

Def: $(\mathbb{K}, +, \cdot)$ è un campo se

- 1) $(\mathbb{K}, +)$ è un gruppo abeliano con el. neutro 0
- 2) $(\mathbb{K} \setminus \{0\}, \cdot)$ è un gruppo abeliano
- 3) Valgono le proprietà distributive

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

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

$$(\mathbb{R}(x), +, \cdot) \text{ ove } \mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \text{ polinomi} \right.$$

in $\mathbb{R}[x]$
a coeff. in $\mathbb{R}$ in x
con $g(x) \neq 0$.

$$\mathbb{F}_2 = \mathbb{Z}_2$$

$$\mathbb{Z}_2 = \{0, 1\}$$

$$0 = F$$

$$1 = V$$

$$\begin{array}{r|l} + & 0 \ 1 \\ 0 & 0 \ 1 \\ 1 & 1 \ 0 \end{array}$$

$$\begin{array}{r|l} \cdot & 0 \ 1 \\ 0 & 0 \ 0 \\ 1 & 0 \ 1 \end{array}$$

XOR

$$A \wedge B = 8 = A$$

$$(a \wedge \neg b) \vee (\neg a \wedge b) \quad (a \wedge b)$$

insieme universale
di operazioni binarie.

$\neg$ NOT

$$\begin{array}{r|l} x & x+1 \\ 0 & 1 \\ 1 & 0 \end{array}$$

$$\text{OR} \begin{array}{r|l} 0 & 0 \ 1 \\ 0 & 0 \ 1 \\ 1 & 1 \ 1 \end{array}$$

$$\begin{array}{r|l} x_1 & x_2 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{array}$$

$$x_1 + x_2 + x_1 x_2$$

$$A \text{ OR } B =$$

$$(A \text{ XOR } B) \text{ XOR } (A \wedge B)$$

$$\begin{array}{r|l} x_1 & x_2 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{array}$$

$$A+1=1$$

$$A \Rightarrow B$$

$$\neg A \text{ or } B$$

$$x_1 \quad x_2$$

$$(x_1+1) + x_2 + (x_1+1)x_2 =$$

$$= 1 + x_1 + x_2 + x_1x_2 + x_2 =$$

$$= 1 + x_1 + x_1x_2$$

$$0 \quad 0 \quad 1$$

$$0 \quad 1 \quad 1$$

$$1 \quad 0 \quad 0$$

$$1 \quad 1 \quad 1$$

è la tabella giusta.

In generale $(\mathbb{Z}_p, +, \cdot)$ è un campo finito se p è primo.

$$e \quad (a+b) := \text{resto}(a+b)/p$$

$$(a \cdot b) := \text{resto}(a \cdot b)/p$$

$$\mathbb{Z}_p = \{0, \dots, p-1\}$$

+	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

$\mathbb{Z}_3$

N.B. $\mathbb{Z}_4$ non è un campo

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

↑ nuovo bene!

2 non è invertib.le.

$\mathbb{F}_4$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$$\mathbb{F}_4 = \{ \overset{0}{(00)}, \overset{1}{(01)}, \overset{2}{(10)}, \overset{3}{(11)} \}$$

$$\in \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$(10)^2 + (10) + (01) = (00)$$

$$x^2 + x + 1$$

Teorema: Sia K un campo, $K[x] = \{ f(x) \mid f(x) \text{ polinomio in } x \text{ a coeff. in } K \}$.

$$\Rightarrow \frac{K[x]}{(f(x))} \quad f(x) \text{ polinomio irriducibile a coeff. in } K$$

è un campo ove

elementi di $\frac{K[x]}{(f(x))}$ = possibili resti della divisione di un polinomio per $f(x)$

= polinomi in $K[x]$ di grado $< \deg f(x)$.

Operations $(f(x) + g(x)) := \text{resto } f(x) + g(x) \text{ in } K[x]$
e $f(x)$

$(h(x) \cdot g(x)) := \text{resto } f(x) \cdot g(x) \text{ in } K[x]$
e $f(x)$.

$$\frac{\mathbb{Z}_2[x]}{(x^2+x+1)} = \{0, 1, x, x+1\}$$

$$\begin{array}{cccc} & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{array}$$

$$x+1 \quad (x+1) \cdot x = 1$$

$$\begin{array}{ccc} 3 & 2 & 1 \end{array}$$

$$x(x+1) = x^2 + x = (x^2 + x + 1) \cdot 1 + 1$$

$$= 1$$

GLI ELEMENTI DI UN CAMPO $(K, +, \cdot)$ SONO DETTI SCALARI

Una sequenza di elementi di un insieme A è una funzione

$$i: \{1, \dots, n\} \rightarrow A$$

Un sistema / multinsieme è una funzione $f: A \rightarrow \mathbb{N}$ (con 0).
 A è detto supporto del multinsieme.

→ Sequenza: collezione ordinata di oggetti con
ripetizioni

→ Sistema / multinsieme: collezione non ordinata di
oggetti con molteplicità.

a_1	$\dots$	a_t
$\downarrow$	$\downarrow$	$\downarrow$
1	5	3

$(1,1,3,4) \neq (1,3,1,4) \neq (4,3,1,3)$ sequenze
 $[1,1,3,4] = [1,3,1,4] \neq (4,3,1,3)$ multiinsieme
 $\{1,1,3,4\} = \{1,3,1,4\} = \{4,3,1,1\} = \{1,4,3\}$ insieme.

Indico con A^n = insieme di tutte le sequenze
 di lunghezza n ad elementi in A

$$A^n := \{ f: \{1 \dots n\} \rightarrow A \mid f \text{ funzione} \}.$$

lo si può anche identificare con

$$\underbrace{A \times (A \times \dots \times (A \times A)) \dots}_{n \text{ volte}} \quad A^2 = A \times A$$

$$A^n = \{ (a_1 \dots a_n) \mid a_i \in A \}.$$

Spazio vettoriale

vetture



oggetto che ha una lunghezza

• una direzione



• un verso



$\neq$ $\rightarrow$ lunghezza



$\neq \rightarrow$ direzione

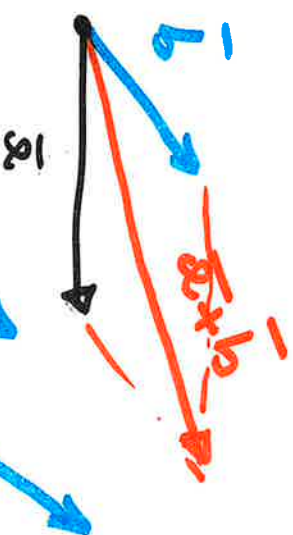


$\neq$ $\rightarrow$ verso.

2 operazioni

1) Somma di vettori

2) prodotto per scalare

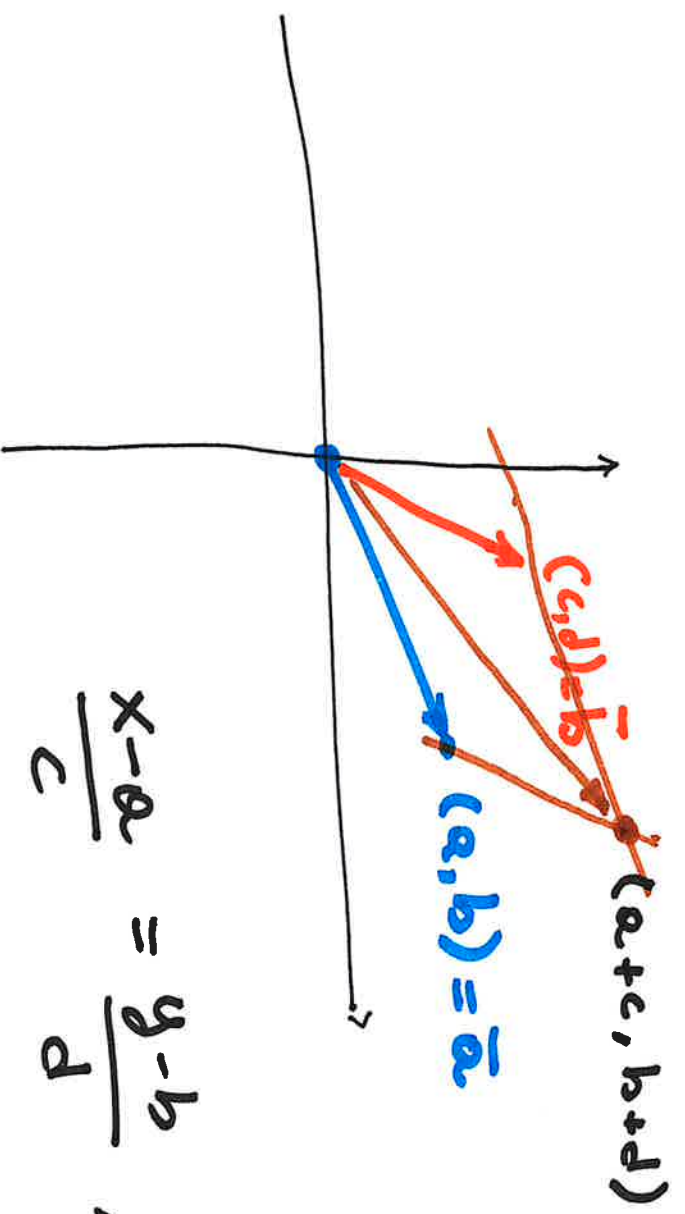


$a > 0$

$2 \rightarrow$

$a < 0$

$-1 \rightarrow$



$$\frac{x-a}{c} = \frac{y-b}{d} \quad \text{recta por } (a,b) \text{ paralela a } (c,d)$$

$$\frac{x-c}{a} = \frac{y-d}{b} \quad \text{recta por } (c,d) \text{ paralela a } (a,b)$$

~~$x = \frac{y-b}{d}c + a$~~

$$x = \frac{(y-b)}{d}c + a \quad x = \frac{y-d}{b}a + c$$

$$(y-h)cb + a db = (y-d)da + chd$$

$$y(ch - da) = chd - da h + hcb - dda \\ = (ch - da)(d + b)$$

$$\Rightarrow y = d + b \quad x = a + c$$

$$(a, b) + (a, b) = 2(a, b) = (2a, 2b)$$

$$(a, b) \hat{+} (c, d) := (a+c, b+d)$$

$$\alpha(a, b) := (\alpha a, \alpha b)$$

$$\alpha = -1 \Rightarrow -1(a, b) + (a, b) = (-a + a, -b + b) = (0, 0)$$

Def: Sia $(V, \hat{+})$ un gruppo abeliano e K un campo.

Si dice che V è uno spazio vettoriale sul campo K (in simboli $V(K)$) se valgono le seguenti proprietà:

1) $(V, \hat{+})$ è un gruppo abeliano

2) $\exists$ funzione $\hat{\cdot} : K \times V \rightarrow V$ che soddisfa le seguenti proprietà:

unitaries [a] $1 \hat{\cdot} \bar{v} = \bar{v} \quad \forall \bar{v} \in V$

pseudo lin. [b] $\forall \alpha, \beta \in K: (\alpha \cdot \beta) \hat{\cdot} \bar{v} = \alpha \hat{\cdot} (\beta \hat{\cdot} \bar{v})$

pseudo assoc. [c] $\forall \alpha, \beta \in K: (\alpha + \beta) \hat{\cdot} \bar{v} = (\alpha \hat{\cdot} \bar{v}) \hat{+} (\beta \hat{\cdot} \bar{v})$

[d] $\forall \alpha \in K \quad \forall \bar{v}, \bar{w} \in V: \alpha \hat{\cdot} (\bar{v} \hat{+} \bar{w}) = (\alpha \hat{\cdot} \bar{v}) \hat{+} (\alpha \hat{\cdot} \bar{w})$

$$V \subseteq \mathbb{R}^2$$

$$(a, b) \hat{+} (c, d) = (a+c, b+d)$$

$$\alpha \hat{\circ} (a, b) = (\alpha \cdot a, \alpha \cdot b).$$

$$1 \hat{\circ} (a, b) = (1a, 1b) = (a, b)$$

$$(\alpha\beta) \hat{\circ} (a, b) = ((\alpha\beta)a, (\alpha\beta)b) =$$

$$= (\alpha(\beta a), \alpha(\beta b)) =$$

$$= \alpha \hat{\circ} (\beta a, \beta b) =$$

$$= \alpha \hat{\circ} (\beta \hat{\circ} (a, b)).$$

$$(\alpha + \beta) \hat{\circ} (a, b) = ((\alpha + \beta)a, (\alpha + \beta)b) =$$

$$= (\alpha a + \beta a, \alpha b + \beta b) =$$

$$= (\alpha a, \alpha b) \hat{+} (\beta a, \beta b) =$$

$$\alpha \circ (a, b) \hat{=} \beta \circ (a, b)$$

$$\begin{aligned} \alpha \circ [(a, b) \hat{+} (c, d)] &= \alpha \circ (a+c, b+d) = \\ &= (\alpha(a+c), \alpha(b+d)) = \\ &= (\alpha a + \alpha c, \alpha b + \alpha d) = \\ &= (\alpha a, \alpha b) \hat{+} (\alpha c, \alpha d) = \\ &= \alpha \circ (a, b) \hat{+} \alpha \circ (c, d). \end{aligned}$$

□

~~Def~~

Oss:

Sia M^n l'insieme di tutte le n -uple
canoniche in M . Allora M^n è uno
spazio vettoriale su M ove le op. sono
definite come

$$(a_1 \dots a_n) \hat{+} (b_1 \dots b_n) := (a_1 + b_1 \dots a_n + b_n)$$

$$\alpha := (a_1 \dots a_n) := (\alpha a_1 \dots \alpha a_n).$$

Teorema: Sia $V(K)$ uno spazio vettoriale su K
 di dimensione finita. Allora $V \cong K^n$ come
 spazio vettoriale (V isomorfo a K^n).