Nozioni di $\cdot$ funzione $A \to B$

$\cdot$ operazione (binaria): $* \; A \times A \to A$

$(A, *)$ gruppo se

1) $\exists e \in A : e * a = a * e = a \quad \forall a \in A$

2) $\forall a \in A \; \exists \bar{a} \in A : a * \bar{a} = \bar{a} * a = e$

3) $\forall a, b, c \in A : a * (b * c) = (a * b) * c.$

gruppo abeliano se

$\forall a, b \in A : a * b = b * a$

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$

$(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}^*, \cdot)$ $(\mathbb{C}, +)$

$(\mathbb{C}^*, \cdot)$ $(\{1, -1\}, \cdot)$

$(\{0, 1\}, \oplus)$

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$GL_n(\mathbb{K}) = \{ M \in \mathbb{K}^{n,n} \mid \det(M) \neq 0 \}.$$

rispetto il prodotto righe per colonne.

↓

GRUPPO NON COMMUTATIVO

ATTENZIONE! Se $A$ e $B$ sono matrici quadrate, invertibili

1) $A^{-1}B \neq BA^{-1}$

2) NON SCRIVETE MAI

$AX = B$ ok

$X = B/A$ NO!!!

$X = A^{-1}B$

---

Gruppo simmetrico su di un insieme $\Omega$

$$S(\Omega) = \{ f : \Omega \to \Omega \mid f \text{ biettiva} \}.$$

~~legge di composizione~~: operazione = comp. di funzioni

1) $\exists\, \iota \in S(\Omega)$ dato da $i \begin{cases} \Omega \to \Omega \\ x \to x \end{cases}$

$\forall$ funzione $f$ : $\quad f \circ i = i \circ f = f$

2) $\forall f \in S(\Omega)\ \exists f^{-1} \in S(\Omega)$ tale che

$$f \circ f^{-1} = f^{-1} \circ f = \iota$$

$$f^{-1} = \{ (b,a) \in \Omega \times \Omega \mid (a,b) \in f \}.$$

3) la composizione di funzioni è

sempre associativa.

$f : A \to B$

$g : B \to C$

$h : C \to D \Rightarrow \quad h \circ (g \circ f) = (h \circ g) \circ f$

$A \longrightarrow D$

in particolare è vero per le

biiezioni $\Omega \to \Omega$.

Def: Una struttura algebrica

$$(A, \tilde{+}, \tilde{\cdot})$$

é detta anello (commutativo con unitá)

se 1) $(A, \tilde{+})$ é un gruppo abeliano.

[ 2) $\exists 1_A \in A : 1_A \tilde{\cdot} a = a \tilde{\cdot} 1_A = a \quad \forall a \in A$

3) $\forall a, b, c \in A : \quad a \tilde{\cdot} (b \tilde{+} c) = a \tilde{\cdot} b \tilde{+} \tilde{a} \cdot c$

$$(a \tilde{+} b) \tilde{\cdot} c = a \tilde{\cdot} c \tilde{+} b \tilde{\cdot} c$$

4) $\tilde{\cdot}$ é associativo $(a \tilde{\cdot} b) \tilde{\cdot} c = a \tilde{\cdot} (b \tilde{\cdot} c)$

[ 5) $\tilde{\cdot}$ é commutativo

ESEMPIO: $(\mathbb{Z}, +, \cdot)$

CAMPO $(\mathbb{K}, +, \cdot)$ é un anello commutativo con unitá in cui $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$ é un gruppo abeliano.

1) $(\mathbb{K}, +)$: gruppo abeliano

2) $(\mathbb{K}^\times, \cdot)$: gruppo abeliano

3) $\forall a, b, c \in \mathbb{K}$: $a \cdot (b+c) = ab + ac$

$(a+b) \cdot c = ac + bc$

ESEMPI: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

$(\mathbb{C}, +, \cdot)$

$GL_n(\mathbb{K})$

$(\mathbb{F}_2, \oplus, \cdot)$ $\qquad \mathbb{F}_2 = \{0, 1\}$.

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

$(\mathbb{F}_2, \oplus, \cdot)$ é un campo

$(\mathbb{F}_3, +', \cdot')$

| +' | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| · | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

$(a+b)\%3$ $\qquad$ $(a \cdot b)\%3$

resto dividendo per 3

$(\mathbb{Z}_4, +', \cdot')$

| +' | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| ·' | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

ANELLO MA NON CAMPO

2 non ammette inverso moltiplic

N.B In un campo $\forall a \in \mathbb{K} : 0 \cdot a = 0$

vale altresí che $a \cdot b = 0 \Rightarrow a = 0$ oppure $b = 0$

In un campo l'equazione

$$a x = b$$

con $a, b \in \mathbb{K}$, $a \neq 0$ é sempre risolubile.

$$\boxed{x = a^{-1} b}$$

$2x = 4$

$3x = 4$

$3x^2 = 4$ in $\mathbb{R}$

$3x^2 = -4$ in $\mathbb{C}$

DIMOSTRIAMO CHE

$\forall a \in \mathbb{K}$ $a \cdot 0 = 0$ in un campo

DIM

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

$$-(a\cdot 0)+a\cdot 0 = -(a\cdot 0)+(a\cdot 0+a\cdot 0)$$

$$\begin{array}{ccc} \| & & \| \\ 0 & & (-(a\cdot 0)+a\cdot 0)+a\cdot 0 \\ & & \| \\ & & 0+a\cdot 0 = a\cdot 0 \end{array}$$

$\square$

# Legge di annullamento del prodotto

$a, b$

Teorema $\forall a, b \in \mathbb{K}$; $a\cdot b = 0 \Leftrightarrow a = 0$ oppure $b = 0$

__DIM__: Se $a=0$ o $b=0 \Rightarrow ab=0$

Supponiamo $ab=0$ se ~~$b=0$~~

$a=0 \Rightarrow$ FINE

sia dunque $a\neq 0 \Rightarrow \exists a' \in \mathbb{K}$:

$a^{-1}\cdot a = 1$

$$\Rightarrow \quad a^{-1}\cdot(ab) = a^{-1}\cdot 0 = 0$$
$$\parallel$$
$$(a^{-1}\cdot a)\,b = 1\cdot b = b$$

$\square$

---

Struttura di Spazio Vettoriale su di un campo $(\mathbb{K}, +, \cdot)$

<u>Def</u>: $(V, \oplus)$ é detto spazio vettoriale su di un campo $\mathbb{K}$ se

1) $(V, \oplus)$ é un gruppo abeliano

2) $\exists\, * : \mathbb{K} \times V \longrightarrow V$ che gode delle seguenti proprietà:

a) $1 * \bar{v} = \bar{v} \quad \forall \bar{v} \in V$

b) $\forall \alpha, \beta \in \mathbb{K}, \forall \bar{v} \in V : (\alpha \cdot \beta) * \bar{v} = \alpha * (\beta * \bar{v})$

c) $\forall \alpha, \beta \in \mathbb{K}, \forall \bar{v} \in V : (\alpha + \beta) * \bar{v} = \alpha * \bar{v} \oplus \beta * \bar{v}$

d) $\forall \alpha \in \mathbb{K}, \forall \bar{v}, \bar{w} \in V$:

$$\alpha * (\bar{v} \oplus \bar{w}) = \alpha * \bar{v} \oplus \alpha * \bar{w}$$

GLI ELEMENTI DI $\mathbb{K}$ sono detti <u>scalari</u>; gli elementi di V <u>vettori</u>

L'operazione $*: \mathbb{K} \times V \to V$ è detta <u>prodotto per scalare</u> e prende uno scalare ed un vettore e restituisce un vettore.

la proprietà a) è detta <u>unitarietà</u>

b) pseudo-associativa

c, d) pseudo-distributive

Idea di spazio vettoriale.

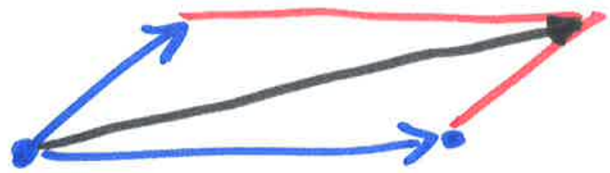
- Elementi di V vettori.

  → vettori geometrici

"frecce orientate"

$\oplus$

somma di vettori



prodotto per scalare $k \in \mathbb{R}$

$k \geq 0 \Rightarrow$ dato $\rightarrow$ costruisco un vettore che ha stessa direzione, stesso verso di $\rightarrow$ e lunghezza $k$ volte la lungh. di $\rightarrow$

$2 * \rightarrow = \longrightarrow$ $\qquad \frac{1}{2} * \nearrow = \nearrow$

$k < 0 \Rightarrow$ dato $\rightarrow$ costruisco un vettore che ha medesima direzione, verso opposto e lunghezza $-k$ volte la lunghezza di $\longrightarrow$

$-2 * \downarrow = \uparrow$

Esempi di spazi vettoriali.

$\mathbb{K}(\mathbb{K})$ un campo $\mathbb{K}$ é spazio vettoriale su se stesso con $* = \cdot$
$\oplus = +$

$\mathbb{R}(\mathbb{Q})$ il campo reale come spazio vettoriale su $\mathbb{Q}$.

$\mathbb{C}(\mathbb{R})$