Numeri reali.

Esiste un insieme $\mathbb{R} \supseteq \mathbb{Q}$ con le proprietà che seguono.

<u>Somma</u>. E' definita in $\mathbb{R}$ una somma che associa a ogni $x, y \in \mathbb{R}$ un unico $x+y \in \mathbb{R}$,

$\forall x, y \in \mathbb{R} \ \exists!\ x+y \in \mathbb{R}$,

in modo che valgano le proprietà:

(SQ) $\forall p, q \in \mathbb{Q} \subseteq \mathbb{R}$, $p+q$ è la somma già definita in $\mathbb{Q}$

(SAss) $\forall x, y, z \in \mathbb{R} : (x+y)+z = x+(y+z)$

(S-comm) $\forall x, y \in \mathbb{R} ;\ x+y = y+x$

(S-neutro) $\exists!\ \underline{0} \in \mathbb{R}\ \forall x \in \mathbb{R} : x+\underline{0} = x = \underline{0}+x$

(S-inverso) $\forall x \in \mathbb{R}\ \exists!\ x' \in \mathbb{R} ;\ x+x' = x'+x = \underline{0}$

Scriviamo $x' = -x$ (<u>opposto</u> di x).

<u>Nota</u> Le ultime quattro proprietà s'esprimono dicendo che $(\mathbb{R}, +)$ è un <u>gruppo commutativo</u>.

<u>Prodotto</u>. E' definito in $\mathbb{R}$ un prodotto: $\forall x, y\ \exists!\ x \cdot y \in \mathbb{R}$, e si ha

(PQ) $\forall p, q \in \mathbb{Q} : p \cdot q \in \mathbb{Q}$ è il prodotto in $\mathbb{Q}$

(PAss) $\forall x, y, z \in \mathbb{R} : (x \cdot y) \cdot z = x \cdot (y \cdot z)$

(PComm) $\forall x, y \in \mathbb{R} :\ x \cdot y = y \cdot x$

(P-Neutro) $\exists!\ \underline{1} \in \mathbb{R} : \forall x \in \mathbb{R} : x \cdot \underline{1} = \underline{1} \cdot x = x$

<u>NOTA</u>. Per il momento, indico con $\underline{0}$ e $\underline{1}$ gli elementi neutri di + e $\cdot$. Per (SQ) e (PQ), $\underline{0} = 0$ e $\underline{1} = 1$.

(P-inverso) $\forall x \in \mathbb{R} \setminus \{0\}\ \exists!\ x' \in \mathbb{R} :\ x \cdot x' = x' \cdot x = \underline{1}$

scriviamo $x' = x^{-1} = \frac{1}{x}$: reciproco di x.

(Notare la lieve asimmetria tra + e $\cdot$: $(\mathbb{R} \setminus \{0\}, \cdot)$ è un gruppo commutativo, ma notiamo che $(\mathbb{R}, \cdot)$ non lo è).

A legare le strutture $(\mathbb{R}, +)$ e $(\mathbb{R}, \cdot)$ c'è

(SP) $\forall x, y, z \in \mathbb{R} :\ (x+y) \cdot z = x \cdot z + y \cdot z$

(proprietà <u>distributiva</u> di + rispetto a $\cdot$).

<u>NOTA</u>: in genere si aggiunge l'assioma $\underline{1} \neq \underline{0}$, che per noi è contenuto nel fatto che $\mathbb{Q} \subseteq \mathbb{R}$ e $1 \neq 0$ già in $\mathbb{Q}$.

Le proprietà (P-Ass) – (P-inv), (S-Ass) – (S-inv) e (SP) si sintetizzano dicendo che $(\mathbb{R}, +, \cdot)$ è un <u>campo</u>.

<u>Nota</u>: anche $(\mathbb{Q}, +, \cdot)$ è un campo ordinato

<u>Ordine</u>. Tra gli elementi di $\mathbb{R}$ c'è una relazione $\leq$ (minore o uguale) con le seguenti proprietà.

(OQ) $\forall p, q \in \mathbb{Q} : p \leq q$ in $\mathbb{R} \iff p \leq q$ in $\mathbb{Q}$.

(O-Trans) $\forall x,y,z \in \mathbb{R}: x \le y$ e $y \le z \Rightarrow x \le z$
(O-antisimm) $\forall x,y \in \mathbb{R}: x \le y$ e $y \le x \Leftrightarrow x = y$
(O-totale) $\forall x,y \in \mathbb{R}: x \le y$ o $y \le x$.

Queste tre proprietà dicono che $(\mathbb{R}, \le)$ è un insieme totalmente ordinato dall'ordine debole $\le$ ("debole" è $\le$, "forte" è $<$).

Occorre legare le strutture d'ordine alle operazioni.

(OS) $\forall x,y,z \in \mathbb{R}: x \le y \Rightarrow x+z \le y+z$
(OP) $\forall x,y \in \mathbb{R}: x \ge 0$ e $y \ge 0 \Rightarrow x \cdot y \ge 0$

Un campo in cui valgono anche questi cinque assiomi d'ordine è un campo ordinato.

- $(\mathbb{R}, +, \cdot, \le)$ è un campo ordinato.

Oss. Anche $\mathbb{Q}$ lo è.

(Archimede) $\forall M > 0\ \forall \varepsilon > 0\ \exists n \in \mathbb{N}:$
$n\varepsilon > M$

L'assioma di Archimede esclude che esistano "infiniti" o "infinitesimi".
$(\mathbb{R}, +, \cdot, \le)$ e $(\mathbb{Q}, +, \cdot, \le)$ sono campi archimedei.

DELUSIONE! Dopo una dozzina di assiomi abbiamo solo proprietà che pure $\mathbb{Q}$ possiede!

Verso l'assioma di completezza.

Def. Sia $A \subseteq \mathbb{R}$. Un maggiorante di A è un elemento $a \in \mathbb{R}$ tale che
$\forall x \in A: x \le a$
A è limitato superiormente se $\exists a \in \mathbb{R}$: a è un maggiorante di A.

Note (1) Alcuni insiemi in $\mathbb{R}$ non sono limitati superiormente. P. es., $\mathbb{R}$ non è limitato superiormente: fissato $a \in \mathbb{R}$, $a+1 \in \mathbb{R}$ e $a+1 > a$.
(2) Sia A limitato superiormente. Allora esistono infiniti maggioranti di A: se a è un maggiorante di A e $n \in \mathbb{N}$, anche $a+n$ è un magg. di A.

Def. Sia $A \subseteq \mathbb{R}$. $M \in \mathbb{R}$ è il massimo di A, $\boxed{M = \mathrm{MAX}\, A}$ se

(1) $M \in A$

(2) M è maggiorante di A: $\forall x \in A: x \leq M$.

Note (1) Se $A \subseteq \mathbb{R}$ ha massimo, A è lim. sup. ($\mathrm{MAX}\, A$ è un maggiorante!).

(2) Esistono insiemi $A \subseteq \mathbb{R}$ che sono limitati superiormente, ma che non hanno massimo. P. es. $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$ è limitato sup. ($a = 0$, $a = 1$, generalmente $a \geq 0$ sono maggioranti di A), ma non ha massimo.

dim. Sia $a = \mathrm{MAX}\, \mathbb{R}^-$. Allora $a < 0$. Consideriamo $\frac{a}{2} = a \cdot \frac{1}{2}$: $a < \frac{a}{2} < 0$, quindi $\frac{a}{2} \in \mathbb{R}^-$ e $\frac{a}{2} > \mathrm{MAX}\, \mathbb{R}^-$, assurdo ∎

(3) Il massimo di A è unico, se esiste.

dim. Siano a, a' massimi per A. Poiché $a' \in A$, $a' \leq a$ perché a è massimo. Allo stesso modo, $a \leq a'$. Quindi $a = a'$ ∎

(4) $\emptyset$ non ha massimo.

Def. $A \subseteq \mathbb{R}$ è limitato inferiormente se $\exists\, b \in \mathbb{R} : \forall x \in A \;\; x \geq b$. Un $b \in \mathbb{R}$ con questa proprietà è detto minorante di A.

Il minimo di A è un elemento $m \in \mathbb{R}$:

(1) $m \in A$

(2) m è minorante di A: $\forall x \in A: x \geq m$

Oss. Definizioni e note precedenti valgono per $\mathbb{Q}$ come per $\mathbb{R}$.

Il particolare ruolo di 0 tra i maggioranti di $\mathbb{R}^-$ merita attenzione.

Definizione. Sia $A \subseteq \mathbb{R}$, $a \in \mathbb{R}$. a è l'estremo superiore di A,

$a = \sup A$,

se (1) a è un maggiorante di A, $\forall x \in A \Rightarrow x \leq a$

(2) $\forall\, a' \in \mathbb{R}$: a' è un maggiorante di A $\Rightarrow a' \geq a$,

cioè $a = \min\{a' \in \mathbb{R} : a'$ è maggiorante di $A\}$

ASSIOMA DI COMPLETEZZA. Sia $A \subseteq \mathbb{R}$, $A \neq \emptyset$, A limitato superiormente. Allora

$$\exists \sup A \in \mathbb{R}.$$

Nota. Definiamo $b = \inf B$ se $b = \text{MAX}\{b' : b' \text{ è minorante di } A\}$. ~~Abbiamo che~~ Proprietà, $A \subseteq \mathbb{R}$, $A \neq \emptyset$, A inferiormente limitato

$$\Rightarrow \exists \inf A \in \mathbb{R}.$$

- L'assioma di completezza non vale in $\mathbb{Q}$. Vedremo perché e come questo c'entri con $\sqrt{2}$. Ciò facendo, vedremo anche alcuni fatti interessanti e utili (densità).

- OSSERVAZIONE. Un campo ordinato è una struttura $(X; +; \cdot; \leq)$ dove
  - X è un insieme (di "numeri")
  - + e · sono operazioni su X
  - ≤ è una relazione d'ordine su X

e valgono le proprietà
(S-Ass); (S-Comm); (S-Neutro); (S-inverso); (P-Ass.); (P-Comm); (P-Neutro); (P-inverso); (SP); (SP-bis): $1 \neq 0$;
(O-Trans); (O-Antisimm); (O-totale); (OS); (OP)

In una struttura siffatta abbiamo sempre dei sottoinsiemi $X_{\mathbb{N}} \subseteq X_{\mathbb{Z}} \subseteq X_{\mathbb{Q}} \subseteq X$ con le proprietà di $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$: possiamo dunque parlare di numeri naturali, interi, razionali in X.

$$X_{\mathbb{N}} = \{\underline{0}; \underline{1}; \underline{2} \overset{\text{df}}{=} \underline{1}+\underline{1}; \underline{3} \overset{\text{df}}{=} \underline{1}+\underline{1}+\underline{1}; \dots\}$$

L'unico dubbio da considerare è che esistano $n, m \in \mathbb{N}$ t.c. $n \neq m$, ma

$$\underline{n} = \underbrace{\underline{1}+\underline{1}+\dots+\underline{1}}_{n \text{ volte}} = \underbrace{\underline{1}+\underline{1}+\dots+\underline{1}}_{m \text{ volte}} = \underline{m}.$$

~~Se ciò accadesse e, per assurdo, n>m,~~ ~~allora~~ Vedremo sotto che ciò non può accadere.

$$X_{\mathbb{Z}} = X_{\mathbb{N}} \cup \{-\underline{n} : \underline{n} \in X_{\mathbb{N}}, \underline{n} \neq \underline{0}\}$$

$$X_{\mathbb{Q}} = \left\{\underline{m} \cdot \underline{n}^{-1} = \underline{m} \cdot \frac{\underline{1}}{\underline{n}} \overset{\text{df}}{=} \frac{\underline{m}}{\underline{n}} : \underline{m}, \underline{n} \in X_{\mathbb{Z}}, \underline{n} \neq \underline{0}\right\}$$

Ci sarà da verificare che $\forall \underline{m}, \underline{n}, \underline{p}, \underline{q} \in X_{\mathbb{Z}}$ con $\underline{n} \neq \underline{0} \neq \underline{q}$ e $\underline{m} \cdot \underline{q} = \underline{n} \cdot \underline{p} \Rightarrow \frac{\underline{m}}{\underline{n}} = \frac{\underline{p}}{\underline{q}}$ (ovvio).

~~• $\forall a \in \mathbb{R}: a \cdot 0 = a$~~

~~dim. $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 - a \cdot 0 = 0$~~

~~Alcune proprietà utili~~ ~~$a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot 0$~~

~~• $-(a \cdot b) = (-1) \cdot (a \cdot b) = (-a) \cdot b$~~

~~dim. $a \cdot b + (-1) \cdot (a \cdot b) =$~~

~~$= 1 \cdot (a \cdot b) + (-1) \cdot (a \cdot b) = (1 + (-1)) \cdot (a \cdot b)$~~

~~$= 0 \cdot (a \cdot b) = 0 \Rightarrow (-1) \cdot (a \cdot b) = -(a \cdot b)$~~

Alcune proprietà utili dimostrate a partire dagli assiomi di campo

(1) ~~Le~~ **Legge di annullamento del prodotto**. $\forall a, b \in \mathbb{R}: a \cdot b = 0 \Leftrightarrow a = 0 \lor b = 0$

dim. ($\Leftarrow$) Mostro che $\forall a \in \mathbb{R}: a \cdot 0 = 0$.

$$
\begin{aligned}
a \cdot 0 &= a \cdot (0+0) \\
&= a \cdot 0 + a \cdot 0
\end{aligned}
$$

$$
\begin{aligned}
\Rightarrow 0 &= a \cdot 0 + (-(a \cdot 0)) \\
&= (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) \\
&= a \cdot 0 + [a \cdot 0 + (-(a \cdot 0))] \\
&= a \cdot 0 + 0 \\
&= a \cdot 0
\end{aligned}
$$

($\Rightarrow$) Mostro che $a \cdot b = 0$ e $b \neq 0 \Rightarrow a = 0$.

$\underset{\shortparallel}{0} \cdot b^{-1} = 0$

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

(1 ½) $\forall a \in \mathbb{R}: -(-a) = a$. dim. $a + (-a) = 0$
$\Rightarrow -(-a) = a$ ∎

(2) $\forall a \in \mathbb{R}: -a = (-1) \cdot a$

dim. $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = [1 + (-1)] \cdot a$
$0 \cdot a = 0 \Rightarrow (-1) \cdot a = -a$ ∎

(3) Se $a \neq 0$, l'equazione $ax = b$ ha l'unica soluzione $x = b \cdot a^{-1}$.

Definiamo in $\mathbb{R}$:

sottrazione: $a - b \overset{\text{df.}}{=} a + (-b)$

divisione: $b \neq 0 \Rightarrow a : b = \frac{a}{b} \overset{\text{df.}}{=} a \cdot b^{-1}$

(4) $\forall a, b \in \mathbb{R}: (-a) \cdot b = -(a \cdot b)$ (4.1)

$(-a) \cdot (-b) = a \cdot b$ (4.2)

dim. (4.1) $(-a) \cdot b + a \cdot b$
$= [(-a) + a] \cdot b = 0 \cdot b = 0 \Rightarrow (-a) \cdot b = -(a \cdot b)$

(4.2) $(-a) \cdot (-b) = -[a \cdot (-b)]$
$= -\{-(a \cdot b)\} = a \cdot b$ ∎

Alcune proprietà dimostrate a partire dagli assiomi di campo ordinato.

Def. $\forall a, b \in \mathbb{R}: a < b \overset{\text{df.}}{\Leftrightarrow} a \leq b$ e $a \neq b$.

(1) $1 > 0$. dim. $1 \neq 0$ e
$1 = 1 \cdot 1 = (-1) \cdot (-1)$. Se fosse $-1 \geq 0$,
allora $1 = (-1) \cdot (-1) \geq 0$. Se $-1 \leq 0 \Rightarrow 0 = 1 + (-1) \leq 1 + 0 = 1$ ∎

(2) $-1 < 0$ Dim. $1 \geq 0 \Rightarrow 0 = 1 + (-1) \geq 0 + (-1) = -1$

e se fosse $-1 = 0$, allora $0 = 1 + (-1) = 1 + 0 = 1$, assurdo.

(3) $\forall a, b \in \mathbb{R} \setminus \{0\}$:

(3.1) $a > 0,\ b > 0 \Rightarrow a \cdot b > 0$

(3.2) $a > 0,\ b < 0 \Rightarrow a \cdot b < 0$

(3.3) $a < 0,\ b > 0 \Rightarrow a \cdot b < 0$

(3.4) $a < 0,\ b < 0 \Rightarrow a \cdot b > 0$

Dim. di (3.2). Poichè $a \neq 0 \neq b$, $a \cdot b \neq 0$.

$a > 0;\ b < 0 \Rightarrow a > 0;\ -b = -b + 0 \geq -b + b = 0$

$\Rightarrow 0 \leq a \cdot (-b) = -ab$

$\Rightarrow ab = a \cdot b + 0 \leq a \cdot b + (-ab) = 0.$

Cioè, $a \cdot b \leq 0$ e $a \cdot b \neq 0$.

Cioè, $ab < 0$ ∎

Gli altri casi sono simili.

(4) $b \geq 0 \Leftrightarrow -b \leq 0$.