

Descrizione dell'insieme dei numeri razionali: $\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\} \right\}$
come campo ordinato

I razionali soddisfanno le seguenti proprietà $\forall a, b, c \in \mathbb{Q}$.

(PS1) $a + b = b + a$ (commutatività di +)

(PS2) $(a + b) + c = a + (b + c)$ (associatività di +)

(PS3) $\exists 0 \in \mathbb{Q}$ t.c. $a + 0 = a$ (elemento neutro di +)

(PS4) $\exists (-a)$ t.c. $a + (-a) = 0$ (esistenza inverso rispetto a +)

(PP1) $a \cdot b = b \cdot a$ (commutatività del $\cdot$)

(PP2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatività del $\cdot$)

(PP3) $\exists 1 \in \mathbb{Q}$ t.c. $a \cdot 1 = a$ ($\exists$ dell'el. neutro del $\cdot$)

(PP4) se $a \neq 0$ $\exists a^{-1}$ t.c. $a \cdot (a^{-1}) = 1$ ($\exists$ dell'inverso risp. a $\cdot$)

(PSP) $a \cdot (b + c) = ab + ac$ (distributività di + risp. a $\cdot$)

Quando un insieme è dotato di 2 operazioni binarie che soddisfano (PS1) - (PSP) si dice "un campo".

È una relazione $\leq$ di ordinamento totale che soddisfa le proprietà seguenti.

(P1) $a \leq a$ (prop. riflessiva)

(P2) se $a \leq b$ e $b \leq a \Rightarrow a = b$ (prop. antisimmetrica)

(P3) se $a \leq b$ e $b \leq c \Rightarrow a \leq c$ (prop. transitiva)

Inoltre

(P4) se $a \leq b \Rightarrow a + c \leq b + c$ (esempio $x + 2 \leq 0 \Rightarrow x \leq -2$)

(P5) se $a \leq b$ e $c > 0 \Rightarrow a \cdot c \leq b \cdot c$ (esempio: $2x \leq 3 \Rightarrow x \leq 3/2$)

Quando un insieme è dotato di $+$, $\cdot$ e $\leq$ t.c. sono soddisfatte (PS1) - (P5) allora si dice un campo ordinato.

Esempio di un campo non ordinato.

$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$ è un campo con

le seguenti operazioni $a \oplus_p b = a + b \bmod p$, $a \odot_p b = a \cdot b \bmod p$
(esempio $2 \oplus_7 6 = 2 + 6 \bmod 7 = \text{resto di } (2+6)/7 = (2+6)\%7 = 1$; $6 \odot_7 5 = 2$)

definiscono un campo quando p è primo. in informatica

Esempio: $2^{-1} = 4$ in $\mathbb{Z}_7$, poiché $2 \odot_7 4 = 1$.

$\mathbb{Z}_7$ non è ^{un campo} ordinato. Infatti, def. $a \lesseqgtr_p b$ quando $a \leq b$

ma $2 \lesseqgtr_7 3 \not\Rightarrow 2 \odot_7 5 \leq 3 \odot_7 5$
 $\parallel \quad \parallel$
 $3 > 1$