Alg. Lin. 1/10/14

Insiemi numerici

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

$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$(n, m) \longmapsto n + m$

Proprietà:

1. $\exists\, 0 \in \mathbb{N}$ t.c. $0+n=n$ $\forall n \in \mathbb{N}$

3. $n+(m+k)=(n+m)+k$ $\forall n,m,k \in \mathbb{N}$

4. $n+m=m+n$ $\forall n,m \in \mathbb{N}$.

Q: Per quali $n \in \mathbb{N}$ l'equazione
$n+x=0$ ha soluzione $x \in \mathbb{N}$?
(Se esiste la soluzione si chiama opposto di n.)

A: Solo per $n=0$ e in tal caso la sol è $x=0$.

Rimedio: si inventa l'opposto:

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

interi relativi

$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$(n, m) \longmapsto n+m$

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

3. ... 4. ...

Inoltre ho:

$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

$(n, m) \mapsto n \cdot m$

Proprietà:

5. $\exists 1 \in \mathbb{Z}$ t.c. $n \cdot 1 = n \quad \forall n \in \mathbb{Z}$
7. $n \cdot (m \cdot k) = (n \cdot m) \cdot k \quad \forall n, m, k \in \mathbb{Z}$
8. $n \cdot m = m \cdot n \quad \forall n, m \in \mathbb{Z}$
9. $n \cdot (m + k) = n \cdot m + n \cdot k \quad \forall n, m, k \in \mathbb{Z}$

Q: Per quali $n \in \mathbb{Z}$ l'equazione $n \cdot x = 1$ ha soluzione $x \in \mathbb{Z}$?

(Se c'è la soluz. è l'inverso moltiplicativo di n.)

A: Per $n = \pm 1$, la soluz. è n.

Rimedio: Si inventano gli inversi:

$\mathbb{Q} = \text{“}\left\{ \frac{n}{m} : n, m \in \mathbb{Z},\ m \neq 0 \right\}\text{”}$ numeri razionali

Però: $\frac{14}{-10}$ vogliamo che sia uguale a $\frac{-21}{15}$;

dunque bisogna convenire quando due frazioni rappresentano lo stesso numero razionale:

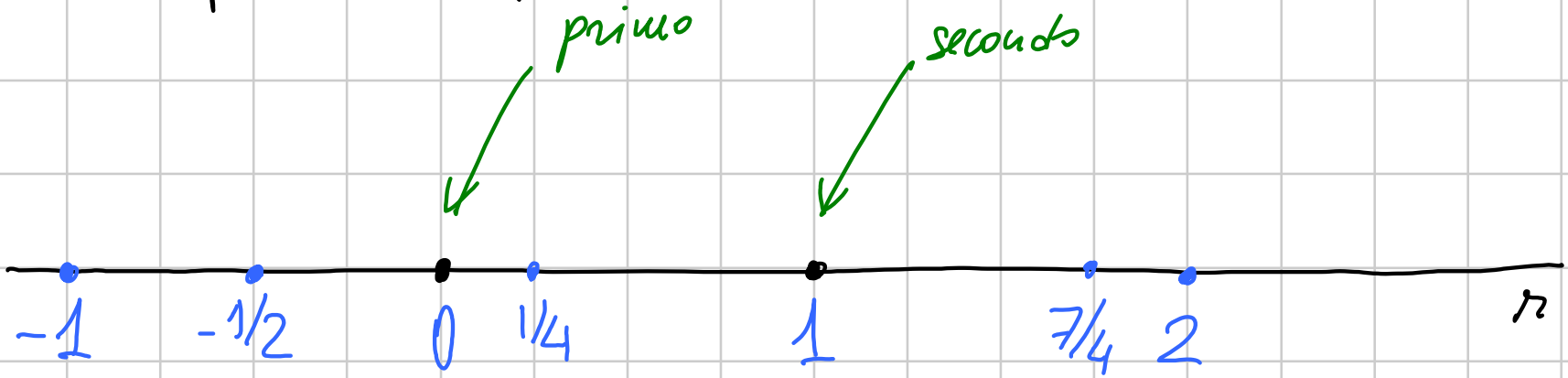
convveniamo che $\frac{n}{m} = \frac{k}{h}$ se $n \cdot h = m \cdot k$.

Ora vale anche: 6. $\forall q \in \mathbb{Q}, q \neq 0 \; \exists q^{-1} \in \mathbb{Q}$ t.c $q \cdot (q^{-1}) = 1$.

(se $q = \frac{n}{m}$ si ha $q^{-1} = \frac{m}{n}$).

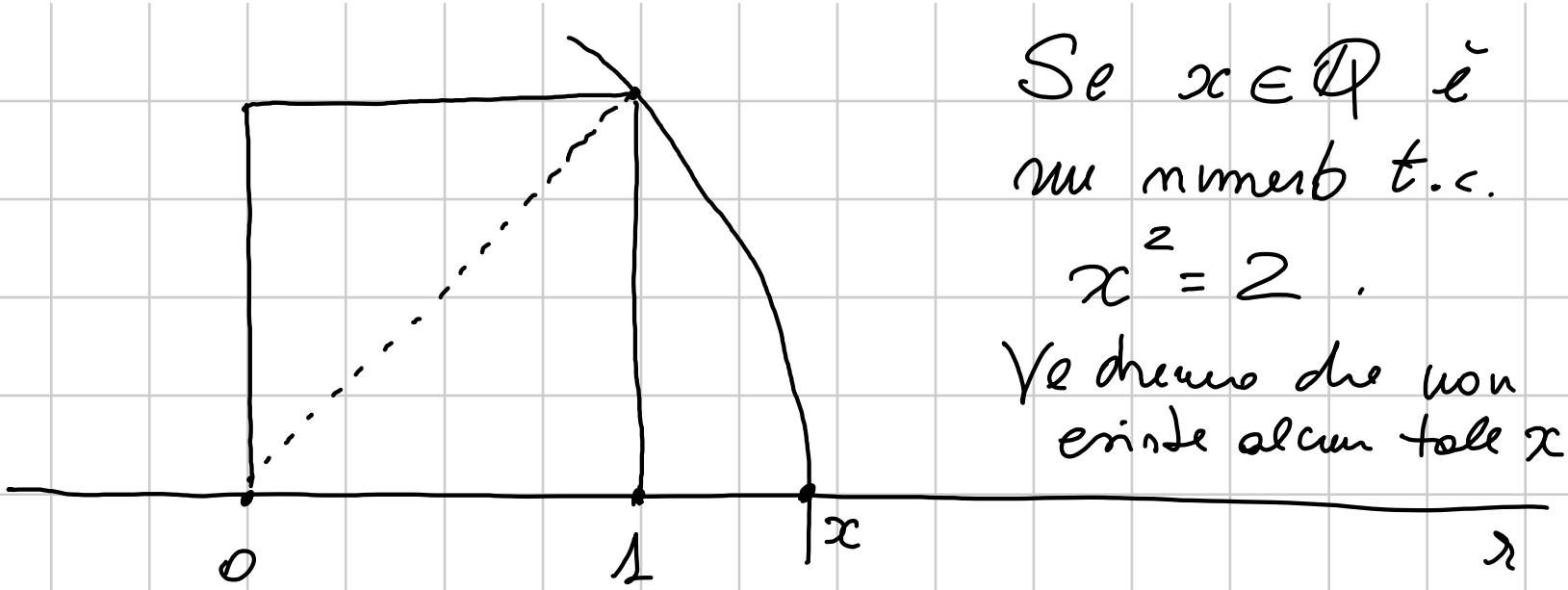
Oss: presa una retta r e su di essa due

punti distinti e ordinati, si può far corrispondere $\mathbb{Q}$ a un sottoinsieme di $\mathbb{R}$:



Dunque posso considerare $\mathbb{Q}$ come sottoinsieme di $\mathbb{R}$.

Fatto: $\mathbb{R}$ contiene punti che non sono in $\mathbb{Q}$:



Se $x \in \mathbb{Q}$ è un numero t.c. $x^2 = 2$.
Vedremo che non esiste alcun tale x.

Def: chiamo $\mathbb{R}$ (numeri reali) l'insieme x _

Fatto 1: $\mathbb{R}$ contiene altri punti oltre a quelli che sono soluzioni di equazioni polinomiali a coefficienti in $\mathbb{Z}$.

(Anzi: scelto un numero reale a caso c'è probabilità nulla che esso sia soluzione di un'equazione polinomiale a coeff. in $\mathbb{Z}$.)

Esempi noti: π, e.

Fatto 2: le operazioni di $\mathbb{Q}$ si estendono a $\mathbb{R}$ con le stesse proprietà:

$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(x, y) \mapsto x + y$

$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(x, y) \mapsto x \cdot y$

1. $x + 0 = x$
2. $\forall x \ \exists (-x)$ t.c. $x + (-x) = 0$
3. $x + (y + z) = (x + y) + z$
4. $x + y = y + x$
5. $x \cdot 1 = x$
6. $\forall x \neq 0 \ \exists x^{-1}$ t.c. $x \cdot (x^{-1}) = 1$
7. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$\mathbb{R}$ con opraz. $+$ e el. neutro 0 è un gruppo comm.

$\Rightarrow \mathbb{R} \setminus \{0\}$ con opraz $\cdot$ e el neutro 1 è un gruppo comm.

8. $x \cdot y = y \cdot x$

9. $x \cdot (y+z) = x \cdot y + x \cdot z$. ← distributiva

Def: chiamiamo **campo** un insieme dotato di due operazioni binarie $+, \cdot$ che soddisfano 1-9.

Es: $\mathbb{Q}, \mathbb{R}$ sono campi. (Vedremo: $\mathbb{C}$).

Def: chiamo **gruppo commutativo** un insieme A con una operazione $*$ con le proprietà

1. $\exists\, e \in A$ t.c. $e * a = a * e = a \quad \forall a \in A$
2. $\exists\, a \in A \ \exists\, \bar{a} \in A$ t.c. $a * \bar{a} = \bar{a} * a = e$

3. $(a * b) * c = a * (b * c)$

4. $a * b = b * a$ (senza questa: gruppo)

Polinomi a coeff. in $\mathbb{R}$ nella indeterminata x:

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

l'insieme di/dei/delle

le scritture formali di questo tipo

al variare di

(insieme definito per elencazione)

Però: $7 + \pi \cdot x + \sqrt{3} \cdot x^3$ Non è una scrittura formale come sopra

$1 + \sqrt{7} \cdot x - 9x^2 \neq 1 + \sqrt{7} \cdot x - 9 \cdot x^2 + 0 \cdot x^3$ Sono scritture diverse

Rimedio: convenzione che si possono aggiungere e togliere monomi con coeff. 0

Def: Se $p(x) \neq 0$ (polinomio nullo)

$p(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$

chiamo grado di $p(x)$

$$\deg(p(x)) = \max\{d : a_d \neq 0\}$$

(tale che)

Sui polinomi sono definite le operazioni $+, \cdot$ binarie. Definizioni:

$+$: si sommano i coeff dei monomi dello stesso grado

• : $(a \cdot x^n) \cdot (b \cdot x^m) = (a \cdot b) \cdot x^{n+m}$
e poi si applica la distributiva

Formule:

+ : $(a_0 + a_1 x + \dots + a_n x^n) + (b_0 + b_1 x + \dots + b_m x^m)$
$= (a_0 + b_0) + (a_1 + b_1) x + \dots$

per scriverlo dovrei distinguere $n \leq m$ $n \geq m$

Invece: conviene di scrivere

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

stabilendo che $a_k = 0 \quad \forall k > n$

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

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

Es. di prodotto: $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$

$$\left(-3+4x+\frac{13}{2}x^2-7x^3\right)\cdot\left(5-2x+9x^2-11x^3+\frac{7}{4}x^4\right)$$

$$=(\dots)+(\dots)x+(\dots)x^2+(\dots)x^3+(\dots)x^4+(\dots)x^5+(\dots)x^6+(\dots)x^7$$

$$-3\cdot\frac{7}{4}+4\cdot(-11)+\frac{13}{2}\cdot 9+(-7)(-2)+0\cdot 5$$

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

$$= \sum_{k=0}^{+\infty} \left(\sum_{n=0}^{k+1} a_n \cdot b_{k-n} \right) x^k$$

Tecniche di dimostrazione

- Argomento diretto:

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

(Σ_5: $1+2+\cdots+17 = \frac{17 \cdot 18}{2} = 153$)

Dim: Chiamo S_n la somma $\sum_{k=0}^{n} k$.

$$S_n = 0 + 1 + 2 + 3 + \cdots (n-2) + (n-1) + n$$
$$S_n = n + (n-1) + (n-2) + (n-3) + \cdots \quad 2 \quad + 1 \quad + 0$$

$$2 \cdot S_n = \underbrace{n + n + n + n \cdots n + n + n}_{n+1}$$

$$\Rightarrow 2 \cdot S_n = n(n+1) \longrightarrow S_n = \frac{n(n+1)}{2}. \qquad \blacksquare$$

Dimostrazioni per induzione_

Per dimostrare che una proposizione $P(n)$ relativa a un intero n è vera per ogni $n \in \mathbb{N}$ basta:

(Passo base): Dimostrare che $P(0)$ è vera

(Passo induttivo): Supponendo $P(n)$ vera per un generico $n \in \mathbb{N}$ (ipotesi induttiva) dimostrare che $P(n+1)$ è vera_ Cioè: provare che "$P(n) \Rightarrow P(n+1)$ $\forall n$"_

Perché basta:

* $P(0)$ è vera applicando il passo base
* Se applico il passo induttivo con $n=0$ trovo che $P(1)$ è vera
* Se applico il passo induttivo con $n=1$ trovo che $P(2)$ è vera

....

Prop: $\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}$.

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

Passo base: $P(0)$: $\sum_{k=0}^{0} k = \frac{0\cdot(0+1)}{2}$ Vera.

Passo induttivo: supposo $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ per qualche generico n. $P(n)$

Devo provare che $\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$. $P(n+1)$

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

per ipotesi induttiva

$$= (n+1)\left(\frac{n}{2}+1\right) = \frac{(n+1)(n+2)}{2}. \qquad \blacksquare$$

Varianti dell'induzione:

Per dimostrare che vale una prop. $P(n)$ $\forall n \geq N$ basta provare $P(N)$ e che $P(n) \Rightarrow P(n+1)$ $\forall n \geq N$.

Prop: $n! \geq 2^n$ $\forall n \geq 4$

Dim: $P(n) =$ "$n! \geq 2^n$"

Passo base $P(4) =$ "$4 \cdot 3 \cdot 2 \cdot 1 \geq 2 \cdot 2 \cdot 2 \cdot 2$" Vera

Passo induttivo: suppongo vera $n! \geq 2^n$ per $n \geq 4$

devo provare che $(n+1)! \geq 2^{n+1}$.

Infatti:

$$(n+1)! = n! \cdot (n+1)$$

$$\geq \quad \geq$$

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

∎

Variante: induzione completa.

Per dimostrare che $P(n)$ vale $\forall n \in \mathbb{N}$ basta:

* Dimostrare $P(0)$
* Supponendo vera $P(k)$ $\forall k \leq n$, con n generico dimostrare $P(n+1)$.

Def: un intero $n \in \mathbb{N}$, $n > 0$ è primo se in qualsiasi espressione $n = k \cdot h$, $k, h \in \mathbb{N}$ si ha $k = 1$ oppure $h = 1$.

Teo: ogni numero intero è prodotto di primi.

Dim: $P(n)$ = "n è prodotto di primi".

$P(1)$: $1 = 1$ ok

$P(2)$: $2 = 2$ ok

Suppongo $\underbrace{P(k) \text{ vera } \forall k \leq n}$ e dimostro $P(n+1)$

"tutti gli interi fino a n sono prodotto di primi"

$n+1$ → è primo

→ non lo è: $n+1 = k \cdot h$, $k, h > 1$

$\Rightarrow k, h \leq n$

Per ipotesi k, h sono prodotto di primi

$\Rightarrow$ anche $n+1$ _ ▨

Dimostrazioni per assurdo:

* Per dimostrare una proposizione P si suppone

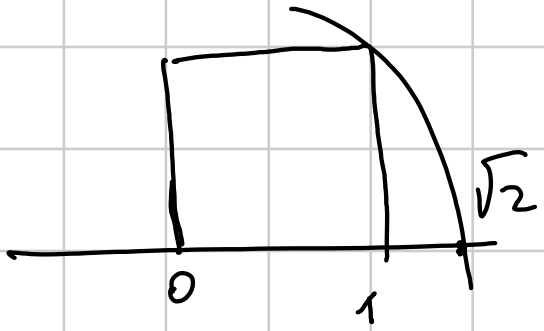
che esse sia falsa e se ne deduce la falsità di un fatto noto come vero.

* Per dimostrare una implicazione $Q \Rightarrow P$ si suppone falsa P e se ne deduce la falsità di Q.

(Prima versione = seconda con Q = "tutto quel che so".)

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

("$\sqrt{2} \notin \mathbb{Q}$")



Dim: Per assurdo supponiamo che ci sia una soluzione $x \in \mathbb{Q}$.

Scrivo $x = \frac{k}{h}$ con k, h primi fra loro.

Ho $\left(\frac{k}{h}\right)^2 = 2 \Rightarrow k^2 = 2h^2 \Rightarrow k^2$ è pari

$\Rightarrow k$ è pari $\Rightarrow k = 2l$, $l \in \mathbb{N}$

$\Rightarrow (2l)^2 = 2h^2 \Rightarrow 4l^2 = 2h^2$

$\Rightarrow h^2 = 2l^2 \Rightarrow h^2$ è pari

$\Rightarrow$ h è pari.

Assurdo.

Prop: Esistono infiniti numeri primi.

Dimo: Supponiamo per assurdo che ci siano soltanto $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11 \dots p_n$

Considero il numero $k = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$.
So che k è prodotto di numeri primi
$\Rightarrow$ è divisibile per qualcuno dei p_j.
Invece la divisione $k : p_j$ ha resto 1
e non 0. Assurdo. □

Def: Si chiama spazio vettoriale su $\mathbb{R}$ un insieme V dotato di due operazioni:

$+ : V \times V \longrightarrow V$

$(v_1, v_2) \mapsto v_1 + v_2$

somma tra "vettori" (= elem. di V)

$\cdot : \mathbb{R} \times V \longrightarrow V$

$(\lambda, v) \mapsto \lambda \cdot v$

prodotto tra uno scalare e un vettore

con le proprietà:

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. $v + (-v) = 0$
3. $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ $\quad \forall v_1, v_2, v_3 \in V$
4. $v_1 + v_2 = v_2 + v_1$ $\quad \forall v_1, v_2 \in V$

V con $+$ e 0 è gruppo comm

5. $\lambda \cdot (v_1 + v_2) = \lambda \cdot v_1 + \lambda \cdot v_2 \qquad \forall \lambda \in \mathbb{R} \ \forall v_1, v_2 \in V$

6. $(\lambda_1 + \lambda_2) \cdot v = \lambda_1 \cdot v + \lambda_2 \cdot v \qquad \forall \lambda_1, \lambda_2 \in \mathbb{R}, \ \forall v \in V$

7. $(\lambda_1 \cdot \lambda_2) \cdot v = \lambda_1 \cdot (\lambda_2 \cdot v)$ " "

8. $1 \cdot v = v \qquad \forall v \in V$ (vecchie opaoz).

Esempi: $\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} : x_1, x_2, \dots, x_n \in \mathbb{R} \right\}$ con

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

vecchio +

operaz. di spazio vett che sto definendo

$$\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}, \qquad 0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

nuova — nuovo

Verifica: 4. $x + y = y + x \quad \forall x, y \in \mathbb{R}^n$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}; \quad x + y = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

uguali per la

$$y + x = \begin{pmatrix} y_1 + x_1 \\ \vdots \\ y_m + x_m \end{pmatrix}$$ Kommutativ in $\mathbb{R}$

6. $(\lambda + \mu) \cdot x \overset{?}{\neq} \lambda \cdot x + \mu \cdot x$

$$(\lambda+\mu)\cdot\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} (\lambda+\mu)x_1 \\ \vdots \\ (\lambda+\mu)x_m \end{pmatrix}$$

$$\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} + \mu \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

$$\begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda \cdot x_m \end{pmatrix} + \begin{pmatrix} \mu \cdot x_1 \\ \vdots \\ \mu \cdot x_m \end{pmatrix} = \begin{pmatrix} \lambda x_1 + \mu \cdot x_1 \\ \vdots \\ \lambda x_m + \mu \cdot x_m \end{pmatrix}$$

Vale la proprietà distributiva in $\mathbb{R}$

Matrici per $n \times m$ (n righe, m colonne) a coeff reali:

$$\mathcal{M}_{n\times m}(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} : \quad a_{ij} \in \mathbb{R} \right\}$$

Es: $M_{2\times 3}(\mathbb{R}) \ni \begin{pmatrix} \sqrt{17} & \pi & -11 \\ 43 & \sqrt{2} & -e \end{pmatrix}$

Operazioni:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix}$$

$$A+B = \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1m}+b_{1m} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nm}+b_{nm} \end{pmatrix}$$

$$\lambda \cdot \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} = \begin{pmatrix} \lambda \cdot a_{11} & \cdots & \lambda \cdot a_{1m} \\ \vdots & & \vdots \\ \lambda \cdot a_{n1} & \cdots & \lambda \cdot a_{nm} \end{pmatrix}$$

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}_{m \times n}$$

Devo dimostrare le proprietà 1-8.

Convenzione: se $A \in M_{m \times n}(\mathbb{R})$ indico con

$(A)_{ij}$ il coeff. di A sulla riga i-esima e colonna j-esima.

Es:
$$A = \begin{pmatrix} 7 & 4 & -3 & \pi \\ \sqrt{2} & 5 & 8 & 61 \\ -7 & 18 & e & 0 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathbb{R})$$

$(A)_{23} = 8$ $\quad (A)_{31} = -7$ $\quad (A)_{14} = \pi$

Riscrivo le def:

- $A, B \in \mathcal{M}_{m\times m}(\mathbb{R})$ definisco $A+B \in \mathcal{M}_{m\times m}(\mathbb{R})$ come $(A+B)_{ij} = (A)_{ij} + (B)_{ij}$

nuovo

vecchio + in $\mathbb{R}$

- $\lambda \in \mathbb{R}$, $A \in \mathcal{M}_{m \times m}(\mathbb{R})$ definisco $\lambda \cdot A \in \mathcal{M}_{m \times m}(\mathbb{R})$ come $(\lambda \cdot A)_{ij} = \lambda \cdot (A)_{ij}$ –

Verifico le proprietà:

7. $\lambda \cdot (\mu \cdot A) \neq (\lambda \cdot \mu) \cdot A$

Sono entrambe matrici $n \times m$ dunque basta vedere che hanno lo stesso coeff. di posto (i,j) per ogni $i = 1, \dots, n$ e $j = 1, \dots, m$

Infatti:

$$(\lambda \cdot (\mu \cdot A))_{ij} = \lambda \cdot (\mu \cdot A)_{ij} = \lambda \cdot (\mu \cdot (A)_{ij})$$

esegno prodotto esegno prodotto

$$((\lambda \cdot \mu) \cdot A)_{ij} = (\lambda \cdot \mu) \cdot (A)_{ij}$$

sono uguali per l'associativa del $\cdot$ su $\mathbb{R}$.

Oss: $\mathbb{R}^n = \mathcal{M}_{n\times 1}(\mathbb{R})$.