$(\mathbb{K}, +, \cdot)$ campo se

1) $(\mathbb{K}, +)$ è un gruppo abeliano con el. neutro 0 ||

$1 \neq 0$

2) $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano con el. neutro 1 ||

3) Valgono le proprietà distributive

a) $\forall x,y,z \in \mathbb{K}: (x+y)z = xz + yz$

b) $\forall x,y,z \in \mathbb{K}: x(y+z) = xy + xz$

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

$(\mathbb{Z}_2, +, \cdot) = (\mathbb{F}_2, +, \cdot)$ ove $\mathbb{F}_2 = \{0, 1\}$.

XOR

+	0	1
0	0	1
1	1	0

AND

·	0	1
0	0	0
1	0	1

Sia p un primo $\Rightarrow$ $\mathbb{F}_p = \{0, \dots p-1\}$ con somma e prodotto definiti "mod p"

$\mathbb{Z}_p$

cioè facendo {la somma / il prodotto} di due elementi $a, b \in \mathbb{F}_p$

$(a+b)\,\%\,p$

$(a \cdot b)\,\%\,p$

e poi prendendo il resto della divisione per p

è un campo.

$\mathbb{Z}_3$

+	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

$\mathbb{Z}_5$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_4$

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$\mathbb{Z}_4^*$ NON È UN GRUPPO

Sia p un primo $n \geq 1 \Rightarrow$ esistono campi di ordine p^n e si indicano con il simbolo $\mathbb{F}_{p^n}$

N.B. se $n=1$ $\mathbb{F}_p = \mathbb{Z}_p$ $\mathbb{Z}_6$ non è un campo.

in generale $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$

$\mathbb{F}_4$

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

·	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

CAMPO

$\mathbb{Z}_4$

·	1	2	3	0
1	2	3	0	1
2	3	0	1	2
3	0	1	2	3
0	1	2	3	0

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

NO

Sia $\mathbb{K}$ campo $a, b \in \mathbb{K}$

$$ax + b = 0$$

- $a = 0, b = 0 \Rightarrow \forall x: 0x + 0 = 0$, $S = \mathbb{K}$
- $a = 0, b \neq 0 \Rightarrow 0 \cdot x + b = 0$ ↯ impossibile, $S = \phi$
- $a \neq 0 \Rightarrow (ax + b) = 0 \iff$

$$(ax + b) + (-b) = 0 + (-b) \iff$$

$$\iff ax + (b + (-b)) = -b \iff$$

$$\iff ax + 0 = -b \iff$$

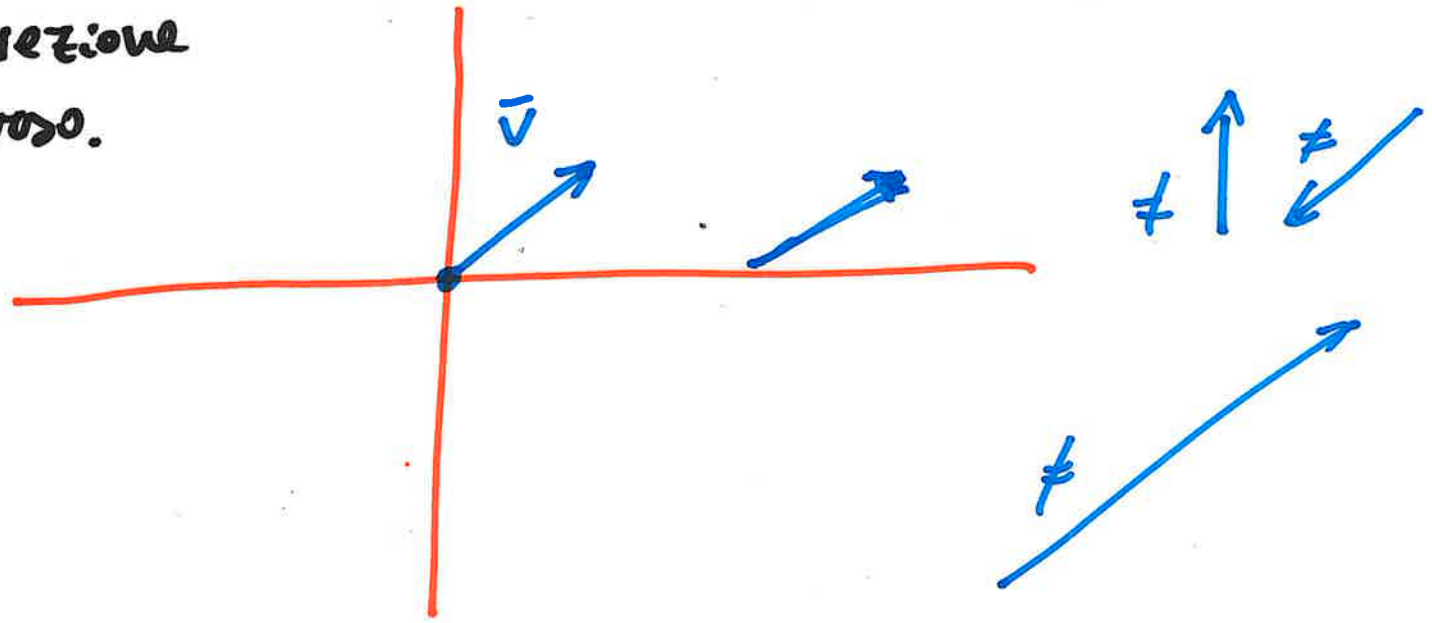
$$\iff ax = -b \iff a^{-1}(ax) = a^{-1}(-b)$$

$$\iff (a^{-1}a)x = -a^{-1}b \iff 1x = -a^{-1}b$$

$$\iff x = -a^{-1}b \Rightarrow S = \{-a^{-1}b\}$$

vettore nel piano euclideo = "freccia" → segmento orientato

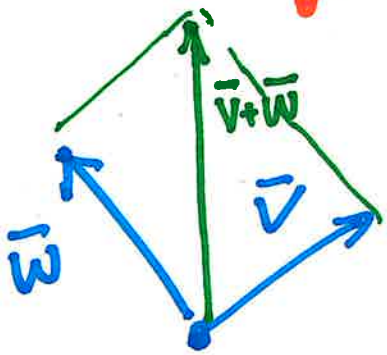
- lunghezza
- direzione
- verso.

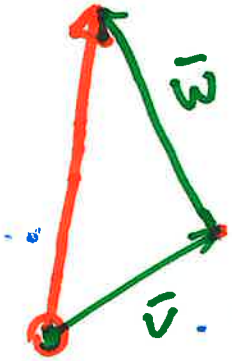


$\vec{v}$ vettore

$\alpha \in \mathbb{R}^+$ definiamo $\alpha\vec{v}$ il vettore che ha stesso verso, stessa direzione e lunghezza $\alpha\|\vec{v}\|$ con $\alpha \geq 0$

α è detto **scalare**



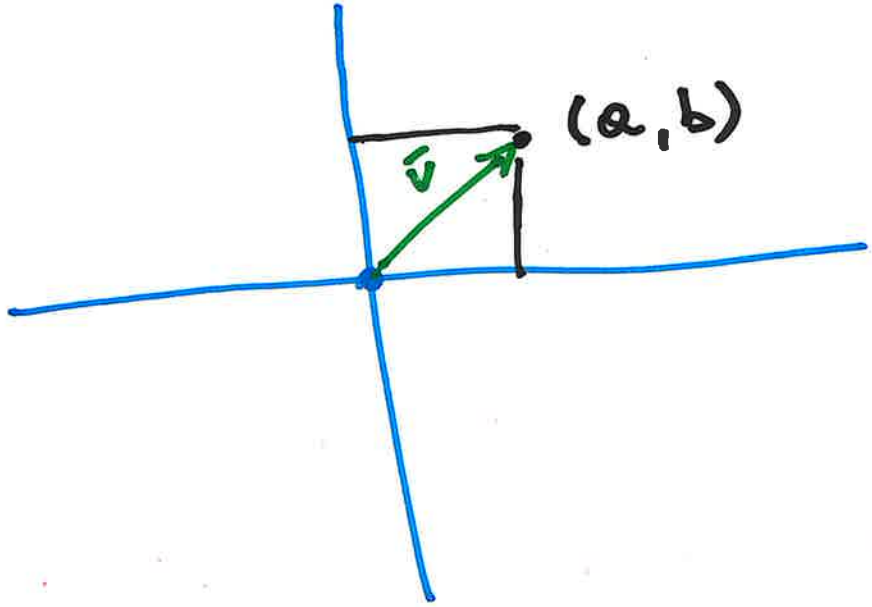


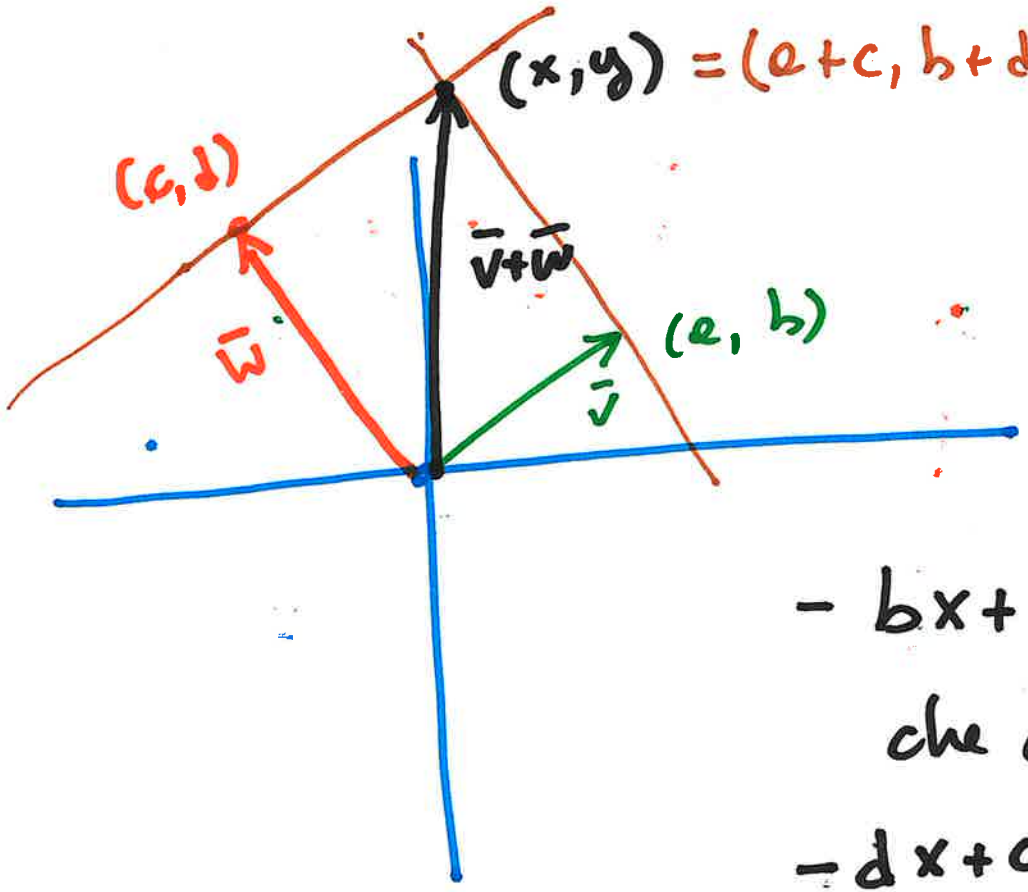
Se $\alpha < 0 \Rightarrow$

$\alpha \cdot \bar{v} = |\alpha| \cdot (-\bar{v})$

ove $-\bar{v}$ = vettore con stessa dir. e lunghezza di $\bar{v}$ e verso opposto.

$\bar{v}+\bar{w}$



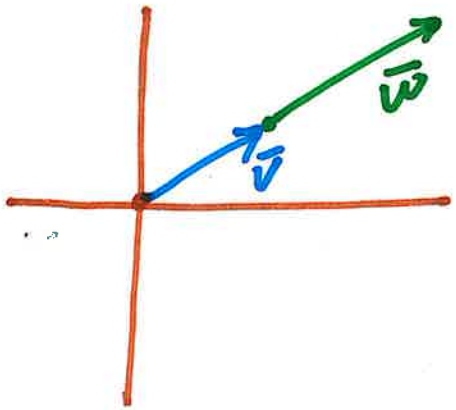


- $bx+ay=0$ è la retta che contiene $\bar{v}$

- $-dx+cy=0$ è la retta che contiene w.

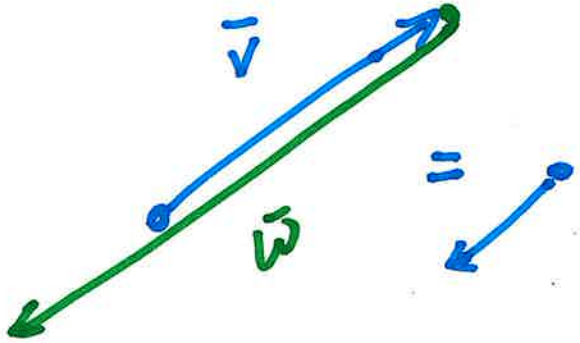
$$\begin{cases} -b(x-c)+a(y-d)=0 \\ -d(x-a)+c(y-b)=0 \end{cases}$$

$\rightarrow$ $(x,y)=(a+c, b+d)$ è soluzione.



$\bar{v}+\bar{w}$ di dir = dir $\bar{v}$
= dir $\bar{w}$

e verso, lunghezza
determinati dai
versi reciprocі.



se verso $\bar{v}$ = verso $\bar{w}$ ⇒
verso $\bar{v}+\bar{w}$ = verso di $\bar{v}$
e $\|\bar{v}+\bar{w}\| = \|\bar{v}\| + \|\bar{w}\|$

se verso $\bar{v}$ ≠ verso $\bar{w}$ ⇒
lunghezza = $|\|\bar{v}\| - \|\bar{w}\||$
verso = verso del più grande.

$$\cdot \begin{cases} \mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ \alpha \quad (x,y) \longrightarrow \alpha \cdot (x,y) = (\alpha x, \alpha y) \end{cases}$$

$$\hat{+} \begin{cases} \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ (a,b),(c,d) \longrightarrow (a,b) \hat{+} (c,d) = (a+c, b+d) \end{cases}$$

Def: Sia $\mathbb{K}$ un campo.

Una struttura algebrica $V(\mathbb{K})$ è detta spazio vettoriale su di $\mathbb{K}$ se

$$V(\mathbb{K}) = (V, \hat{+}: V\times V \to V, \cdot : \mathbb{K}\times V \to V).$$

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

2) $\cdot\ \mathbb{K}\times V \longrightarrow V$ soddisfa le seguenti proprietà:

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

pseudo distributive

b) $(\alpha+\beta)\cdot\bar{v} = \alpha\cdot\bar{v} \hat{+} \beta\cdot\bar{v} \quad \forall \alpha,\beta\in\mathbb{K}\ \forall \bar{v}\in V$

c) $\alpha(\bar{v}\hat{+}\bar{w}) = \alpha\cdot\bar{v} \hat{+} \alpha\cdot\bar{w} \quad \forall \alpha\in\mathbb{K}\ \forall \bar{v},\bar{w}\in V$

pseudo associativa.

d) $(\alpha\beta)\cdot\bar{v} = \alpha\cdot(\beta\cdot\bar{v}) \quad \forall \alpha,\beta\in\mathbb{K},\ \bar{v}\in V.$

Gli elementi di $\mathbb{K}$ sono detti scalari

di V sono detti vettori

- $\cdot$ è detto prodotto per scalare.

oss: $\mathbb{R}^2(\mathbb{R})$ definito da

$$\cdot \begin{cases} \mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ a, (x,y) \longrightarrow (ax, ay) \end{cases}$$

$$+ \begin{cases} \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ (a,b), (c,d) \longrightarrow (a+c, b+d) \end{cases}$$

è uno spazio vettoriale su $\mathbb{R}$.

Teorema: Sia $V(\mathbb{K})$ uno s. vettoriale sul campo $\mathbb{K}$.

$(V, \hat{+})$

1) Se $0 \in \mathbb{K}$ e $\bar{v} \in V \Rightarrow 0 \cdot \bar{v} = \underline{0}$ $\quad \underline{0}$ = el. neutro di $\hat{+}$ = vettor nullo.

2) Supponiamo $\alpha \cdot \bar{v} = \underline{0} \Rightarrow \bar{v} = \underline{0}$ oppure $\alpha = 0$

3) $(-1) \cdot \bar{v} = (\hat{-}\bar{v})$ ove $(\hat{-}v) \hat{+} \bar{v} = \underline{0}$ per def.

DIM: 1) $0 \cdot \bar{v} = (0+0) \cdot \bar{v} = 0 \cdot \bar{v} \hat{+} 0 \cdot \bar{v}$

sommando a dx e sx $(\hat{-} 0 \cdot \bar{v})$

$$\underline{0} = (\hat{-} 0 \cdot \bar{v}) \hat{+} 0 \cdot \bar{v} = (\hat{-} 0 \cdot \bar{v}) + 0 \cdot \bar{v} + 0 \cdot \bar{v} = \underline{0} + 0 \cdot \bar{v} = 0 \cdot \bar{v}$$

2) $\alpha \cdot \bar{v} = \underline{0}$ e $\alpha \neq 0 \Rightarrow \exists\, \alpha^{-1} \in \mathbb{K} \Rightarrow \alpha^{-1} \cdot (\alpha \cdot \bar{v}) = \alpha^{-1} \cdot \underline{0}$

da cui $(\alpha^{-1} \cdot \alpha) \cdot \bar{v} = \alpha^{-1} \cdot \underline{0} \Rightarrow \bar{v} = \alpha^{-1} \cdot \underline{0}$

$\parallel$

$1 \cdot \bar{v} = \bar{v}$

$$\alpha^{-1}\cdot \underline{0} = \alpha^{-1}\cdot(\underline{0} \hat{+} \underline{0}) = \alpha^{-1}\cdot\underline{0} \hat{+} \alpha^{-1}\cdot\underline{0}$$

$\Rightarrow$ come prima sommando a dx e sx

$$\alpha^{-1}\cdot\underline{0} = \underline{0}$$

$$\Rightarrow \bar{v} = \underline{0}$$

3) $$\bar{v} \hat{+} (-1)\cdot\bar{v} = 1\cdot\bar{v} \hat{+} (-1)\cdot\bar{v} = (1-1)\cdot\bar{v} = 0\cdot\bar{v} = \underline{0}$$

$$\Rightarrow (-1)\cdot\bar{v} = \hat{-}\bar{v}.$$ □

Def Sia V = spazio vettoriale su $\mathbb{K}$

W = sottospazio vettoriale di V

W è detto sottospazio di $V(\mathbb{K})$ se

$W \subseteq V(\mathbb{K})$

e W soddisfa gli assiomi di sp. vettoriale su $\mathbb{K}$

rispetto le operazioni di prodotto per scalare e somma di vettori

opportunamente ristrette a $\mathbb{K}\times W$ e $W\times W$ e troncate a W.

$$V(\mathbb{K}) = (V,\ +: V\times V \to V \quad \cdot: \mathbb{K}\times V \to V)$$

$$(W,\ +|^{W}_{W\times W}: W\times W \to W$$

$$\cdot|^{W}_{\mathbb{K}\times W}: \mathbb{K}\times W \to W)$$

$W \subseteq V$ $W \neq \emptyset$

W deve soddisfare le def. di s.v. nel momento in cui si restringe ovunque a "V" "W"

oss: 1) $(W, +|^{-})$ deve essere un gruppo commutativo.

OVVIAMENTE $+|^{W}_{W\times W}$ è associativa.

Deve valere che

1.a ⟶ $\forall u, w \in W : u + w \in W$

1.b ⟶ $\forall u \in W : -u \in W$

1.c (e come conseguenza $(-u) + (u) \in W \Rightarrow 0 \in W$)

1.a & 1.b $\Rightarrow$ 1.c

(!) ma 1.a & 1.b $\Leftrightarrow \forall u, w \in W : u - w \in W$

2) $\cdot|_{\mathbb{K}\times W \to W}$ si deve poter trovare a W.

(2) $\forall \alpha \in \mathbb{K}\ \forall \bar{w} \in W : \alpha \cdot \bar{w} \in W$

le prop. a), b), c), d) della def. di sp. vettoriale valgono banalmente se vale (2) perché valgono $\forall \bar{v} \in V$ e dunque anche $\forall \bar{w} \in W \subseteq V$

W è sottospazio di V $(W \leq V)$ $W \neq \emptyset$

$\Leftrightarrow$ (1) & (2) cioé

(*) $\forall \bar{u}, \bar{w} \in W : \bar{u} - \bar{w} \in W$ e $\forall \alpha \in \mathbb{K}, \forall \bar{w} \in W$: $\alpha \bar{w} \in W$

(*) è equivalente a dire

(S) $\boxed{\forall \alpha,\beta \in \mathbb{K} : \forall \bar{u},\bar{w} \in W : \alpha\bar{u}+\beta\bar{w} \in W}$

(S) $\Rightarrow$ (1) & (2)

(S) con $\alpha=\beta=0 \Rightarrow \underline{0} \in W$

con $\alpha=1$ e $\beta=-1 \Rightarrow$ ~~$\alpha\bar{u}-\beta\bar{w} \in W$~~

$\forall \bar{u},\bar{w} \in W : \bar{u}-\bar{w} \in W$ (1)

con $\alpha \in \mathbb{K}$, $\beta=0 \Rightarrow \alpha\bar{u}+0\bar{w}=\alpha\bar{u} \in W$

$\forall \bar{u} \in W$ (2)

(1) & (2) $\forall \bar{u},\bar{w} \in W \; \forall \alpha,\beta \in \mathbb{K}$, $\alpha\bar{u} - \beta\bar{w} \in W$ (2)

$\Rightarrow \alpha\bar{u}+\beta\bar{w} \in W$ (1) $\Rightarrow$ (S).

$\forall \alpha, \beta \in \mathbb{K} \cdot \forall \bar{u}, \bar{w} \in W : \alpha \bar{u} + \beta \bar{w} \in W$

W è "chiuso per combinazioni lineari di (2) vettori"

↓

prendendo 2 vettori di W e $\bar{u}, \bar{w}$

2 scalari di $\mathbb{K}$ α, β

e facendo una <u>combinazione lineare</u>

$$\alpha \bar{u} + \beta \bar{w}$$

non si può uscire da W.