel corso della dimostrazione si devono usare soltanto le ipotesi assunte ed eventualmente altri risultati dimostrati in precedenza.

Alcune affermazioni esprimono concetti che appaiono evidenti. Tali affermazioni si chiamano assiomi. Altre affermazioni che non sono evidenti come gli assiomi e che si pongono a base di una teoria si chiamano postulati.

Nella formulazione degli assiomi e dei postulati di una teoria e nelle successive deduzioni si utilizzano termini di cui è necessario stabilire il significato. Inevitabilmente, tentando di spiegare il significato di uno di questi termini, si è costretti ad usare altri termini che debbono essere a loro volta spiegati. Se non si decide di assumere alcuni concetti come primitivi si genera un pericoloso regresso all'infinito che rende impossibile qualsiasi deduzione. Da qui la necessità di porre delle definizioni.

Ricapitolando, per sviluppare una teoria è necessario stabilire un elenco di assiomi, postulati e definizioni. A partire da questi, con deduzione logica, si provano i risultati. Il linguaggio che si adotta è quello della teoria degli insiemi.

2. Funzioni

Definizione 1.1. Siano X, Y due insiemi non vuoti e sia f una legge che ad ogni elemento di X associa uno ed un solo elemento di Y . La terna ordinata (X, Y, f) si dice *funzione* o *applicazione*. L'insieme X si chiama *dominio* e Y *codominio*. Per indicare la funzione si scrive $f : X \rightarrow Y$. Detto x il generico elemento di X , il suo corrispondente in Y si denota con $f(x)$.

L'insieme $f(X) = \{y \in Y : \exists x \in X \text{ tale che } y = f(x)\}$ si chiama *immagine* di f . L'insieme $G_f = \{(x, y) \in X \times Y : x \in X, y = f(x)\}$ si chiama *grafico* di f .

Osservazione 1.1. Siccome una funzione è definita come una terna di oggetti, è sufficiente cambiarne anche uno solo perché la funzione cambi.

Definizione 1.2. Siano X, Y, Z insiemi non vuoti tali che $X \subseteq Z$. Siano $f : X \rightarrow Y$ e $g : Z \rightarrow Y$ due funzioni tali che $f(x) = g(x)$ per ogni x in X . La funzione f si chiama *restrizione* di g a X . La funzione g si chiama *prolungamento* di f a Z .

Definizione 1.3. Siano X, Y insiemi non vuoti e $f : X \rightarrow Y$ una funzione. Diciamo che la funzione f è *iniettiva* se comunque scelti x_1 e x_2 elementi distinti di X si ha $f(x_1) \neq f(x_2)$. Diciamo che la funzione f è *suriettiva* se $f(X) = Y$. Diciamo che la funzione f è una *corrispondenza biunivoca* oppure che è *biettiva* se è sia iniettiva che suriettiva.

Definizione 1.4. Siano X, Y, Z, T insiemi non vuoti e $f : X \rightarrow Y, g : Z \rightarrow T$ due funzioni. Supponiamo che $f(X) \subseteq Z$. La funzione $h : X \rightarrow T$ definita mediante la legge $h(x) = g(f(x))$ per ogni $x \in X$ si dice *funzione composta* da f e g . La funzione composta si indica anche con il simbolo $g \circ f$.

Definizione 1.5. Siano X, Y due insiemi non vuoti e $f : X \rightarrow Y$ una funzione iniettiva. Per ogni $y \in f(X)$ esiste un unico elemento $x \in X$ tale che $y = f(x)$. Consideriamo la legge che associa ad ogni $y \in f(X)$ l'unica soluzione $x \in X$ dell'equazione $f(x) = y$. La funzione $f^{-1} : f(X) \rightarrow X$ definita mediante la legge $f^{-1}(y) = x$ si dice funzione inversa di f . Si ha:

$$(f^{-1} \circ f)(x) = x \quad \forall x \in X, \quad (f \circ f^{-1})(y) = y \quad \forall y \in f(X).$$

3. Relazioni di equivalenza.

Sia A un insieme non vuoto. Un sottoinsieme \mathcal{R} del prodotto cartesiano $A \times A$ si dice relazione binaria in A . Scriveremo $a \mathcal{R} b$ invece di $(a, b) \in \mathcal{R}$.

Definizione 1.6 (Relazioni di equivalenza). Sia A un insieme non vuoto. Indichiamo con \sim una relazione binaria in A che verifichi le seguenti proprietà:

1. proprietà riflessiva: $a \sim a \quad \forall a \in A$.
2. proprietà simmetrica: $a \sim b \Rightarrow b \sim a \quad \forall a, b \in A$.
3. proprietà transitiva: $a \sim b, b \sim c \Rightarrow a \sim c \quad \forall a, b, c \in A$.

In tal caso la relazione si dice di equivalenza in A .

La relazione di equivalenza estende il concetto di uguaglianza e perciò talvolta scriveremo $a = b$ invece di $a \sim b$.

Esempio 3.1 (Congruenza di triangoli). Sia A l'insieme dei triangoli del piano. Poniamo

$$\mathcal{R} = \{(T_1, T_2) \in A \times A : T_1 \text{ e } T_2 \text{ sono congruenti}\}.$$

La relazione così definita è la ben nota relazione di congruenza dei triangoli e si vede facilmente che è una relazione di equivalenza.

Esempio 3.2 (Similitudine tra triangoli). Sia A l'insieme dei triangoli del piano. Poniamo

$$\mathcal{R} = \{(T_1, T_2) \in A \times A : T_1 \text{ e } T_2 \text{ sono simili}\}.$$

La relazione così definita è la ben nota relazione di similitudine tra i triangoli e si vede facilmente che è una relazione di equivalenza.

Definizione 1.7. *Siano A un insieme non vuoto e \mathcal{R} una relazione di equivalenza in A . Se a è un elemento di A , il sottoinsieme di A che contiene tutti gli elementi di A equivalenti all'elemento a si chiama classe di equivalenza di a e si indica con $[a]$.*

Ogni insieme non vuoto può essere visto come l'unione delle sue classi di equivalenza rispetto ad una fissata relazione \mathcal{R} . In tal caso diremo che è stata effettuata una partizione di A in classi di equivalenza.

Definizione 1.8. *Siano A un insieme non vuoto e \mathcal{R} una relazione di equivalenza in A . L'insieme i cui elementi sono le classi di equivalenza rispetto alla relazione \mathcal{R} si chiama insieme quoziente di A rispetto alla relazione \mathcal{R} e si indica con A/\mathcal{R} . La naturale corrispondenza tra gli elementi di A e le classi di equivalenza che associa ad ogni elemento di A la sua classe si chiama proiezione canonica e si indica con $\Pi : A \rightarrow A/\mathcal{R}$ definita dalla legge $\Pi(a) = [a]$.*

Elementi della stessa classe di equivalenza in A hanno la stessa immagine nell'insieme quoziente. Per esempio, se pensiamo a due triangoli congruenti - pensandoli come oggetti distinti - stiamo ragionando nell'insieme di tutti i triangoli. Se non ci importa pensare ad un preciso triangolo ma pensiamo al generico triangolo ignorando tutti quelli ad esso congruenti allora stiamo pensando alla sua immagine nell'insieme quoziente.

4. Relazioni di ordinamento e insiemi ordinati

Definizione 1.9. *Sia A un insieme non vuoto. Indichiamo con il simbolo \leq una relazione binaria in A che verifichi le seguenti proprietà:*

1. *proprietà riflessiva: $a \leq a$ per ogni $a \in A$.*
2. *proprietà antisimmetrica: $a \leq b$ e $b \leq a \Rightarrow a = b$.*
3. *proprietà transitiva: $a \leq b$ e $b \leq c \Rightarrow a \leq c$.*

Una tale relazione si dice di ordinamento parziale in A e l'insieme A si dice parzialmente ordinato e si scrive (A, \leq) . Se A è parzialmente ordinato e per ogni coppia di elementi a e b vale una delle due relazioni $a \leq b$, $b \leq a$ allora l'ordinamento si dice totale e l'insieme A si dice totalmente ordinato. Scriveremo $a < b$ per indicare che $a \leq b$ e $a \neq b$.

Definizione 1.10. Siano (A, \leq) un insieme parzialmente ordinato e E un suo sottoinsieme non vuoto. Se esiste $k \in A$ tale che $x \leq k$ per ogni $x \in E$ allora E si dice limitato superiormente e k un maggiorante di E . Un maggiorante appartenente all'insieme E si dice massimo di E .

Definizione 1.11. Siano (A, \leq) un insieme parzialmente ordinato e E un suo sottoinsieme non vuoto. Se esiste $h \in A$ tale che $h \leq x$ per ogni $x \in E$ allora E si dice limitato inferiormente e h un minorante di E . Un minorante appartenente all'insieme E si dice minimo di E .

Teorema 1.1. Siano (A, \leq) un insieme parzialmente ordinato e E un suo sottoinsieme non vuoto. Se E ammette massimo (minimo) esso è unico.

DIMOSTRAZIONE. Se M_1, M_2 sono entrambi massimo di E si ha $M_1 \leq M_2 \leq M_1$ da cui $M_1 = M_2$ per la proprietà antisimmetrica dell'ordinamento. \square

Definizione 1.12. Siano (A, \leq) un insieme parzialmente ordinato e E un suo sottoinsieme non vuoto. Se E è limitato superiormente indichiamo con E^* l'insieme dei maggioranti di E . Se E è limitato inferiormente indichiamo con E_* l'insieme dei minoranti di E .

Definizione 1.13. Siano (A, \leq) un insieme parzialmente ordinato e E un suo sottoinsieme limitato superiormente. Supponiamo che esista $L \in A$ tale che

1. $L \in E^*$.
2. Se $\gamma < L$ allora $\gamma \notin E^*$.

Diciamo L estremo superiore di E e lo denotiamo con $\sup E$. Si ha $L = \min E^*$.

Definizione 1.14. Siano (A, \leq) un insieme parzialmente ordinato e F un suo sottoinsieme limitato inferiormente. Supponiamo che esista $l \in A$ tale che

1. $l \in F_*$.
2. Se $l < \gamma$, allora $\gamma \notin F_*$.

Diciamo l estremo inferiore di F e lo denotiamo con $\inf F$. Si ha $l = \max F_*$.

Osserviamo che estremo superiore ed estremo inferiore sono unici.

Definizione 1.15. Un insieme parzialmente ordinato (A, \leq) ha la proprietà dell'estremo superiore se ogni suo sottoinsieme E limitato superiormente ammette estremo superiore in A .

L'esistenza dell'estremo superiore è equivalente all'esistenza dell'estremo inferiore come mostra il seguente risultato.

Teorema 1.2. Siano (A, \leq) un insieme parzialmente ordinato verificante la proprietà dell'estremo superiore e E un suo sottoinsieme limitato inferiormente. Allora esiste $\inf E$ e si ha $\inf E = \sup E_*$.

DIMOSTRAZIONE. L'insieme E_* è non vuoto perché E è limitato inferiormente. L'insieme E_* è limitato superiormente perché ogni elemento di E è maggiorante per E_* . Per la proprietà dell'estremo superiore esiste $\sup E_*$. Proviamo che $\inf E = \sup E_*$ verificando le due proprietà caratteristiche dell'estremo inferiore. Ogni elemento $x \in E$ è maggiorante per E_* e quindi $\sup E_* \leq x$ per ogni x in E quindi la proprietà 1. Proviamo la 2. Sia $\gamma \in A$ tale che $\gamma > \sup E_*$. Allora $\gamma \notin E_*$ altrimenti $\sup E_*$ non sarebbe maggiorante per E_* e ciò prova la 2. \square

Teorema 1.3. Sia (A, \leq) un insieme parzialmente ordinato verificante la proprietà dell'estremo superiore. Siano E, F sottoinsiemi non vuoti di A tali che $E \subseteq F$, E limitato inferiormente, F limitato superiormente. Allora

$$\inf F \leq \inf E \leq \sup E \leq \sup F .$$

DIMOSTRAZIONE. Vista l'inclusione $E \subseteq F$ si ha $x \leq \sup F$ per ogni $x \in E$ e quindi $\sup E \leq \sup F$. La disuguaglianza $\inf F \leq \inf E$ si prova in modo analogo. La disuguaglianza $\inf E \leq \sup E$ è ovvia. \square

5. Gruppi, Campi e Campi Ordinati.

Definizione 1.16. Sia A un insieme non vuoto. Una legge che associa ad ogni coppia di elementi di A uno ed un solo elemento di A si dice operazione binaria in A . L'elemento corrispondente alla coppia (a, b) si indica con $a \circ b$ e si chiama risultato dell'operazione.

In seguito avremo bisogno di operazioni che verifichino particolari requisiti.

Definizione 1.17 (Gruppo). Sia \mathbb{G} un insieme non vuoto in cui sia definita un'operazione \circ verificanti le seguenti proprietà:

1. $a \circ (b \circ c) = (a \circ b) \circ c$ per ogni a, b, c in \mathbb{G} - proprietà associativa.
2. Esiste $e \in \mathbb{G}$ tale che $a \circ e = e \circ a$ per ogni a in \mathbb{G} - esistenza dell'elemento neutro.
3. Per ogni a in \mathbb{G} esiste a' in \mathbb{G} tale che $a \circ a' = a' \circ a = e$ - esistenza dell'inverso.

L'insieme \mathbb{G} si dice un gruppo rispetto all'operazione \circ e si indica con (\mathbb{G}, \circ) . Se inoltre vale anche

$$a \circ b = b \circ a \quad \forall a, b \in \mathbb{G}$$

allora il gruppo si dice abeliano o commutativo.

Definizione 1.18 (Isomorfismo di gruppi). Siano (\mathbb{G}_1, \circ) e $(\mathbb{G}_2, \bar{\circ})$ due gruppi. Diciamo che i gruppi sono isomorfi se esiste una funzione $f : \mathbb{G}_1 \rightarrow \mathbb{G}_2$ biettiva e tale che

$$f(x \circ y) = f(x) \bar{\circ} f(y) \quad \forall x, y \in \mathbb{G}_1.$$

In tal caso la funzione f si dice un isomorfismo tra gruppi.

Definizione 1.19 (Campo). *Un insieme non vuoto \mathbb{K} , in cui sono definite due operazioni $+$ e $*$ dette rispettivamente somma e prodotto, si dice un campo se*

1. \mathbb{K} è un gruppo abeliano rispetto alla somma. L'elemento neutro della somma si indica con il simbolo 0 . L'inverso di un elemento a si indica con il simbolo $-a$ e si chiama opposto di a .
2. L'insieme \mathbb{K}^* degli elementi di \mathbb{K} diversi da 0 è un gruppo abeliano rispetto al prodotto. L'elemento neutro del prodotto si indica con il simbolo 1 . L'inverso di un elemento $a \neq 0$ si indica con il simbolo a^{-1} oppure $1/a$ e si chiama reciproco di a .
3. $a*(b+c) = a*b+a*c$ per ogni $a, b, c \in \mathbb{K}$ - proprietà distributiva della somma rispetto al prodotto.

Il campo si indica con $(\mathbb{K}, +, *)$.

Valgono i seguenti risultati che ci limitiamo a richiamare.

Teorema 1.4. *Sia $(\mathbb{K}, +, *)$ un campo. Siano a, b e c elementi di \mathbb{K} . Si ha:*

1. Se $a + b = a + c$ allora $b = c$.
2. Se $a + b = a$ allora $b = 0$.
3. Se $a + b = 0$ allora $b = -a$.
4. $-(-a) = a$.

Teorema 1.5. *Sia $(\mathbb{K}, +, *)$ un campo. Siano a, b e c elementi di \mathbb{K} . Si ha:*

1. Se $a \neq 0$ e $a * b = a * c$ allora $b = c$.
2. Se $a \neq 0$ e $a * b = a$ allora $b = 1$.
3. Se $a \neq 0$ e $a * b = 1$ allora $b = a^{-1}$.
4. Se $a \neq 0$ allora $(a^{-1})^{-1} = a$.

Teorema 1.6. *Sia $(\mathbb{K}, +, *)$ un campo. Siano a e b elementi di \mathbb{K} . Si ha:*

1. $0 * a = 0$.
2. Se $a \neq 0$ e $b \neq 0$ allora $a * b \neq 0$.
3. $(-a) * b = -(a * b) = a * (-b)$.
4. $(-a) * (-b) = a * b$.

Definizione 1.20 (Isomorfismo di campi). *Siano $(\mathbb{K}_1, +, *)$ e $(\mathbb{K}_2, \circ, \cdot)$ due campi. Diciamo che i campi sono isomorfi se esiste una funzione biettiva $f : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ tale che*

$$f(x + y) = f(x) \circ f(y) \quad f(x * y) = f(x) \cdot f(y) \quad \forall x, y \in \mathbb{K}_1.$$

In tal caso la funzione f si dice un isomorfismo tra campi.

Un campo può essere anche un insieme ordinato. In alcuni casi la relazione di ordinamento è compatibile con la struttura algebrica già esistente. La nuova struttura si chiama campo ordinato.

Definizione 1.21 (Campo ordinato). *Un campo $(\mathbb{K}, +, *)$ si dice ordinato se in \mathbb{K} è definito un ordinamento parziale \leq che verifichi le seguenti proprietà:*

1. $x \leq y \implies x + z \leq y + z$ per ogni $z \in \mathbb{K}$.
2. $x \leq y, \gamma > 0 \implies x * \gamma \leq y * \gamma$.

*Il campo ordinato si indica con $(\mathbb{K}, +, *, \leq)$. Sia $E \subseteq \mathbb{K}$. Se E è campo ordinato rispetto alle stesse operazioni e allo stesso ordinamento di \mathbb{K} allora $(E, +, *, \leq)$ si chiama sottocampo ordinato di \mathbb{K} .*

Dagli assiomi di campo ordinato si ha

Teorema 1.7. *Sia $(\mathbb{K}, +, *, \leq)$ un campo ordinato. Si ha*

1. *Se $x > 0$ allora $-x < 0$ e viceversa.*
2. *Se $x < 0$ e $y < z$ allora $x * y > x * z$.*
3. *Se $0 < x < y$ allora $0 < \frac{1}{y} < \frac{1}{x}$.*
4. *Se $x \leq y$ e $z \leq t$ allora $x + z \leq y + t$.*
5. *Se $0 \leq x \leq y$ e $0 \leq z \leq t$ allora $x * z \leq y * t$.*

Una interessante proprietà dei campi ordinati è la seguente

Teorema 1.8. *Siano $(\mathbb{K}, +, *)$ un campo e \leq un ordinamento parziale definito in \mathbb{K} . Se il campo \mathbb{K} è ordinato rispetto alla relazione \leq allora $x^2 \equiv x * x \geq 0$ per ogni $x \in \mathbb{K}$. In particolare $1 > 0$.*

DIMOSTRAZIONE. Infatti, se \mathbb{K} è ordinato, dalla relazione $x \geq 0$, moltiplicando ambo i membri per x segue $x^2 \geq 0 \cdot x = 0$. \square

Osservazione 1.2. La proprietà espressa nel Teorema precedente non è invertibile. Possiamo esibire un esempio di campo in cui i quadrati sono tutti non negativi ma tale campo non è ordinato. Consideriamo l'insieme dei numeri reali con le usuali operazioni algebriche. Definiamo il seguente ordinamento in \mathbb{R} . Se x e y sono due numeri reali non nulli allora l'ordinamento coincide - per definizione - con quello usuale. Se invece uno dei due numeri è nullo - per definizione - tale numero è minore dell'altro. Poniamo cioè $0 \leq x$ per ogni $x \in \mathbb{R}$. I quadrati risultano così automaticamente non negativi. Tuttavia, il campo così definito non è ordinato. Infatti, se fosse ordinato dalla disuguaglianza $-2 \leq -1$ dovrebbe seguire (sommando 1 ad ambo i membri) $-1 \leq 0$ ma ciò è in palese contrasto con la definizione di ordinamento.

La seguente proprietà è molto importante ed è verificata dai campi che useremo.

Definizione 1.22 (Proprietà di Archimede). *Sia $(\mathbb{K}, +, *, \leq)$ un campo ordinato. Il campo si dice archimedeo se per ogni coppia x e y di elementi di \mathbb{K} tali che $x > 0$ esiste $n \in \mathbb{N}$ tale che $nx \equiv \underbrace{x + \dots + x}_{n \text{ volte}} > y$.*

In un campo ordinato si può introdurre il concetto di valore assoluto.

Definizione 1.23. *Sia $(\mathbb{K}, +, *, \leq)$ un campo ordinato. Per ogni elemento x di \mathbb{K} poniamo*

$$|x| = \max\{x, -x\}.$$

L'elemento $|x|$ si chiama valore assoluto di x .

Osservazione 1.3. La definizione di valore assoluto si può dare anche nel seguente modo equivalente. Per ogni x in \mathbb{K}

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

Il valore assoluto gode di molte proprietà. Ne riportiamo alcune.

Teorema 1.9. *Sia $(\mathbb{K}, +, *, \leq)$ un campo ordinato. Si ha:*

1. $|x| \geq 0$ per ogni $x \in \mathbb{K}$.
2. $|x + y| \leq |x| + |y|$ per ogni $x, y \in \mathbb{K}$ - prima disuguaglianza triangolare.
3. $||x| - |y|| \leq |x - y|$ per ogni $x, y \in \mathbb{K}$ - seconda disuguaglianza triangolare.
4. $|x \cdot y| \leq |x| \cdot |y|$ per ogni $x, y \in \mathbb{K}$.
5. $\left| \frac{1}{x} \right| = \frac{1}{|x|}$ per ogni $x \in \mathbb{K}^*$.
6. $\left| \frac{x}{y} \right| = \frac{|x|}{|y|}$ per ogni $x \in \mathbb{K}$ e $y \in \mathbb{K}^*$.

DIMOSTRAZIONE. A titolo di esempio dimostriamo soltanto le due disuguaglianze triangolari. La prima delle due è in realtà una verifica che si esegue facilmente tenendo conto della definizione di valore assoluto. Infatti, se x, y sono entrambi positivi oppure entrambi negativi la disuguaglianza è ovvia perché è un'uguaglianza. Supponiamo x positivo, y negativo e $x + y$ positivo. Allora si ha: $x + y \leq x - y$ che è equivalente a $y \leq -y$ che è vera perché $y < 0$. In modo simile si ragiona se la somma è negativa.

Proviamo la seconda triangolare. Utilizzando la prima triangolare si ha:

$$|x| = |x - y + y| \leq |x - y| + |y|$$

da cui

$$|x| - |y| \leq |x - y|.$$

Vista l'arbitrarietà di x e y , vale anche

$$|y| - |x| \leq |y - x|$$

da cui la tesi. □

Per concludere formuliamo il concetto di isomorfismo di campi ordinati sulla falsariga di quello già introdotto per i campi.

Definizione 1.24 (Isomorfismo di campi ordinati). *Siano $(\mathbb{K}_1, +, *, \leq)$ e $(\mathbb{K}_2, \circ, \cdot, \leq')$ due campi ordinati. Diciamo che i campi sono isomorfi se esiste una funzione $f : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ biettiva e tale che*

$$f(x + y) = f(x) \circ f(y) \quad f(x * y) = f(x) \cdot f(y) \quad \forall x, y \in \mathbb{K}_1.$$

Inoltre

$$x \leq y \implies f(x) \leq' f(y) \quad \forall x, y \in \mathbb{K}_1.$$

In tal caso la funzione f si dice un isomorfismo tra campi ordinati.