campo $\mathbb{K}$ (es $\mathbb{R}$, $\mathbb{Q}$) → scalari sono elementi del campo.

vettori V → spazio vettoriale su $\mathbb{K}$

⇓

posso moltiplicare un vettore per uno scalare.

es: $V=\mathbb{R}^2$ $V=\mathbb{R}^3$ $V=\mathbb{R}[x]$ $V=\mathbb{R}[x]^{\leq 2}$

↳ polinomi.

dato uno spazio vettoriale possiamo considerare lo $\text{span}(v_1, \dots, v_n) \subseteq V$

↳ sottoinsieme.

$$\text{span}(v_1 \dots v_n) = \{a_1 v_1 + \dots + a_n v_n \mid a_1, \dots, a_n \in \mathbb{K}\}$$

es: $V=\mathbb{R}$ $v_1 = (0,1,0)$

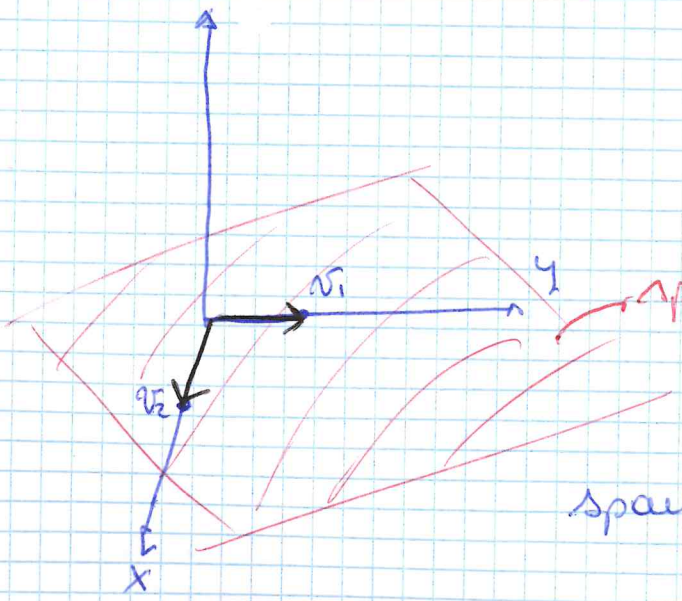
$v_2 = (1,0,\ )$

$$\text{span}(v_1, v_2) = \{a(0,1,0) + b(1,0,0) \mid a, b \in \ \}$$

$$(0,a,0) + (b,0,0)$$

$$=$$

$$(b,a,0)$$



span ⇒ tutto il piano x, y.

$\text{span}(v_1, v_2) \supseteq \text{span}(v_1)$

Algebra lineare 01/03/2017

campo $\mathbb{K}$ (es $\mathbb{R}$, $\mathbb{Q}$) → scalari sono elementi del campo.

vettori V → spazio vettoriale su $\mathbb{K}$

⇓

posso moltiplicare un vettore per uno scalare.

es: $V=\mathbb{R}^2$ $V=\mathbb{R}^3$ $V=\mathbb{R}[x]$ $V=\mathbb{R}[x]^{\leq 2}$

↳ polinomi.

dato uno spazio vettoriale possiamo considerare lo $\text{span}(v_1, \dots, v_n) \subseteq V$

↳ sottoinsieme.

$$\text{span}(v_1 \dots v_n) = \{a_1 v_1 + \dots + a_n v_n \mid a_1, \dots, a_n \in \mathbb{K}\}$$

es: $V=\mathbb{R}$ $v_1 = (0,1,0)$

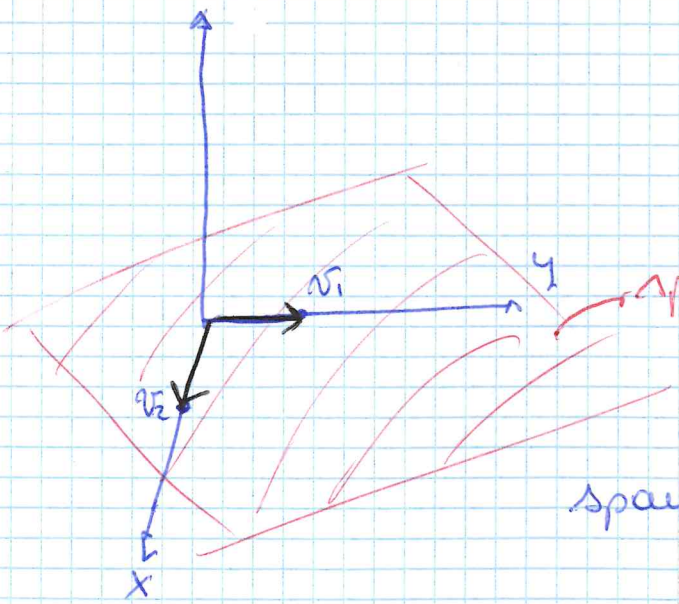
$v_2 = (1,0,\ )$

$$\text{span}(v_1, v_2) = \{a(0,1,0) + b(1,0,0) \mid a, b \in \ \}$$

$$(0,a,0) + (b,0,0)$$

$$=$$

$$(b,a,0)$$



span ⇒ tutto il piano x, y.

$\text{span}(v_1, v_2) \supseteq \text{span}(v_1)$

V

$v_1, v_2 \in V \quad W = \text{span}(v_1, v_2) \subseteq V$

se prendo tutto V, v_1 e v_2 si chiamano generatori

(W) è un SOTTOSPAZIO vettoriale di V

↓

è un sottoinsieme di V ma è anche lui uno spazio vettoriale.

↳ • passa per lo $\emptyset$.

• se $w_1, w_2 \in W \Rightarrow (w_1 + w_2) \in W$

la somma è possibile perché sono in un sottospazio di V (e in V è possibile fare la somma).

$w_1 = a v_1 + b v_2$
$w_2 = \bar{a} v_1 + \bar{b} v_2$ } sommo

$w_1 + w_2 = (a + \bar{a}) v_1 + (b + \bar{b}) v_2$

con la somma sta nello span.

• $cw \in W$

$w = a v_1 + b v_2$

$cw = c(a v_1 + b v_2) \Rightarrow cw = ca v_1 + cb v_2$

somo e scalari

è possibile quindi fare la moltiplicazione in W

una circonferenza non è uno spazio vettoriale.

Teorema: Sistemi lineari omogenei

$$a_{11} x_1 + \dots + a_{1n} x_n = 0$$
$$\vdots$$
$$a_{k1} x_1 + \dots + a_{kn} x_n = 0$$

$$\left[\begin{array}{ccc|c} a_{11} & \dots & & 0 \\ & & & 0 \\ & & & \vdots \\ a_{k1} & & & 0 \end{array}\right]$$

$x_1, \dots, x_n \in K$

V

$v_1, v_2 \in V \quad W = \text{span}(v_1, v_2) \subseteq V$

se prendo tutto V, v_1 e v_2 si chiamano generatori

(W) è un SOTTOSPAZIO vettoriale di V.

è un sottoinsieme di V ma è anche lui uno spazio vettoriale.

↳ • passa per lo $\emptyset$.

• se $w_1, w_2 \in W \Rightarrow (w_1 + w_2) \in W$

la somma è possibile perché sono in un sottospazio di V (e in V è possibile fare la somma).

$w_1 = av_1 + bv_2$
$w_2 = \bar{a}v_1 + \bar{b}v_2$ } sommo

$w_1 + w_2 = (a+\bar{a})v_1 + (b+\bar{b})v_2$

con la somma sta nello span.

• $cw \in W$

$w = av_1 + bv_2$

$cw = c(av_1 + bv_2) \Rightarrow cw = \underbrace{ca}v_1 + \underbrace{cb}v_2$

sono scalari

è possibile quindi fare la moltiplicazione in W

una circonferenza non è uno spazio vettoriale.

Teorema: Sistemi lineari omogenei

$$a_{11}x_1 + \dots + a_{1n}x_n = 0$$
$$\vdots$$
$$a_{k1}x_1 + \dots + a_{kn}x_n = 0$$

$$\left[\begin{array}{ccc|c} a_{11} & \dots & & 0 \\ & & & 0 \\ & & & \vdots \\ a_{k1} & & & 0 \end{array}\right]$$

$x_1, \dots, x_n \in K$

le soluzioni x_1, ∞, x_n del sistema formano un sottospazio di K^n

I sottospazi possiamo scriverli come:
- soluzioni di un sistema
- span di vettori.

Es: $V = \mathbb{R}^3$

$x + 2y + 3z = 0$ sistema con una sola equazione.

Trovare (x, y, z) soluzioni.
Voglio scriverlo come span di qualcosa.

$$[1 \quad 2 \quad 3 \mid 0]$$

1 → pivot; 2 3 → libere y e z

$$\begin{cases} z = z_0 \\ y = y_0 \\ x_0 = -2y_0 - 3z_0 \end{cases}$$

cerco di scriverlo come uno span.

$$\begin{pmatrix} -2y_0 - 3z_0 \\ y_0 \\ z_0 \end{pmatrix} = (-2y_0 - 3z_0, y_0, z_0)$$

Separiamo i contributi di y_0 e z_0.

con la somma ottengo le varie iniziali

Le soluzioni sono del tipo $(-2y_0, y_0, 0) + (-3z_0, 0, z_0)$

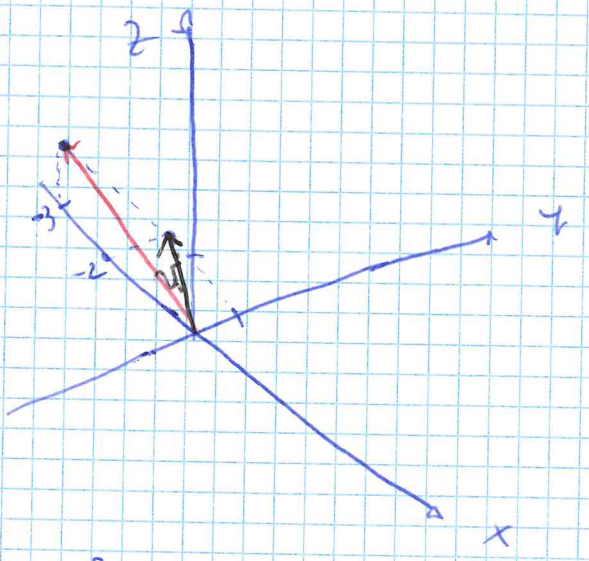
raccogliamo y_0 e z_0

$$y_0(-2, 1, 0) + z_0(-3, 0, 1)$$

y_0 → a; $(-2, 1, 0) = v_1$; z_0 → b; $(-3, 0, 1) = v_1$

le soluzioni del sistema sono uguali allo $\text{span}\{(-2,1,0),(-3,0,1)\}$

questi due vettori generano poi tutti gli altri nello spazio vettoriale



es: $V=\mathbb{R}^3$

$$\begin{cases} x+y+z=0 \\ 2x+3y+4z=0 \end{cases}$$

cerchiamo le soluzioni (x,y,z)

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 2 & 3 & 4 & 0 \end{array}\right] \quad \text{posiamo attenzione questa colonna}$$

$R2-2R1$

$$\left[\begin{array}{ccc} \textcircled{1} & 1 & 1 \\ 0 & \textcircled{1} & 2 \end{array}\right] \quad R1-R2$$

2 pivot

$$\left[\begin{array}{ccc} 1 & 0 & -1 \\ 0 & 1 & 2 \end{array}\right]$$

convenzionalmente scegliamo libere le incognite che non sono pivot

z è libero $z=z_0$

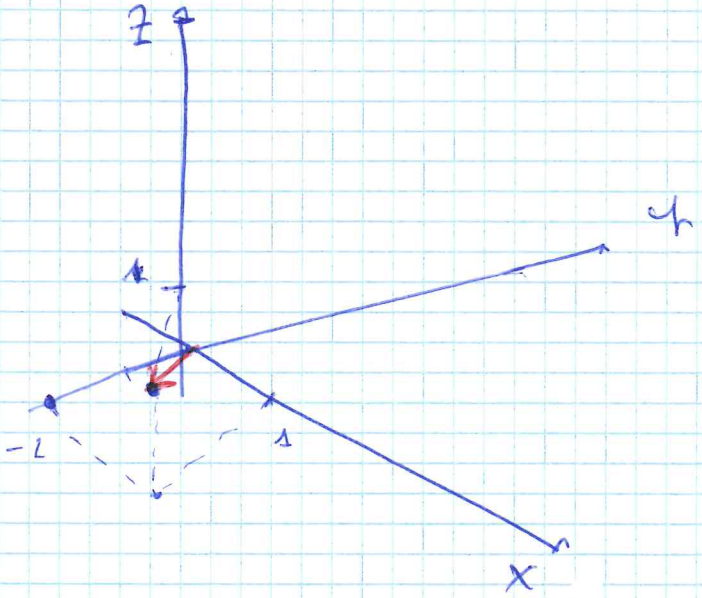
$$\begin{cases} y = -2z_0 \\ x = z_0 \\ z = z_0 \end{cases}$$ soluzioni:

$$(z_0, -2z_0, z_0) =$$

$$= z_0 (1, -2, 1) \Rightarrow$$

$\Rightarrow$ span$((1,-2,1))$ → soluzioni

È una retta



Le equazioni possono essere viste come vettori e devono essere linearmente indipendenti per far calare la dimensione di K.

es: 0 equazioni $\mathbb{R}^3 = V$

1 // $\mathbb{R}^{3-1} = \mathbb{R}^2$ piano

2 // $\mathbb{R}^{3-2} = \mathbb{R}$ retta.

3 equazioni indipendenti

↓

ie punto $(0,0,0)$ è la sola soluzione.

$(0,0,0) = \text{span}((0,0,0))$

span dello stesso vettore moltiplicato per un coefficiente $\neq 0$

$$\text{span}(v) = \text{span}(av) \qquad a \neq 0.$$

$$\text{span}(v_1, v_2, \dots, v_n) = \text{span}(v_1 + av_2, v_2, \dots, v_n)$$

posso usare tipo delle "mosse di Gauss" anche con i vettori

$v_1 = v_1 + av_2 \Rightarrow$ non cambia lo span.

es:

$$\text{span}(3v_1, v_1, v_3)$$

$\bar{v}_1 \quad \bar{v}_2$

$v_1 - 3v_2$

$$\text{span}(0, v_1, v_3)$$

la dimensione non è data dal numero di vettori, questi devono essere <u>indipendenti</u>.

devo dimostrare che

$v_1 + av_2$ sta nello $\text{span}(v_1, v_2, \dots, v_n)$

viene fuori da $1 \cdot v_1 + a \cdot v_2 + 0 \cdot v_3 + 0 \cdot \dots + 0 \cdot v_n$

il contrario, cioè da $v_1 + av_2$ voglio ottenere v_1

$w_1 = v_1 + av_2 \qquad v_1 = w_1 - av_2$

lo span non cambia utilizzando delle mosse simili a QUELLE di GAUSS.

Definizione: $v_1, v_2, \dots, v_n \in V$

sono linearmente indipendenti se l'unica combinazione lineare $a_1v_1 + \dots + a_nv_n = \bar{0}$ è quella con $a_1 = a_2 = \dots = a_n = 0$

$\Downarrow$

i coefficienti sono $= 0$.

$V = \mathbb{R}^3$

$v_1 = (1, 2, 3)$

$v_2 = (2, 4, 6) = 2v_1$ } Dipendenti.

$v_2 - 2v_1 = 0$

teorema $v_1, v_2, \dots, v_n$ sono dipendenti se e solo se:

1) $\exists (a_1, \dots, a_n) \neq (0, \dots, 0)$ (cioè almeno uno $a_i \neq 0$) tale che $a_1 v_1 + \dots + a_n v_n = 0$

⇕

2) almeno uno dei v_i è nello span degli altri vettori.

es:

$0v_1 + 3v_2 + 4v_3 + 5v_4 = 0$

↓

sono dipendenti per la def. 1)

$3v_2 = -4v_3 - 5v_4$

$v_2 = -\frac{4}{3}v_3 - \frac{5}{3}v_4$ → per 2) v_2 è stato ottenuto dagli altri due vettori

$\text{span}(v_1, v_2, v_3, v_4) = \text{span}(v_1, v_3, v_4)$

teorema: Supponiamo che $v_1, v_2, \dots, v_n$ siano indipendenti e consideriamo $w \in \text{span}(v_1, v_2, \dots, v_n)$

Esistono unici $(a_1, \dots, a_n)$ che mi fanno trovare $w = a_1 v_1 + \dots + a_n v_n$.

coordinate di w rispetto a $v_1, \dots, v_n$

ESEMPIO $v_1 = (1, 2, 3)$

$v_2 = (2, 4, 6)$ sono dipendenti

$w = (3, 6, 9)$ è span (v_1, v_2)

$w = v_1 + v_2$ $\quad w = 3v_1 + 0 \cdot v_2$

$1 + 1$ le coordinate non si sono perché non sono uniche e v_1 e v_2 non sono indipendenti.

se indipendenti $\Rightarrow$ coordinate uniche

$$- \begin{cases} w = a_1 v_1 + \dots + a_n v_n \\ w = b_1 v_1 + \dots + b_n v_n \end{cases}$$

$$= (a_1 - b_1) v_1 + \dots + (a_n - b_n) v_n = 0$$

$a_1 - b_1 = 0 \Rightarrow a_1 = b_1$

$\vdots$ $\quad \vdots$

$a_n - b_n = 0 \Rightarrow a_n = b_n$

$\Big\}$ sono uguali $\Downarrow$ sono uniche

ESEMPIO 2 vettori in $\mathbb{R}^2$

$V = \mathbb{R}^2$ $\quad v_1 = (3, 2)$ $\quad v_2 = (2, 3)$

Sono indipendenti? sì

applico la definizione:

$a(3, 2) + b(2, 3) = (0, 0)$ cerchiamo di ottenere $(0, 0)$

$$\begin{cases} 3a + 2b = 0 \\ 2a + 3b = 0 \end{cases} \quad \begin{cases} a = 0 \\ b = 0 \end{cases} \Rightarrow \text{sono indipendenti}$$

Quali sono le coordinate di $(2, 1)$?

$a(3, 2) + b(2, 3) = (2, 1)$

$$\begin{cases} 3a + 2b = 2 \\ 2a + 3b = 1 \end{cases} \quad \begin{cases} b = 4/5 \\ a = -1/5 \end{cases}$$

le coordinate di $(2, 1)$ rispetto a $(2, 3)$ $(3, 2)$ sono $a = -1/5$ $\quad b = 4/5$

ESEMPIO $v_1=(1,2,3)$

$v_2=(2,4,6)$ sono dipendenti

$w=(3,6,9)$ è span (v_1, v_2)

$w = v_1 + v_2$ $\quad w = 3v_1 + 0\cdot v_2$

$1+1$

le coordinate non si sono perché non sono uniche e v_1 e v_2 non sono indipendenti.

se indipendenti $\Rightarrow$ coordinate uniche

$$-\begin{cases} w = a_1 v_1 + \dots + a_n v_n \\ w = b_1 v_1 + \dots + b_n v_n \end{cases}$$

$$= (a_1 - b_1)v_1 + \dots + (a_n - b_n)v_n = 0$$

$a_1 - b_1 = 0 \Rightarrow a_1 = b_1$

$\vdots \qquad\qquad \vdots$

$a_n - b_n = 0 \Rightarrow a_n = b_n$

$\Big\}$ sono uguali $\Rightarrow$ sono uniche

ESEMPIO 2 vettori in $\mathbb{R}^2$

$V=\mathbb{R}^2 \qquad v_1=(3,2) \qquad v_2=(2,3)$

Sono indipendenti? sì

applico la definizione:

$a(3,2)+b(2,3) = (0,0)$ vediamo di trovare $(0,0)$

$$\begin{cases} 3a+2b=0 \\ 2a+3b=0 \end{cases} \quad \begin{cases} a=0 \\ b=0 \end{cases} \Rightarrow \text{sono indipendenti}$$

Quali sono le coordinate di $(2,1)$?

$a(3,2)+b(2,3)=(2,1)$

$$\begin{cases} 3a+2b=2 \\ 2a+3b=1 \end{cases} \quad \begin{cases} b=4/5 \\ a=-1/5 \end{cases}$$

le coordinate di $(2,1)$ rispetto a $(2,3)$ $(3,2)$ sono $a=-1/5 \quad b=4/5$

Matematica discreta 2/03/2017

Interi modulo n

$n \in \mathbb{Z}$ consideriamo $x, y \in \mathbb{Z}$

Def.

$x \equiv y \mod(n)$ $\Rightarrow$ cioè $\exists k$.

se n divide $x-y$

$x-y$ multiplo di n.

$nk = x-y$

$\Downarrow$

cioè $x = y + nk$.

Es:

$3 \equiv 17 \mod(7)$

$17 = 3 + 14$, 14 è un multiplo di 7 $\Rightarrow 2 \cdot 7 = 14$

congruenza modulo 7

Divisione (con resto) euclidea

$7 : 2 = 3,5$ senza resto

$7 : 2 = 3$ con resto 1

$7 = 2 \cdot 3 + 1$

quoziente, resto.

$7 \equiv 1 \mod(3)$

Teorema:

- Dati x e $y \in \mathbb{Z}$ con $y \neq 0$

$\exists q \in \mathbb{Z}$ ed $\exists r \in \mathbb{Z}$ tale che

$x = y \cdot q + r$

con $0 \leq r < y$

dimostrazione formale:

utilizzato il Principio del minimo → vale se in $\mathbb{R}$.

se ho un insieme di numeri naturali (non vuoto) questo ha un minimo.

$\emptyset \neq S \subseteq \mathbb{N} \Rightarrow S$ ha minimo.

$m_0 = \min\{ m : y m > x \}$

$\min$ → numero che esiste per il principio del minimo.

$y \neq 0$ quindi sicuramente c'è un m.

$q = m_0 - 1$ → perché $y \cdot q \leq x < y(q+1)$ → $(q+1)$ è il minimo che moltiplicato per y supera $x \Rightarrow x < y(q+1)$

Classe di un numero modulo m

$$[x]_m$$

$x \equiv y \ (n)$ se e solo se x e y hanno lo stesso resto modulo n.

↳ quando divisi per n.

es: $8 \equiv 3 \ (5)$

8 | 5	3 | 5
3 | 1	3 | 0

stesso resto

$-8 \equiv 1 \ (3)$

-8 | 3	8 | 3
1 | 9	2 | 2

$8 = 2 \cdot 3 + 2$

$-8 = (-2)3 - 2$ → moltiplico per (-1)

$-8 = (-3) \cdot 3 + 1$ → altero il quoziente e modifico il resto

x | n	y | n
r | q_1	r | q_2

r è uguale altrove

$x \equiv y \ (n)$

$\Rightarrow$ dimostriamo

$$\begin{cases} x = nq_1 + r \\ y = nq_2 + r \end{cases}$$

$$x - y = n(q_1 - q_2)$$

multiplo di n e quindi $x \equiv y \ (n)$.

se hanno lo stesso resto allora sono congrui, è vero anche che se sono congrui allora hanno lo stesso resto

$\bar{x}$ = resto di x modulo n.

$x = 0, 1, 2, 3, 4, 5, 6, 7, 8$

$n = 3$

$\bar{x} = 0, 1, 2, 0, 1, 2, 0, 1, 2$ ⇒ vado tutti i resti

resto associato

dire che $x \equiv y \ (n)$

vuol dire anche $\bar{x} = \bar{y} \Rightarrow [x]_n = [y]_n$ con n segnato

congruenza tra numeri ⇔ uguaglianza tra resti.

classe resto è un insieme

$$[x]_n = \{ y \mid y \equiv x (n) \}$$

es: $[5]_3 = \{ 5, 2, -1, -4, \infty$

$8, 11, 14, 17, \infty \}$

$\bar{x}$ è il resto.

$[8]_3 = [5]_3 \qquad 8 \equiv 5 \mod (3)$

$\Updownarrow$

$[8]_3 = [5]_3$

ragioniamo con le classi perché è più facile ragionare con le uguaglianze rispetto alle congruenze.

$$x = y \ (n) \Leftrightarrow [x]_n = [y]_n \Leftrightarrow \bar{x} = \bar{y}$$

interi modulo n.

$$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z} \qquad \mathbb{Z}/(n) = \{ [x]_n \mid x \in \mathbb{Z} \}$$

insieme delle classi

es:

$$\mathbb{Z}/(3) = \{[0]_3, [1]_3, [2]_3, [3]_3, [9]_3 = [-1]_3, \infty\} =$$

$$\mathbb{Z}/(3) = \{[0]_3, [1]_3, [2]_3\}$$

$$\hookrightarrow = \{0, 1, 2\}$$

Addizione tra modulo n:

definizione:

$$[x]_n \oplus [y]_n = [x \oplus y]_n$$

$\oplus$: addizione tra classi

$\oplus$: addizione tra interi

es:

$$[5]_3 + [4]_3 = [9]_3 = [0]_3$$

moltiplicazione tra moduli n:

$$[x]_n \cdot [y]_n = [x \cdot y]_n$$

es:

$$[4]_5 \cdot [3]_5 = [12]_5 = [2]_5$$

$\equiv$

$$4 \cdot 3 \equiv 2 \mod(5)$$

sottrazione

$$[x]_n - [y]_n = [x - y]_n$$

es:

$$[2]_3 - [1]_3 = [1]_3$$

$$[1]_3 - [2]_3 = [-1]_3 = [2]_3$$

$-1+3$

DIVISIONE:

↳ non sempre è possibile farla

$[2]_5^{-1} = [3]_5$

$2 \cdot \boxed{\ } \equiv 1 \ (5)$

3

$x^{-1} \cdot x = 1$

esercizio:

$$x \equiv y \ (3)$$

ne segue che

$$2^x \equiv \quad (3) \quad ?$$

NO!

trovare un esempio che non funziona

$1 \equiv 4 \ (3)$

$2^1 \not\equiv 2^4 \ (3)$) non è vero!

$2 \not\equiv 16 \ (3)$

se operiamo solo con addizioni, sottrazioni e moltiplicazioni le congruenze possono essere considerate come uguaglianze

$$x \equiv y \ (n) \Rightarrow x - y = kn$$

$$\Downarrow \qquad n \mid x-y$$

$c + x \equiv y + c \ (n)$ n divide $(x-y)$

significa che

$(x+c)-(y+c)$ è multiplo di n?

questo perché "c" si sottrae.

es:

$x \equiv y \ (n)$

$\Downarrow$

$c \cdot x \equiv y \cdot c \ (n)$

ipotesi:

$\exists\, k \in \mathbb{Z}$ t.c. $x = y + nk$

$x \cdot c$ sostituisco

$\Leftrightarrow$ $c(y + nk) = y \cdot c + nkc$

nkc è un multiplo di n $\equiv$

possiamo concludere che

$x \cdot c \equiv y \cdot c \ (n)$

divisione:

$[2]_5^{-1} = [3]_5$ $\qquad [x]_n = \{x + nk \mid k \in \mathbb{Z}\}$

$[3]_5 \cdot [2]_5 = [6]_5 = [1]_5$

$\Downarrow$

$[3] = [2]_5^{-1} \Rightarrow 3 \cdot 2 \equiv 1 \ (5)$

esistano sempre questi inversi?

inverso di 3 modulo 6?

$3 \cdot x \equiv 1 \ (6)$ NO!

$[3]_6 \not\exists$

Se il numero è composto $\Rightarrow n = a \cdot b$ con $a, b \neq 1$

allora $a \cdot b \equiv 0 \ (n)$

→ nei reali non è possibile

es $2 \cdot 3 \equiv 0 \ (6)$ $\qquad 3 \cdot 5 \equiv 0 \ (15)$

Se $a \cdot b \equiv 0 \ (n) \Rightarrow [a]_n^{-1}$ non esiste

dimostrazione per assurdo

per assurdo

$\exists c$ t.c. $[\ ]_n = [a]_n^{-1}$

$[c]_n \cdot [a]_n^{-1} = [1]_n$

$c \cdot a \equiv 1 \ (n)$

sappiamo che $a \cdot b \equiv 0 \ (n)$

posso fare

$c \cdot a \cdot b \equiv 0 \cdot c \ (n)$

$1 \cdot b \equiv 0 \ (n)$

b non può essere (vuol dire che b non è multiplo)

$n = a \cdot b$

b non è multiplo di n.

i fattori di un numero non possono essere suoi multipli

se anche b fosse un multiplo

$b = n \cdot k$

$n = b \cdot a \quad \rightarrow \quad n = n \cdot k \cdot a \quad \Rightarrow \quad 1 = k \cdot a$

assurdo

esempio:

$\mathbb{Z}/(5)$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

c'è sempre un 1 tra le righe

↓

indicano gli inversi

$\mathbb{Z}/(4)$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ma l'inverso di 2 non c'è.

↓

non compaiono "1" nella sua riga.

(l'inverso di 3 c'è) ed è proprio 3

$\mathbb{Z}/(12)$

$[2]_{12}^{-1} = ?$ non esiste

$2X \equiv 1 \ (12)$

$2 \cdot 6 \equiv 1 (12)$ se $x \cdot 2 \equiv 1 (12)$

$x \cdot 2 \cdot 6 \equiv x \cdot 0 \ (12)$

assurdo.

2 è un fattore di 12 $\Rightarrow$ non ha inverso

3 è un fattore di 12 $\Rightarrow$ non ha inverso

5 non è un fattore di 12 $\Rightarrow$ ha un inverso $\quad 5 \cdot 5 = 25 \equiv 1 (12)$

8 non è un fattore di 12 ma è scomponibile in fattori di 12

$\Downarrow$ non ha inverso

$8 \cdot X \equiv 1 \ (12)$

$8 \cdot X - 1$ è multiplo di 12

non tutti pari

ma questo è un numero dispari

9 non è un fattore di 12 ma è scomponibile in fattori di 12

$\Downarrow$

non ha inverso.

Teorema:

I numeri che hanno inverso mod (n) sono quelli che non hanno fattori in comune con n.

Basta avere un solo fattore comune!

ALGEBRA lineare 7/03/2017

SOTTOSPAZIO vettoriale:

se V → spazio vettoriale su K (es $= \mathbb{R}$)

se $W \subseteq V$ è un sottospazio allora se

presa una combinazione lineare di vettori di W rimane in W

$$a_1 w_1 + a_2 w_2 + \dots + a_n w_n$$

$a_i \in K \quad w_i \in W$

es: $V = \mathbb{R}^2$

$$W = \{(x, y) \mid 2x + y = 0\} \subseteq \mathbb{R}^2$$

è un sottospazio?

- lo $\emptyset$ appartiene ✓
- se $(x_1, y_2) \in W$

  e $(x_2, y_2) \in W \Rightarrow (x_1 + x_2, y_1 + y_2) \in W$?

$$\begin{cases} 2x_1 + y_1 = 0 \\ 2x_2 + y_2 = 0 \end{cases}$$ ipotesi

$$2x_1 + 2x_2 + y_1 + y_2 = 0$$

$$2(x_1 + x_2) + (y_1 + y_2) = 0$$ quindi

è un SOTTOSPAZIO

- se $(x_1, y_1) \in W$

$\Rightarrow (ax_1 + ay_1) \in W$ SOTTOSPAZIO!

esempio:

$V = \mathbb{R}[x]$ spazio dei polinomi

se $P(x) \in \mathbb{R}[x] \Rightarrow P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$W = \{ P(x) \in V \mid P(1) = 0 \}$ → polinomi che valutati in 1 danno 0.

è un sottospazio?

1) chi è lo 0?

i polinomi con i coefficienti $a_i = 0$.

- $0 \in W$? $0(1) = 0$ ✓ lo 0 appartiene a W
- moltiplicazione tra scalari

$P(x) \in W$, $a \in \mathbb{R}$

$q(x) = aP(x) \in W$?

si perché se $P(1) = 0$

$3P(1) = 0$ $(aP(1) = 0)$ ✓

- somma tra vettori

$P(x), q(x) \in W \Rightarrow P(x) + q(x) \in W$?

$\begin{cases} P(1) = 0 \\ q(1) = 0 \end{cases}$ ipotesi

$(P+q)x = P(x) + q(x)$

$(P+q)(1) = P(1) + q(1) = 0 + 0$ ✓

→ lo $\emptyset \in W$

→ la somma $\in W$

→ la moltiplicazione $\in W$

⇒ W è un SOTTOSPAZIO.

W è un sottospazio se lo span $(W) = W$
(non aggiungo quindi uno spazio più grande).

$v_1, \dots, v_n \in V$ sono indipendenti

se $\forall a_1, \dots, a_n \in K$

$a_1 v_1 + \dots + a_n v_n = 0 \Rightarrow a_1, \dots, a_n = 0$

Teorema: Se $w \in \text{span}(v_1, \dots, v_n)$

e $v_1, \dots, v_n$ sono indipendenti

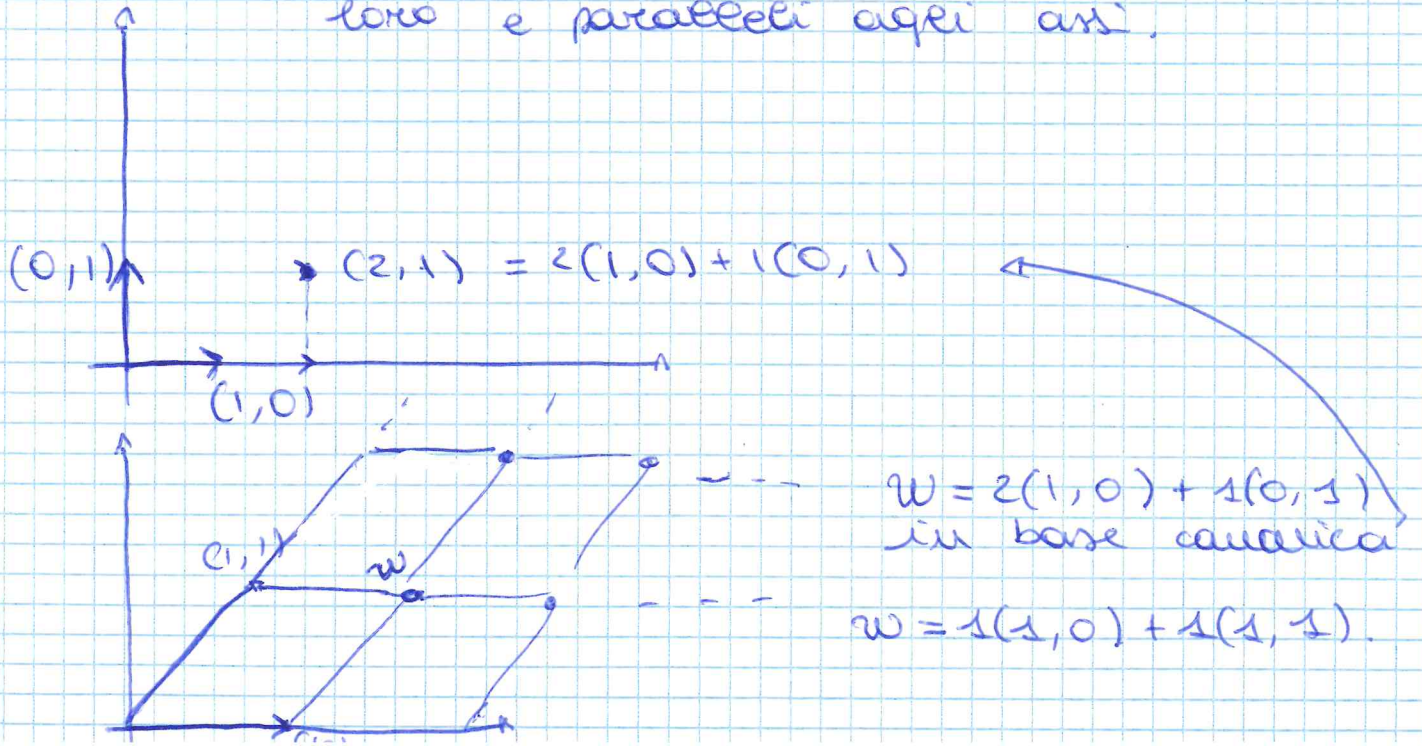
⇒ ∃! coefficienti $(a_1, \dots, a_n)$ → coordinate di w rispetto a $v_1, \dots, v_n$.

esistenza ✓ unicità

$w = a_1 v_1 + \dots + a_n v_n$.

es:

se prendo vettori perpendicolari tra loro e paralleli agli assi.



Base: V spazio vettoriale

$v_1, \dots, v_n \in V$

$v_1, \dots, v_n$ sono generanti se facendo

$$\text{span}(v_1, \dots, v_n) = V$$

sono una base di V se sono

- generanti
- indipendenti

} due caratteristiche per essere base.

es: $V = \mathbb{R}^3$

$v_1 = (1, 0, 0)$

$v_2 = (0, 1, 0)$ sono indipendenti ma non generanti.

↓

genero solo il piano.

$$\text{span}(v_1, v_2) = \{ a(1,0,0) + b(0,1,0) \}$$

$$(a, b, 0)$$

⇓

piano x, y.

es:

$(1,0,0)$
$(0,1,0)$
$(0,0,1)$ } base di $\mathbb{R}^3$

$v_1 = (1,0,0)$
$v_2 = (0,1,0)$
$v_3 = (0,0,1)$
$v_4 = (1,1,1)$ } sono generanti ma non indipendenti.

↓

$$v_4 = v_1 + v_2 + v_3$$

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

i coefficienti sono diversi da 0.

Teorema:

V è uno spazio con base.

Tutte le basi di V hanno lo stesso numero di elementi.

dimensione di V.

es: $\mathbb{R}^3$ ha dimensione 3

$(0,0,1)$
$(0,1,0)$
$(1,0,1)$

Può capitare una base infinita (come nei polinomi $\mathbb{R}[x]$).

Esercizio:

$V = \mathbb{R}^4$

$$\begin{bmatrix} 1 & 2 & 1 & 0 \\ 2 & 4 & 4 & 3 \end{bmatrix} \Rightarrow \begin{cases} x + 2y + z = 0 \\ 2x + 4y + 4z + 3t = 0 \end{cases} \quad (*)$$

$$W = \{(x,y,z,t) \mid (x,y,z,t) \text{ è soluzione di } (*)\}$$

è uno spazio vettoriale?
Trovare una base?

È un sistema omogeneo $\Rightarrow$ è un sottospazio di $\mathbb{R}^4$.

Trovo la base. Devo riuscire a generare lo spazio con il minor numero possibile di vettori.

Semplifico la matrice:

$$R_2 - 2R_1 \Rightarrow \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 0 & 2 & 3 \end{bmatrix}$$

matrice a scalini: ogni riga ha più 0 in partenza rispetto alla riga precedente.

risolvo il sistema:

t la scelgo libera

$$z_0 = -\frac{3}{2}t_0$$

y la scelgo libera

scelgo liberamente i valori delle variabili sulle colonne senza pivot.

$$y = y_0$$

$$x_0 = -2y_0 + \frac{3}{2}t_0$$

soluzioni
$$\begin{cases} x_0 = \frac{3}{2}t_0 - 2y_0 \\ t = t_0 \\ y = y_0 \\ z_0 = -\frac{3}{2}t_0 \end{cases}$$

$$\left(-2y_0 + \frac{3}{2}t_0,\ y_0,\ -\frac{3}{2}t_0,\ t_0\right)$$

$$\begin{pmatrix} \frac{3}{2}t_0 - 2y_0 \\ y_0 \\ -\frac{3}{2}t_0 \\ t_0 \end{pmatrix} =$$

$$= y_0 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t_0 \begin{pmatrix} 3/2 \\ 0 \\ 3/2 \\ 1 \end{pmatrix}$$

span dei due vettori colonna

$$\text{span}\left((-2,1,0,0),\ (3/2,0,3/2,1)\right)$$

soluzioni — vettori generanti

per vedere due vari indipendenti:

$$a\begin{pmatrix}-2\\1\\0\\0\end{pmatrix} + b\begin{pmatrix}3/2\\0\\-3/2\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$\Rightarrow a=0 \quad b=0$ (Vari indipendenti

allora dimensione $W=2$

—

v:

$v \in V$

$\{v\}$ è indipendente?

Si se $v \neq \bar{0}$

$(0,0)$ è dipendente

$$3\cdot(0,0) = (0,0)$$

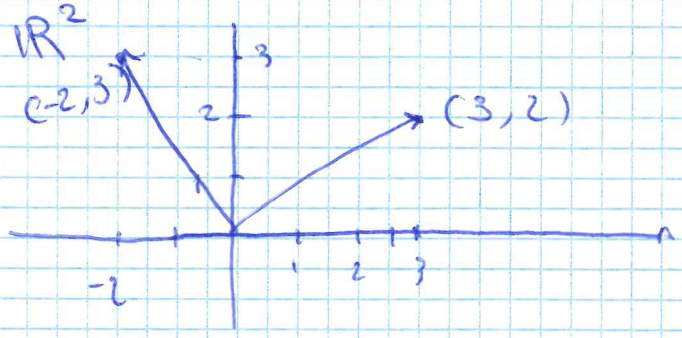
$(2,3) \in \mathbb{R}^2$ è indipendente

$$a(2,3) = (0,0)$$

$$a=0.$$

Vettori ortogonali:

es in $\mathbb{R}^2$



prodotto scalare di due vettori:

K campo $\quad V = K^n$

$$v = (a_1, a_2, \dots, a_n)$$
$$w = (b_1, b_2, \dots, b_n)$$

per moltiplicarli

$$v \cdot w = \langle v, w \rangle =$$

$$= a_1 \cdot b_1 + a_2 b_2 + \infty + a_n \cdot b_n$$

↓

ottengo uno scalare perché somma.

es $(-2, 3) \cdot (3, 2) = -6 + 6 = 0$

due vettori sono perpendicolari quando il loro prodotto vettoriale da come risultato $\emptyset$.

$v, w \in K^n$ sono ortogonali

se $v \cdot w = 0 \in K$.

es:

$$\begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 3/2 \\ 0 \\ -3/2 \\ 1 \end{pmatrix} = -3 + 0 + 0 + 0 \neq 0$$

ma è una base ortogonale.