es: $K = \mathbb{R}$ $V = \mathbb{R}$ $W = \mathbb{R}$

$f: V \to W \Rightarrow f: \mathbb{R} \to \mathbb{R}$

$f(x) = x^2$ è lineare?

- $f(0) = 0$ ✓
- $f(2) = 4 \Rightarrow f(1+1) = f(1) + f(1) = 2$

$4 \neq 2$ ✗

$\Downarrow$

non è lineare

es:

$f: \mathbb{R} \to \mathbb{R}$ $f(x) = 3x$

è lineare:

- $f(0) = 0$ ✓
- $f(x+y) = f(x) + f(y)$

$\Downarrow$ $\Downarrow$

$3(x+y) = 3x + 3y$ ✓

- $f(a \cdot x) = a \cdot f(x)$

$\Downarrow$ $\Downarrow$ $\Rightarrow$ è lineare

$3xa = 3 \cdot ax$ ✓

Teorema

- Applicazioni lineari sono della forma:

$f(x) = a \cdot x$ per $f: \mathbb{R} \to \mathbb{R}$

- Se conosco $f(1)$ allora so anche come è fatta $f(x)$

es: $f(1) = 3 \Rightarrow f(x) = f(x \cdot 1) = x \cdot f(1) =$

$= 3x$

$\dim_{\mathbb{R}}(\mathbb{R}) = 1$ 1 è la base di $\mathbb{R}$ su $\mathbb{R}$

Teorema:

$f: V \to W$ spazi su $K = \mathbb{R}$
lineare

Se so che $v_1, \dots, v_n$ base di V conosco

$f(v_1) = w_1, \dots, f(v_n) = w_n \in W$

conosco $f(v)$ $\forall v \in V$.

dimostrazione:

$v \in V$ scrivo $v = a_1 v_1 + \dots + a_n v_n$
con $a_1, \dots, a_n$ unici

$f(v) = f(a_1 v_1) + \dots + f(a_n v_n)$

f è lineare
$\Downarrow$

$f(v) = a_1 f(v_1) + \dots + a_n f(v_n)$

$f(v_1), \dots, f(v_n)$ li conosco.

Matematica discreta 9/03/2017
interi modulo n.

$\mathbb{Z}/(n)$ se abbiamo $y, x \in \mathbb{Z}$

$x \equiv y \ (n) \iff n \mid x - y$

$\Updownarrow$

$[x]_n = [y]_n$

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

$= \{ \underbrace{x + kn}_{y} \mid k \in \mathbb{Z} \}$

es:

$[3]_5 = \{ 3 + 5k \mid k \in \mathbb{Z} \}$

- se $x \equiv y \ (n)$ e $y \equiv z \ (n)$

$\Rightarrow x \equiv z \ (n)$ valida la proprietà transitiva

dimostrazione:

$$x = y + kn \qquad \Rightarrow \qquad x = z + \ell n + kn$$

$$y = z + \ell n \qquad\qquad x = z + n(\ell + k)$$

$$\Rightarrow x \equiv z \ (n)$$

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

- relazione di equivalenza:

relazione binaria che gode delle proprietà:

- transitiva
- simmetrica
- riflessiva

Possiamo fare delle classi che godono di relazioni di equivalenza.

$$[3]_5 = \{ y \mid y \equiv 3 \ (5) \}$$

$$[3]_5 = [8]_5$$

tutta la classe di 3 = a tutta la classe di 8.

$$[3]_5 \cap [4]_5 = \emptyset$$

mai si possono sovrapporre le classi (solo per una parte).

[le classi ci aiutano ad astrarre dei concetti concreti]

- dire che $x \equiv y \ (n)$ equivale $[x]_n = [y]_n$

Quante classi ci sono mod(5)?

5: $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$

(poi si ricomincia da $\emptyset$)

mod(2)? 2

n° pari $[0]_2$

n° dispari $[1]_2$

Se $\begin{array}{r|l} x & \underline{y} \\ r & q \end{array}$ $\qquad x = y \cdot q + r \Rightarrow x \equiv r\,(y)$

ogni numero è congruo al suo resto

$\Downarrow$

ci sono tante classi quanti i resti possibili delle divisioni per y

es:

$\begin{array}{r|l} x & \underline{5} \\ 4 & q \end{array}$ e $\begin{array}{r|l} y & \underline{5} \\ 4 & q' \end{array}$

sicuramente $x \equiv y\,(5)$

$x = 5q + 4 \qquad y = 5q' + 4$

$x - y = 5q - 5q'$

$x - y = 5\underbrace{(q - q')}_{\text{multiplo}}$

$x \equiv y\,(5)$.

Viceversa:

se $x \equiv y\,(5)$ $\qquad \begin{array}{r|l} x & \underline{5} \\ r & q \end{array} \qquad \begin{array}{r|l} x & \underline{5} \\ r' & q' \end{array}$

sicuramente $r = r'$ perché congrui.

$x \equiv y \ (5)$ allora $x = y + K5$

$$\begin{array}{c|l} y & 5 \\ \hline r & q \end{array} \qquad\qquad \begin{array}{c|l} x & 5 \\ \hline r & q+K \end{array}$$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$y = 5q + r$

$x = y + 5K$

sostituisco

$x = 5q + r + 5K$

$x = 5(q+K) + r$

essere congrui vuol dire avere lo stesso resto

- Se $x \equiv x' \ (n)$, $y \equiv y' \ (n)$

  allora $x + y = x' + y' \ (n)$

- Se $x \equiv x' \ (n) \not\Rightarrow 2^x \equiv 2^{x'} \ (n)$

  la somma, moltiplicazione funzionano

  l' ESPONENZIAZIONE non funziona

- $x \equiv x' (n) \quad y \equiv y' (n)$

  $\Rightarrow x \cdot y \equiv y' x' \ (n)$.

Grazie alla somma e alla moltiplicazione:

rappresentante di classe $[x]_n + [y]_n = [x+y]_n$

es: $[3]_5 + [4]_5 = [7]_5 = [2]_5$

$3 + 4 \equiv 2 \ (5)$

Teorema di Bezout.

$$\underset{\Downarrow\atop 1}{\mathrm{mcd}(98,11)} = \underbrace{\boxed{}\cdot 98 + \boxed{}\cdot 11}_{\text{combinazione lineare}}$$

$$\mathrm{mcd}(98,11) = \mathrm{mcd}(10,11) \xrightarrow{11-10} = \mathrm{mcd}(10,1)$$

$\hookrightarrow 98 - \underset{\Downarrow\atop 8\cdot 11}{88} = 10$

$= \mathrm{mcd}(0,1) = 1$ $10-(10\cdot 1)$

$$
\begin{array}{lll}
 & 98 & = \boxed{1}\,98 + \boxed{0}\,11 \\
 & 11 & = \boxed{0}\,98 + \boxed{1}\,11 \\
R_1 - 8R_2 & 10 & = \boxed{1}\,98 + \boxed{-8}\,11 \\
R_2 - R_1 & 1 & = \boxed{-1}\,98 + \boxed{9}\,11
\end{array}
$$

$m = ax + by$

mcd.

es:

$33 = 98\boxed{} + \boxed{}\,11$

$= 33\cdot 1 = 33\left(98(-1) + 11(9)\right)$

$3 = 33(-98) + 99\cdot 33$

possiamo risolvere:

$\underbrace{6x}_{\text{multiplo di }3} + \underbrace{21y}_{\text{multiplo di }3} = 4$ → non multiplo di 3

$\Downarrow$

non è possibile.

Teorema

Se n non è multiplo di $d = \mathrm{mcd}(a,b)$
allora l'equazione
$n = ax + by$ non ha soluzioni in $\mathbb{Z}$

dimostrazione:

ax multiplo di d

by " di d.

$ax + by$ multiplo di d

ma n non è multiplo di d

quindi $n \neq ax + by$ per qualunque x, y.

es:

$$1 = \boxed{-1} \cdot 98 + \boxed{9} \cdot 11$$

$$1 = \boxed{-1+11}\, 98 + \boxed{9-98}\, 11$$

$$1 = \boxed{-1+k11}\, 98 + \boxed{9-k98}\, 11$$

in generale:

$n = ax_0 + by_0$ per non far cambiare il risultato

$$n = a(x_0 + kb) + b(y_0 - ka)$$

es:

$$(252, 198) \underset{252-198=54}{=} (54, 198) \underset{198-3\cdot 54=36}{=} (54, 36) \underset{54-36=18}{=}$$

$$= (18, 36) \underset{36-2\cdot 18=0}{=} (18, 0) = 18$$

$$252 = 1 \cdot 252 + 0 \cdot 198$$

$$198 = 0 \cdot 252 + 1 \cdot 198$$

$$54 = 1 \cdot 252 + -1 \cdot 198$$

$$36 = -3 \cdot 258 + 4 \cdot 198$$

$$18 = 4 \cdot 258 + -5 \cdot 198$$

equazione diofantea.

$$18 = x \cdot 252 + y \cdot 198$$

$x_0 = 4$

$y = -5$

Quante soluzioni abbiamo?

$$\begin{cases} x = 4 + k198 \\ y = -5 - k252 \end{cases}$$ sono tutte le soluzioni? NO

altre soluzioni:

- dividere l'equazione per il massimo possibile

$$18 = 252x + 198y$$

$$\Updownarrow$$

$$1 = 14x + 11y \qquad 1 = 14 \cdot 4 - 5 \cdot 11$$

↳ così le soluzioni sono più "fitte"

$$\begin{cases} \text{le } x \text{ si aumentano di } 11 \\ \text{le } y \text{ si diminuiscono di } 14 \end{cases}$$

$$1 = 14 \cdot (4 + k11) + 11 \cdot (-5 - k14)$$

$$\begin{cases} x' = 4 + 11 = 15 \\ y' = -5 - 14 = -19 \end{cases}$$ così le ho trovate tutte

teorema

$a \in \mathbb{Z}$ è invertibile modulo n allora $(a, n) = 1$

Def. a invertibile modulo n vuol dire che

$$\exists b \quad a \cdot b \equiv 1 (n)$$

(il resto di $a \cdot b$ diviso $n = 1$).

es:

11 è invertibile mod (14)?

$11 \cdot y \equiv 1 (14)$ si!

$\Rightarrow \exists x : 11y + 14x = 1$?

Teorema dimostrazione:
se a, n non hanno fattori comuni
$\Rightarrow$ posso risolvere

$$ax \equiv 1 \mod(n)$$ (esiste l'inverso)

dim:

$$1 = mcd(a, n)$$

Bezout:
$\exists x, y \in \mathbb{Z}$ $1 = ax + by$

trovati x_0, y_0

osservo che $1 = ax_0 + by_0$ $b = n$

$$1 \equiv ax_0 \mod(n).$$ $\square$ fine dimostrazione

es:

$$4x \equiv 7 \ (9)$$

Trovare $\underline{x}$ $\rightarrow$ l'inverso di $4 \mod(9)$

1) calcolare il $mcd(4, 9)$
con euclide.

$$(4,9) = (4,1) = (0,1) = 1$$
$-2 \cdot 4$

$$9 = 1 \cdot 9 + 0 \cdot 4$$
$$4 = 0 \cdot 9 + 1 \cdot 4$$
$$1 = 1 \ 9 + (-2) 4$$

trasformiamo in una congruenza $\mod(9)$

$$1 \equiv -2 \cdot 4 \ (9)$$

$$-2 \equiv 7 \mod(9)$$

l'inverso di $4 = \underline{\underline{7}} \mod(9)$

$$x \cdot \underbrace{4 \cdot 7}_{1} \equiv 7 \cdot 7 \mod(9)$$

$$x \equiv \underbrace{49}_{} \mod(9)$$
$$\equiv 4 \mod(9)$$

$x \equiv 4 \mod(9)$

es: $3X \equiv 7 \mod (9)$

$\exists x$? mai è risolubile.

$\exists k$ t.c. $3x = 7 + 9 \cdot k$

$7 = \underbrace{3x - 9k}_{\text{multipli di } 3}$

non multiplo di 3

teorema

$ax \equiv b \ (n)$ ha soluzione

se il $mcd(a, n)$ divide anche b.

ALGEBRA lineare 14/03/2017

$f: V \to W$ lineare $\Rightarrow$ dominio e codominio sono spazi vettoriali su K

$\Downarrow$

- $f(v_1 + v_2) = f(v_1) + f(v_2)$
- $f(a \cdot v_1) = a \cdot f(v_1)$

es:

$f: \mathbb{R} \to \mathbb{R}$ $\quad f(x) = 3X$ lineare

$g(x) = 3^x$ non lineare

$\hookrightarrow 3^{x+y} \neq 3^x + 3^y$

associare ad una funzione lineare una matrice

$f(x) = 3x \Rightarrow [3]$

se ho una base di V $\underbrace{v_1, \ldots, v_n}$

sono indipendenti

V è lo span di $v_1, \ldots, v_n$

base di W $w_1, \ldots, w_m$

n = dimensione di V

m = " di W

Fissate le basi posso associare una matrice

f lineare, gli associo una matrice:

$$[f]^{v_1,\dots,v_n}_{w_1,\dots,w_m}$$ matrice di numeri

$$= \begin{bmatrix} & a_{1i} & \\ & a_{2i} & \\ & \vdots & \\ & a_{mi} & a_{mn} \end{bmatrix}$$

a_{mi} ↓ colonna i

(m) dimensione dello spazio di arrivo → RIGHE

(n) → colonne

Quali numeri ci vanno?

Calcolo la f nell'i-esimo vettore della base di partenza

$$f(v_i) = \boxed{}\, w_1 + \dots + \boxed{}\, w_m$$

$\in W = \text{span}(w_1, \dots, w_m)$

i numeri della combinazione lineare sono i numeri da introdurre nella colonna i-esima della matrice

es:

$$f: \mathbb{R}^2 \to \mathbb{R}^3$$

$$f(x,y) = (x+2y,\ 2x+4y,\ x+5y)$$

$$f(1,0) = (1, 2, 1)$$

$$f(0,1) = (2, 4, 5)$$

1) È lineare? si

preso un altro vettore

somma interna:

$$f((x,y)+(x',y')) = f((x+x'),(y+y')) =$$

$$= ((x+x')+2(y+y'),\ 2(x+x')+4(y+y'),\ x+x'+5(y+y'))$$

somma dopo la f:

$$= f(x,y) + f(x',y') = (x+2y,\ 2x+4y,\ x+5y) +$$

$$+ (x'+2y',\ 2x'+4y',\ x'+5y')$$

somma interna = somma dopo la f.

matrice da associare:

1) cerco le basi $\left\langle\begin{array}{l}\text{partenza}\\ \\ \text{arrivo}\end{array}\right.$

base di $\mathbb{R}^2$

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

base di $\mathbb{R}^3$ $\quad (1,0,0),\ (0,1,0)\ ,\ (0,0,1)$ $\Big\}$ basi canoniche

$$[f]^{\text{canonica } \mathbb{R}^2}_{\text{canonica } \mathbb{R}^3} =$$

$f(1,0) = (1,2,1) \longrightarrow$ devo scriverlo come combinazione di W

$$= 1\cdot(1,0,0) + 2(0,1,0) + 1(0,0,1)$$

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \\ 1 & 5 \end{bmatrix} = [f]$$ matrice 3×2

$$f(0,1) = (2,4,5) = 2(1,0,0) + 4(0,1,0) + 5(0,0,1)$$

altro metodo: scrivo f in un'altra forma:

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2y \\ 2x+4y \\ x+5y \end{pmatrix} = x\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + y\begin{pmatrix} 2 \\ 4 \\ 5 \end{pmatrix}$$

divido i contributi x, y

coefficienti della matrice.

Definizione di

prodotto matrice $m\times n$ per vettore colonna $n\times 1$
il risultato è un vettore $m\times 1$.

es.: $$\begin{bmatrix} 1 & 2 \\ 2 & 4 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x+2y \\ 2x+4y \\ x+5y \end{bmatrix}$$

es:

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

$$W = \mathbb{R}[x]^{\leq 2}$$

$d : V \to W$ $\qquad d(ax^2+bx+c) = 2ax+b$

$\frac{d}{dt}$

è lineare? si

$$d\big((ax^2+bx+c)+(a'x^2+b'x+c')\big) =$$

somma interna

$$d\big((a+a')x^2+(b+b')x+c+c'\big) =$$
$$= 2(a+a')x+(b+b')$$

prima deriv.

$$d(ax^2+bx+c) + d(a'x^2+b'x+c') =$$
$$= 2ax+b+2a'x+b+b'$$

=

$$d\big((ax^2+bx+c)\cdot e\big) = d(aex^2+bex+ce)$$
$$= 2aex+be$$
$$\Updownarrow$$
$$e\cdot d(ax^2+bx+c) = e(2ax+b) = 2aex+be$$

=

[matrice associata] $\qquad [d]$

- cerco la base:

x^2, x, 1 } 3 polinomi (vettori di V) $\to$ sono una base

$\downarrow$

verifico:

dato un polinomio qualunque in V voglio ottenerlo come combinazione delle basi

$$p(x) = ax^2+bx+c$$

$$a\cdot x^2 + b\cdot x + c\cdot 1 \quad \checkmark$$

generano $\boxed{\text{si}}$

indipendenti?

vettore $\vec{0}$

$$ax^2+bx+c = 0x^2+0x+0$$

$\boxed{\text{si}}$ $\leftarrow$ unica possibilità $a, c, b = 0$

$v_1 = x^2 \qquad v_2 = x \qquad v_3 = 1.$

$$[D]^{x^2,x,1}_{x^2,x,1} \qquad 3\times 3$$

prima colonna : applico al primo vettore della base

$$D(v_1) = D(x^2) = 2x$$

$$2x = \underbrace{\boxed{0}\,x^2 + \boxed{2}\,x + \boxed{0}\,1}_{\text{base di arrivo}}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = [D]$$

$$D(v_2) = D(x) = 1$$

$$1 = \boxed{0}\,x^2 + \boxed{0}\,x + \boxed{1}\,1$$

$$D(v_3) = D(1) = 0$$

$$0 = \boxed{0}\,x^2 + \boxed{0}\,x + \boxed{0}\,1$$

La matrice applicata alle coordinate dell' input fornisce le coordinate dell'output.

es:

$$D(\underbrace{3x^2+5x+2}_{\text{INPUT}}) = \underbrace{6x+5}_{\text{OUTPUT}}$$

coordinate:

$$[D]\cdot\begin{pmatrix} 3 \\ 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ 5 \end{pmatrix}$$

verifica:

$$\begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 5 \\ 2 \end{pmatrix} = 3\begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} + 5\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ 5 \end{pmatrix}$$

per definizione di moltiplicazione

Dopo aver scelto la base di $\mathbb{R}[x]^{\leq 2}$

$$\begin{array}{ccc} ax^2+bx+c & \xrightarrow{D} & 2ax+b \\ \downarrow & & \downarrow \\ \begin{pmatrix} a \\ b \\ c \end{pmatrix} & \xrightarrow[\text{applico la } [D]]{} & \begin{pmatrix} 0 \\ 2a \\ b \end{pmatrix} \end{array}$$

possiamo considerare solamente le coordinate associate

↓

lavoro solo con le matrici

$$F(a,b,c) = (0,2a,b)$$

$$F : \mathbb{R}^3 \to \mathbb{R}^3$$

stessa funzione ma vista a livello di coordinate

↓

lavoro con $\mathbb{R}^n$

es:

$f : \mathbb{R}^3 \to \mathbb{R}^2$ lineare

$$f\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \qquad f\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

$$f\begin{pmatrix} 8 \\ 13 \\ 18 \end{pmatrix} = ? \qquad \begin{pmatrix} 8 \\ 13 \\ 18 \end{pmatrix} \overset{?}{\in} \operatorname{span}\left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}\right)$$

$$\begin{pmatrix} 8 \\ 13 \\ 18 \end{pmatrix} = a\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + b\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$$ è un sistema

$$\begin{cases} 1a + 2b = 8 \\ 2a + 3b = 13 \\ 3a + 4b = 18 \end{cases} \qquad \left[\begin{array}{cc|c} 1 & 2 & 8 \\ 2 & 3 & 13 \\ 3 & 4 & 18 \end{array}\right]$$

$a=2$
$b=3$