Numeri Reali

L'insieme $\mathbb{R}$ dei numeri reali è dotato delle operazioni $+$ (somma) e $\cdot$ (prodotto), e di una relazione d'ordine $\leq$. Pensiamo dunque ad essi come a una struttura $(\mathbb{R}; +; \cdot; \leq)$.
Estendono i numeri razionali, nel senso che $\mathbb{Q} \subseteq \mathbb{R}$.
Valgono le seguenti proprietà:

(S0) $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ è ben definita; cioè
$\forall a, b \in \mathbb{R} : \ a + b \in \mathbb{R}$

(S1) [proprietà associativa]. $\forall a, b, c \in \mathbb{R} : (a+b)+c = a+(b+c)$

(S2) [elemento neutro]. $\exists 0 \in \mathbb{R} \ \forall a \in \mathbb{R} : \ a + 0 = 0 + a = 0$

(S3) [elemento inverso]. $\forall a \in \mathbb{R} \ \exists -a \in \mathbb{R} : \ a + (-a) = (-a) + a = 0$

(S4) [proprietà commutativa]. $\forall a, b \in \mathbb{R} : \ a + b = b + a$

(S0)-(S4) s'esprimono dicendo che $(\mathbb{R}, +)$ è un <u>gruppo commutativo</u>.

(P0) $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ è ben definita; cioè
$\forall a, b \in \mathbb{R} : \ a \cdot b = b \cdot a$

(P1) $\forall a, b, c \in \mathbb{R} : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(P2) $\exists 1 \in \mathbb{R} \ \forall a \in \mathbb{R} : \ a \cdot 1 = 1 \cdot a = a$

(P3) $\forall a \in \mathbb{R} \ \ a \neq 0 \Rightarrow \left(\exists a^{-1} \in \mathbb{R} : \ a \cdot a^{-1} = a^{-1} \cdot a = 1 \right)$

(P4) $\forall a, b \in \mathbb{R} : \ a \cdot b = b \cdot a$

Quindi $(\mathbb{R} - \{0\}, \cdot)$ è un gruppo commutativo.

(SP) [proprietà distributiva].

$$\forall a, b, c \in \mathbb{R} : \ (a + b) \cdot c = a \cdot c + b \cdot c$$

(S0)-(S4), (P0)-(P4), (SP) s'esprimono dicendo che $(\mathbb{R}; +; \cdot)$ è un <u>campo</u>

Esempio di utilizzo delle proprietà di campo.

Teorema. $\forall a \in \mathbb{R}: \quad a \cdot 0 = 0$

dim. $a \cdot 0 \overset{(S2)}{=} a \cdot (0+0) \overset{(SP)}{=} a \cdot 0 + a \cdot 0, \quad (*)$

ma poiché esiste $-(a \cdot 0)$ (per (S3)):

$0 \overset{(S3)}{=} -(a\cdot 0) + a \cdot 0 \overset{(*)}{=} -(a\cdot 0) + [a \cdot 0 + a \cdot 0]$

$\overset{(S1)}{=} [-(a\cdot 0) + a \cdot 0] + a \cdot 0 \overset{(S3)}{=} 0 + a \cdot 0 \overset{(S2)}{=} a \cdot 0.$

Cioè, $0 = a \cdot 0$, come volevamo mostrare. $\blacksquare$

Abbiamo usato (S1), (S2), (S3), (SP) e, implicitamente, (S0) e (P0).

simbolo di fine dimostrazione

(O1) $\forall a, b \in \mathbb{R}: \quad a \leq b$ o $b \leq a$

(O2) $\forall a, b \in \mathbb{R}: \quad a \leq b$ e $b \leq a \Rightarrow a = b$

(O3) $\forall a, b, c \in \mathbb{R}: \quad a \leq b$ e $b \leq c \Rightarrow a \leq c$

(O1)–(O3) dicono che $\leq$ è una relazione d'ordine totale. Poniamo $a > 0 \Leftrightarrow a \geq 0$ e $a \neq 0$.

Da (O1) segue che $\forall a \in \mathbb{R}: \quad a \leq a$.

(OS) $\forall a, b, c \in \mathbb{R}: \quad a \leq b \Leftrightarrow a + c \leq b + c$

(OP) $\forall a, b, c \in \mathbb{R}$ con $c > 0$: $\quad a \leq b \Leftrightarrow a \cdot c \leq b \cdot c$

Esempio di utilizzo delle proprietà d'ordine.

Proprietà. $\forall a, b \in \mathbb{R}: \quad a \geq 0$ e $b \geq 0 \Rightarrow a \cdot b \geq 0$.

dim. ~~a~~ Se $b = 0$: $\quad 0 \leq 0 = a \cdot 0$

Se $b > 0$, allora $\quad 0 \leq a \Rightarrow 0 = 0 \cdot b \leq a \cdot b$ $\blacksquare$

Le proprietà viste sinora, (S0)–(S4) e (P0)–(P4) e (SP) e (O1)–(O3) e (OS) e (OP), dicono che $(\mathbb{R}; +; \cdot; \leq)$ è un campo ordinato

Le proprietà viste finora valgono anche per $\mathbb{Q}$.

Def. Sia $A \in \mathbb{R}$ un insieme di numeri reali. Diciamo che $M \in \mathbb{R}$ è un maggiorante di A se

$$\forall a \in A : a \leq M.$$

Diciamo che A è superiormente limitato se ha un maggiorante.

Analogamente, $m \in \mathbb{R}$ è un minorante di A se $\forall a \in \mathbb{R} : a \geq m$ e, se un minorante di A esiste, diciamo che A è inferiormente limitato. A è limitato se è inferiormente e superiormente

Def. Sia $A \in \mathbb{R}$ e $M \in \mathbb{R}$. M è il massimo di A se (i) $\forall a \in A : a \leq M$ (M è maggiorante di A)

(ii) $M \in A$. $\boxed{\text{Scriviamo } M = \max A}$

Analogamente, $m \in \mathbb{R}$ è il minimo di A se (i) $\forall a \in A : a \geq m$ e (ii) $m \in A$. $\boxed{\text{Scriviamo } m = \min A}$

Esempio. Non tutti gli insiemi superiormente limitati hanno massimo. Per esempio,

$$A = (0,1) := \{ x \in \mathbb{R} : 0 < x < 1 \}$$

non ha massimo.

dim. Sia $M \in \mathbb{R}$ un maggiorante di A.

Quindi $M \geq \frac{1}{2} > 0$ poiché $\frac{1}{2} \in A$.

Se $0 < M < 1$, allora $M < \frac{M+1}{2} < 1$ e quindi

(a) $\frac{M+1}{2} \in (0,1)$ e (b) M non è un maggiorante di A.

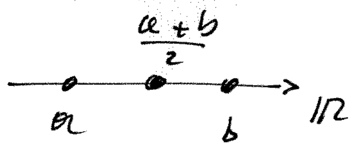
Ne segue che $M \geq 1$, quindi che $M \notin A$.

Cioè, se M soddisfa (i), allora non soddisfa (ii): A non ha massimo ∎

Una proprietà usata nella dimostrazione merita d'essere enunciata a parte.

(D) [densità]. $\forall a, b \in \mathbb{R} : a < b \Rightarrow \exists c \in \mathbb{R}$ t.c. $a < c < b$.

dim. Consideriamo $c = \frac{a+b}{2}$, il punto medio dell'intervallo $[a, b]$:



$\blacksquare$

Ci serve uno strumento più flessibile.

<u>Def.</u> Sia $A \subseteq \mathbb{R}$. Diciamo che $M \in \mathbb{R}$ è l'<u>estremo superiore</u> di A, e lo scriviamo

$$M = \sup A,$$

se (i) $\forall a \in A : a \leq M$ (M è maggiorante di A)

(ii) $\forall N \in \mathbb{R}$: N è maggiorante di $A \Rightarrow N \geq M$ (M è il minimo dei maggioranti).

Analogamente, $m \in \mathbb{R}$ è <u>l'estremo inferiore</u> di A, scritto $m = \inf A$,

se (i) m è minorante di A e (ii) $\forall n$ minorante di $A \Rightarrow n \leq m$ (m è il massimo dei minoranti).

<u>Esempio.</u> $\sup(0,1) = 1$; $\inf(0,1) = 1$.

<u>OSS.</u> $\exists \text{MAX} A = M \in \mathbb{R} \Rightarrow \exists \sup A = \text{MAX} A$.

(C) [completezza]. $\forall A \subseteq \mathbb{R}$: se A è superiormente limitato, allora $\exists \sup A \in \mathbb{R}$.

<u>Nota Bene</u>. La proprietà (C) non vale in $\mathbb{Q}$: è uno specifico attributo dell'insieme dei numeri reali.

Chiudiamo con un'ultima proprietà di base.

(A) [Proprietà di Archimede].

$\forall a, b \in \mathbb{R}$: $0 < a < b \Rightarrow \exists n \in \mathbb{N}$ t.c. $na > b$.

La struttura $(\mathbb{R}; +; \cdot; \leq)$ è caratterizzata dal fatto che $\mathbb{Q} \subseteq \mathbb{R}$ e che valgono le proprietà:

(S0)–(S4); (P0)–(P4); (SP); (O1)–(O3); (OS); (OP); (D); (C); (A).

Tutte queste proprietà, tranne (C), valgono anche per $(\mathbb{Q}; +; \cdot; \leq)$.

Nei numeri reali valgono alcune proprietà che non valevano in $\mathbb{Q}$.

<u>Teorema</u> (esistenza della radice n-esima). Sia $n \in \mathbb{N}, n \geq 2$

$\forall b \in \mathbb{R}, b > 0 \Rightarrow \exists! \, x \in \mathbb{R}, x > 0$ t.c.

$$x^n = b$$

<u>Df.</u> Scriviamo $x = \sqrt[n]{b} = b^{1/n} > 0$: x è la <u>radice n-esima</u> di $b > 0$.

<u>Df.</u> Se $b > 0$ e $\frac{m}{n} \in \mathbb{Q}$ con $m \in \mathbb{Z}$ e $n \in \mathbb{N}, n > 0$;

definiamo $\forall b > 0$: $\quad b^{\frac{m}{n}} := \left(b^{1/n}\right)^m = \left(\sqrt[n]{b}\right)^m = \sqrt[n]{b^m}$.

<u>Proprietà delle potenze</u>. (0) $\forall p \in \mathbb{Q}: 1^p = 1$.

(1) $\forall a > 0, a \in \mathbb{R} \quad \forall p, q \in \mathbb{Q}: \quad a^{p+q} = a^p \cdot a^q$

(2) $\forall a > 0, a \in \mathbb{R} \quad \forall p, q \in \mathbb{Q}: \quad (a^p)^q = a^{p \cdot q}$

(3) $\forall a, b > 0; a, b \in \mathbb{R} \quad \forall p \in \mathbb{Q}: \quad (ab)^p = a^p \cdot b^p$

(4) $\forall 0 < a < b; a, b \in \mathbb{R} \quad \forall p \in \mathbb{Q}: p > 0 \Rightarrow a^p < b^p$

(5) $\forall 0 < a < b; a, b \in \mathbb{R} \quad \forall p \in \mathbb{Q}: p < 0 \Rightarrow a^p > b^p$

(6) $\forall a \in (0, 1) \quad \forall p, q \in \mathbb{Q}: \quad p < q \Rightarrow a^p > a^q$

(7) $\forall a > 1, a \in \mathbb{R} \quad \forall p, q \in \mathbb{Q}: \quad p < q \Rightarrow a^p < a^q$

Possiamo estendere la definizione di potenza da esponenti $p \in \mathbb{Q}$ a esponenti $c \in \mathbb{R}$

Teorema - definizione.

Sia $a > 1$, $a \in \mathbb{R}$ e $c \in \mathbb{R}$, $c > 0$. Allora esiste

$$b := \sup \{ a^p : p \in \mathbb{Q}, \ 0 \leq p < c \}.$$

~~[illegible]~~ Definiamo in tal caso:

$$\boxed{b = a^c}$$

Se $a > 1$, $a \in \mathbb{R}$, $d < 0$ e $d \in \mathbb{R}$, poniamo

$$a^d = \frac{1}{a^{-d}}$$

Se $0 < a < 1$ e $c \in \mathbb{R}$, poniamo

$$a^c = \left[(a^{-1})^c \right]^{-1}.$$

Per le potenze così definite valgono le proprietà (1)-(7).

Teorema - definizione (di logaritmo).

Sia $a > 1$. Allora $\forall b > 0 \ \exists c \in \mathbb{R}$:

$$b = a^c$$

Poniamo $c = \log_a b$.

Valgono le proprietà:

(1) $\forall a > 1 \ \forall b, c > 0$: $\log_a (b \cdot c) = \log_a b + \log_a c$

(2) $\forall a > 1 \ \forall b > 0 \ \forall x \in \mathbb{R}$: $\log_a (b^x) = x \cdot \log_a b$

(3) $\forall a > 1 \ \forall 0 < b < c$: $\log_a b < \log_a c$

(4) $\forall a, b > 1 \ \forall c > 0$: $\log_a b \cdot \log_b c = \log_a c$.