Algebra lineare 2/10/23

$\mathbb{N} = \{0, 1, 2, \dots\}$ Numeri naturali

addizione $+$; proprietà:

1. $n + 0 = 0 + n = n \quad \forall n$ 0 el. neutro

3. $n + (m + k) = (n + m) + k \quad \forall n, m, k$ associativa

4. $n + m = m + n$ commutativa

Oss: dato $n \in \mathbb{N}$ l'equazione $n + x = 0$

ha soluzione solo per $n = 0$ (e in tal caso è $x = 0$).

Aggiungiamo soluzioni:

$\mathbb{Z} = \{ \ldots -3, -2, -1, 0, 1, 2, \ldots \}$ Numeri interi

addizione $+$; proprietà:

1. $n + 0 = 0 + n = n \quad \forall n$
2. $\forall n \in \mathbb{Z} \ \exists (-n) \in \mathbb{Z}$ t.c. $n + (-n) = 0$

3. $n+(m+k)=(n+m)+k \quad \forall n,m,k$

4. $n+m=m+n$

moltiplicazione $\cdot$; proprietà

5. $1\cdot k=k\cdot 1=k \quad \forall k$

7. $k\cdot(n\cdot m)=(k\cdot n)\cdot m$

8. $k\cdot n=n\cdot k$

9. $k\cdot(n+m)=k\cdot n+k\cdot m \quad \left(=(k\cdot n)+(k\cdot m)\right)$

Oss: dato $n \in \mathbb{Z}$ l'equazione $n \cdot x = 1$ ha soluzione in $\mathbb{Z}$ ha soluzione solo per $n = \pm 1$ (e in tal caso è $x = n$).

Aggiungiamo soluzioni:

$$\mathbb{Q} = \underbrace{\text{``}\left\{\frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0\right\}\text{''}}$$

Numeri razionali

può $\frac{-3}{6} = \frac{8}{-16}$

cioè $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ se $p_1 \cdot q_2 = p_2 \cdot q_1$.

Su $\mathbb{Q}$ ci sono $+, \cdot$

1. $q+0 = 0+q = q$
2. $\forall q \in \mathbb{Q}\ \exists -q \in \mathbb{Q}$ t.c. $q+(-q)=0$
3. $q+(s+t) = (q+s)+t$
4. $q+s = s+q$

$\Bigg\}$ $\mathbb{Q}$ con $+$ è un gruppo commutativo

5. $q \cdot 1 = 1 \cdot q = q$

6. $\forall q \in \mathbb{Q}, q \neq 0 \quad \exists q^{-1} \in \mathbb{Q}$ t.c. $q \cdot q^{-1} = 1$

$$\left(\left(\frac{m}{n}\right)^{-1} = \frac{n}{m} \right)$$

7. $q \cdot (s \cdot t) = (q \cdot s) \cdot t$

8. $q \cdot s = s \cdot q$

9. $q \cdot (s + t) = q \cdot s + q \cdot t$ distributiva.

implicano che $\mathbb{Q} \setminus \{0\}$ con $\cdot$ è gruppo commutativo

Def: Un insieme con due operazioni binarie $+, \cdot$ che soddisfano le proprietà 1-9 si dice campo

(Vedremo altri campi, in particolare finiti)

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

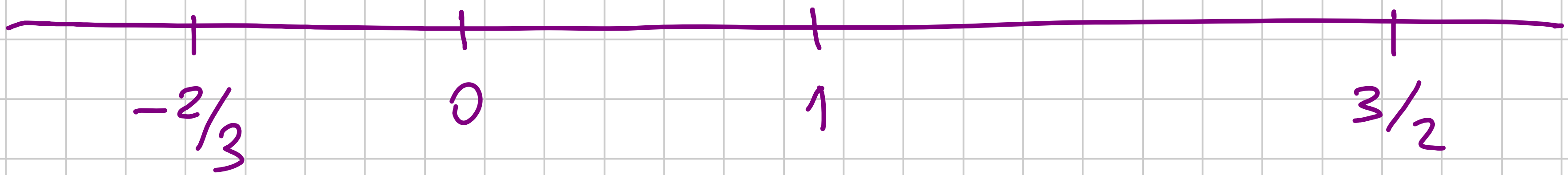
aggiunto soluz. di $n+x=0$

aggiunto soluzioni di $n \cdot x = 1$ (con $n \neq 0$)

Estensioni motivate dell'algebra

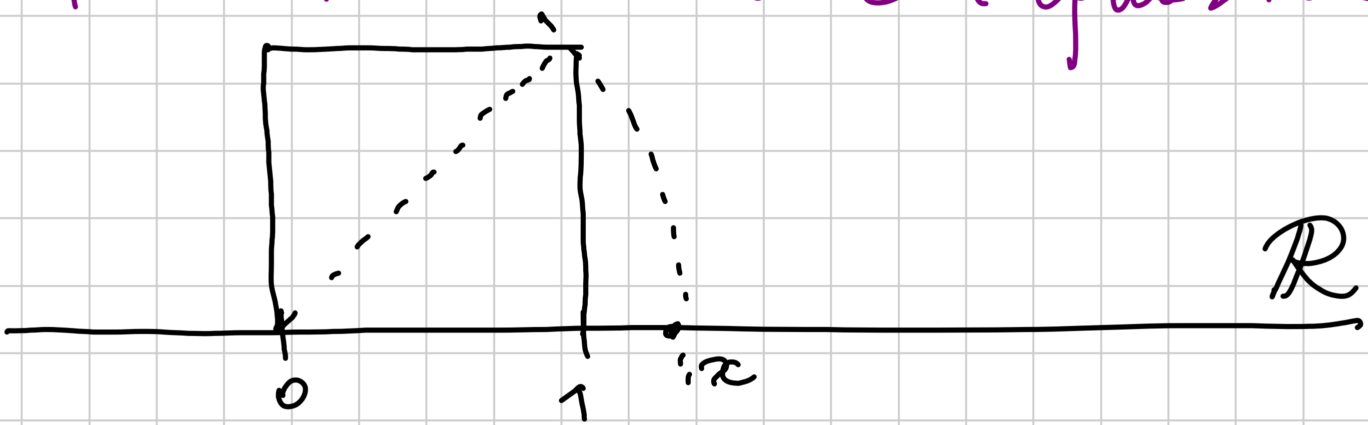
Oss: ci sono equazioni in $\mathbb{Q}$ prive di soluzione (es. $x^2=2$).

Oss: Fissati su una retta due punti distinti 0 e 1 si può identificare $\mathbb{Q}$ a un sottoinsieme di tale retta:



$\mathbb{R}$ = i punti di tale retta

<u>Oss</u>: $\mathbb{R}$ contiene soluzioni dell'equazione $x^2 = 2$



Però ci sono "moltissimi" punti di $\mathbb{R}$ che non sono soluzioni di equazioni polinomiali a coeff. in $\mathbb{Q}$ (ad es. π, e). Anzi: se si sceglie $x \in \mathbb{R}$ a caso, la probabilità che sia soluz. di equaz. polinomiale a coeff in $\mathbb{Q}$ è <u>nulla</u>.

<u>Fatto</u>: le operazioni $+, \cdot$ si estendono da $\mathbb{Q}$ a $\mathbb{R}$ e godono delle proprietà 1-9 ($\Rightarrow$ $\mathbb{R}$ è un campo).

(Vedremo altro campo $\mathbb{C}$ = numeri complessi.)

— o —

Polinomi

$\mathbb{R}[x]$ = l'insieme dei polinomi nella indeterminata x a coefficienti in $\mathbb{R}$ (dove $x \notin \mathbb{R}$ è un simbolo)

$$= \text{“}\left\{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n : n \in \mathbb{N},\ a_0, \dots, a_n \in \mathbb{R}\right\}\text{”}$$

l'insieme di... al variare di... / dove... / con...

Però: •) $\frac{7}{4} - 5\pi x^4$ non è una scrittura come sopra

•) $e - \frac{5}{4}x \neq e - \frac{5}{4}x + 0 \cdot x^2$ come scritture

Soluzione: dalle scritture $a_0 + a_1 x + \dots + a_n x^n$ si possono mettere e togliere monomi con coefficiente 0 senza effetti.

Su $\mathbb{R}[x]$ ci sono le operazioni $+, \cdot$ ottenute

$+$) Raccogliendo i coeff. dei monomi dello stesso grado

$\cdot$) Applicando la distributiva e poi usando $+$.

<u>Def</u>: grado di $(a \cdot x^k) = k$

grado di $p(x) \in \mathbb{R}[x]$:

$(\deg(1 - 7 + \sqrt{3}x^2 + 0 \cdot x^3) = 2)$

$$\deg(p(x)) = \begin{cases} \text{max grado di monomio con coeff} \neq 0 & \text{se } p(x) \neq 0 \\ -\infty / -1 / \text{non esiste} & \text{se } p(x) = 0 \end{cases}$$

Somma: $(1 - 3x + 4x^2) + (-2 + 5x + x^2 - 7x^3)$

$$= -1 + 2x + 5x^2 - 7x^3$$

$$(a_0 + a_1 \cdot x + a_2 x^2 + \dots + a_n x^n) + (b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m)$$

(per scriverlo bisogna distinguere se $n \leq m$ o $n \geq m$)

Prodotto: $(2+x+3x^2)(-1+5x) =$

$$\begin{aligned} = & -2+10x \\ & \quad -x \quad +5x^2 \\ & \qquad\quad -3x^2+15x^3 \end{aligned}$$

$$= -2+9x+2x^2+15x^3$$

$(a_0+a_1x+\dots+a_nx^n)(b_0+b_1x+\dots+b_mx^m) = \dots$

formule esplicite: complicata

Convenzione: scriviamo

$$a_0 + a_1 x + \cdots + a_n x^n = \sum_{k=0}^{\infty} a_k \cdot x^k$$

Sommatoria

dove $a_k = 0$ per $k > n$

dunque

$$\mathbb{R}[x] = \left\{ \sum_{k=0}^{\infty} a_k \cdot x^k : \ a_h \in \mathbb{R} \ \forall h, \text{ tutti nulli tranne un numero finito} \right\}$$

Oraz:

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty} (a_k + b_k) \cdot x^k$$

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{h=0}^{\infty} b_h x^h\right) = \sum_{j=0}^{\infty} \left(\sum_{i=0}^{j} a_i \cdot b_{j-i}\right) x^j$$

——— o ———

<u>Dimostrazioni</u>

DIRETTA

Prop: $\displaystyle\sum_{j=0}^{n} j = \frac{n(n+1)}{2}.$ $\left(\text{ES: } 0+1+\cdots+13 = \frac{13\cdot 14}{2} = 91\right)$

Dim:
$$2\sum_{j=0}^{n} j = 0+1+2+\cdots+(n-1)+n+$$
$$+\;n+(n-1)+(n-2)+\cdots+1+0$$
$$=\underbrace{n+n+n+\cdots+n+n}_{n+1}$$
$$=n(n+1).$$

$\boxtimes$

Prop: se $n \in \mathbb{N}$ è divisibile per 2 e per 3 allora è divisibile per 6.

Dim: n divisibile per 3 significa che $n = 3 \cdot k$ con $k \in \mathbb{N}$. Siccome n è pari, 3 è dispari e il prodotto di due dispari è dispari, k è pari $\Rightarrow k = 2h$ con $h \in \mathbb{N}$ $\Rightarrow n = 6h$ con $h \in \mathbb{N}$ cioè n è divisibile per 6. $\boxtimes$

Richiamo: $f : X \to Y$ funzione è

dominio

codominio

una legge che a ogni $x \in X$ associa un certo $f(x) \in Y$.

f si dice iniettiva se elementi distinti di X vengono mandati da f in elementi distinti di Y

f si dice suriettiva se ogni elemento di Y è immagine tramite f di qualche elemento di X

f si dice bijettiva se è iniettiva e surjettiva

Prop: $f : \mathbb{Z} \to \mathbb{N}$ data da $f(n) = n^2$
(cioè $f : n \longmapsto n^2$) non è né iniettiva né surjettiva.

Dimo: non iniettiva: $f(-2) = f(2)$ ma $-2 \neq 2$
non surjettiva: $3 \notin \mathrm{Im}(f)$. $\boxtimes$

PER ASSURDO : Si suppone che la tesi sia falsa; facendo implicazioni logiche se ne deduce che è falsa l'ipotesi o qualche fatto noto come vero.

Prop: l'equazione $n^2 = 1 + m^2$ non ha soluz. $n, m \in \mathbb{Z}$ con $m \neq 0$

Dim: supponiamo per assurdo che ci sia una soluzione $n, m \in \mathbb{Z}$ con $m \neq 0$. Allora

$$1 = n^2 - m^2 = (n+m)(n-m)$$ con $n+m, n-m \in \mathbb{Z}$

$$\begin{cases} n+m = 1 \\ n-m = 1 \end{cases} \Longrightarrow m = 0$$

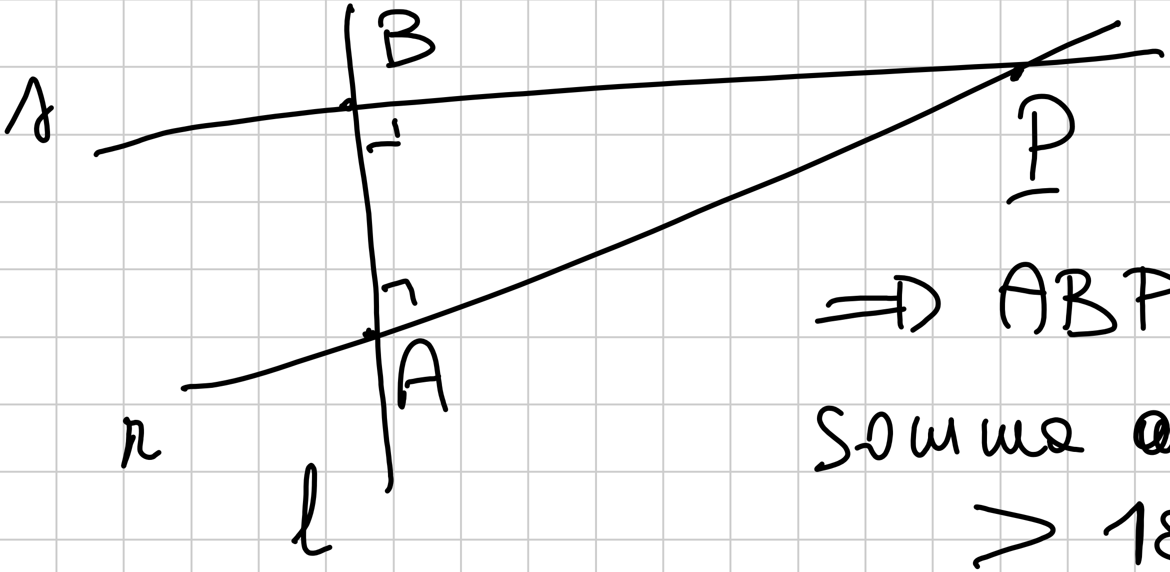
$\Longrightarrow$ o

$$\begin{cases} n+m = -1 \\ n-m = -1 \end{cases} \Longrightarrow m = 0$$

assurdo: avevo supposto $m \neq 0$. $\blacksquare$

Prop: Se r, s, l sono rette nel piano euclideo, $r \neq s$, $r \perp l$, $s \perp l \Longrightarrow r \parallel s$

Dimo: Per assurdo supponiamo che si intersechino in P:



$\Rightarrow$ ABP triangolo con somma angoli interni $> 180°$. Assurdo

Prop: l'equazione $x^2=2$ non ha soluzioni $x \in \mathbb{Q}$.

Dim: per assurdo sia $x \in \mathbb{Q}$ una soluzione.

So che posso scrivere $x = \frac{p}{q}$ con $p, q \in \mathbb{Z}$ primi fra loro (privi di divisori comuni > 1).

Ora $\left(\frac{p}{q}\right)^2 = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2$ è pari $\Rightarrow p$ pari $\Rightarrow \exists k \in \mathbb{Z}$ t.c. $p = 2k$

$\Rightarrow (2k)^2 = 2q^2 \Rightarrow 4k^2 = 2q^2 \Rightarrow q^2 = 2k^2$

$\Rightarrow q^2$ è pari $\Rightarrow q$ è pari : Assurdo. $\blacksquare$

PER INDUZIONE

Si applica a un predicato relativo a $n \in \mathbb{N}$
cioè "una frase in cui compare n e che
ha senso per $n \in \mathbb{N}$"

PRINCIPIO DI INDUZIONE : Se :

PASSO BASE : $\mathcal{P}(0)$ è vera

PASSO INDUTTIVO : Supponendo $\mathcal{P}(n)$ vera (con $n \geq 0$ generico)
si riesce a dimostrare che $\mathcal{P}(n+1)$ è vera

ipotesi induttive

allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

tesi induttiva

Perché? $P(0)$ è vera : passo base

$P(1)$ applico passo induttivo con $n = 0$

+ passo base $\Longrightarrow$ vera

$P(2)$ applico passo base con $n = 1$

+ scoperta precedente $\Longrightarrow$ vera

...

Prop: $\sum_{j=0}^{n} j = \frac{n(n+1)}{2}$.

Dimo per induzione. $P(n) =$ " $\sum_{j=0}^{n} j = \frac{n(n+1)}{2}$. "

Passo base: devo vedere che $P(0)$ è vera:

$$P(0) = \text{“} \sum_{j=0}^{0} j = 0 \text{”} \qquad \underline{\text{Vera}}.$$

Passo induttivo:

Suppongo $\mathcal{P}(n)$ vera per un generico n, cioè

$$\sum_{j=0}^{n} j = \frac{n(n+1)}{2}.$$

Devo verificare che allora è vera $\mathcal{P}(n+1)$, cioè

$$\sum_{j=0}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

Infatti:

$$\sum_{j=0}^{n+1} j = \sum_{j=0}^{n} j + (n+1) \underset{\text{grazie a ipotesi induttiva}}{=} \frac{n(n+1)}{2} + n+1$$

$$= n \cdot \frac{n+1}{2} + 2 \cdot \frac{n+1}{2}$$

$$= \frac{n+1}{2} \cdot (n+2) . \qquad \boxed{/\!/}$$

<u>Prop</u>: $\displaystyle\sum_{j=0}^{n} 2^j = 2^{n+1} - 1 .$

<u>Dim.</u> per induzione.

Passo base $(n=0)$:

$$\sum_{j=0}^{0} 2^j = 2^1 - 1$$

$$\begin{array}{ccc} \sum_{j=0}^{0} 2^j & & 2^1 - 1 \\ \| & & \| \\ 1 & & 1 \end{array}$$

Vera.

Passo induttivo:

Suppongo $\sum_{j=0}^{n} 2^j = 2^{n+1} - 1$; devo vedere che

allora
$$\sum_{j=0}^{n+1} 2^j = 2^{n+2} - 1.$$

Infatti:

$$\sum_{j=0}^{n+1} 2^j = \sum_{j=0}^{n} 2^j + 2^{n+1} \underset{\text{ip. indutt.}}{=} 2^{n+1} - 1 + 2^{n+1}$$

$$= 2 \cdot 2^{n+1} - 1$$

$$= 2^{n+2} - 1. \qquad \boxtimes$$

Oss: se voglio dimostrare che $P(n)$ è vero $\forall n \geq \overline{n}$ basta

- vedere che $P(\overline{n})$ è vero
- supponendo $P(n)$ vero per $n \geq \overline{n}$ generico provare che $P(n+1)$ è vero

Prop: $4n < 2^n \quad \forall n \geq 5$

Dim: P.B. $\quad 4 \cdot 5 < 2^5$ $\quad$ Vera

$$\underset{20}{\overset{\shortparallel}{4\cdot 5}} < \underset{32}{\overset{\shortparallel}{2^5}}$$

P.I. Suppongo $n \geq 5$ e $4n < 2^n$; devo vedere che $4(n+1) < 2^{n+1}$; infatti:

$$4(n+1) = 4n + 4 \underset{\text{ip. ind.}}{<} 2^n + 4 \underset{\text{poiché } n \geq 5 \geq 2}{<} 2^n + 2^n = 2^{n+1}. \quad \boxed{}$$

Formulazione alternative del principio di induzione:

P.I.

Se $P(0)$ è vera e
$P(n)$ vera $\Rightarrow P(n+1)$ vera
allora $P(n)$ vera $\forall n$

P.I.-bis

Dato $A \subset \mathbb{N}$, se
$0 \in A$ e
$m \in A \Rightarrow m+1 \in A$
allora $A = \mathbb{N}$

(principî assiomatici)

Fatto: P.I. $\Longleftrightarrow$ P.I.bis

Dim: $\underline{\Rightarrow}$ Preso $A \subset \mathbb{N}$ come nelle ipotesi di P.I.-bis poniamo $\mathcal{P}(n) =$ "$n \in A$". Allora:

$\mathcal{P}(0)$ vera perché $0 \in A$

$\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ perché $n \in A \Rightarrow n+1 \in A$.

Grazie a P.I $\mathcal{P}(n)$ è vera $\forall n$ cioè

$n \in A \ \forall n \in \mathbb{N}$ cioè $A = \mathbb{N}$

$\underline{\Leftarrow}$: Sia $\mathcal{P}(n)$ come nelle ipotesi di P.I.

Poniamo $A = \{ n \in \mathbb{N} : \mathcal{P}(n) \text{ è vera} \}$; allora

$A \ni 0$ poiché $\mathcal{P}(0)$ è vera

$n \in A \Rightarrow n+1 \in A$ poiché $\mathcal{P}(n)$ vera $\Rightarrow \mathcal{P}(n+1)$ vera

Grazie a P.I.-bis ho $A = \mathbb{N}$ cioè

$\mathcal{P}(n)$ è vera $\forall n \in \mathbb{N}$.

$\boxtimes$

<u>Esercizio</u>: Provare per induz che $8^n - 3^n$ è divisibile per 5 $\forall n \in \mathbb{N}$.

<u>Def</u>: Si dice spazio vettoriale su $\mathbb{R}$ un insieme V dotato di due operazioni:

$$V \times V \longrightarrow V \qquad \text{somma (binaria interna)}$$
$$(v_1, v_2) \longmapsto v_1 + v_2$$

$$\mathbb{R} \times V \longrightarrow V \qquad \text{prodotto per scalare}$$
$$(\lambda, v) \longmapsto \lambda \cdot v$$

tali che:

1. $\exists 0 \in V$ t.c. $v+0=0+v=v \quad \forall v \in V$

2. $\forall v \in V \ \exists (-v)$ t.c. $(-v)+v = v+(-v) = 0$

3. $v_1+(v_2+v_3) = (v_1+v_2)+v_3 \quad \forall v_1, v_2, v_3 \in V$

4. $v_1+v_2 = v_2+v_1 \quad \forall v_1, v_2 \in V$

$\left.\right\}$ V con + è gruppo commutativo

5. $\lambda_1 \cdot (\lambda_2 \cdot v) = (\lambda_1 \cdot \lambda_2) \cdot v \quad \forall \ldots$

6. $\lambda \cdot (v_1+v_2) = \lambda \cdot v_1 + \lambda \cdot v_2 \quad (= (\lambda \cdot v_1) + (\lambda v_2)) \quad \forall \ldots$

7. $(\lambda_1 + \lambda_2) \cdot v = \lambda_1 \cdot v + \lambda_2 \cdot v \quad \forall \ldots$

8. $0 \cdot v = 0, \quad 1 \cdot v = v \quad \forall v \in V$

— = vecchio

Esempio: $\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_1, \dots, x_n \in \mathbb{R} \right\}$

Verificare che con:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n \cdot y_n \end{pmatrix} \quad e \quad \lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}$$

risulta uno spazio vettoriale.

$(\underbrace{\text{Spazio vettoriale}}_{\text{Esempio di}}$: bisogna indicare V e definire le operaz $+ : V \times V \to V$, $\cdot : \mathbb{R} \times V \to V$ e verificare 1-8.)