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.

matematica discreta
8/03/2017

$\mathbb{Z}/(12)$ interi modulo 12 ⇒ alcuni hanno l'inverso.

$5 \cdot 5 \equiv 1 \ (12)$
$7 \cdot 7 \equiv 1 \ (12)$

$11 \equiv -1 \ (12) \quad (-1)(-1) \equiv 1 \ (12)$

$11 \cdot 11 \equiv 1 \ (12)$

$8 \cdot$ ↓ $\equiv 1 \ (12)$

ma c'è perché 8 ha un fattore in comune con 12.

Per assurdo

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

$8 = 4 \cdot 2 \qquad n = ?$

$4 \cdot 3 = 12 \equiv 0 \ (12)$

$$8 \cdot n \equiv 4 \cdot 2 \cdot n \ (12)$$

$$3 \cdot 8 \cdot n \equiv 3 \cdot 4 \cdot 2 \cdot n \ (12)$$

$$3 \cdot 8 \cdot n \equiv 0 \ (12)$$

non è soluzione

8 ha un fattore primo con 12 allora non ha inverso.

massimo comun divisore.

$$a, b \in \mathbb{Z}$$

$MCD(a,b) = (a,b) \qquad MCD(8,12) = 4$

↓

il più grande intero positivo che divide entrambi i numeri.

$MCD(-8, 12) = 4$

↳ il segno non influisce sul risultato di mcd.

$a \mid b \iff b$ è multiplo di a
$\iff a$ divide b
$\iff \exists k \in \mathbb{Z} \ . \ ak = b$

osservazione:

$mcd(0,0) = \nexists$ $\qquad$ 0 è un multiplo di tutti
$\Rightarrow$ il massimo non c'è.

$mcd(0,4) = 4$

Se a e b non hanno fattori comuni allora

$mcd(a,b) = 1$ → quindi minimo.

$mcd(5,12) = 1$

teorema:

se $mcd(a,b) = 1 \Rightarrow$ a ha un inverso modulo b.

$\exists x \quad a(x) \equiv 1 (b)$.

es:

$$mcd(2^3 \cdot 3^5 \cdot 7^{21}, 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^{30}) =$$

$$= 2^2 \cdot 3^2 \cdot 7^{21}$$

↓ calcolando la fattorizzazione in primi.

$$a = \prod_{i=1}^{k} p_i^{x_i} \qquad p_i = \text{primi.}$$

$$b = \prod_{i=1}^{k} p_i^{y_i}$$

$$(a,b) = \prod_{i=1}^{k} p_i^{\min(x_i, y_i)}$$

regola inefficiente se i numeri sono grandi

~~metodo più veloce~~:

- a è primo se $a > 1$ $\quad a \in \mathbb{Z}$ e gli unici divisori positivi sono a e 1.

teorema

ogni numero intero $\neq 0$ si fattorizza in primi.

$\exists$ dei primi p_i e degli esponenti x_i, k

$$a = \prod_{i}^{k} p_i^{x_i}$$

dimostrazione con induzione forte e principio del minimo.

$P(a) \equiv$ a si può scomporre in primi.

dimostro $P(a)$ supponendo vere i casi precedenti } PASSO.

prendiamoli TUTTI

vera $P(2), P(3), \dots, P(a-1)$.

distinguo 2 casi

1) a è primo.

allora anche che vale $P(a)$.

2) a non è primo.

$\exists b, c \neq 1$ t.c. $a = b \cdot c$

$1 < b, c < a$

per ipotesi induttiva

b si scompone perché $b < a$

c " " " $c < a$

mettendo insieme le due scomposizioni ottengo a.

$$b = \prod_{i=0}^{k} p_i^{x_i} \qquad c = \prod_{i=0}^{k} p_i^{y_i}$$

$$a = \prod_{i=0}^{k} p_i^{x_i + y_i}$$

per dimostrare ~~il~~

P(60) devo sapere

$60 = 6 \cdot 10$ vero

P(6) e P(10)

$6 = 2 \cdot 3$ vero

$10 = 2 \cdot 5$ vero

$P(2) \wedge P(3)$ vero vero

$P(2) \wedge P(5)$ vero vero

i casi base

sono TUTTI i numeri primi (infiniti)

Principio del minimo:

voglio dimostrare P(a).

Per assurdo: prendo il minimo a

che mai si scampa

caso 1) a è primo

⇓

assurdo

caso 2) a non è primo ⇒ ci sono numeri b, c t.c.

P(b) e P(c) sono veri

perché a era il minimo che non si scampava.

Visto che b e c si scampano, si scampa anche $a = b \cdot c$.

⇓

raggiungo l'assurdo.

Tutti i numeri si scampano.

Teorema (Euclide)

Esistono infiniti numeri primi.

dim. Per assurdo ne esistano un numero finito, diciamo

$$p_0, p_1, \dots p_k$$

$p_k! + 1 = n$ e n è primo ho un assurdo $n > p_k$

$p_k! + 1 = n$ n si scompone in primi

$\Rightarrow \exists q$ primo t.c. $q \mid n$

$\Rightarrow p_0 \le q \le p_k$

dimostro che q non può essere p_i.

Se $q = p_i \le p_k \Rightarrow p_i \mid p_k!$

$\boxed{a \le b \Rightarrow a \mid b!}$

$\boxed{\text{se } a \mid b \Rightarrow a \nmid b+1}$ (non divide)

$q \nmid (p_k! + 1) = n$

quindi assurdo. (n è lo nostro numero).

es:

$101! + 1 = n$

$q \mid n$

primo $q > 101 \Rightarrow$ ci sono infiniti primi.

per calcolare il M.C.D in modo efficiente:

$$(a, b) = (a + kb, b)$$ algoritmo di euclide.

es:

$MCD(252, 198)$

$252 = 198 + 54$

$252 = 252 - 198 = 54$

252	198
54	1

$MCD(54, 198)$

198	54
36	3

SOSTITUISCO CON IL RESTO DELLA DIVISIONE

↓

"tolgo da un numero i multipli dell'altro"

$MCD(54, 36)$

54	36
18	1

$MCD(18, 36) = 18.$

$MCD(a, 0) = a \quad a \neq 0$

"caso base"

dimostrazione del teorema:

$$MCD(a, b) = MCD(a + kb, b)$$

dimostro che un intero $x \mid a$ e b

x è uno se x divide $a + kb, b$

supponiamo $x \mid a$ e $x \mid b$

$x \mid a + kb$?

$b = x \cdot m$

$a = x \cdot \ell$

$\Rightarrow \exists \ell, m.$

$$a + kb = x \cdot \ell + k \cdot x \cdot m$$
$$= x(\ell + km) \rightarrow \text{sempre un multiplo}$$
$$x \mid a + kb.$$

viceversa:

x $x \mid a+kb$ $x \mid b$ ne deduco che $x \mid a$ $\rightarrow$ $x \mid b$ ovvio.

$$\begin{cases} a+kb = x \cdot m \\ b = x \cdot \ell \end{cases} \qquad a = x \cdot m - k \cdot x \cdot \ell$$

$$a = x(m - k\ell)$$

multiplo

$x \mid a$ ✓

Teorema di Bezout.

$mcd(a,b)$ è una combinazione lineare di a e b.

cioè $\exists\, \alpha, \beta \in \mathbb{Z}$ t.c. $mcd(a,b) = \alpha \cdot a + \beta \cdot b$.

es: $(252, 198) = 18 = \boxed{\cdot} \cdot 252 + \boxed{\cdot} \cdot 198$

$(252, 198) = (54, 198) = (54, 36) = (18, 36)$

$= (18, 0)$

$252 = \boxed{1} \cdot 252 + 198 \cdot \boxed{0}$

$198 = \boxed{0}\, 252 + \boxed{1}\, 198$

riempiamo i box dall'alto in basso.

$252 - 198 = 54 = \boxed{1}\, 252 + \boxed{-1}\, 198$

$198 - 3 \cdot 54 = 36 = \boxed{-3}\, 252 + \boxed{4}\, 198$

$54 - 36 = 18 = \boxed{4}\, 252 + \boxed{-5}\, 198$

Equazioni Diofantea

$(-5) \cdot 198 \equiv 18 \bmod 252$

$4\, 252 \equiv 18 \bmod 198$

} perdiamo l'informazione del multiplo per arrivare a 18.

Dati $n, a, b \in \mathbb{Z}$. Trovare $x, y \in \mathbb{Z}$

$n = ax + by$ $\Rightarrow$ soluzioni interi $\Rightarrow$ equazione Diofantea

eq. diofantea

$$18 = 258x + 198y$$

soluzione $\begin{cases} x = 4 \\ y = -5 \end{cases}$

↳ ottenuto tramite l'algoritmo di Bezout.

es: risolvere

$$36 = 252x' + 198y'.$$

$18 = 252 \cdot 4 + 198 \cdot (-5)$

moltiplico per 2

$$36 = 252 \cdot 8 + 198 (-10).$$

Se no risolvere

$n = a \cdot x + b y$ $\quad$ x, y ricavate n, a, b, note

so fare

$$kn = ax' + by'$$

$$\begin{cases} x' = x \cdot k \\ y' = y \cdot k \end{cases}$$

ALGEBRA lineare 8/03/2017

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

sottospazi $A, B \subseteq V$

✓ $A \cap B$

x $A \cup B$ sottospazi?

es: $V = \mathbb{R}^2$ $\quad A = \{(x, y) \mid 3x - y = 0\}$ ↗ sottospazio ✓

$B = \{(x, y) \mid x - y = 0\}$ ↘ sottospazio

$A \cap B = \{\bar{0}\}$ → è un sottospazio.

$A \cup B$ ma è un sottospazio.

↳ devo fare $A + B = \{ v_1 + v_2 \mid v_1 \in A, v_2 \in B \}$

è un sottospazio.

ma lo è perché se faccio la somma dei due vettori esco fuori dall'unione di questi.

$A + B$ è un sottospazio?

Teorema

$A + B$ è un SOTTOSPAZIO.

$w \in A + B$

$a \in K \quad aw \in A + B$

$w = v_1 + v_2 \quad v_1 \in A \quad v_2 \in B$

$aw = av_1 + av_2$

$av_1 \in A$ perché era un sottospazio

$av_2 \in B$ perché è un sottospazio

$\Rightarrow aw \in A + B.$

ovviamente

$0 = \bar{0} + \bar{0} \in A + B$

$w_1 \in A + B \quad e \quad w_2 \in A + B$

allora $w_1 + w_2 \in A + B$

$v_1 + v_2 \in A \quad v_2 \in B$

$\bar{v}_1 + \bar{v}_2 \quad \bar{v}_1 \in A \quad \bar{v}_2 \in B$

$w_1 + w_2 = (v_1 + \bar{v}_1) + (v_2 + \bar{v}_2)$

$(v_1 + \bar{v}_1) \in A \quad (v_2 + \bar{v}_2) \in B$

$\Rightarrow \in A + B.$

es: $V = \mathbb{R}^4$

$v_1 = (1, 3, 7, 5)$

$v_2 = (0, 4, 3, 2)$

$v_3 = (0, 0, 0, 4)$

sono <u>indipendenti</u>!

Se messi in una matrice questa è a scalini.

$$a_1 v_1 + a_2 v_2 + a_2 v_3 = \bar{0} \quad (*)$$

sostituisco

$$a_1(1, 3, 7, 5) + a_2(0, 4, 3, 2) + a_3(0, 0, 0, 4) = \bar{0}$$

$a_1 \cdot 1 = 0$ per forza

$a_1 = 0$

l'equazione (*) diventa $a_2 v_2 + a_3 v_3 = \bar{0}$

cioè:

$$a_2(0, 4, 3, 2) + a_3(0, 0, 0, 4) = (0, 0, 0, 0)$$

$$(0, 4a_2, ?, ?) = (0, 0, 0, 0)$$

$\downarrow$

$a_2 = 0$

(*) diventa

$a_3 v_3 = \bar{0}$ $\quad a_3(0, 0, 0, 4) = (0, 0, 0, 0)$

$4 \cdot a_3 = 0$

$$\begin{cases} a_3 = 0 \\ a_2 = 0 \\ a_1 = 0 \end{cases}$$

Se ho dei vettori in $\mathbb{R}^n$, che sistemate in una matrice, le cui componenti formano la matrice a scalini $\Rightarrow$ sono indipendenti.

es: Trovare una base di $V \subseteq \mathbb{R}^4$

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

$v_1 = (1, 3, 7, 5)$

$v_2 = (0, 4, 3, 2)$

$v_3 = (1, 7, 10, 7)$

creo la matrice e riduco a scalini

lo $\text{span}(v_1, v_2, v_3) = \text{span}(v_1, v_2, v_3 - kv_1)$.

$$\begin{bmatrix} 1 & 3 & 7 & 5 \\ 0 & 4 & 3 & 2 \\ 1 & 7 & 10 & 7 \end{bmatrix} \xrightarrow{R_3 - R_1} \begin{bmatrix} 1 & 3 & 7 & 5 \\ 0 & 4 & 3 & 2 \\ 0 & 4 & 3 & 2 \end{bmatrix} \xrightarrow{R_3 - R_2}$$

$$\begin{bmatrix} 1 & 3 & 7 & 5 \\ 0 & 4 & 3 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} w_1 \\ w_2 \end{matrix}$$

una carta come vettore

$\text{span}(v_1, v_2, v_3) = \text{span}(w_1, w_2)$.

la base diventa v_1, v_2

Calcolare la dimensione della somma:

$A = \text{span}((1, 3, 7, 5), (0, 4, 3, 2)) \subset \mathbb{R}^4$

$B = \text{span}((1, 7, 10, 7))$

$A + B = \text{span}(v_1, v_2, v_3)$

↳ la somma è lo span di tutti i vettori, quando A e B sono span.

la dimensione è 2.

[L'intersezione di due piani è una retta.]

Passare dallo span al sistema.

$$V = \text{span}\left(\begin{pmatrix}1\\2\\3\\-1\\2\end{pmatrix}, \begin{pmatrix}2\\4\\7\\2\\-1\end{pmatrix}\right) \subseteq \mathbb{R}^5$$

ci sono 2 vettori
⇓
dimensione 2
⇓
per ogni equazione a sistema diminuisce la dimensione di $\mathbb{R}$

V = soluzioni di un sistema.

dovrò avere 3 equazioni a sistema ⟸

$$\mathbb{R}^{5-1-1-1} = \mathbb{R}^2$$

$$\begin{pmatrix}b_1\\b_2\\b_3\\b_4\\b_5\end{pmatrix}$$

↳ per definizione appartiene allo span

se $\exists\, x, y \in \mathbb{R}$

$$\begin{pmatrix}b_1\\b_2\\b_3\\b_4\\b_5\end{pmatrix} = x\begin{pmatrix}1\\2\\3\\-1\\2\end{pmatrix} + y\begin{pmatrix}2\\4\\7\\2\\-1\end{pmatrix}$$

se $\exists\, x, y$

$$\Longleftrightarrow \begin{cases} x + 2y = b_1 \\ 2x + 4y = b_2 \\ 3x + 7y = b_3 \\ -x + 2y = b_4 \\ 2x - y = b_5 \end{cases}$$

$$\left[\begin{array}{cc|c} 1 & 2 & b_1 \\ 2 & 4 & b_2 \\ 3 & 7 & b_3 \\ -1 & 2 & b_4 \\ 2 & -1 & b_5 \end{array}\right]$$

ha soluzioni?

un sistema ha soluzione se il rango della matrice ridotta = al rango della matrice aggiunta.

$$\left[\begin{array}{cc|c} 1 & 2 & b_1 \\ 2 & 4 & b_2 \\ 3 & 7 & b_3 \\ -1 & 2 & b_4 \\ 2 & -1 & b_5 \end{array}\right] \begin{array}{l} R_5-2R_1 \\ R_2-2R_1 \\ \longrightarrow \\ R_3-3R_1 \\ R_4+R_1 \end{array} \left[\begin{array}{cc|c} 1 & 2 & b_1 \\ 0 & 0 & b_2-2b_1 \\ 0 & 1 & b_3-3b_1 \\ 0 & 4 & b_4+b_1 \\ 0 & -5 & b_5-2b_1 \end{array}\right] \begin{array}{l} R_4-4R_3 \\ \longrightarrow \\ R_5+5R_3 \end{array}$$

$$\left[\begin{array}{cc|c} 1 & 2 & b_1 \\ 0 & 0 & b_2-2b_1 \\ 0 & 1 & b_3-3b_1 \\ 0 & 0 & b_4+b_1-4(b_3-3b_1) \\ 0 & 0 & b_5-2b_1+5(b_3-3b_1) \end{array}\right]$$

$$\left[\begin{array}{cc|c} 1 & 2 & b_1 \\ 0 & 0 & b_2-2b_1 \\ 0 & 1 & b_3-b_1 \\ 0 & 0 & 13b_1-4b_3+b_4 \\ 0 & 0 & b_5-17b_1+5b_3 \end{array}\right] \begin{array}{l} \longrightarrow =0 \\ \\ \\ \longrightarrow =0 \\ \longrightarrow =0 \end{array}$$

così che dopo la barra non ci siano più scalini rispetto a quelli prima.

$$\begin{cases} b_2-2b_1=0 \\ 13b_1-4b_3+b_4=0 \\ b_5-17b_1+5b_3=0 \end{cases}$$

→ mettere in matrice e ridurre a scalini

↳ sistema che viene fuori dallo SPAN.

Applicazione lineare (funzione)

$f: V \to W$

spazio vettoriale → spazio vettoriale su K.

f è lineare se:

1) $f(a \cdot v) = a \cdot f(v) \quad a \in K \quad v \in V$
2) $f(v_1+v_2) = f(v_1)+f(v_2)$
3) $f(\bar{0}) = \bar{0}$

$f(a_1v_1+\dots+a_nv_n) = a_1f(v_1)+a_2f(v_2)+\dots+a_nf(v_n)$