Definizione di campo

$(\mathbb{K}, +, \cdot)$ → struttura algebrica che "cattura" le proprietà degli insiemi numerici con le usuali operazioni di $+$ e $\cdot$ che servono per le equazioni di I grado.

→ $(\mathbb{K}, +)$ gruppo abeliano

$(\mathbb{K} \setminus \{0\}, \cdot)$ gruppo (abeliano)

valgono le proprietà distributive

$$a(b+c) = ab + ac$$

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

oss: Sia 1 l'elemento neutro per il prodotto in $\mathbb{K}$

(1 come numero in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$;
in generale $[1]$ in $\mathbb{Z}_2$).

Indichiamo con (-1) l'opposto di 1 rispetto $+$

$$(-1) + 1 = 0$$

- ALLORA $\forall x \in \mathbb{K} \quad (-1)\cdot x = -x$

DIM: $x + (-1)\cdot x = 1\cdot x + (-1)\cdot x =$

$$= (1 + (-1))\cdot x = 0\cdot x$$

Ma $0\cdot x = (0+0)\cdot x = 0\cdot x + 0\cdot x$

"sommando a dx e Sx) ho $\cdots - (0\cdot x)$ si ottiene

$$0 = -(0\cdot x) + 0\cdot x = \underbrace{-(0\cdot x) + (0\cdot x)}_{0} + (0\cdot x) =$$

$$= 0 + 0\cdot x = 0\cdot x.$$

In particolare $x + (-1)\cdot x = 0\cdot x = 0$

DA cui sommando a dx e sx $-x$ si ottiene

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

□

N.B: Moltiplicare per 0 in un campo dà sempre 0. !!!

oss: Sia data l'equazione $xy = 0$ in un campo $\mathbb{K}$.

Allora le soluzioni sono tutte del tipo

$$x = 0 \quad \text{oppure} \quad y = 0$$

o, scritto in altro modo

$$S = \{(x,0) \mid x \in \mathbb{K}\} \cup \{(0,y) \mid y \in \mathbb{K}\}.$$

Legge di annullamento del prodotto.

Se $x=0$ oppure $y=0 \Rightarrow xy=0$ appena visto.

Supponiamo $xy=0$ con $x \neq 0 \Rightarrow$

$\exists x^{-1} \in \mathbb{K} \Rightarrow$ $x^{-1}(xy) = x^{-1} \cdot 0 = 0$

$(x^{-1}x)y = 1 \cdot y = y$

Esempi $(\mathbb{R}, \mathbb{Q}$

$(\mathbb{Z}_2, +, \cdot)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$(\mathbb{Z}_3, +, \cdot)$

+	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

è un campo con 3 elementi

partiamo dall'insieme $\mathbb{Z}$ dei numeri interi

consideriamo $n \in \mathbb{N}$ $n > 1$ e definiamo

$\mathbb{Z}_n$ come insieme $\{0, 1, \dots, n-1\}$.

con le operazioni $+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(a, b) \longrightarrow (a+b) \,\%\, n$

resto della divisione per n
di $(a+b)$.

- $\mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$
  $(a, b) \longrightarrow (a \cdot b) \,\%\, n$

resto ottenuto dividendo per n

In $\mathbb{Z}_{31}$

$17 + 26 = 43 \,\%\, 31 = 12$

$6 \cdot 11 = 66 \,\%\, 31 = 4$

Si può dimostrare che
1) $(\mathbb{Z}_n, +)$ gruppo abel.
2) valgono le prop. distr. della somma rispetto il prod.

3) $\exists\, 1 \in \mathbb{Z}_n$ el. neutro per il prodotto

4) Il prodotto è associativo.

Teorema $(\mathbb{Z}_n, +, \cdot)$ è un campo $\Leftrightarrow$ n è un numero primo.

$(\mathbb{Z}_2, +, \cdot)$, $(\mathbb{Z}_3, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$ campi.

$(\mathbb{Z}_4, +, \cdot)$ non è un campo!

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

Consideriamo l'insieme di tutte le coppie ordinate (a, b) di elementi di $\mathbb{R}$.

$z = (a, b) \to a + ib$.

per convenzione scriviamo a per la coppia $(a, 0) \to a + i \cdot 0$.

Somma: $(a + ib) + (c + id) := (a + c) + i(b + d)$

prodotto: $(a + ib) \cdot (c + id) := (ac - bd) + i(bc + ad)$

In particolare $i^2 = (0 + i \cdot 1) = -1$

Teorema: $(\mathbb{C}, +, \cdot)$ è un campo.

DIM: 1) $(\mathbb{C}, +)$ gruppo abeliano.

→ vale perché $(\mathbb{C}, +)$ corrisponde ad

$(\mathbb{R} \times \mathbb{R}, +)$

A) $(a+ib) + (0+i\cdot 0) = (a+0) + i(b+0) = a+ib$

B) $(a+ib) + (-a + i(-b)) = (a-a) + i(b-b) = 0 + i\cdot 0$

$\vdots$

0

C) ASSOCIATIVA

2) Valgono le prop. distributive.

$$(a+ib)[(c+id)+(e+if)] = (a+ib)[(c+e)+i(d+f)]$$

$$= [a(c+e) - b(d+f)] + i[a(d+f) + b(c+e)] =$$

$$= [(ac+ae) - (bd+bf)] + i[(ad+af) + (bc+be)]$$

$\vdots$

$$(a+ib)(c+id)+(a+ib)(e+if)=$$

$$=(ac-bd)+i(bc+ad)+(ae-bf)+$$

$$+i(af+be)$$

valgono le distributive.

Con il prodotto:

1) $(1+i0)(a+ib)=a+ib.$

2) $(a+ib)(x+iy)=1+i\cdot 0$

$$\begin{cases}(ax-by)=1\\(ay+bx)=0\end{cases}$$

se $a=b=0 \Rightarrow$ l'inverso non esiste!

$a \neq 0$ e $b = 0$.

$$\begin{cases} ax = 1 \\ ay = 0 \end{cases}$$

$x = a^{-1}$ $\quad a \in \mathbb{R}$

$y = 0$

~~$a \neq 0, b \neq 0$~~

$a = 0, \ b \neq 0$

$$\begin{cases} -by = 1 \\ bx = 0 \end{cases} \rightarrow \begin{array}{l} y = -1 \\ x = 0 \end{array}$$

$i^{-1} = -i$

$-i^2 = 1$

$i \cdot (-i) = -i^2 = 1$

$a \neq 0, \ b \neq 0$ $\quad \begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases}$

$$y = -\frac{bx}{a} = -a^{-1}bx$$

$$ax + b(a^{-1}bx) = 1$$

$$(a + b^2a^{-1})x = 1 \qquad \frac{a^2+b^2}{a}x = 1$$

$$x =$$

$$\begin{cases} x = \dfrac{a}{a^2+b^2} \\ y = \dfrac{-b}{a^2+b^2} \end{cases} \qquad a^2+b^2 > 0$$

ABBIAMO VISTO CHE L'INVERSO MOLTIPLICATIVO
ESISTE SEMPRE TRANNE CHE PER $0 = 0 + i0$

$$(a+ib)\cdot[a-ib]\cdot\frac{1}{a^2+b^2} =$$

$$= \frac{(a^2+b^2)}{a^2+b^2} = 1 \qquad \text{ok.}$$

3) con un po' di conti si dimostra anche la prop. associativa.

$\rightarrow$ $(\mathbb{C}, +, \cdot)$ <u>campo</u>

Th $(\mathbb{C}, +, \cdot)$ è un campo <u>algebricamente chiuso</u>

Sia $f(x)$ un polinomio in x di grado ≥ 1

Teorema (fondamentale dell'algebra)

ogni equazione del tipo $f(x) = 0$
con $f(x)$ polinomio a coeff. in $\mathbb{C}$
di grado ≥ 1 ammette almeno una
soluzione (e conseguentemente ne ammette
sempre $n = \deg f(x)$ contate con molteplicità)

→ $\mathbb{C}$ è algebricamente chiuso

$(\mathbb{R}, +, \cdot)$ $\quad \sqrt{-1} =? \sqrt{-1} \notin \mathbb{R}$

$\forall a \in \mathbb{R}, \ a^2 \geq 0$

$$ax^2+bx+c=0 \qquad a\neq 0$$

$$\Delta = b^2-4ac$$

$$ax^2+bx+c=(\alpha x+\beta)^2 \qquad \Delta \geq 0$$

$\Delta > 0$ due soluzioni reali e distinte

$\Delta = 0$ due soluzioni reali e coincidenti

$\Delta < 0$ due soluzioni immaginarie (e coniugate).

oss 1: Il teorema fond. dell'algebra dice che il polinomio $f(x) \in \mathbb{C}[x]$ (polinomio in x a coeff. in $\mathbb{C}$) con $\deg f(x) = n \geq 1$ ha sempre almeno una radice α.

$$\exists \alpha \in \mathbb{C} : f(\alpha) = 0$$

per i polinomi a coeff. su di un campo $\mathbb{K}$ vale il teorema di Ruffini:

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \quad \text{e} \quad f(\alpha) = 0$$

$$\Rightarrow f(x) = (x - \alpha)(b_0 + b_1 x + \dots + b_{n-1} x^{n-1}).$$

CONSEGUENZA DELLA LEGGE DI ANNULLAMENTO DEL PRODOTTO.

$\deg f(x) = n$; $f(\alpha) = 0$

se $n = 1 \Rightarrow$ $f(x) = a(x-\alpha)$ $\quad$ fine. $\alpha \neq 0$

se $n > 1 \Rightarrow$ $f(x) = a(x-\alpha)\, g(x)$

con $\deg g(x) = n-1$

$(x-\alpha)^n$

$\deg f(x) = 5 \quad f(\alpha_1) = 0 \Rightarrow$

$\Rightarrow f(x) = (x-\alpha_1)\, g_1(x)$

$\deg g_1(x) = 4 \qquad g_1(\alpha_2) = 0$

$\Rightarrow f(x) = (x-\alpha_2)(x-\alpha_1)\, g_2(x)$

con $\deg g_2(x) = 3$

$$f(x) = a(x-a_1)(x-a_2)\dots(x-a_5)$$

Si dice che $f(x)$ si spezza in fattori di primo grado.

→ si può sempre fare su $\mathbb{C}$.

Su $\mathbb{R}$ un polinomio si può fattorizzare in termini di grado 1 e 2.

(x^2+1) in $\mathbb{R}[x]$

$(x+i)(x-i)$ in $\mathbb{C}[x]$

Sia $z = a + ib \in \mathbb{C}$

Definiamo "z coniugato" $\overline{z} := a - ib$

proprietà:

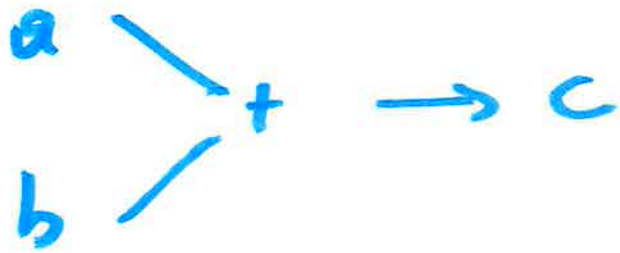
1) $\overline{a+b} = \overline{a} + \overline{b} \quad \forall a, b \in \mathbb{C}$

2) $\overline{ab} = \overline{a} \cdot \overline{b} \quad \forall a, b \in \mathbb{C}$

Il coniugio è un automorfismo di $\mathbb{C}$

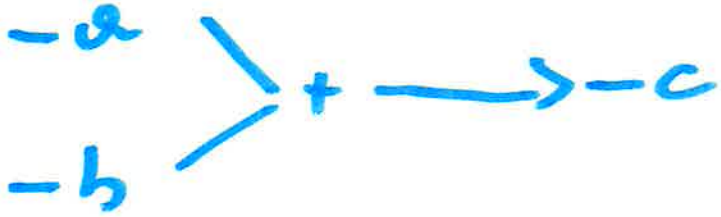
→ è una operazione $\mathbb{C} \to \mathbb{C}$ che

"è compatibile/rispetta le operazioni algebriche di campo".



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

$= -c$



$a(-1)+b(-1) = -c$

$$\overline{(a+ib)(c+id)} = \overline{(ac-bd)+i(ad+bc)} =$$

$$= (ac-bd)-i(ad+bc) =$$

$$= (ac-bd)+i(-ad-bc).$$

$$\overline{(a+ib)}\ \overline{(c+id)} = (a-ib)(c-id) = (ac-bd)+i(-bc-ad)$$

✓

Def Sia $z = a + ib$.

1) $\bar{z} = z \iff b = 0$ cioè $z = a + i0 = a$

in tale caso si identifica z col numero reale a.

2) $\bar{z} + z = 0$ cioè $\bar{z} = -z \iff a = 0$. In tale caso $z = ib$ è detto numero immaginario puro.

3) $\frac{1}{2}(z + \bar{z}) = \frac{[(a+ib)+(a-ib)]}{2} = a =: Re(z) \in \mathbb{R}$

parte reale di z.

4) $\frac{1}{2i}(z - \bar{z}) = \frac{(a+ib)-(a-ib)}{2i} = \frac{2ib}{2i} = b =: Im(z)$

parte immaginaria di z.

5) $z \cdot \bar{z} = (a+ib)(a-ib) = a^2+b^2 \geq 0 \quad \in \mathbb{R}$

poniamo $|z| := \sqrt{z\bar{z}} \in \mathbb{R}$.

N.B: Se z reale $\Rightarrow |z| = |a| = \sqrt{a^2}$

~~$\sqrt{a^2} = a$~~ NO!! $\quad \sqrt{a^2} = |a|$

$\sqrt{(-1)^2} = 1$ in $\mathbb{R}$

$\sqrt{-1}$ in $\mathbb{C}$?

$(i)^2 = -1$

$(-i)^2 = -1$

In $\mathbb{R}$ $\sqrt{\ } : \mathbb{R}^+ \to \mathbb{R}^+$

$(\mathbb{R}^+ := \{x \in \mathbb{R} \mid x \geq 0\}$.

In $\mathbb{C}$ vorremmo

$\sqrt{\ } : \mathbb{C} \to \mathbb{C}$

6) $z = a + ib. \quad z \neq 0 \quad \Rightarrow \quad z^{-1} = \dfrac{\overline{z}}{z \cdot \overline{z}}$

$$\overline{z} = \frac{a - ib}{a^2 + b^2} = \underbrace{\frac{a}{a^2+b^2}}_{\in \mathbb{R}} - i \underbrace{\frac{b}{a^2+b^2}}_{\in \mathbb{R}}$$

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z}\, z}$$

7) Sia $f(x) \in \mathbb{C}[x] \quad \Rightarrow \quad \overline{f(x)} \in \mathbb{C}[\overline{x}]$

$a_0 + a_1 x + a_2 x^2 + \dots \qquad \overline{a}_0 + \overline{a}_1 \overline{x} + \overline{a}_2 \overline{x^2} + \dots$

$\overline{f}(x) \Rightarrow \quad \overline{a}_0 + \overline{a}_1 x + \overline{a}_2 \overline{x}^2 + \dots$

Sia α tale che $f(\alpha) = 0$

$$\Rightarrow \overline{f(\alpha)} = \bar{0} = 0$$

Se α è radice di $f(x) \Rightarrow \bar{\alpha}$ è radice di $\bar{f}(x)$

$$\overline{f(\alpha)} = \bar{f}(\bar{\alpha}).$$

↑ per le proprietà di automorfismo.

Supponiamo $f(x) \in \mathbb{R}[x]$ a coeff. in $\mathbb{R}$.

Allora se $f(x) = \bar{f}(x)$.

Da questo discende che se α è radice (complessa) di $f(x)$ polinomio a coeff. reali $\Rightarrow$

$\bar{\alpha}$ è anche essa radice.

$f(\alpha)=0 \iff f(\bar{\alpha})=0$ con $f(x)\in\mathbb{R}[x]$

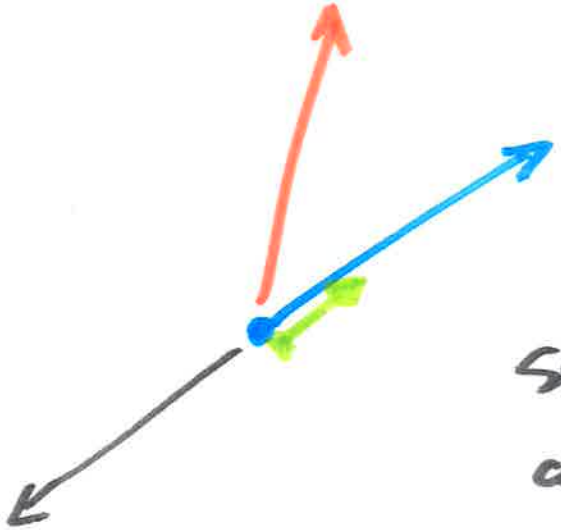
ci sono 2 possibilità. in $\mathbb{R}$

1) $\alpha=\bar{\alpha} \Rightarrow \alpha\in\mathbb{R} \Rightarrow (x-\alpha)\in\mathbb{R}[x]$
divide $f(x)$.

2) $\alpha\neq\bar{\alpha} \Rightarrow (x-\alpha)$ e $(x-\bar{\alpha})$ dividono entrambi
$\alpha\in\mathbb{R}$ $f(x)$ e sono polinomi complessi.

$\Rightarrow (x-\alpha)(x-\bar{\alpha})$ divide $f(x)$

e $(x-\alpha)(x-\bar{\alpha}) = (x^2 - \underbrace{(\alpha+\bar{\alpha})}_{\in\mathbb{R}}x + \underbrace{\alpha\bar{\alpha}}_{\in\mathbb{R}}) \in\mathbb{R}[x]$

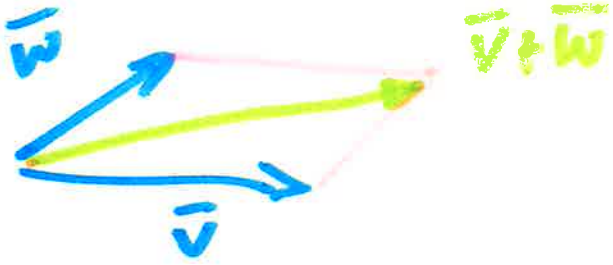


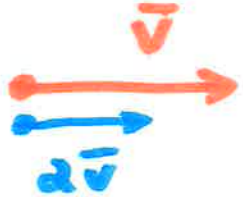
vettore.

segmento orientato

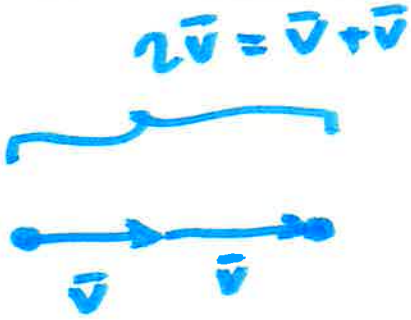
con
- direzione
- verso
- lunghezza.

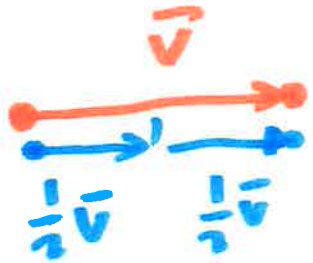
operazioni "fondamentali" sui vettori:



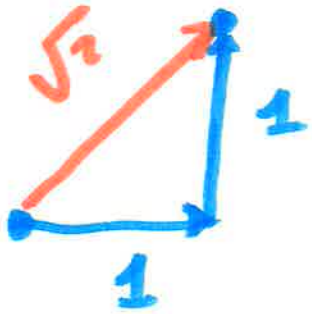


$2 \in \mathbb{R}$





π



Operazione : moltiplicare uno scalare $\in \mathbb{K}$ per un vettore → OTTENERE UN VETTORE

poter cambiare il verso di un vettore

Ci serve una struttura algebrica

$\xi V_n(\mathbb{K})$

spazio vettoriale su di un campo $\mathbb{K}$.

→ gli elementi di $V(\mathbb{K})$ sono vettori.

1) è definita una somma fra vettori che dà una struttura di gruppo abeliano.

2) è definita una operazione di prodotto per scalare

- $\mathbb{K} \times V \to V$

tale che.

$(2+3)\bar{v} = 2\bar{v} + 3\bar{v} = 5\bar{v}$

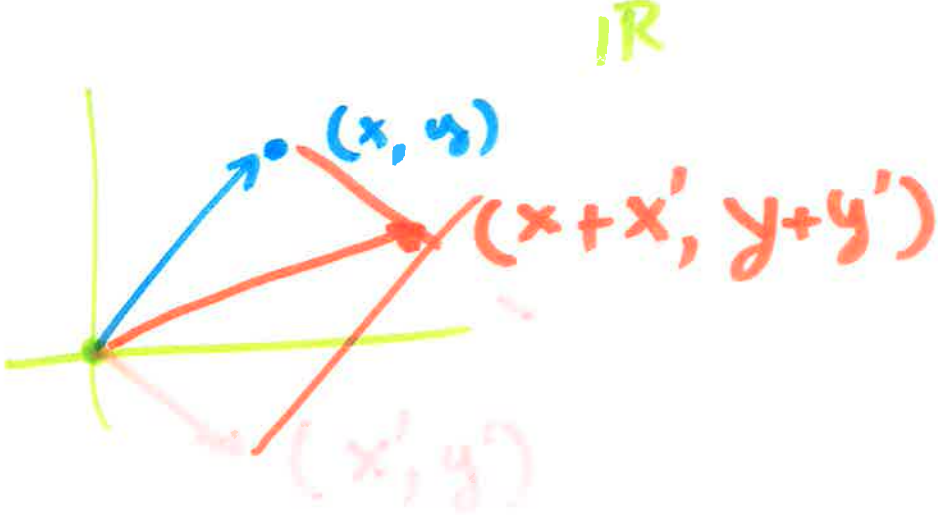
1) $1 \cdot \bar{v} = \bar{v} \quad \forall \bar{v} \in V$
2) $(\alpha+\beta)\cdot\bar{v} = \alpha\bar{v} + \beta\bar{v} \in V \quad \forall \bar{v} \in V, \alpha, \beta \in \mathbb{K}$
3) $(\alpha\cdot\beta)\cdot\bar{v} = \alpha\cdot(\beta\bar{v}) \quad \forall \bar{v} \in V, \alpha, \beta \in \mathbb{K}$

$(2\cdot 3)\,\bar{v} = 6\,\bar{v} = 2\cdot(3\bar{v})$

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

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

STRUTTURA ALGEBRICA



$\alpha \cdot (x,y) \to (\alpha x, \alpha y)$