

Lezione 3-10-18

Divisione Euclidea:

Dati $a, b \in \mathbb{Z}$ $\exists!$ $r, q \in \mathbb{Z}$ tali che
 $\begin{matrix} \neq \\ 0 \end{matrix}$ $\begin{matrix} \in \\ \mathbb{N} \end{matrix}$

$$a = b \cdot q + r, \text{ con } r \underset{\neq}{0} \leq r < |b|$$

$\swarrow$ dividendo $\swarrow$ divisore $\searrow$ resto

$\nearrow$ quoziente

Oss: a è divisibile per $b \Leftrightarrow$ il resto $r=0$

Teri: n è divisibile per 6 $\Leftrightarrow$ è divisibile per 2 e 3.

n non è div. per 6 $\Rightarrow$ n non è divisibile per 2
oppure per 3.

$\hookrightarrow$ Il resto della divisione euclidea di n per 6
è $\neq$ da 0

$\nearrow$ div. euclidea di n per 2.

resto = 1 $n = 6 \cdot q + 1 = \left. \begin{array}{l} 2 \cdot (3q) + 1 \\ 3 \cdot (2q) + 1 \end{array} \right\} \begin{array}{l} n \text{ non è divisibile} \\ n \text{ è per 2 ne' per 3} \end{array}$

Spazi vettoriali

Def: Uno spazio vettoriale reale è un insieme V dotato di due operazioni:

$$+ : V \times V \longrightarrow V$$

$$(v, w) \longrightarrow v + w$$

↳ somma

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

$$(1, v) \longrightarrow 1 \cdot v$$

↳ prodotto scalare

che soddisfanno le seguenti proprietà:

—

1. $\exists 0 \in V$ tale che $0 + v = v \quad \forall v \in V.$

2. $\forall v \in V \exists (-v) \text{ t.c. } v + (-v) = 0$
 $\quad \quad \quad \uparrow$
 $\quad \quad \quad V$

3. $v + (w + z) = (v + w) + z \quad \forall v, w, z \in V$

4. $v + w = w + v \quad \forall v, w \in V$

$(V, +, 0)$
è un gruppo
commutativo

$$5. (\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v) \quad \forall \lambda, \mu \in \mathbb{R}, \forall v \in V$$

↓
prodotto
su $\mathbb{R}$

↓ ↓ ↙
prodotto scalare su V

$$6. (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \quad \forall \lambda, \mu \in \mathbb{R}, \forall v \in V$$

$$7. \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w \quad \forall \lambda \in \mathbb{R}, \forall v, w \in V$$

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

Gli elementi di uno sp. vett. si dicono vettori.

Osservazione: Per definire uno spazio vettoriale V occorre:

1) Dire chi è V come insieme

2) Dire chi siano $+$, $\cdot$

3) Dire chi è $0 \in V$

Esempi:

• $\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_1, \dots, x_n \in \mathbb{R} \right\}$ - definiamo l'insieme

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

↳ somma su $\mathbb{R}^n$.
(la stiamo definendo)

↳ somma su $\mathbb{R}$

• Prodotto scalare

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

• Vettore nullo $\underset{\uparrow}{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

Verifichiamo la proprietà 7: $\underset{\uparrow}{\lambda} \cdot \underset{\uparrow}{(x+y)} = \underset{\uparrow}{\lambda} \cdot \underset{\uparrow}{x} + \underset{\uparrow}{\lambda} \cdot \underset{\uparrow}{y}$
 $\mathbb{R} \quad \mathbb{R}^n \quad \mathbb{R}^n$

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

$$\lambda \cdot (x+y) = \lambda \cdot \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot (x_1+y_1) \\ \vdots \\ \lambda \cdot (x_n+y_n) \end{pmatrix}$$

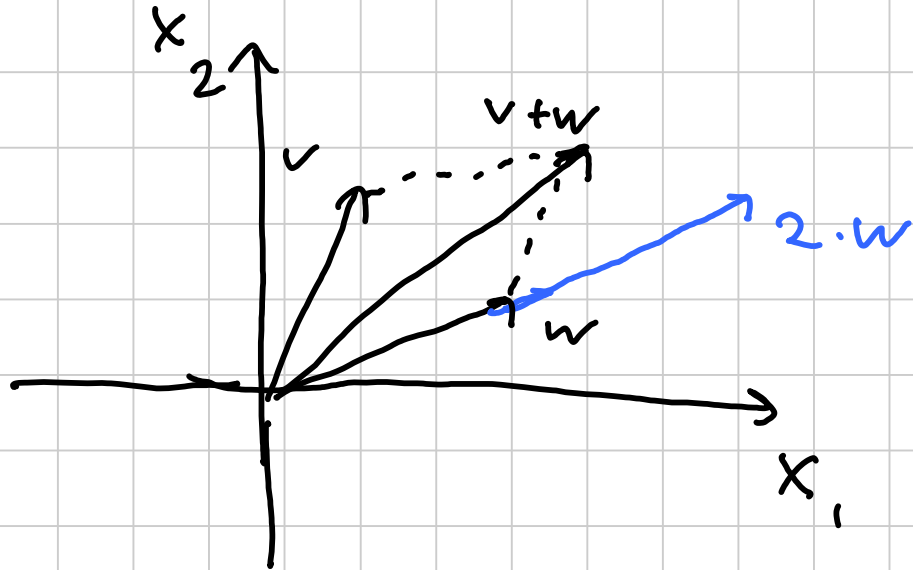
sono uguali
per distributività
di + rispetto
a $\cdot$ su $\mathbb{R}$

$$1 \cdot x + 1 \cdot y = 1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + 1 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 1 \cdot x_1 \\ \vdots \\ 1 \cdot x_n \end{pmatrix} + \begin{pmatrix} 1 \cdot y_1 \\ \vdots \\ 1 \cdot y_n \end{pmatrix} = \begin{pmatrix} 1 \cdot x_1 + 1 \cdot y_1 \\ \vdots \\ 1 \cdot x_n + 1 \cdot y_n \end{pmatrix}$$

Esercizio: Verificare che valgono tutte le proprietà della def. di spazio vettoriale su $\mathbb{R}^n$ con $+$, $\cdot$, 0 come definiti.

Sfruttare le proprietà di $+$ e $\cdot$ su $\mathbb{R}$.

Esempio: $\mathbb{R}^2$



• Matrici a coefficienti reali:

$$\mathcal{M}_{m \times n}(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} : a_{ij} \in \mathbb{R} \right. \\ \left. i=1, \dots, m, \quad j=1, \dots, n \right\}.$$

$$\text{con } \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

$$\text{con } \begin{matrix} \mathbb{R} \\ \lambda \end{matrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda \cdot a_{11} & \dots & \lambda \cdot a_{1n} \\ \vdots & & \vdots \\ \lambda \cdot a_{m1} & \dots & \lambda \cdot a_{mn} \end{pmatrix}$$

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}.$$

Esempio: $M_{2 \times 3}(\mathbb{R})$

$$\begin{pmatrix} 1 & 4 & 3 \\ 2 & -1 & \frac{5}{2} \end{pmatrix} + \begin{pmatrix} \sqrt{2} & 6 & 4 \\ 1 & 9 & -\frac{5}{2} \end{pmatrix} = \begin{pmatrix} 4\sqrt{2} & 10 & 7 \\ 3 & 8 & 0 \end{pmatrix}$$

$M_{3 \times 2}(\mathbb{R}) :$

$$\begin{matrix} 3. \\ \mathbb{M} \\ \mathbb{R} \end{matrix} \begin{pmatrix} 1 & 4 \\ 7 & 1 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 12 \\ 21 & 3 \\ 0 & 15 \end{pmatrix}.$$

Notazioni: $A = (a_{ij})_{\substack{i=1 \dots m \\ j=1 \dots n}} \in \mathcal{M}_{m \times n}$

$$A \in \mathcal{M}_{m \times n}$$

$$(A)_{ij} = a_{ij}$$

$\hookrightarrow$ coefficiente i -esima riga
 j -esima colonna

$$A \in \mathcal{M}_{3 \times 3}(\mathbb{R}) \quad A = \begin{pmatrix} 4 & \pi & 1 \\ \frac{3}{2} & 0 & 5 \\ 2 & \sqrt{2} & 4 \end{pmatrix}$$

$$(A)_{31} = 2$$

$$(A)_{12} = \pi$$

Riscriviamo le operazioni $+$, $\cdot$, riscriviamo $\circ$

$$\bullet (A + B)_{ij} = (A)_{ij} + (B)_{ij}$$

$\downarrow$ somma matrice $\downarrow$ somma su $\mathbb{R}$

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

$$\bullet \quad (0)_{ij} = 0 \in \mathbb{R}$$

matrice nulla

Verificăm proprietăți 4 (comutativitate)

$$A + B \stackrel{?}{=} B + A$$

$$(A+B)_{ij} = A_{ij} + B_{ij}$$

$$(B+A)_{ij} = B_{ij} + A_{ij} \quad \text{per commutatività.} \quad \left. \begin{array}{l} \forall i=1, \dots, m \\ \forall j=1, \dots, n \end{array} \right\} \text{ di } \text{Mat}(m, n, \mathbb{R})$$

Verificare le altre proprietà nella def. di spazio vettoriale.

Def: Se V è uno spazio vettoriale e $W \subset V$,
 diciamo che W è un **sottospazio vettoriale** di V se:

$$1) 0 \in W \quad (\text{s.s.v.})$$

$$2) \forall w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$$

$$3) \forall \lambda \in \mathbb{R}, \forall w \in W \Rightarrow \lambda \cdot w \in W$$

W è un sottoinsieme di V chiuso rispetto alle operazioni $+$ e $\cdot$ scalare

W è a sua volta uno spazio vettoriale con le operazioni ereditate da V .

(Le proprietà di spazio vett. di W discendono da

quelle di V)

Esempi di s.s.v. di V : $V \subset V$ e' s.s.v.

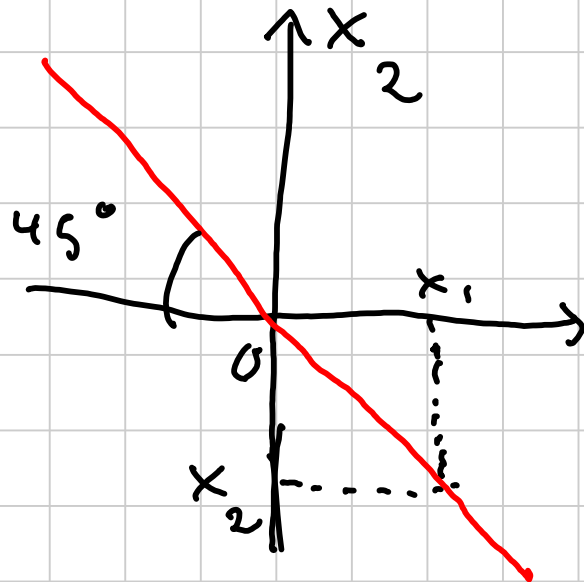
$\{0\} \subset V$ e' s.s.v.

$\downarrow$
vettore nullo

Esempio: $W = \left\{ x \in \mathbb{R}^n : \sum_{j=1}^n x_j = 0 \right\} \neq \emptyset$

$$x_1 + x_2 + \dots + x_n = 0$$

$$n=2$$



$$\sum_{i=1}^2 x_i = 0$$

$$x_1 + x_2 = 0$$

$$W = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : x_1 = -x_2 \right\}$$

Dimostriamo che W definito da (*) è s.s.v. di $\mathbb{R}^n$.

$$1) 0 \stackrel{?}{\in} W \quad 0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \sum_{j=1}^n x_j = \sum_{j=1}^n 0 = \underbrace{0 + \dots + 0}_n = 0$$

$$2) x, y \in W \stackrel{?}{\Rightarrow} x+y \in W$$

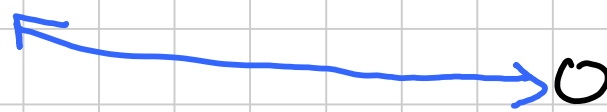
$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \quad x+y = \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$$

Poiché $x, y \in W$, sappiamo che $\sum_{i=1}^n x_i = 0$

$$\sum_{i=1}^n y_i = 0$$

$$\sum_{i=1}^n (x_i + y_i) = \sum_{i=1}^n x_i + \sum_{i=1}^n y_i = 0 + 0 = 0 \Rightarrow x+y \in W.$$

$$3. \lambda \in \mathbb{R}, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in W \stackrel{?}{\Rightarrow} \lambda \cdot x \in W.$$

$$x \in W \Rightarrow \sum_{i=1}^n x_i = 0$$


$$\lambda \cdot x = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix} \quad \sum_{i=1}^n \lambda \cdot x_i = \lambda \cdot \left(\sum_{i=1}^n x_i \right) = \lambda \cdot 0 = 0$$

$$\Rightarrow W \text{ e' un s.s.v. di } \mathbb{R}^n.$$

Esercitazione

Es. 2.3.2.

Dimostrare con argomento diretto che qualsiasi numero della forma $1\underbrace{0\dots 0}_{3k-1}1$ è composto (non primo).

$k \geq 1 \in \mathbb{N}$

1001 ($k=1$), $k=2$ 10000001 , $k=3$ 10000000001

$$\text{Dim: } 1\underbrace{0000\dots 0}_{3k-1}1 = 1\underbrace{00\dots 0}_{3k} + 1 = 10^{3k} + 1 =$$

$$= (10^k)^3 + 1^3.$$

$$\begin{aligned} (1001) &= (1001 - 1) + 1 = \\ &= 1000 + 1 \end{aligned}$$

Per ogni $A, B \in \mathbb{R}$ vale

$$A^3 + B^3 = (A+B) \cdot (A^2 - AB + B^2)$$

Ponendo $A = 10^k$, $B = 1$ otteniamo

$$(10^k)^3 + 1^3 = (10^k + 1) \cdot (10^{2k} - 10^k + 1)$$

$\begin{array}{c} \times \times \\ 1 \quad 10^{3k} + 1 \end{array}$

$\begin{array}{c} \times \times \\ 1 \quad 10^{3k} + 1 \end{array}$

poiché
 $k \geq 1$ $0 < 1$

Es. 2.3.5. Dimostrare per assurdo che se
 $m, n \in \mathbb{Z}$, e $m^2 + n^2$ e' pari, allora $n+m$ e' pari.

Dim. per assurdo

Supponiamo $n+m$ sia dispari.

Negazione
tesi

$n+m$ dispari $\Rightarrow (n+m)^2$ e' dispari.

$n^2 + m^2 + 2mn$ - pari
e' dispari

Per dim $P \Rightarrow Q$
abbiamo dim.
 $\neg(Q) \Rightarrow \neg(P)$

Es. 2.3.6. Dimostrare per induzione che un insieme X con n elementi ha 2^n sottoinsiemi (incluso $\emptyset$, e X).

Dim. per induzione:

Passo base: per $n=0$ $X = \emptyset$

Dato X insieme

$$\#P(X) = 2^0 = 1$$

$$P(X) = \{A \subseteq X\}. \text{ Se } X = \emptyset \quad P(X) = \{\emptyset\} \quad \square$$

$$X = \{2, 5\} \quad P(X) = \{\emptyset, \{2\}, \{5\}, \{2, 5\}\}$$

- Passo induttivo

Supponiamo $P(n)$ vera, dimostriamo $P(n+1)$ vera.

Un insieme di n elementi ha 2^n sottoinsiemi

passo
induttivo

Un insieme di
 $n+1$ elementi ha
 2^{n+1} sottoinsiemi

Sia X un insieme con $n+1$ elementi.

Preniamo un qualsiasi $a \in X$.

Definiamo

$$Y = \{A \subseteq X \mid a \in A\}$$

$$Z = \{A \subseteq X \mid a \notin A\}$$

$$\mathcal{P}(X) = Y \cup Z \text{ e } Y \cap Z = \emptyset$$

$$\# P(X) = \# Y + \# Z$$

↓
cardinalità
numero
di elementi
di un insieme

• Calcoliamo la cardinalità di Z $\#X = n+1$

• $A \in Z \Leftrightarrow A \subseteq X \setminus \{a\}, \#(X \setminus \{a\}) = n$

$\#P(X \setminus \{a\}) = 2^n \Rightarrow \#Z = 2^n$ per ipotesi induttiva

• Cardinalità di Y .

Definiamo $F: Y \rightarrow \mathcal{P}(X \setminus \{a\})$

$$A \mapsto A \setminus \{a\}$$

Definiamo $G: \mathcal{P}(X \setminus \{a\}) \rightarrow Y$

$$B \mapsto B \cup \{a\}$$

F e G sono una l'inversa dell'altra

$$F \circ G: P(X \setminus \{a\}) \longrightarrow P(X \setminus \{a\}) = \text{id}$$

$$A \xrightarrow{G} A \cup \{a\} \xrightarrow{F} A$$

$$G \circ F: Y \longrightarrow Y = \text{id}$$

$$A \xrightarrow{F} A \setminus \{a\} \xrightarrow{G} A$$

F e G stabiliscono una corrispondenza biunivoca

tra Y e $P(X \setminus \{a\})$. In particolare: $\# Y = \# P(X \setminus \{a\})$

Applichiamo ipotesi induttiva:

$$\# X \setminus \{a\} = n \Rightarrow \# P(X \setminus \{a\}) = 2^n$$

$$\# P(X) = \# Y + \# Z = 2^n + 2^n = 2^{n+1} \quad \square$$

$\overset{||}{2^n} \quad \overset{||}{2^n}$

Passo induttivo.