

Algebra Lineare 10/10/17

2.1.2 (unicità inverso multipl.).

L'equazione $x \cdot y = 1$ per $x \in \mathbb{Q}, x \neq 0$ ha soluz. unica.

Proviamo che se $x \cdot y = x \cdot z$ con $x \neq 0$ allora $y = z$.

Gufetti (6) dice $\exists x^{-1}$ t.c. $x^{-1} \cdot x = 1$; allora

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

$$\xRightarrow{(7)} (x^{-1} \cdot x) \cdot y = (x^{-1} \cdot x) \cdot z \xRightarrow{(6)} 1 \cdot y = 1 \cdot z \xRightarrow{(5)} y = z.$$

2.3.2. Provare che $\underbrace{10 \dots 01}_{3k-1}$ è composto, $k \geq 0$

$$\begin{aligned} \underbrace{10 \dots 01}_{3k-1} &= \underbrace{10 \dots 0}_{3k} + 1 = 10^{3k} + 1 = (10^k)^3 + 1^3 \\ &= \underbrace{(10^k + 1)}_{>1} \underbrace{(10^{2k} - 10^k + 1)}_{>1} \end{aligned}$$

2.3.5 : $m, m \in \mathbb{Z}$, $m^2 + m^2$ pari $\Rightarrow m + m$ pari.

Per assurdo : supponiamo $m + m = 2k+1$ $k \in \mathbb{Z}$;
allora $m = 2k - m + 1$ e

$$\begin{aligned}
 n^2 + m^2 &= m^2 + 4k^2 + m^2 + 1 - 4km + 4k - 2m \\
 &= 2(\dots) + 1 \quad \text{assunto.}
 \end{aligned}$$

2.3.8 : provare che $\frac{n(n+1)(2n+1)}{6}$ è intero $\forall n \in \mathbb{N}$

e $\sum_{j=0}^n j^2 = \frac{n(n+1)(2n+1)}{6}$.

Devo vedere che $n(n+1)(2n+1)$ è sempre multiplo di 6, cioè di 2 e di 3.

di 2 : già $n(n+1)$

di $\exists$: $m = 3k$ ✓

$m = 3k+1 \Rightarrow 2m+1 = 6k+2+1 = 3(2k+1)$ ✓

$m = 3k+2 \Rightarrow m+1 = 3(k+1)$ ✓

Per induz:
$$\sum_{i=0}^m i^2 = \frac{m(m+1)(2m+1)}{6}$$

PB: $m=0$ $0=0$ ✓

PI: Supponiamo
$$\sum_{i=0}^m i^2 = \frac{m(m+1)(2m+1)}{6}$$

Dobbiamo provare:

$$\sum_{j=1}^{m+1} j^2 = \frac{(m+1)(m+2)(2m+3)}{6}$$



$$\begin{aligned} \left(\sum_{j=1}^m j^2 \right) + (m+1)^2 &= \frac{m(m+1)(2m+1)}{6} + (m+1)^2 \\ &= \frac{m+1}{6} (2m^2 + m + 6m + 6) \\ &= \frac{m+1}{6} (2m^2 + 7m + 6) \\ &= \frac{m+1}{6} (m+2)(2m+3) \end{aligned}$$



2.3.10 : verificare che per provare che
una proposizione $P(n)$ è vera
 $\forall n \in \mathbb{N}$ basta fare questo:

induzione
completa

PB : provare che $P(0)$ è vera

PI : supponendo vera $P(k)$ per ogni
 $k \leq n$, provare che $P(n+1)$ è vera.

$P(0)$: vera per PB

$P(1)$: PI per $n = 0 \Rightarrow$ vera

$P(2)$: PI per $n = 1 \Rightarrow$ vera

2.3.11 : provare che ogni numero naturale $n \in \mathbb{N}$,
 $n \geq 2$ è prodotto di numeri primi.

induzione completa

PB : $n=2$ vera, è primo

PI : Supponiamo che ogni $k \leq n$ sia prodotto
di primi; dimostriamo che $n+1$ lo è,
 $\Rightarrow$ Primo $\checkmark$

$n+1$ $\Rightarrow$ non primo $n+1 = k \cdot h$

con $k, h < n+1$; per ipotesi
induttive k, h sono prodotto
di primi $\Rightarrow$ anche $n+1$. $\square$

2.3.12 . Provare che esistono infiniti numeri primi.

Per assurdo, supponiamo che la lista dei numeri primi finisca:

$$P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7, P_5 = 11, P_6 = 13, \dots, P_N.$$

Consideriamo il numero $m = P_1 \cdot P_2 \cdot \dots \cdot P_N + 1$.

L'esercizio precedente dice che m è prodotto di primi, quindi esiste j t.c. m è multiplo di P_j . Tuttavia la divisione $m : P_j$ ha resto 1: assurdo. 

2.3.13 : (principio del minimo)

ogni $X \subset \mathbb{N}$ non vuoto ha minimo.

2.3.14 (divisione euclidea in $\mathbb{Z}$) :

dati $n, m \in \mathbb{Z}$, $m > 0$ esistono unici
 $q, r \in \mathbb{Z}$ t.c. $n = q \cdot m + r$ e $0 \leq r < m$.

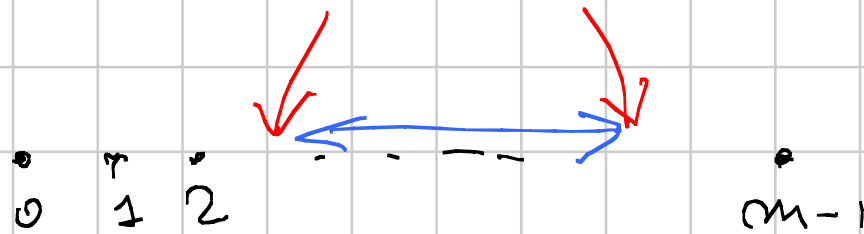
Unicità: supponiamo di avere

$$q_1, r_1 \quad \text{t.c.} \quad n = q_1 \cdot m + r_1, \quad 0 \leq r_1 < m$$

$$q_2, r_2 \quad \text{t.c.} \quad n = q_2 \cdot m + r_2, \quad 0 \leq r_2 < m$$

$$0 = (q_1 - q_2) \cdot m + \pi_1 - \pi_2$$

$$|\pi_1 - \pi_2| = |q_1 - q_2| \cdot m$$



$0 \leq \dots < m$
 $0 \leq \dots < m$

$$\Rightarrow |q_1 - q_2| = 0 \quad \text{cioe'} \quad q_1 = q_2$$

$$\text{e } |\pi_1 - \pi_2| = 0 \quad \text{cioe'} \quad \pi_1 = \pi_2$$

Esistenza :

$$73 : 9$$

$$73 = 4 \cdot 9 + 37$$

finita? No! $37 \geq 9$

miglioro :

$$\begin{aligned} 73 &= (4+1) \cdot 9 + (37-9) \\ &= 5 \cdot 9 + 28 \end{aligned}$$

miglioro

$$\begin{aligned} 73 &= (5+1) \cdot 9 + 28-9 \\ &= 6 \cdot 9 + 19 \end{aligned}$$

...

$$73 = 8 \cdot 9 + 1$$

Il resto giusto è il più piccolo numero del tipo
 $m - q \cdot m$

Poniamo $\mathcal{R} = \{ m - q \cdot m : q \in \mathbb{Z} \} \cap \mathbb{N}$

$\mathcal{R} \neq \emptyset$ poiché per $m \geq 0$ posso prendere $q = 0$
e trovo $m \in \mathcal{R}$

per $m < 0$ posso prendere $q = m$
e trovo $m(1-m) = (-m) \cdot (m-1) \geq 0$
sta in $\mathcal{R}$

Per principio minimo $\mathcal{R}$ ha un minimo
 $\pi_0 = m - q_0 \cdot m$ - Dunque

$$m = q_0 \cdot m + \pi_0$$

Devo vedere che $0 \leq \pi_0 < m$; $0 \leq \pi_0$ ok ;

se per assurdo avessi $\pi_0 \geq m$ avrei

$$m = q_0 \cdot m + \pi_0 = (q_0 + 1) \cdot m + (\pi_0 - m)$$

$$\Rightarrow \pi_0 - m \geq 0, \pi_0 - m \in \mathcal{R}, \pi_0 - m < \pi_0$$

quindi non è vero che π_0 è min di $\mathcal{R}$. $\square$

$\text{Span}(v_1, \dots, v_m)$ = il più piccolo
sottospazio di V
che contiene $v_1, \dots, v_m$

sottospazio generato

visto: $\text{Span}(v_1, \dots, v_m) =$

$$= \left\{ \underbrace{\sum_{j=1}^m \alpha_j v_j}_{\text{combinazioni lineari di } v_1, \dots, v_m} : \alpha_j \in \mathbb{R}, j=1, \dots, m \right\}$$

combinazioni lineari di $v_1, \dots, v_m$

con coeff. $\alpha_1, \dots, \alpha_m$.

Q: l'espressione di $w \in \text{Span}(v_1, \dots, v_m)$
come comb. lin. di $v_1, \dots, v_m$ è unica?

Q': l'espressione di $0 \in \text{Span}(v_1, \dots, v_m)$
come $0 = 0 \cdot v_1 + \dots + 0 \cdot v_m$ è l'unica?

Ovvio: $\bar{u} \in \mathbb{Q} \Rightarrow \bar{u} \in \mathbb{Q}$

Vero: anche viceversa.

Def: diciamo $v_1, \dots, v_m$ sono linearmente indipendenti se

- l'unica comb. lin. con risultato nullo è quella con coeff. tutti nulli

ovvero • dati $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ con $\alpha_1 v_1 + \dots + \alpha_m v_m = 0$
 $\Rightarrow$ ha per forza $\alpha_1 = \dots = \alpha_m = 0$.

Sarebbe meglio dire

" $v_1, \dots, v_m$ è un sistema di vettori lin. indep."

$\hookrightarrow$ è una proprietà non loro
individuale ma come insieme.

Es 1: $\begin{pmatrix} 3 \\ -1 \\ 5 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ -7 \end{pmatrix} \in \mathbb{R}^3$

lin. indep. ? $\alpha \begin{pmatrix} 3 \\ -1 \\ 5 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 4 \\ -7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \stackrel{?}{\Rightarrow} \alpha = \beta = 0$



$$\begin{cases} 3\alpha + 2\beta = 0 \\ -\alpha + 4\beta = 0 \checkmark \\ 5\alpha - 7\beta = 0 \end{cases} \Rightarrow$$

$$\begin{cases} \alpha = 4\beta \\ 14\alpha = 0 \\ 13\alpha = 0 \end{cases}$$

$$\Rightarrow \alpha = \beta = 0 \quad \text{lin.}$$

Es 2: $\begin{pmatrix} 2 \\ -5 \end{pmatrix} \begin{pmatrix} 4 \\ 7 \end{pmatrix} \begin{pmatrix} 1 \\ -9 \end{pmatrix} \in \mathbb{R}^2$

Sono lin. indep?

$$\alpha \begin{pmatrix} 2 \\ -5 \end{pmatrix} + \beta \begin{pmatrix} 4 \\ 7 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ -9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \stackrel{?}{\Rightarrow} \alpha = \beta = \gamma = 0$$



$$\begin{cases} 2\alpha + 4\beta + \gamma = 0 \\ -5\alpha + 7\beta - 9\gamma = 0 \end{cases} \Leftrightarrow \begin{cases} \gamma = -2\alpha - 4\beta \\ 13\alpha + 43\beta = 0 \end{cases}$$

ha la soluz $\alpha = 43, \beta = -13, \gamma = -34$

(oppure $\alpha = -1$ $\beta = \frac{43}{13}$ $\gamma = \dots$)
No

Prop: $v_1, \dots, v_m$ lin. indep. $\iff$ ogni $w \in \text{Span}(v_1, \dots, v_m)$
ha espr. unica -

Dim: $\Leftarrow$ ovvia

$\Rightarrow$: prendiamo $w \in \text{Span}(v_1, \dots, v_m)$ scritto
come $w = \alpha_1 v_1 + \dots + \alpha_m v_m$
 $w = \beta_1 v_1 + \dots + \beta_m v_m$

$$\Rightarrow 0 = (\alpha_1 - \beta_1)v_1 + \dots + (\alpha_m - \beta_m)v_m$$

ho comb. lin. di $v_1, \dots, v_m$ con coeff
 $\alpha_1 - \beta_1, \dots, \alpha_m - \beta_m$ e risultato 0

ma $v_1, \dots, v_m$ lin. indep. dunque $\alpha_1 - \beta_1 = \dots = \alpha_m - \beta_m = 0$

$$\Rightarrow \alpha_1 = \beta_1, \dots, \alpha_m = \beta_m.$$



Q: quando accade che un sistema di k vett. è
 lin. indep.?

$$\boxed{k=1}$$

v_1 lin. indep.?

$$\alpha_1 \cdot v_1 = 0 \quad \not\Rightarrow \alpha_1 = 0$$

Sì se $v_1 \neq 0$, altrimenti no.

$k=2$

Oss: se $v_1, \dots, v_m$ sono
lin. dipendenti, aggiungendo
un vettore u allora
 $v_1, \dots, v_m, u$ restano lin. dip:

$$\begin{aligned} &(\alpha_1 v_1 + \dots + \alpha_m v_m = 0 \\ &\Rightarrow \alpha_1 v_1 + \dots + \alpha_m v_m + 0 \cdot u = 0) \end{aligned}$$

v_1, v_2 possono essere lin. indep. solo se
non nulli ($k=1$)

Supponiamo non nulli;
lin. dip? l'eq. $\alpha_1 v_1 + \alpha_2 v_2 = 0$ ha
soluzioni non nulle (con
 $\alpha_1 \neq 0$ o $\alpha_2 \neq 0$)?

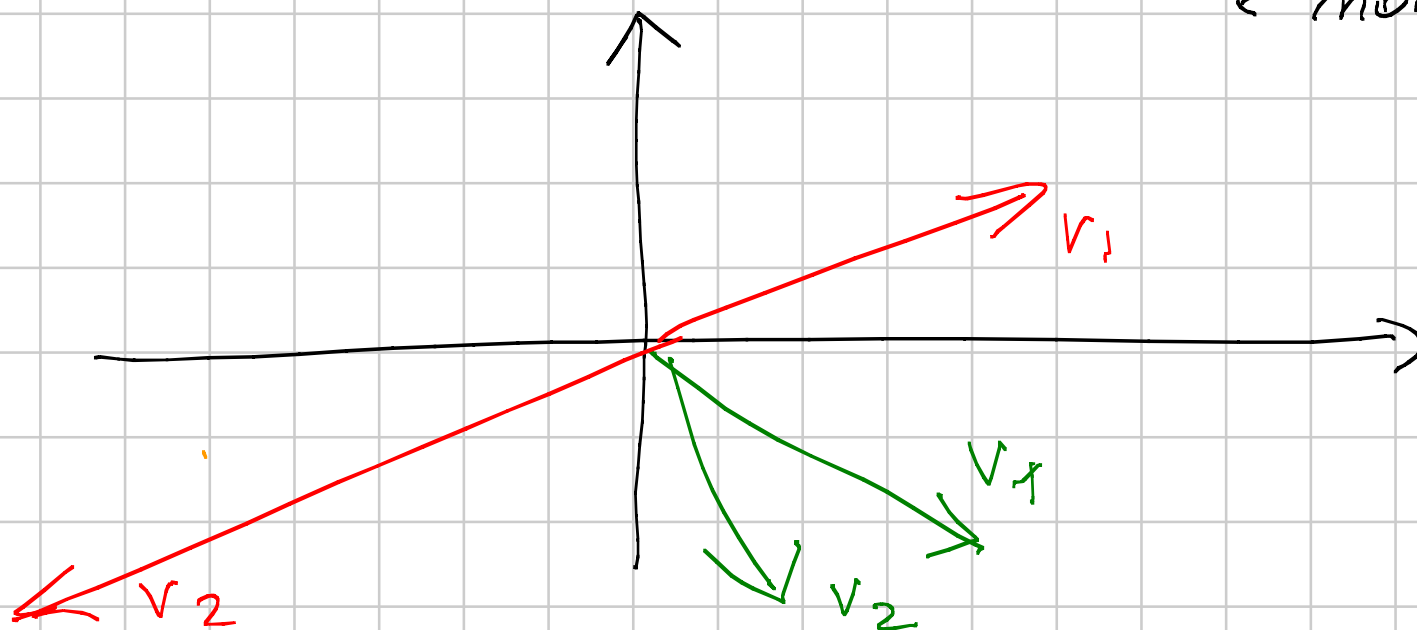
Se s $\bar{}$, sono entrambi $\neq 0$, dunque ho

$$v_1 = \left(-\frac{\alpha_2}{\alpha_1}\right) v_2 \quad \text{e} \quad v_2 = \left(-\frac{\alpha_1}{\alpha_2}\right) v_1$$

Cio $\bar{e}$ sono dip. se sono ciascuno
multiplo dell'altro.

Visto: v_1, v_2 lin. dip. $\iff$ uno nullo o
multiplici uno dell'altro

Cioè: v_1, v_2 lin. indep. $\iff$ entrambi non nulli
e non multipli fra loro.



lin. dip.

lin. indep.

Def: chiamo base di V un insieme $(v_1, \dots, v_m)$ ordinato di vettori che sono generatori di V e linearmente indipendenti.

$$\left(\begin{pmatrix} 3 \\ 7 \end{pmatrix}, \begin{pmatrix} -1 \\ 5 \end{pmatrix} \right) \neq \left(\begin{pmatrix} -1 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 7 \end{pmatrix} \right)$$

ogni elemento di V è comb. lin. di $v_1, \dots, v_m$

ogni elemento di V si esprime in modo unico come comb. lin. di $v_1, \dots, v_m$

Def: se $B = (v_1, \dots, v_m)$ è base di V , preso $v \in V$ trovo l'unica comb. lin. di

$v_1, \dots, v_m$ che dà v , cioè

$$v = x_1 v_1 + \dots + x_m v_m \quad \text{con } x_1, \dots, x_m \in \mathbb{R}$$

e chiamo $x_1, \dots, x_m$ coordinate di v rispetto
a $\mathcal{B}$, che indico con $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = [v]_{\mathcal{B}} \in \mathbb{R}^m$

$$\underline{\text{Es}}: \quad V = \{y \in \mathbb{R}^3 : 2y_1 - 5y_2 + 3y_3 = 0\}$$

$$\mathcal{B} = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ -1 \end{pmatrix} \right) \quad v = \begin{pmatrix} 17 \\ 5 \\ -3 \end{pmatrix}$$

Fatto: $\mathcal{B}$ è base di V (vedremo)

Calcoliamo $[v]_{\mathcal{B}}$: risolviamo

$$\begin{pmatrix} 17 \\ 5 \\ -3 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 4 \\ 1 \\ -1 \end{pmatrix}$$

$$\begin{cases} x_1 + 4x_2 = 17 \\ x_1 + x_2 = 5 \quad \checkmark \\ x_1 - x_2 = -3 \quad \checkmark \end{cases}$$

$$\begin{cases} x_1 = 1 \\ x_2 = 4 \\ 1 + 4 \cdot 4 = 17 \quad \checkmark \end{cases}$$

$$\Rightarrow [v]_{\mathcal{B}} = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \in \mathbb{R}^2$$