



RIASSUNTO x me

• prodotto scalare

$$\langle v, w \rangle = v_1 w_1 + v_2 w_2 + v_3 w_3$$

• prodotto Vettoriale $v = (x_1, x_2, x_3)$ $w = (y_1, y_2, y_3)$

$$v \wedge w = \begin{pmatrix} 123 \\ 231 \\ 312 \end{pmatrix} \quad (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1)$$

PROPRIETA'

- 1) $w \wedge v = -w \wedge v \Rightarrow v \wedge v = 0$
- 2) $v \wedge w$ e' ORTOGONALE DI v e w
- 3) $\|v \wedge w\| = \|v\| \|w\| \sin \theta$

• NORMA (lunghezza del vettore)

$$\|v\| = \sqrt{\langle v, v \rangle}$$

+ DISTANZA $\text{dist}(v, w) = \|v - w\| = \sqrt{\langle v - w, v - w \rangle}$

+ Teorema di Pitagora

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2 + 2 \langle v, w \rangle$$

+ Disegualanza Cauchy Schwartz

$$\langle v, w \rangle \leq \|v\| \|w\|$$

$$\langle v, w \rangle$$

$$\cos \theta = \frac{\langle v, w \rangle}{\|v\| \|w\|}$$

• Angolo tra vettori

$$pr_v(w) = \frac{\langle v, w \rangle}{\|v\|^2} \cdot v$$

- $pr_v(w)$ e' un multiplo di v

- $w - pr_v(w)$ e' ORTOGONALE DI v

• Teorema di Rouché Capelli

Sis. RISOLUVIBILE \rightarrow \forall ogni riga nulla dei coefficienti e' nulla anche il termine noto

$$\rightarrow \text{rg}(A|b) = \text{rg}(A)$$

Altrimenti il # di parametri da cui dipende e':

$$\# \text{ parametri} = \# \text{ variabili} - \text{rg}(A)$$

RETTE

eq. retta $X = P + tA$

PUNTO DIREZIONE

→ eq. CARTESIANA

$$z: \begin{cases} ax_1 + bx_2 + cx_3 = d \\ a'x_1 + b'x_2 + c'x_3 = d' \end{cases}$$

$$X = \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} + t \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$



→ eq. PARAMETRICHE

Dette due rette:

$$z: X = P + tA \quad \rightarrow A \text{ mom è multiplo di } A'$$

$\Rightarrow z$ e z' mom sono la stessa retta

$$z': X = P' + tA' \quad \rightarrow A' \text{ è multiplo di } A$$

1) mom hanno punti in comune

\Rightarrow sono rette diverse

2) hanno un punto in comune

\Rightarrow coincidono

PIANI

$$d = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mid ax + by + cz + d = 0 \right\}$$

$x, y, z \rightarrow$ possibili soluzioni

$a, b, c \rightarrow$ numeri

+

COORDINATE del VETTORE

NORMALE AL PIANO

→ eq. CARTESIANA

$$d: ax + by + cz = d$$

$$n_d = (a, b, c)$$



→ eq. PARAMETRICHE

$$d: X = P + tA_1 + sA_2$$

I grado di libertà
II grado di libertà

→ II grado di libertà

HUTUE POSIZIONI

1) RETTA e RETTA

METODO 1: Vettori Direzione

$$z: \mathbf{X} = \mathbf{P} + t\mathbf{A}$$

$$\text{z: } \mathbf{X} = \mathbf{P}' + t\mathbf{A}'$$

a) $\mathbf{A} = k\mathbf{A}'$ 1) PARALLELE COINCIDENTI, ne hanno un

punto in comune

2) PARALLELE NON COINCIDENTI, ne non hanno

punti in comune

b) $\mathbf{A} \neq k\mathbf{A}'$ 1) INCIDENTI, hanno un punto in comune

2) SGHENBE, non hanno punti in comune

c) $\mathbf{A} \perp \mathbf{A}'$, allora le rette sono ORTOGONALI

METODO 2: Sistemi lineari

$$\begin{array}{l} z: \begin{cases} ax + b'y + c'z = d \\ a'x + b'y + c'z = d' \end{cases} \quad \text{a: } \begin{cases} ex + f'y + g'z = h \\ e'x + f'y + g'z = h' \end{cases} \end{array}$$

$$\left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \\ e & f & g & h \\ e' & f' & g' & h' \end{array} \right) \quad (\mathbf{A} | \mathbf{b})$$

SIS. COMPATIBILE



$$\operatorname{rg} \mathbf{A} = \operatorname{rg}(\mathbf{A} | \mathbf{b})$$

se compatibile, # param = # var - rg(A)

3 - ?

$$\operatorname{rg} \mathbf{A} = \underline{\underline{0, 1, 2, 3, 4}}$$

PERCHÉ OGNI RETTA HA 2 EQ.

Gauss: $\operatorname{rg} \mathbf{A} \leq \# \text{ colonne}$
(3)

a) $\operatorname{rg} \mathbf{A} = 2$ RETTE PARALLELE

SIS. compatibile \Rightarrow rette PARALLELE COINCIDENTI

$$\operatorname{rg}(\mathbf{A} | \mathbf{b}) = 2$$

SIS. non e' compatibile \Rightarrow rette PARALLELE NON COINCIDENTI

b) $\operatorname{rg} \mathbf{A} = 3$ RETTE NON PARALLELE

$$\operatorname{rg}(\mathbf{A} | \mathbf{b}) = 3$$

SIS. compatibile \Rightarrow INCIDENTI

$$\operatorname{rg}(\mathbf{A} | \mathbf{b}) = 4$$

SIS. non compatibile \Rightarrow SGHENBE

2) PIANO e PIANO

METODO 1: vettori normali

$$\alpha: ax + by + cz = d \quad m_\alpha = (a, b, c)$$

$$\beta: a'x + b'y + c'z = d' \quad m_\beta = (a', b', c')$$

a) $m_\alpha = k m_\beta$

1) PARALLEI COINCIDENTI, ne abbiamo un punto in comune

2) PARALLEI NON

COINCIDENTI, non hanno punti in comune

b) $m_\alpha \neq k m_\beta$ PIANI INCIDENTI, si intersecano in una retta

c) CASO PARTICOLARE : $m_\alpha \perp m_\beta$, PIANI ORTOGONALI

METODO 2: sistemi lineari

$$\begin{cases} \alpha: ax + by + cz = d \\ \beta: a'x + b'y + c'z = d' \end{cases}$$

$$(A|b) = \left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \end{array} \right)$$

$\text{rg } A = \underline{\underline{X}}_{12}$

a) $\text{rg } A = 1$ PIANI PARALLELI

$\text{rg } (A|b) = 1$

sist. compatibile \Rightarrow COINCIDENTI

$\text{rg } (A|b) = 2 \Rightarrow$ NON COINCIDENTI

sist. non compatibile

b) $\text{rg } A = 2 \quad \text{rg } (A|b) = 2 \Rightarrow$ INCIDENTI

sist. compatibile, si intersecano in una retta

(# parametri = $3 - 2 = 1$) ✓

c) Per trovare l'**ortogonalità** confrontiamo i vettori normali

3) RETTA e PIANO

$$\text{c: } X = P + tA$$

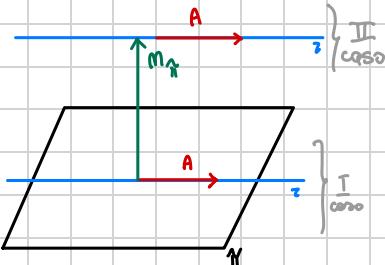
$$\pi: ax + by + cz = d$$

$$m_{\pi} = (a, b, c)$$

METODO 1:

a) $m_{\pi} \perp A$ 1) $\pi \cap A \neq \emptyset \Rightarrow \pi$ giace in π
 2) $\pi \cap A = \emptyset \Rightarrow \pi$ è comtemuta in π

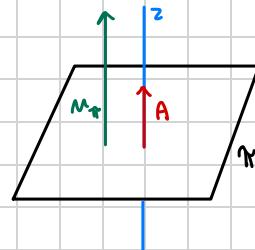
PARALLEI COINCIDENTI



2) $\pi \cap A = \emptyset \Rightarrow \pi$ non giace in π

PARALLEI NON COINCIDENTI

b) m_{π} mom e' ortogonale ad $A \Rightarrow$ INCIDENTI
 (si intersecano in un punto)



METODO 2: sistemi lineari (guardiamo l'intersezione)

$$\text{c: } \begin{cases} ax + by + cz = d \\ a'x + b'y + c'z = d' \end{cases}$$

$$(A|b) = \left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \\ e & f & g & h \end{array} \right)$$

$$\operatorname{rg} A = \underline{\underline{0}}, \underline{\underline{1}}, \underline{\underline{2}}, \underline{\underline{3}}$$

a) $\operatorname{rg} A = 2$ PARALLEI

1) $\operatorname{rg}(A|b) = 2$
 sis. compatibile \Rightarrow PARALLEI COINCIDENTI

$$(\# \text{var} = 3 - 2 = 1)$$

2) $\operatorname{rg}(A|b) = 3$

sis. mom compatibile \Rightarrow PARALLEI NON COINCIDENTI

b) $\operatorname{rg} A = 3 \quad \operatorname{rg}(A|b) = 3 \Rightarrow$ INCIDENTI

sis. compatibile

c) Per vedere l'ORTOGONALITÀ devo tornare ai vettori

MATRICI

- quadrate $\# \text{ righe} = \# \text{ colonne}$

- mille formata solo da zeri.

- PRODOTTO RIGHE PER COLONNE

prodotto scalare riga i

della prima matrice,

colonna j della seconda

$$A \times B = AB$$

$$A \in M_{m \times m}$$

$$B \in M_{m \times p}$$

$$AB \in M_{m \times p}$$

- triangolari

SUPERIORE se $A_{ij} = 0$ per $i > j$ (tutti i coeff. sotto la diagonale sono nulli)

INFERIORE se $A_{ij} = 0$ per $i < j$ (tutti i coeff. sopra la diagonale sono nulli)

- identità

$$I_m \quad I_{ij} = 1 \text{ se } i=j \\ (\text{ha tutti 1 sulla diagonale principale}) \quad = 0 \text{ se } i \neq j$$

$$\text{es. } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\forall A \in M_{m \times m} \quad AI = IA$$

- traccia

$\text{tr } A = \text{somma degli elementi sulla diagonale}$

$$\text{es. } I_m \quad \text{tr } I_m = m$$

PROPRIETÀ:

- $\text{tr}(A+B) = \text{tr } A + \text{tr } B$

- $\text{tr}(cA) = c \text{tr } A$

- $\text{tr}(AB) = \text{tr}(BA)$

- $\text{tr}(A^T) = \text{tr}(A)$

- diagonali

$D_{ij} = 0$ per $i \neq j$ (gli elementi sono nulli se non si trovano sulla diagonale)

$$D = \begin{pmatrix} a_{11} & 0 & \dots \\ 0 & a_{22} & \dots \\ \dots & & \dots \\ 0 & \dots & a_{nn} \end{pmatrix}$$

• somma/prodotto di due mat. diagonali è diagonale

• due mat. diagonali commutano sempre

- Invertibili (quadratiche)

$A \in M_{m \times m}$ e' invertibile se \exists un'altra mat. $m \times m$ detta A^{-1} , t.c.

$$A \cdot (A^{-1}) = (A^{-1}) \cdot A = I_m$$

- $(AB)^{-1} = B^{-1}A^{-1}$

es (perche' non ha capito)

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \text{ e' invertibile : } A^{-1} = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/5 \end{pmatrix}$$

$$\text{Infatti: } AA^{-1} = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1/3 & 0 \\ 0 & 1/5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ NON e' invertibile}$$

\Rightarrow se la matrice contiene una riga/colonna di 0 allora NON e' INVERTIBILE

• Algoritmo per calcolare A^{-1} (versione di Gauss)

$$\left(\begin{array}{c|c} A & I \end{array} \right) \xrightarrow{\text{operazioni righe}} \left(\begin{array}{c|c} I & A^{-1} \end{array} \right)$$

• SIMMETRICA e ANTISIMMETRICA

Definisco la **TRASPOSTA** di una matrice come la matrice in cui ri-scegliamo le righe con le colonne.

$$(A^T)_{ij} = A_{ji}$$

sceglio indica di riga

com indica di colonna

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix}$$

$$A^T = \begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{pmatrix}$$

Def. [matrici quadrate]

$$A \in \mathbb{M}_{m \times m}$$

SIMMETRICA se $A = A^T$ $A_{ij} = (A^T)_{ij} = A_{ji}$

ANTISIMMETRICA se $A = -A^T$ $A_{ij} = (A^T)_{ij} = -A_{ji}$



es.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$$

$$A^T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$$

SIMMETRICA ✓

$$B = \begin{pmatrix} 0 & 2 & 3 \\ -2 & 0 & 4 \\ -3 & -4 & 0 \end{pmatrix}$$

$$B^T = \begin{pmatrix} 0 & -2 & -3 \\ 2 & 0 & -4 \\ 3 & 4 & 0 \end{pmatrix}$$

ANTISIMMETRICA ✓

• MATRICI ORTOGONALI

matrice ortogonale se $A^{-1} = A^T$ ovvero $A^T A = A A^T = I$

PROPRIETÀ: • i vettori che formano le righe/colonne di A sono **mutualmente ortogonali** e hanno **norma = 1**

- Dato $w \in \mathbb{R}^m$, se v_1, \dots, v_m sono le colonne di A $\Rightarrow \exists c_1, \dots, c_m \in \mathbb{R}$ t.c.
 $w = c_1 v_1 + \dots + c_m v_m$

preservano
gli angoli

• DETERMINANTE

Associa un numero a una matrice quadrata (ok rispetto al prodotto)

def. Ricorsiva sull'ordine della matrice. Sia A $\in \mathbb{M}_{m \times m}$

$$\text{se } m=1 \Rightarrow A=a \quad \det A = a$$

$$\text{se } m>1 \Rightarrow A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m1} & \dots & \dots & \dots \end{pmatrix}$$

sviluppo di
LAPLACE rispetto alla
prima colonna

$$\det A = + a_{11} \det A_{11} - a_{21} \det(A_{21}) + \dots (-1)^{n+1} a_{m1} \det A_{m1}$$

A_{ij} : minori (sottomatrici) che si ottengono cancellando
la riga i e la colonna j

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \dots & a_{ij} & \dots \\ a_{m1} & \dots & a_{mm} \end{pmatrix}$$

es. $\det(5) = 5$

$$\det \begin{pmatrix} -2 & 3 \\ 7 & 5 \end{pmatrix} = -2 \cdot 5 - 7 \cdot 3 = -31$$

$$\begin{aligned} \det \begin{pmatrix} 2 & 0 & 3 \\ 1 & -5 & 0 \\ 0 & 1 & 2 \end{pmatrix} &= 2 \cdot \begin{vmatrix} 1 & -5 & -(-1) \\ 0 & 2 & 1 \end{vmatrix} + 0 \cdot \begin{vmatrix} 3 & 0 & 3 \\ 1 & 2 & 1 \end{vmatrix} = \\ &= 2 \cdot (1 \cdot 2 - 1 \cdot (-5)) + 1 \cdot (0 \cdot 2 - 1 \cdot 3) + 0 \cdot (0 \cdot 3 - 1 \cdot 3) \\ &= 2 \cdot (14 + 5) - 3 + 0 = 2 \cdot 19 - 3 = \textcircled{35} \quad \checkmark \end{aligned}$$

• posso sviluppare il determinante rispetto a qualsiasi riga/colonna

es. $\begin{pmatrix} 1 & 4 & 6 \\ 2 & 0 & 0 \\ 3 & 5 & 7 \end{pmatrix}$ come si sviluppa il
det rispetto a questa

$$\det = 2 \begin{vmatrix} 4 & 6 & 0 & 1 & 6 & 0 & 1 & 4 \\ 5 & 7 & 3 & 7 & 3 & 5 \end{vmatrix} =$$

$$= 2 \cdot (4 \cdot 7 - 5 \cdot 6) = 2 \cdot (28 - 30) = 2 \cdot -2 = \textcircled{-4} \quad \checkmark$$

• Se ho una riga/colonna di zeri, il determinante è sempre uguale a 0.

es. $\det \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} = 0$

• Algoritmo di Gauß

- Scombiare due righe
- moltiplico una riga per $k \neq 0$
- $R_i \rightarrow R_i + kR_j$

Determinante

- det. viene moltiplicato per -1
- det. viene moltiplicato per k
- det non cambia

• PROPRIETÀ Determinante

$$\textcircled{1} \quad \det A = \det A^T$$

$$\textcircled{2} \quad \det \begin{pmatrix} | & | & | \\ A^1 & tA^i & A^m \\ | & | & | \end{pmatrix} = t \det \begin{pmatrix} | & | & | \\ A^1 & A^i & A^m \\ | & | & | \end{pmatrix} = t \det A$$

> moltiplico una colonna per t

$$\det(tA) = \det(tA^1 \dots tA^m) = t^m \det A$$

\textcircled{3} Se scombio due colonne il determinante cambia segno

\textcircled{3'} Se A ha due colonne uguali, $\det A = 0$.

$$\textcircled{4} \quad \det(AB) = \det A \cdot \det B \implies \underline{\text{Formula di Binet}}$$

conseguenza
↓
 A ortogonale $\implies \det A = \pm 1$

$$\textcircled{5} \quad A \text{ e' invertibile} \iff \det A \neq 0 \text{ e } \det(A^{-1}) = \frac{1}{\det A}$$

$$\text{INVERSA } 2 \times 2 \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

• Rango per minori (mat. rettangolari)

def. A E $M_{m \times n}$,

Un minore di ordine p e' una matrice quadrata $p \times p$ ottenuta da A cancellando $m-p$ righe e $n-p$ colonne

ho m righe, cancello $m-p$ righe \rightarrow restano $m-(m-p) = m-p$ righe $\Rightarrow p$ righe

ho n colonne, cancello $n-p$ colonne \rightarrow restano $n-(n-p) = p$ colonne $\Rightarrow p$ colonne

• minori di ordine 3

- eliminiamo la 1^a riga

$$\begin{pmatrix} 2 & 3 & 4 \\ 6 & 7 & 8 \\ 10 & 11 & 12 \end{pmatrix}$$

- eliminiamo la 3^a riga

$$\begin{pmatrix} 1 & 2 & 4 \\ 5 & 6 & 8 \\ 9 & 10 & 12 \end{pmatrix}$$

- eliminiamo la 2^a riga

$$\begin{pmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & 11 & 12 \end{pmatrix}$$

- eliminiamo la 1^a riga

$$\text{es. } A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 6 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$$

scelta riga scatta 2^a

$\begin{pmatrix} 7 & & & \\ & 3 & 4 & 6 \\ & & & \end{pmatrix}$ colonna da togliere

• minori di ordine 2 [ho]

$$3 \times 4 \times 3 = 36 \text{ scelte}$$

scatta 1^a colonna

da togliere.

$$- \begin{pmatrix} 1 & 2 \\ 9 & 10 \end{pmatrix}, \begin{pmatrix} 6 & 7 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 8 \\ 11 & 12 \end{pmatrix}$$

[dimensione]

det. Rango per minori di A e' il massimo ordine dei minori di A con $\det \neq 0$.

Ovvero, guardo tutti i minori di A, salgo il più grande com $\det \neq 0$, la sua dim.

se il rg A.

mat. non nulla \Rightarrow rg è almeno 1
3 righe e 3 colonne \Rightarrow rg al max 3

es.

$$A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

trovo un minore di rg 2, com $\det \neq 0$

$$\det \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

$\operatorname{rg} A = 2 \text{ o } 3$] Comitizzo il det A

$$\det A = 1 \begin{vmatrix} 1 & 0 & -(-1) \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} + 0 \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$$

$$= 1[(1 \cdot 1) - (1 \cdot 0)] + 1[(0 \cdot 1) - (1 \cdot 1)] + 0 = 1 - 1 + 0 = 0 \Rightarrow \text{l'unico minore di ordine 3 ha det} = 0 \Rightarrow \operatorname{rg} A = 2$$

- Gauss non fa diventare 0 il det di nessun minore e non crea minori nuovi con det $\neq 0$

- $A \xrightarrow{\text{Gauss}} S \Rightarrow \operatorname{rg} \text{ per minori di } A = \operatorname{rg} \text{ per minori di } S$

OSS. Se una matrice A ha m righe e n colonne, $\operatorname{rg} A \leq \min(m, n)$

$$A \in M_{m \times n}$$

• Una matrice è invertibile se il $\det A \neq 0$ e $\operatorname{rg} A = m$ (rango massimo)

• **teo Rouché-Capelli per matrici dei coeff. invertibili**

$$A \in M_{m \times m}, \det A \neq 0 \Rightarrow$$

• Il sistema $Ax=b$ è compatibile $\forall b \in \mathbb{R}^m$

• La soluzione è unica

● STRUTTURA DI GRUPPO

def. Un gruppo è un insieme S con

• una operazione * t.c. $s_1 * s_2 = s \in S$

• $\exists e \in S$ elemento neutro t.c. $s * e = e * s = s \quad \forall s \in S$

• \exists inverso: $\forall s \in S \exists s^{-1} \in S$ t.c. $s * s^{-1} = e$

Gruppi di matrici rispetto alla somma, Gruppi di matrici rispetto alla moltiplicazione

$$S = M_{m \times n}, +, e = 0$$

[mat. nulla]

Dovendo considerare le mat $m \times n$, non tutte le moltiplicazioni sono possibili

- OK perché la somma di matrici è una matrice della stessa dimensione
- OK perché $A + 0 = 0 + A = A$
- $(-A) + A = A + (-A) = 0$
- $S = M_{m \times m}$ invertibili ($\det \neq 0$)
- OK: $s_1 * s_2 = s \in M_{m \times m}$
- $\exists e: I: I * A = A * I = A \quad \forall A$
- $\exists A^{-1}$ t.c. $A * A^{-1} = A^{-1} * A = I$

tontri sottogruppi:

simm., antisimm., traccia nulla ...

sottogruppi:

matrici ortogonali, simm., det=1, diagonali ...



08.04.24

Numeri

- numeri naturali (e numeri primi) $\mathbb{N} = \{0, 1, 2, \dots\}$
- numeri interi $\mathbb{Z} = \{\dots -2, -1, 0, 1, \dots\}$
- numeri razionali $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$
- numeri reali \mathbb{R}
- numeri complessi $\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\}$
 $i^2 = -1$

Studiamo la loro struttura:

- Proprietà dell'insieme
- Operazioni legate

NUMERI NATURALI

Due proprietà fondamentali

1. Assioma del buon ordinamento

"Ogni sottoinsieme non vuoto di \mathbb{N} ha un elemento minimo"



Se $S \subset \mathbb{N}$, $S \neq \emptyset \Rightarrow \exists m \in S$ t.c. $m \leq m \quad \forall n \in S$

OSS. • S potrebbe essere infinito $\Rightarrow S$ non aveva un elemento massimo

• Peculiarità di \mathbb{N} : - i m \mathbb{Z} , $S = \{ \text{negativi multipli di } 3 \}$

S non ha un elemento minimo

- i m \mathbb{R} , $S = (0, 1]$ S non c'è elemento minimo perché

dovrebbe essere 0, ma $0 \notin S$.

aperto

2. Principio di Induzione

Associamo a ogni m una asserzione $A(m)$. Allora, se

* $A(0)$ è vera

* $\forall m$, $A(m)$ implica $A(m+1) \Rightarrow A(m)$ è vero $\forall m$.

• è equivalente all'assioma di buon ordinamento

Operazioni sui naturali

- somma $m+m \in \mathbb{N}$ com $m, m \in \mathbb{N}$

Oss $0+m=m \quad \forall m \in \mathbb{N}$

0 e' l'elemento neutro della somma

- moltiplicazione $m \cdot m \in \mathbb{N}$ com $m, m \in \mathbb{N}$

Oss $1 \cdot m = m \quad \forall m \in \mathbb{N}$

1 e' l'elemento neutro della moltiplicazione

- divisione con resto

Non possiamo fare:

- sottrazione $\rightsquigarrow \mathbb{Z}$
- divisione "mormale" $\rightsquigarrow \mathbb{Q} \quad (1:2=0.5 \in \mathbb{Q})$
- radici/zisolvere equazioni ($x^m=5?$) $\rightsquigarrow \mathbb{R}$
 $\rightsquigarrow \mathbb{C}$

NUMERI INTERI

operazioni: somma, moltiplicazione,
divisione con resto, sottrazione

illecite: divisione mormale, soluzioni di eq.

I numeri primi sono naturali,
ma la def. si basa su concetti
che valgono anche per gli interi

DIVISIONE CON RESTO

- naturali : $55:9=6$ resto 1

Abbiamo cercato il più grande x
tale che $9 \cdot x < 55$; $x=6$
 $65 \cdot 9 - 6 = 1$ (resto)

- interi: Convenzione: il resto deve essere positivo

Oss. Se il numero per cui divido è negativo, moltiplico entrambi per -1
in modo da farlo divenire positivo

$$55:(-9) \rightarrow -55:9=-7 \text{ resto } 8$$

Divisione con resto : \mathbb{N}

$$a:b=q \text{ resto } z$$

$$\equiv a = q \cdot b + z$$

Ci sono ∞ soluzioni, l'una se chiedo $z < b$

\mathbb{Z}

l'una se chiedo $0 \leq z < b$

convenzione

def. (divisore) Siamo $a, b \in \mathbb{Z}$ diciamo che b divide a
 $(b$ è un divisore di a se
 $\exists c \text{ t.c. } a = b \cdot c$

- (la divisione di a per b dà resto 0)
- a è multiplo di b
- bla

Attenzione! Anche i negativi sono divisori

Esempio i divisori di 12: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$
di 7: $\pm 1, \pm 7$

tutti i numeri sono divisori di 0, perché $\forall b \in \mathbb{Z}$
(penso prendere $c=0$)

$$0 = b \cdot 0$$

0 non è divisore di nessun b , perché $\forall b \in \mathbb{Z}$,
 $b \neq 0 \cdot c \quad \forall c \in \mathbb{Z}$

OSS. ① Ogni intero a ha almeno 4 divisori: $\pm 1, \pm a$

② Se d divide a e $b \Rightarrow d$ divide $a+b$

dim: $d | a \Rightarrow \exists c_1 \text{ t.c. } a = d \cdot c_1$

$d | b \Rightarrow \exists c_2 \text{ t.c. } b = d \cdot c_2$

$$\Rightarrow a+b = \underbrace{d \cdot c_1}_{a} + \underbrace{d \cdot c_2}_{b} = d(\underbrace{c_1+c_2}_{c})$$

$$d | b = \dots$$

③ Se d divide $a \neq 0 \Rightarrow |d| < |a|$

$a \neq 0$ poiché tutti i d sono divisori di 0
ma 0 è il più piccolo

dim. $d | a, \exists c \text{ t.c. } a = d \cdot c \rightarrow |a| = |d| \cdot |c|$

Se $a \neq 0, c \neq 0$

$$\Rightarrow |c| \geq 1 \Rightarrow$$

$$|a| > |d| \wedge |a| = |d|$$

$$-5 | -10, \text{ ma } -5 > -10$$

\Rightarrow devo usare il modulo

$$|-10| > |-5|$$

Teorema (divisione con resto)

Siamo $a, b \in \mathbb{Z}$, $b > 0$. Allora \exists unici due interi q, r (quoziente e resto) tali che
 $a = qb + r$, $0 \leq r < b$
Sovviaamo $a : b = q$ resto r

Divisori, congruenze e numeri primi

Vale per \mathbb{Z} e \mathbb{N}

Studia i casi in cui la divisione di un numero "a" per un numero b dà resto 0.

def. Divisore Siamo $a, b \in \mathbb{Z}$ diciamo che b divide a
(b è un divisore di a) se
 $\exists c \text{ t.c. } a = b \cdot c$

- (la divisione di a per b da resto 0)
- a è multiplo di b
- $b | a$

! Anche i negativi sono divisori!

Esempio • i divisori di 12 sono

$$\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 12$$

• i divisori di 7 sono $\pm 1, \pm 7$

• tutti i numeri sono divisibili di 0, perché $\forall b \in \mathbb{Z}, 0 = b \cdot 0$

• 0 non è divisore di alcun b, perché $\forall b \in \mathbb{Z}, b \neq 0 \cdot c \quad \forall c \in \mathbb{Z}$

Oss. ① Ogni intero a ha almeno 4 divisori: $\pm 1, \pm a$

② Se d divide a e b \Rightarrow d divide a+b

$$\text{dim. } d | a \Rightarrow \exists c_1 \text{ t.c. } a = d \cdot c_1$$

$$d | b \Rightarrow \exists c_2 \text{ t.c. } b = d \cdot c_2$$

$$\Rightarrow (a+b) = \underbrace{d \cdot c_1}_{a} + \underbrace{d \cdot c_2}_{b} = d(\underbrace{c_1+c_2}_{c}) \quad \checkmark$$

$$(a-b) = \dots$$

③ Se d divide $a \neq 0 \Rightarrow |d| \leq |a|$

$a \neq 0$ perché tutti i d sono divisori di 0 ma 0 è il più piccolo

$$\text{dim. } d | a, \exists c \text{ t.c. } a = d \cdot c \rightarrow |a| = |d| \cdot |c|$$

$$\text{Se } a \neq 0, c \neq 0$$

$$\Rightarrow |c| \geq 1 \Rightarrow$$

$$|a| \geq |d| \cdot 1 = |d|$$

def. Massimo Comum Divisore

GCD greatest common divisor

Siamo $a, b \in \mathbb{Z}$, non entrambi 0. Il loro massimo comum divisore (MCD) è il più grande intero che divide sia a che b .

Definiamo $\text{MCD}(0,0) = 0$

$$\text{MCD}(0,a) = |a|$$



Tutti i numeri dividono 0, e il più grande divisore di a è $|a|$.

Esempio. $\text{MCD}(12, 52) = 4$

Div. di 12 = ...

Div. di 52 = 4, 13

Come si trova? [Scomposizione fattori primi]

Algoritmo di Euclide

(vedere dopo)

Altre proprietà del MCD

- è sempre positivo (Il più grande tra i divisori)
- $\text{MCD}(a, a) = \text{MCD}(-a, -a) = |a|$
- $\text{MCD}(1, a) = 1$
- $\text{MCD}(b, a) = \text{MCD}(a, b) = \text{MCD}(a, -b) = \text{MCD}(-a, b)$
- Se $(a, b) \neq (0, 0) \Rightarrow \text{MCD}(a, b) > 0$

↓ a e b non sono

entrambi nulli

ma solo! NON interi

def. Numeri primi $p \in \mathbb{N} \setminus \{0\}$ [p intero positivo]

p è un numero primo se ha esattamente due divisori positivi: 1 e p .

! 1 non è un numero primo

Prop. (Proprietà del MCD)

Se $a, b \in \mathbb{Z}, \forall q \in \mathbb{Z}$, $\text{MCD}(a, b+qa) = \text{MCD}(a, b)$

(Il MCD non cambia se aggiunge a un numero il multiplo di un altro.)

Esempio: $a=3$ $b=7$ $\text{MCD}(3, 7) = \text{MCD}(3, 7+5 \cdot 3) =$
 $q=5$ $= \text{MCD}(3, 22) = 1$

• $a=10$ $\text{MCD}(10, 100003) = \text{MCD}(10, 3)$
 $b=3$ $"$ $"$
 $q=10^5$ $10 \cdot 10^5 + 3$ $"$
 $"$ 1

dim. Sia $q \in \mathbb{Z}$ (a, b fissati) Dobbiamo dimostrare:

① Se d divisore di a e di b , $\Rightarrow d$ divisore di $b+qa$

② Se d divisore di a e di b , $\Rightarrow d$ divisore di $b+qa$

[\equiv l'insieme dei divisori di a e b coincide con l'insieme dei div. di a e $b+qa$]

① $d | b$ e $d | a \Rightarrow$

$$\begin{aligned} a &= m_1 d \\ b &= m_2 d \end{aligned} \Rightarrow b+qa = m_2 d + qm_1 d = (m_2 + qm_1) d$$
$$\Rightarrow d | (b+qa)$$

② $d | a$ e $d | b+qa$

$$\begin{aligned} a &= m_1 d & \rightarrow b = (b+qa) - qa = \\ b+qa &- m_1 d & = m_2 d - qm_1 d = (m_2 - qm_1) d \\ & & \Rightarrow d | b \end{aligned}$$

• Somma / sottrazione / moltiplicazione di numeri interi danno numeri interi

Abbiamo usato: $d | a \Leftrightarrow \exists m, a = md$

② Cosa non si può fare sui numeri

10/04/24

Prop. Se $a, b \in \mathbb{Z}$, $\forall q \in \mathbb{Z}$ $\text{MCD}(a, b) = \text{MCD}(a, b + qa)$

$d \mid a \Leftrightarrow \exists m \in \mathbb{Z} \text{ t.c. } a = md$ massimo che divide

Applicazione: Algoritmo di Euclideo

$$\begin{aligned} \text{es. } \text{MCD}(48, 32) &= \left| \begin{array}{l} 48 = 32 \cdot 1 + 16 \rightarrow b \\ b + qa \rightarrow a \\ 32 = 16 \cdot 2 + 0 \end{array} \right. \\ &= \text{MCD}(32, 16) \\ &= \dots \Rightarrow \text{Il MCD e' l'ultimo resto prima di ottenere } \emptyset. \\ &\Rightarrow 16 \end{aligned}$$

• Siamo $a, b > 0$ definiamo r_0, r_1, r_2, \dots come:

$$r_0 = a \quad r_1 = b \quad r_{k+1} = \text{resto di } r_{k-1} : r_k$$

$(r_i) \rightarrow$ e' una successione decrescente di interi positivi \Rightarrow prima o poi

\downarrow resto < quoziente \rightarrow arrivo a \emptyset .

d'ultimo resto non
nullo e' il MCD

$$\begin{aligned} \text{es. } \text{MCD}(66, 100) &= \left| \begin{array}{l} 100 = 66 \cdot 1 + 34 \\ 66 = 34 \cdot 2 + 0 \\ 34 = 0 \cdot 1 + 34 \\ 0 = 0 \cdot 2 + 0 \end{array} \right. \\ &= \text{MCD}(100, 66) \\ &= \text{MCD}(66, 34) \\ &= \text{MCD}(34, 0) \\ &= \text{MCD}(66, 0) \\ &= \text{MCD}(100, 66) \\ &= \text{MCD}(66, 34) \\ &= \text{MCD}(34, 0) \\ &= \text{MCD}(0, 0) \\ &\Rightarrow \text{MCD} = 66 \end{aligned}$$

Proprietà: Se $d = \text{MCD}(a, b) \Rightarrow \exists x, y \in \mathbb{Z} \text{ t.c. Identità di Bezout}$
 $d = ax + by$ (x e y possono essere negativi)

$$\text{es. } \text{MCD}(25, 10) = 5 \quad 5 = 25 \cdot 1 - 10 \cdot 2$$

Lemma di Bezout Sia $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$

$S = \{ax + by \mid x, y \in \mathbb{Z}\} \Rightarrow \text{MCD}(a, b) = \text{più piccolo elemento positivo di } S.$

dim. $S \neq \emptyset$ infatti $a \in S$ Prendiamo solo gli elementi in S che sono positivi: S_+

$\Rightarrow S_+ \neq \emptyset$ infatti $a > -a \in S_+$.

$S_+ \subset \mathbb{N}$, $S_+ \neq \emptyset \Rightarrow$ principio del buon ordinamento

$\Rightarrow \exists d$ elemento minimo $d = a \in S_+$

Dobbiamo far vedere $d = \text{MCD}(a, b)$ avendo:

• $d | a$, $d | b$ e

• Se $c | a$, $c | b$ e $c \in S$ $\Rightarrow c \leq d$

• Usando divisione con resto $a = dq + r$ per $q, r \in \mathbb{Z}$, $0 \leq r < a$

$$\rightarrow r = a - dq = a - (as + bt)q = a(1-sq) - btq \Rightarrow r \in S_+ \quad \boxed{x} \quad \boxed{-q}$$

• $r \geq d$ perch'è d era minimo $\Rightarrow r=0$

• $r < d$ perch'è è il resto

$\Rightarrow d | a$.

Stesso per $b \Rightarrow d | b$ $\Rightarrow d$ divisore di a e di b

• Gia' $c | a$, $c | b$ $\exists u, v$ t.c. $a = cu$, $b = cv$

\Rightarrow poiché $d = as + bt = (cu) \cdot s + (cv) \cdot t = c(us + vt) \Rightarrow$

$c | d \Rightarrow c \leq d$.

Conseguenze di Bezout

(unici)

• $\text{MCD}(a, b) = d \Rightarrow d = ax + by$ per qualche $x, y \in \mathbb{Z}$

• Se $d | a$, $d | b \Rightarrow d | \text{MCD}(a, b)$

Dimm. \leftarrow Se $\text{MCD}(a, b) = 1$ sono primi tra loro
 \Rightarrow se $a | bc$, abbiamo anche $a | c$

Ese. • $\text{MCD}(25, 10) = 5 = 25 \cdot 1 - 10 \cdot 2$

• $\text{MCD}(12, 18) = 6$ 2, 3 dividono 12 e 18 e di conseguenza anche 6

• $a = 4$, $b = 7 \Rightarrow \text{MCD}(4, 7) = 1$ (Euclide)

Se $c = 8$, $a | 8 \cdot 7 \Rightarrow a | c$ (infatti $4 | 8$)
" "
 $c | b$

Bezout

*Dimm. $\text{d} = \text{MCD}(a, b) \stackrel{\downarrow}{=} ax + by$ per qualche $x, y \in \mathbb{Z} \Rightarrow$

$$c = c \cdot 1 = c \cdot (ax + by)$$

poiché $a | bc \Rightarrow bc = a \cdot m$ per qualche $m \in \mathbb{Z}$

$$\Rightarrow c = c \cdot ax + c \cdot by = c \cdot ax + a \cdot cmy = \\ = a(cx + my) \Rightarrow a | c.$$

prop Siamo $a, b \in \mathbb{Z}$ p primo

Se $p | ab \Rightarrow p | a$ o $p | b$

dim Supponiamo $p | ab$, $p \nmid a$. Voglio mostrare $p | b$.

$\text{MCD}(a, p)$ divide sia p che a MA gli unici divisori di p sono $\pm p, \pm 1$

$\text{MCD} > 0 \Rightarrow \text{MCD}(a, p) = 1$ o p .

Poiché $p \nmid a \Rightarrow \text{MCD}(a, p) = 1 \Rightarrow$ poiché $p | ab$, $p | b$

Teo. Fondamentale dell'Arithmetica

(DECOMPOSIZIONE IN FATTORI PRIMI)

Sia $m \in \mathbb{N}$, $m \neq 0 \Rightarrow \exists k$ numeri primi (m non necessariamente distinti)

Tali che $m = p_1 \cdot p_2 \cdot \dots \cdot p_k$

$p_1 \dots p_k$ si chiamano fattori primi di m e sono unici a meno dell'ordine.

(su \mathbb{Z} : o mom va bene

$m \neq 0$, scrivo $m = -$ (decomposizione di $-m$)

1 teoricamente mom c'è decomposizione)

dim Esistenza. {Suppongo mom vero. $\Rightarrow \exists m > 1$ minimo senza decomposizione.

mom non è primo (altrimenti $m = p$)

m mom primo $\Rightarrow m = ab$ per qualche $1 < a, b < m$

per minimialità di m , a e b si scompongono in fattori primi e quindi anche m . }
Percorso alternativo facile: osservo che vale per tutti i primi,

$\Rightarrow \exists m > 1$ minimo e mom primo per cui il teo mom vale.

Oss Abbiamo visto p primo, $a, b \in \mathbb{Z} \Rightarrow p | a \cdot b$, p divide a o b .

p mom primo \Rightarrow falso

Corollario: I numeri primi sono ∞

Supponiamo che siano finiti: $p_1 \dots p_k$

Consideriamo il loro prodotto $a = p_1 \cdot \dots \cdot p_k$

$$b = p_1 \cdot \dots \cdot p_k + 1 = a + 1$$

$$\text{MCD}(a, b) = 1$$

• poiché $\text{MCD}(a+1, a) = \text{MCD}(1, a) = 1$

• poiché $1 \cdot b - a = 1 \cdot b - 1 \cdot a \in S^+$ del lemma di Bezout

\Rightarrow poiché MCD è il più piccolo intero > 0

Per la scomposizione in fattori primi,

b = prodotto di primi $\underline{\text{HA}}$ questo prodotto non può contenere messa in comune dei primi $p_1 \dots p_m$ perché

$$\text{MCD}(a, b) = 1$$

$\Rightarrow b$ è primo

def. Ordine di un intero Sia $a \in \mathbb{N}$, $a \neq 0$, 1. sia p primo

$\Rightarrow \text{ord}_p(a) = \#$ volte che p compone mei fattori primi di a

Se $a \in \mathbb{Z}$, a negativo

$\rightarrow \text{ord}_p(a) = \text{ord}_p(-a) \overset{\hat{0}}{> 0}$

$\text{Ord}_p(0)$ non def.

$\text{Ord}_p(1) = \cancel{0}$ non def.

$$\text{Es. } \text{Ord}_2(12) = 2$$

$$\text{Ord}_3(12) = 1$$

$$\text{Ord}_7(12) = 0$$

\Rightarrow Si può scrivere la decomposizione in fattori primi come

$a \in \mathbb{N}$, $a \neq 0, 1$

$$a = \prod_p p^{\text{ord}_p(a)}$$

p primi

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \dots$$

Oss. $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$

① $\forall p$ primo, $\text{ord}_p(ab) = \text{ord}_p(a) \cdot \text{ord}_p(b)$

② $d \in \mathbb{Z}$, $d \neq 0 \Rightarrow$

$d|a \iff \text{ord}_p(a) \geq \text{ord}_p(d) \forall p$ primo

(i fattori primi di d devono apparire in a con ordini \geq)

③ $\text{MCD}(a, b) = \prod_p p^{\min(\text{ord}_p(a), \text{ord}_p(b))}$

prendendo tutti i fattori primi in comune con l'esponente + piccolo

def. Minimo Comune Multiplo dati $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$

$\text{mcm}(a, b)$ è il più piccolo $m > 0$ t.c. $a|m$, $b|m$

(multiplo di entrambi)

$$\text{es. } \text{mcm}(5, 12) = 60$$

$$\text{mcm}(4, 6) = 12$$

$$\text{mcm}(a, b) = a \cdot b \quad \text{se } \text{MCD}(a, b) = 1$$

$$\text{mcm}(a, b) = \prod_{p \text{ primo}} p^{\max(\text{ord}_p(a), \text{ord}_p(b))}$$

$$\text{mcm}(a, b) \cdot \text{mcd}(a, b) = |ab|$$

[faccio il conto usando la decom.

in f. primi]

Numeri Razionali

Sono i numeri della forma $\frac{p}{q}$, con $p, q \in \mathbb{Z}$, $q \neq 0$

C'è solo un modo per scrivere ogni razionale.

Formalmente si fa così:

$$\mathbb{Q} = \left\{ (\rho, q) \in \mathbb{Z} \times \mathbb{Z}^*, (\rho, q) \sim (\rho', q') \iff \rho \cdot q' = q \cdot \rho' \right\}$$

Classe di equivalenza: un modo di rappresentare la stessa cosa

$$\frac{2}{3} \text{ è un rappresentante della classe}$$

$$\left\{ \frac{2}{3}, \frac{4}{6}, \frac{-2}{-3}, \frac{200}{300}, \dots \right\}$$

(posso scegliere qualunque altra frazione)

• classi di equivalenza che contengono $(m, 1)$ avranno le coppie (bm, b) e $\mathbb{Z} \times \mathbb{Z}^*$

Si possono identificare con gli interi, \Rightarrow

$$\mathbb{Z} \subset \mathbb{Q}$$

Operazioni su \mathbb{Q}

- somma e sottrazione $\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}$

elem. neutro 0

inverso di $\frac{p}{q}$ è $-\frac{p}{q}$

- moltiplicazione $\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$

elem. neutro 1

inverso di $\frac{p}{q}$ è $\frac{q}{p}$ ($p \neq 0$)

inverso moltiplicativo di $\frac{p}{q}$

- divisione $\frac{p}{q} : \frac{p'}{q'} = \frac{p}{q} \cdot \frac{q'}{p'}$

• Non zodici! Non equationi! $\sqrt{\frac{2}{3}} \notin \mathbb{Q}$

Oss. Aggiungendo gli irrazionali da \mathbb{Q} si ottiene \mathbb{R} .

\hookrightarrow zodici ... , π , ...

\mathbb{Q} densissim \mathbb{R} ($\forall z \in \mathbb{R} \exists q \in \mathbb{Q}$ arbitrariamente vicino)

\mathbb{Q} ha area \emptyset .

Numeri Complessi \mathbb{C}

$$\mathbb{C} = \{ \text{numeri complessi} \} \\ = \{ z = a + ib \mid a, b \in \mathbb{R}, i^2 = -1 \}$$

$$x^2 = -1 \quad \text{su } \mathbb{R} \times \\ i^2 = -1 \quad \checkmark$$

$\text{Re } z = a = \text{parte Reale}$

$\text{Im } z = b = \text{parte immaginaria}$

Operazioni $z_1 = a_1 + ib_1$

$$z_2 = a_2 + ib_2$$

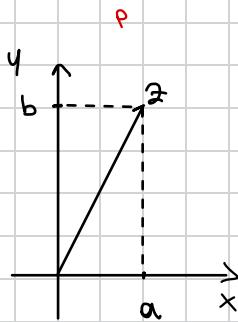
$$\cdot z_1 \pm z_2 = (a_1 \pm a_2) + i(b_1 \pm b_2)$$

$$\cdot z_1 z_2 = (a_1 + ib_1)(a_2 + ib_2) = a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)$$

$$\cdot |z_1| = \sqrt{a_1^2 + b_1^2} \quad (\text{modulo di un numero complesso})$$

$$\cdot \overline{z_1} = a_1 - ib_1 \quad \underline{\text{Comiugio}}$$

Interpretazione Geometrica dei numeri complessi



$$z = a + ib$$

\vec{z} vettore $(a, b) = \sqrt{ }$

- $|z| = \|\vec{v}\| = \sqrt{a^2 + b^2} \Rightarrow$ Raggio
- \bar{z} e' il riflesso di z rispetto all'asse x



$$\begin{aligned} \bullet z \cdot \bar{z} &= (a+ib)(a-ib) = a^2 + iba - iba - (-b^2) \\ &= a^2 + b^2 = |z|^2 \end{aligned}$$

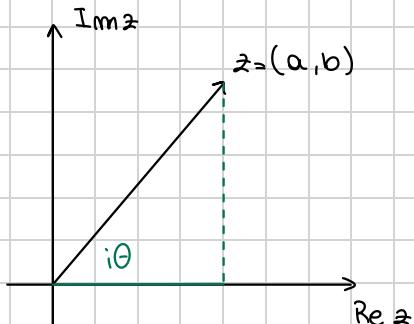
$$\bullet z = a + ib$$

$$\frac{1}{z} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{\overline{z}}{|z|^2}$$

$$\bullet \frac{1}{i} = -i$$

Forma Trigonometrica dei numeri complessi

Usando Taylor (espansione in serie di potenze) si può vedere che :



$$e^{i\theta} = \cos \theta + i \sin \theta \quad (\theta \in \mathbb{R})$$

$$z = a + ib$$

$$\begin{aligned} z &= r \cos \theta + i r \sin \theta \Rightarrow z = r e^{i\theta} \\ &= r(\cos \theta + i \sin \theta) \end{aligned}$$

IMPORTANTE

$$a > 0 \Rightarrow \theta = \arctan \frac{b}{a}$$

$$a = 0 \Rightarrow \theta = \frac{\pi}{2} \Leftrightarrow b > 0$$

$$\Rightarrow \theta = -\frac{\pi}{2} \Leftrightarrow b < 0$$

$$a < 0 \Rightarrow \theta = \pi - \arctan \frac{b}{a}$$

$r, \theta \in \mathbb{R}$ come a, b

Passare da $z = r e^{i\theta}$ a $z = a + ib$

$$a = r \cos \theta \quad \text{e} \quad b = r \sin \theta$$

Forme Trigonometriche utili per prodotti e potenze:

$$\begin{aligned} z &= a + ib & z^m &= (a + ib)^m \\ &= z e^{i\theta} & &= r^m e^{im\theta} \end{aligned}$$

$$+ \text{Se } w = s e^{iq} \rightarrow z \cdot w = r \cdot s e^{i(\theta+q)}$$

$$\begin{cases} a = |z| \cos \theta \\ b = i \sin \theta \end{cases}$$

Radici dei numeri complessi

$\sqrt[m]{z} = z^{\frac{1}{m}}$ tutti i numeri complessi che elevati alla m fanno z.

TEOREMA FONDAMENTALE DELL'ALGEBRA

Un polinomio di grado m su \mathbb{C} ha esattamente m radici contate con molteplicità

In formulæ: Dato $p_m(w) = a_0 + a_1 w + a_2 w^2 + \dots + a_m w^m$

$\exists w_1, \dots, w_m$, m numeri complessi distinti, t.c.

$$p_m(w) = (w-w_1)(w-w_2) \dots (w-w_m)$$

$$\text{es. } p(w) = (w-3)^3(w-1)$$

3 radice molteplicità 3

1 radice molteplicità 1

Torniamo alle radici

Problema: Fissare z , trovare w t.c. $w^m = z e^{i\theta}$

Fissare m

$$z = \lambda = 1 \cdot e^0 = 1 \cdot e^{2k\pi i}$$

$$m=1 \quad w=1 \Rightarrow$$



Sono distinte finché $\frac{2\pi k}{m}$ diventa multiplo

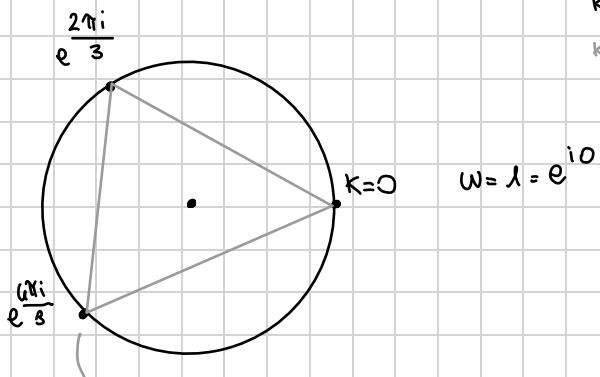
$$m=2 \quad (z e^{i\theta})^2 = w^2 = 1 \Rightarrow$$

$$\begin{aligned} z=1 & \quad z^2 e^{2i\theta} = 1 \cdot e^{i(0+2k\pi)} \\ \text{perche' } |z|=1 & \quad \Rightarrow w = \sqrt[2]{1} e^{\frac{i2k\pi}{2}} \end{aligned}$$

$K=0 \rightarrow w = e^{i0} = 1$
 $K=1 \rightarrow w = e^{i\pi} = -1$

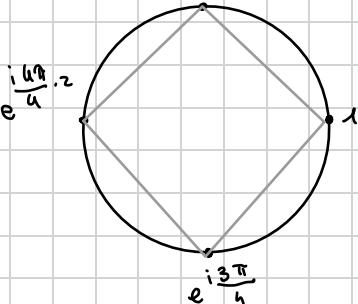
$$m=3 \quad e^{i\theta} = w^3 = 1 = e^{i2k\pi + i0} \rightarrow 3i\theta = 2k\pi i$$

$$\begin{aligned} \rightarrow \theta &= \frac{2k\pi}{3} \\ K=0 &\rightarrow w = e^{i0} = 1 \\ K=1 &\rightarrow w = e^{i\frac{2\pi}{3}} \\ K=2 &\rightarrow w = e^{i\frac{4\pi}{3}} \\ K=3 &\rightarrow w = e^{i\frac{2\pi \cdot 3}{3}} = e^{i2\pi} = 1 \end{aligned}$$

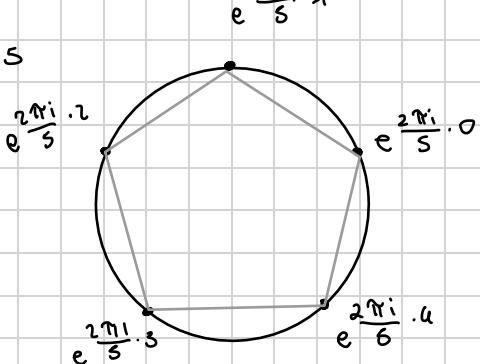


Nicogli

$$m=4$$



$$m=5$$



→ le radici emmesime di 1 sono

$$S_m = \{ w \in \mathbb{C} \mid w^m = 1 \}$$

$$= \left\{ w = e^{i \frac{2\pi}{m} \cdot k} \mid k = 0, \dots, m-1 \right\}$$

E sono esattamente i vertici di un poligono regolare con m lati che ha un vertice in 1.

Proprietà: Se $z_1, z_2 \in S_m \Rightarrow z_1 \cdot z_2 \in S_m$ infatti

$$\begin{aligned} z_1 &= e^{i \frac{2\pi}{m} \cdot k_1} & z_2 &= e^{i \frac{2\pi}{m} \cdot k_2} \\ z_1 \cdot z_2 &= e^{i \frac{2\pi}{m} (k_1 + k_2)} & &= e^{i \frac{2\pi}{m} (k_1 + k_2)} \in S_m \end{aligned}$$

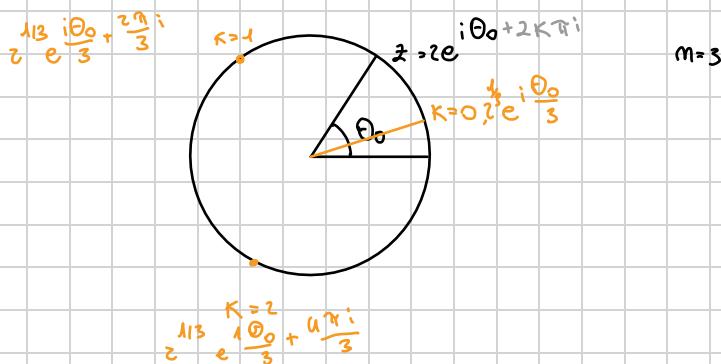
Radici emmesime di un numero $z \neq 1$

$$\begin{aligned} z &= r e^{i(\theta_0 + i2k\pi)} \\ \text{Cerco } w &= s e^{i\theta} \text{ t.c. } w^m = z \\ &\Leftrightarrow s^m e^{im\theta} = r e^{i(\theta_0 + i2k\pi)} \end{aligned}$$

radice

$$\begin{aligned} s^m &= r \rightarrow s = \sqrt[m]{r} \\ im\theta &= i(\theta_0 + i2k\pi) \\ \rightarrow \theta &= \frac{\theta_0}{m} + \frac{2k\pi}{m} \end{aligned}$$

→ In teoria k varia su \mathbb{Z} , ma per $k \geq m$, si ripetono i valori
⇒ Radici ($z = r e^{i(\theta_0 + i2k\pi)}$) = $\{ w = r^{\frac{1}{m}} e^{i(\frac{\theta_0}{m} + \frac{i2k\pi}{m})} \mid k = 0, 1, \dots, m-1 \}$



Errore: Nelle divisioni con resto non posso moltiplicare per -1

$$\Rightarrow -17 : 6 \quad \xrightarrow{\quad} 17 : 6 = 2 \text{ resto } 5$$

$$-17 = 5 \cdot (-1) + 3$$

$$\downarrow 9 \quad \downarrow 7$$

Teoria dei Gruppi

- gruppi } muove "strutture"
- campi } algebriche = insiemi su cui possiamo compiere operazioni con certe proprietà
- omomorfismi }
- isomorfismi } applicazioni tra gruppi

def. Una operazione su un insieme S è una funzione $f: S \times S \rightarrow S$.

(prende due elementi di S e restituisce un elemento di S)

Si indica con $\ast, +, \cdot, \circ$.

Proprietà:

- Associativa $(a \ast b) \ast c = a \ast (b \ast c)$ → sempre
- Commutativa $a \ast b = b \ast a$ bonus es. prodotto tra matrici quadrate
composizione di funzioni

def. Un elemento $e \in S$ è detto **elemento neutro** per un'operazione \ast se

$\forall a \in S, a \ast e = e \ast a = a$

es. 0 è l'elemento neutro per $+$ su \mathbb{R}

• il vettore/matrice nulla è l'elemento neutro per $+$ su \mathbb{R}^m /spazi vettoriali

• 1 è l'elemento neutro per la moltiplicazione su \mathbb{R}

• I è l'elemento neutro per la moltiplicazione sulle matrici $m \times n$.

def. Un elemento $a \in S$ è detto **invertibile** (rispetto all'operazione \ast) se esiste

un altro elemento a^{-1} detto **inverso** di a , t.c. $a \ast a^{-1} = a^{-1} \ast a = e$

es. $(\mathbb{Z}, +, 0)$ $q \in \mathbb{Z}$

$(M \times M, -, I)$

$$3^{-1} = -3 \quad q^{-1} = -q$$

gli elementi invertibili

sono le matrici invertibili

elemento

neutro

Notazione Se \ast è associativa, denotiamo $\underline{a \ast a \ast \dots \ast a}$ come a^m
in verde

Def. (**gruppo**) Un gruppo è una **forma** (G, \ast, e) dove G è un **insieme**, \ast è una **operazione associativa** su G con **elemento neutro** e , e tale che **ogni elemento di G** ha un **inverso** in G .

es.

1. $(\mathbb{R}, +, 0), (\mathbb{Z}, +, 0), (\mathbb{C}, +, 0), (\mathbb{Q}, +, 0)$ sono gruppi.

$(\mathbb{N}, +, 0)$ non è un gruppo perché non esiste l'inverso (eccetto per 0)

$$3^{-1} = -3 \notin \mathbb{N}$$

2. $(\mathbb{R}^*, \cdot, 1), (\mathbb{C}^*, \cdot, 1), (\mathbb{Q}^*, \cdot, 1)$ sono gruppi

$(\mathbb{Z}^*, \cdot, 1) \text{ NO, perché non ci sono gli inversi}$

$$a^{-1} = \frac{1}{a} \notin \mathbb{Z}$$

$$\mathbb{S}^* = \mathbb{S} \setminus \{0\}$$

3. $(\mathbb{R}^m, +, 0), (\mathbb{C}^m, +, 0), (\mathbb{M}_{m \times m}, +, 0)$ sono gruppi

matrice nulla

vettore nulla

sia su \mathbb{C} che su \mathbb{R}

4. Matrici invertibili $m \times m$ (sia su \mathbb{R} che su \mathbb{C}):

Sono un gruppo per la moltiplicazione con la matrice identità come elemento neutro d'insieme delle matrici invertibili $m \times m$ (su \mathbb{C} o su \mathbb{R}) si denota con $GL(m, \mathbb{R})$ o

Quindi in formule,

$$GL(m, \mathbb{C})$$

$(GL(m, \mathbb{R}), \cdot, I)$ e $(GL(m, \mathbb{C}), \cdot, I)$ sono gruppi per ogni m .

Oss. Se m è l'insieme di tutte le matrici su \mathbb{R} o su \mathbb{C} , $(m, +, 0)$ non è un gruppo perché per poter sommare due matrici è necessario che abbiano la stessa dimensione.

I gruppi di matrici rispetto alla somma e alla moltiplicazione sono comunque diversi.

All'interno di questi gruppi "fondamentali" possiamo trovare sottogruppi.

def. (Sottogruppo) Sia $(G, *, e)$ un gruppo. Un sottogruppo H di G è un insieme $H \subset G$

tale che:

$$\textcircled{1} \quad e \in H$$

$\textcircled{2} \quad \forall a, b, a * b \in H$ chiuso rispetto a *

$\textcircled{3} \quad \forall a \in H, a^{-1} \in H$

Si indica con $H \subset G$

Ovvero, un sottogruppo è un gruppo rispetto alle operazioni del gruppo più grande. Praticamente, il sottogruppo eredita l'operazione del gruppo più grande, che a sua volta determina l'elemento neutro.

Quindi l'operazione è associativa di default, devo solo controllare che il sottogruppo contenga l'elemento neutro, sia chiuso rispetto all'operazione, e contenga gli inversi: in formule, la def. di sottogruppo.

Esempi di sottogruppi

- $(\mathbb{R}, +, 0)$ è un sottogruppo di $(\mathbb{C}, +, 0)$ $\mathbb{R} \subset \mathbb{C}$
- $(\mathbb{R}^*, \cdot, 1)$ è un sottogruppo di $(\mathbb{C}^*, \cdot, 1)$ $\mathbb{R}^* \subset \mathbb{C}^*$
- $(m\mathbb{Z}, +, 0)$ è un sottogruppo di $(\mathbb{Z}, +, 0)$ $m\mathbb{Z} \subset \mathbb{Z}$
 \hookrightarrow multipli di $m = \{mk \in \mathbb{Z}, k \in \mathbb{Z}\}$

- le matrici diagonali $m \times m$ sono un sottogruppo di $(M_{m \times m}, +, 0)$
- le matrici invertibili diagonali sono un sottogruppo di $(M_{m \times m}, \cdot, I)$
- $\forall m$, le radici m -esime dell'unità δ_m

$$\delta_m \subset (\mathbb{C}^*, \cdot, 1)$$

Notazione: se H è un sottogruppo di G , si scrive $H \subset G \Rightarrow (\mathbb{Z}, +, 0) \subset (\mathbb{R}, +, 0)$

insieme
 \downarrow op.
 $\{$ elem.
 $\}$ neutro
 $(G, *, e)$

15.04.24

Come controllo se G è un gruppo?

- 1) Vedo se l'operazione è ben definita $g_1 * g_2 \in G \quad \forall g_1, g_2 \in G$
- 2) Esistono inversi $\forall g \in G \exists g^{-1}, g * g^{-1} = e$

PROPRIETÀ DI
TUTTI I GRUPPI

es. Se $G = \text{insieme matrici invertibili } m \times m$

$GL(m)$

$* = \cdot$

$e = \text{matrice nulla}$

la somma di due matrici può non essere
invertibile \Rightarrow non è un gruppo

! OK se prendo il prodotto tra matrici

- $(\mathbb{N}, +, 0)$ non è un gruppo perché mancano gli inversi

- $(\mathbb{Z}, \cdot, 1)$ non è un gruppo perché mancano gli inversi

! L'inverso di un numero dipende dall'op. scelta

inverso di 2 rispetto alla somma è -2

moltiplicazione è $\frac{1}{2}$ \rightarrow notazione
gruppo 2^{-1}

Tipi particolari di gruppi

- Abeliani e non abeliani
- Finiti e Infiniti

def. (gruppo Abeliano) È un gruppo in cui l'operazione è commutativa.

$$(G, *, e) \quad a * b = b * a \quad \forall a, b \in G$$

def. (gruppo Finito) Un gruppo si dice finito se ha un numero finito di elementi

Q: Quali gruppi finiti conosciamo?

$$\{0, \dots, m-1\} \text{ modulo } m$$

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \cdot, e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

matrici ortogonali con ± 1

• Radice dell'unità

• permutazioni di m oggetti

oss. Essere abeliano dipende sia dall'operazione che dall'insieme.

es. $(GL(m), \cdot, I)$ non abeliano \rightarrow le matrici quadrate invertibili

$(\text{matrici diagonali invertibili } mxm, \cdot, I)$ sono abeliane

oss. La differenza tra gruppo e sottogruppo è che il sottogruppo eredita l'operazione del gruppo \Rightarrow non deve contraddirne le proprietà dell'operazione

Notazione: Il numero di elementi di G si indica:
1) $\# G \rightarrow$ cardinalità: si utilizza + spesso
 \times gli insiemi
2) $|G| \rightarrow$ modulo

esercizio

- 1) Se $H \subset G$, G gruppo finito $\Rightarrow |H| \mid |G|$ (il # di elementi di H divide il numero di G)
- 2) Riconoscere gli esempi di gruppi e trovare quelli finiti e abeliani

OSS. Un gruppo può non essere abeliano se avere sottogruppi abeliani

(matrici diagonali invertibili sono un sottogruppo abeliano delle matrici diagonali $(GL(m), \cdot, I)$ che non è abeliano)

Q: un gruppo è un insieme G o una forma

def. (Gruppo Abeliano) $(G, *, e)$ se $*$ è commutativa.

PROPR. DELL'INSIEME CON QUALEVA SR.

$$a * b = b * a \quad \forall a, b \in G$$

def. (Gruppo Finito) $(G, *, e)$ è finito se ha un numero finito di elementi

Q: Che gruppi finiti conosciamo?

$$\cdot \{0, \dots, m-1\} \text{ modulo } m \quad \cdot \text{Radice dell'unità}$$

$$\cdot G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \dots, e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Matrici di ortogonali con ± 1

$$g^2 = e$$

OSS. Essere abeliano dipende sia dall'op che dall'insieme

ES. $(\mathbb{Z}/m\mathbb{Z}), \cdot, I)$ non abeliano

$(\text{matr. diag. invert. } M \times M, \cdot, I)$ sono abeliane

OSS. La differenza tra gruppo e sottogruppo è che il sottogruppo eredita l'operazione del gruppo
⇒ non devo controllare le proprietà dell'operazione

Notazione: Il num. di elementi di G si indica: 1) $\#G$ cardinalità si usa + per gli insiemi

2) $|G|$

ES. Se $H \subset G$, G gruppo finito $\Rightarrow |H| \mid |G|$

(il # di elem di H divide il numero di G)

ES. Riconoscere gli esempi di gruppi delle pag. precedenti e trovare quelli finiti/abeliani

OSS. Un gruppo può non essere abeliano MA avere sottogruppi abeliani

mat inv. e mat diag

Notazione: $(G, *, e)$ spesso si scrive solo G (sotto intendo $*$, e .

→ "posso semplificare gli elementi"

Legge di cancellazione

Se $(G, *, e)$ è un gruppo, e $a, b, c \in G \Rightarrow$

$$a * b = a * c \Leftrightarrow b = c \quad | \quad \text{posso semplificare } a$$
$$b * a = c * a \Leftrightarrow b = c$$

potrebbe non esistere

abeliano

$$\stackrel{e}{\cancel{a}} \stackrel{e}{\cancel{b}} = \stackrel{e}{\cancel{a}} \stackrel{e}{\cancel{c}} \Rightarrow b = c$$

$$\text{es. } (\mathbb{R}, +, 0) \Rightarrow x + y = z + y \Leftrightarrow x = z$$

$$(\mathbb{Z}/m\mathbb{Z}, \cdot, I) \Rightarrow AB = CB \Leftrightarrow A = C \quad (\text{invertibili})$$

$$\underbrace{ABB^{-1}}_I = \underbrace{CBB^{-1}}_I \Rightarrow A = C$$

$$\begin{array}{ccc} AC = BC & & \\ A = B & \nearrow & \searrow \\ CA = CB & & \end{array}$$

posso semplificare solo se c è invertibile

! Se il gruppo è abeliano, l'elem. da semplificare deve essere dello stesso lato

$AB = CA$ non posso semplificare

dim. (legge di cancellazione) $(a, *, e)$

Siamo $a, b, c \in G$ $\exists a^{-1}$

$$\text{Se } a * b = a * c \Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c)$$

associaziva

$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$$

prop. inverso

$$\Rightarrow e * b = e * c$$

prop di e $\Rightarrow b = c$

Per tornare indietro,

$$\text{se } b = c \Rightarrow a * b = a * c$$

Stessa cosa per $b * a = c * a$

Dalla legge di cancellazione segue la risolvibilità delle eq. (lineari) ovvero

$\forall a, b \in G$, l'eq. $a * x = b$ ha come soluzione unica $x = a^{-1} * b$

Theorem Sottogruppi di \mathbb{Z}

I sottogruppi di \mathbb{Z} sono tutti e soli i gruppi della forma $(b\mathbb{Z}, +, 0)$ con $b \in \mathbb{Z}$

$(\mathbb{Z}, +, 0)$

$$\begin{aligned} b\mathbb{Z} &= \{a \in \mathbb{Z}, a = kb, \text{ con } k \in \mathbb{Z}\} \\ &= \{\text{multipli di } b\} \end{aligned}$$

$$7\mathbb{Z} = \{-21, -14, -7, 0, 7, 14, 21, \dots\}$$

(oss. $\Rightarrow \mathbb{Z}$ non ha sottogruppi finiti tranne il sottogruppo banale $\{0\}$)

dim. I sottogruppi banali sono $\{0\} = 0\mathbb{Z}$, e $\mathbb{Z} = 1\mathbb{Z} \checkmark$

Suppongo $H \subset \mathbb{Z}$ non banale. \Rightarrow ha elementi $\neq 0 \Rightarrow$ ha elementi positivi (perche' i soli contengono gli inversi).

Sia b il più piccolo intero positivo in H . (principio del buon ordinamento)

Dimostreremo che $H = b\mathbb{Z}$

$b\mathbb{Z} \subset H$ Sia $kb \in b\mathbb{Z}$. Se $k > 0 \Rightarrow kb = \underbrace{b+b+\dots+b}_{k \text{ volte}}$

elemento generico

$\Rightarrow kb \in H$ perche' H chiuso rispetto a $+$

$$\text{Se } k < 0 \Rightarrow (-k)b = \underbrace{-(b+\dots+b)}_{k \text{ volte}} \in H$$

$\Rightarrow -kb \in H$ perche' H contiene gli inversi

(Se $b \in H$, contiene anche tutti i suoi multipli $\Rightarrow b\mathbb{Z}$)

$H \subset b\mathbb{Z}$ Sia $m \in H$ usando la divisione con resto, $m = qb + r$ voglio far vedere $r=0$

Poiché $qb \in H \Rightarrow r = m - qb \in H$ ma per tesa divisione resto, $0 \leq r < b$

Poiché b era il più piccolo intero positivo in $H \Rightarrow r=0 \Rightarrow m = qb$

Resta da fare vedere che $b\mathbb{Z} \subset H$. (avendo che i multipli di un numero sono sottogruppi di \mathbb{Z})

• $\forall g_1, g_2 \in b\mathbb{Z}$ | se $g_1, g_2 \in b\mathbb{Z} \Rightarrow \exists k_1, k_2 \in \mathbb{Z}$ t.c.

$$g_1 + g_2 \in b\mathbb{Z} \quad g_1 = k_1 b \quad g_2 = k_2 b \\ \Rightarrow g_1 + g_2 = k_1 b + k_2 b = (k_1 + k_2) b$$

$\Rightarrow g_1 + g_2$ è multiplo di $b \Rightarrow g_1 + g_2 \in b\mathbb{Z}$

,
 g

• $\forall g \in b\mathbb{Z}, g^{-1} \in b\mathbb{Z}$

$$\text{Se } g = kb \Rightarrow -g = -(kb) = (-k)b \in b\mathbb{Z}$$

Esempio Gruppo delle Permutazioni

(es. di gruppo finito, tavola di moltiplicazione)

def.

S_m = gruppo delle permutazioni di m elementi

Prendo un insieme T con m elementi li posso rappresentare come $1, 2, \dots, m$.

$S_m = \{$ tutte le applicazioni da $T \rightarrow T$ bijective $\}$

= Aut(T)

= Automorfismi di T

= tutti i modi in cui posso scambiare gli elem. di T

Esempio $T = \{1, 2\}$

$$1, 2: 1 \mapsto 1 \quad 2, 1: 1 \mapsto 2$$

composizione $S_2 = \{(1, 2), (2, 1)\}$

$$2 \mapsto 2 \quad 2 \mapsto 1$$

(S_2, \circ, e)

$e = I$, è la permutazione che mantiene inalterato l'ordine degli elementi ($1, 2, \dots, n$)

Esempio $T = \{1, 2, 3\}$

$S_3 = \{(1, 2, 3), (1, 3, 2), (2, 3, 1), (2, 1, 3), (2, 3, 1), (3, 2, 1), (3, 1, 2)\}$

$$(1, 2, 3): 1 \mapsto 1$$

$$2 \mapsto 3$$

$$3 \mapsto 2$$

$$(2, 3, 1): 1 \mapsto 3$$

$$2 \mapsto 1$$

$$3 \mapsto 2$$

Esercizio Scrivere il gruppo di permutazioni di n elem. (sotto $n \cdot 3 \cdot 2 \cdot 1 = n!$)

Esercizio Dimostrare che (S_m, \circ, Id) è un gruppo.

- capire chi è $S_1 \circ S_2$

$$S_2^{-1}$$

$$1 \mapsto b_1, i \mapsto b_i$$

$$\downarrow$$

- Un elemento generico di S_m si scrive come $q = (b_1, \dots, b_m)$

$$p = (a_1, \dots, a_m)$$

$$p \circ q = (a_{b_1}, a_{b_2}, \dots, a_{b_m})$$

$$q \circ p = (b_{a_1}, b_{a_2}, \dots, b_{a_m})$$

$$1 \xrightarrow{q} b_1, 1 \xrightarrow{p} a_{b_1}$$

$$2 \xrightarrow{q} b_2, 2 \xrightarrow{p} a_{b_2}$$

$$1 \xrightarrow{p} a_1, 1 \xrightarrow{q} b_{a_1}$$

- Usiamo la composizione × scrivere l'inverso

$$q \text{ cerchiamo } q = p^{-1} \text{ t.c. } q \circ p = (1, 2, \dots, m)$$

$$\text{Se } q = (b_1, \dots, b_m) \Rightarrow q \circ p = (b_{a_1}, b_{a_2}, \dots, b_{a_m}) = (1, 2, \dots, m)$$

$$p = (a_1, \dots, a_m)$$

$$\Rightarrow a_1 \text{ t.c. } b_{a_1} = 1$$

$$a_m \text{ t.c. } b_{a_m} = m$$

$$\exists. \quad q = (2, 4, 1, 3)$$

$$q^{-1} = 1 \cdot (a_1, \dots, a_m)$$

$$b_{a_1} = 1 \Rightarrow b_3 = 1$$

$$b_{a_2} = 2 \Rightarrow$$

$$b_{a_3} = 3$$

$$a_3 = 4$$

$$\circ (3, 1, 4, 2)$$

$$q \circ p = 1 \xrightarrow{p} 1 \xrightarrow{q} 1$$

$$2 \xrightarrow{p} 1 \xrightarrow{q} 2$$

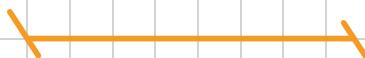
$$\circ S_m \ni Id : Id \rightarrow (1, 2, \dots, m)$$

$$\circ p \circ q \in S_m \quad \forall p, q \in S_m \text{ espl. } *$$

(Alternativa: la composizione di funz. biiettive è biiettiva.)

$$\circ p^{-1} \in S_m \quad \text{Or per la f. espl.}$$

(Alt.: l'inversa di una funz. biiettiva è biiettiva)



19.04.24

$(S, *, e)$

$* : S \times S \rightarrow S$

esistono gli inversi legge di cancellazione

	Finiti $\xrightarrow{\text{perm}}$ (S_2, \circ, I)	Infiniti $(\mathbb{Z}, +, 0), (\mathbb{R}, +, 0), (\mathbb{R}^*, \cdot, 1), (\mathbb{Q}^*, \cdot, 1)$
Abeliani	$(\text{Radici m-esima unità}, \circ, 1)$	$(M_{m \times m}, +, 0), (\mathbb{C}, +, 0), (\mathbb{C}^*, \cdot, 1), (\mathbb{Q}, +, 0)$
Non Abeliani	$\xrightarrow{\text{perm}}$ (S_m, \circ, I)	$(GL(m), \cdot, I)$ \downarrow mat. inv. $m \times m$

Permutazioni S_m

Sono i modi possibili di ordinare m oggetti

$$p \in S_m$$

$$p = (p_1 \dots p_m)$$

$$1 \mapsto p_1$$

$$2 \mapsto p_2$$

$$3 \mapsto p_3$$

$$\dots$$

$$m \mapsto p_m$$

Tavola di Moltiplicazione

Modo di sintetizzare le proprietà di un gruppo

S_2 : (permutazioni di due elementi)

$$S_2 = \{(1,2), (2,1)\}$$

"

id

	s_1	s_2
\circ	$(1,2)$	$(2,1)$
s_1	$(1,2)$	$(1,2)$
s_2	$(2,1)$	$(1,2)$

Nella posizione ij metto $s_j \circ s_i$

Info che ci dà la tavola di moltiplicazione

- Il gruppo è abeliano \Leftrightarrow è simmetrico rispetto alla diagonale principale
- Vedo subito quale è l'inverso di un elemento: trovo in quale posizione della sua riga/colonna compare e

! In ogni riga e in ogni colonna compare e

• Si vedono bene i sottogruppi (e se sono abeliani)

• Un gruppo si può definire attraverso una tavola di moltiplicazione (\equiv definire $*$)

es. $S = \{e, b, c, d\}$ insieme di 4 elementi

*	e	b	c	d
e	e	b	c	d
b	b	c	d	e
c	c	d	e	b
d	d	e	b	c

*	e	b	c	d
e	e	b	c	d
b	b	e	d	c
c	c	d	e	b
d	d	c	b	e

Tavola di moltiplicazione per S_3

(avendo come trovare sottogruppi abelliani)

*	(1,2,3)	(2,1,3)	(1,3,2)	(3,2,1)	(2,3,1)	(3,1,2)
(123)	123	213	132	321	231	312
(213)	213	123	312	231	321	132
(132)	132	231	123	312	213	321
(321)	321	312	231	123	132	213
(231)	231	132	321	213	312	123
(312)	312	321	213	132	123	231

Altri sottogruppi: Permutazioni cicliche, preservano ordine circolare

123 123123 ...

$$S_3^+ = \{(1,2,3), (231), (312)\}$$

le permutazioni non circolari?

321321 ...

$$S_3^- = \{(1,2,3), (321), (213), (132)\} \\ \rightsquigarrow (213)(321) = (312) \times$$

Esempio (gruppo di segni)

.	+	-
+	+	-
-	-	+

Stessa tabella di S_2

(e di qualunque gruppo con due elementi)

CAMP

Un campo è un gruppo (abeliano) con una operazione aggiuntiva \cdot con certe proprietà

def. un campo è un insieme F con due operazioni $+$, \cdot tali che

• $(F, +, 0)$ gruppo abeliano

• $(F^*, \cdot, 1)$ gruppo abeliano $F^* = F \setminus \{0\}$

• $\forall abc \in F, (a+b)c = ac+bc$ (proprietà distributiva)

Si indica con $(F, +, \cdot, 0, 1)$ o semplicemente $(F, +, \cdot)$

OSS In un gruppo le operazioni sono sempre omosociali

• campi con ∞ elementi

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (matrici no perché il prodotto non è commutativo)

• compi finiti

$\mathbb{Z}_p = \{ \text{classi di congruenza modulo } p \text{ con } p \text{ primo} \}$

Cosa vuol dire? Perche' p primo?

Conguenza modulo m

Sia $p, q \in \mathbb{Z}$ e sia $m \in \mathbb{N}$
non è
mezzodolmente
primo

Divisione con resto: $p = k_1 m + r_1 \quad 0 \leq r_1 < m$

$$* \quad q = k_2 m + r_2 \quad k_1, k_2 \in \mathbb{Z}$$

$p = q \pmod m$ (congruente a q modulo m)

Se hanno lo stesso resto, ovvero

$$p = q + km \quad \text{per qualche } k \in \mathbb{Z}$$

($p = q$ a meno di multipli di m)

Esempio $m=7$: Tutti i multipli di 7 sono uguali mod 7

es. $p = -21 \quad p = 35 + (-8) \cdot 7$

$$q = 35$$

$m=7 \quad 4 = 11 \pmod 7$ perche' $11 - 4 = 7 = 7 \cdot 1$ è multiplo di 7

oppure

$$4 : 7 = 0 \quad \bar{r}_4$$

$$11 : 7 = 1 \quad \bar{r}_4$$

oppure $11 = 4 + 1 \cdot 7$

Due numeri $p, q \in \mathbb{Z}$ appartengono alla stessa classe di congruenza mod $m \in \mathbb{N}$ se

- hanno lo stesso resto quando diviso per m

$$p = k_1 m + r_1 \quad \text{com } r_1 = r_2$$

$$q = k_2 m + r_2$$

$$p - q = km \quad \text{com } k \in \mathbb{Z}$$

$$p = q + km \quad \text{com } k \in \mathbb{Z}$$

equivalente

- la loro differenza è multiplo di m

- uno è uguale all'altro a meno di sommare

un multiplo di m

Questo induce una partizione di \mathbb{Z} in m classi di equivalenza,

siamo nella $\rightarrow p \sim q \Leftrightarrow p = q \pmod m \quad (p - q = km, \dots)$

stessa classe ovvero p è congruente a q modulo m .

(Relazioni di equivalenza, classi di \sim e partitioni hanno def. matematiche precise)

Ci sono ∞ elementi e un numero finito di classi ciascuna delle quali contiene ∞ elementi.

Per ogni classe di n posso scegliere un rappresentante di solito è la classe di resto, ovvero il rappresentante tra 0 e n

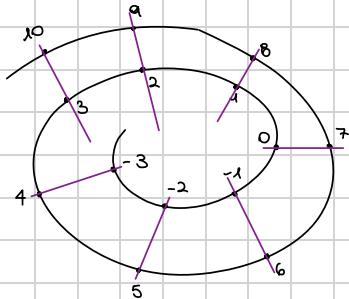
Ese. $m=7$

classi di eq.
contiene 60 numeri
coppia esponente

$$\left\{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \right\}$$

$\bar{0}$ = tutti i multipli di 7

$\bar{1}$ = tutti i numeri con resto 1 $\Rightarrow 1, 8, 15, -6, -13 \dots$



Com le classi di congruenza si possono fare somme e moltiplicazioni Modulo m

- le faccio normalmente e tolgo i multipli di m per ottenerne il coppia esponente che avevo scelto

Ese. $m=7$

$$\bar{3} + \bar{5} = \bar{8} = \bar{1}$$

$$\left\{ \bar{0}, \bar{1}, \dots, \bar{6} \right\}$$

$$\bar{8} = \bar{1} \bmod 7 \quad \bar{1} - \bar{8} = -7 = -7(-1) \text{ multiplo di 7}$$

$$\bar{3} \cdot \bar{6} = \bar{18} = \bar{4}$$

$$\bar{4} - \bar{18} = -14 = 7(-2) \text{ multiplo di 7}$$

$$[18 = \cancel{7} + 4]$$

Oss. $\bar{6} + \bar{5} = \bar{11} = \bar{4} \bmod 7$

$$[\bar{11} = \cancel{7} + 4]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{2} \bmod 9$$

$$[\bar{11} = \cancel{9} + 2]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{3} \bmod 8$$

$$[\bar{11} = \cancel{8} + 3]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{1} \bmod 10$$

$$[\bar{11} = \cancel{10} + 1]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{11} \bmod m \text{ se } m > 12$$

Matrici a coefficienti modulo p primo

Potrò usare come coefficienti delle matrici le classi di congruenza mod p

Ottengo gruppi finiti non abeliani

il prodotto tra matrici non è abeliano

Ese. $m=3$

$$\left\{ \bar{0}, \bar{1}, \bar{2} \right\}$$

Matrici:

$$\left\{ \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{2} & \bar{0} \end{pmatrix}, \dots, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \dots, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \dots \right\}$$

Compo $(K, +, \cdot, e_+, e_\cdot)$ $(K, +, e_+), (K^*, \cdot, e_\cdot)$
 $(K, +, \cdot, 0, 1)$ Abeliani

Esempi $C, \mathbb{R}, \mathbb{Z}_p$ primo

$$\mathbb{Z}_p = \{\text{classi di congruenza modulo } p\} \text{ ok per } p \in \mathbb{N}$$

$$= \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{p-1}\}$$

Teo Se p primo, \mathbb{Z}_p è un compo (no dim) Se p non è primo, potrebbero non esistere gli inversi moltiplicativi
 es. $p=3 \quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} \Leftrightarrow$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

diagonale

Abeliano

*	0	1	2
0	0		
1		1	2
2		2	1

diagonale

Abeliano

• Cosa succede se p non è primo?

$$\text{es. } p=4 \quad \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

.	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

fuori dal gruppo

\Rightarrow non è un gruppo

due moni ha l'inverso

Gli elementi che creano problemi se p non è primo
 sono i divisori di p

Eseguire le tavole di moltiplicazione per $(\mathbb{Z}_6, +)$ (\mathbb{Z}_6^*, \cdot)

$(\mathbb{Z}_6, +)$ (\mathbb{Z}_6^*, \cdot)

CURIOSITÀ

de classi di congruenza si possono usare per generare numeri pseudocasuali

Lc a (linear congruential generator)

seed: x_0 m. intero

$$x_{n+1} = (ax_n + c) \bmod m \quad \text{parametri}$$

variabili

Tante possibili scelte delle relazioni tra a, c, m.

Teo. (Hull-Dobell Thm) • Se $\text{MCD}(m, c) = 1$ (relativamente primi)

• $(a-1)$ divisibile per tutti i fattori primi di m

• $(a-1)$ divisibile per 4 se anche m lo è

\Rightarrow periodo dei numeri generati è $= a m$

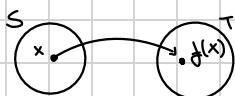
OMOAFORFISMI e ISOMAFORFISMI (tra gruppi e tra applicazioni lineari)

Applicazioni e funzioni:

da $\mathbb{R}^m / \mathbb{C}^m$ in se (spazi vettoriali)

def. Dati due insiemi S e T una funzione (o applicazione) $f: S \rightarrow T$ è qualcosa che associa ad ogni elemento $x \in S$ uno ed uno solo elemento $f(x) \in T$.

S si dice **dominio**.



T si dice **codomino**.

S
v
v
v

Notazione $f(x) = t$

$f: x \mapsto t = f(x)$

- f, g sono uguali se hanno lo stesso dominio S e codomino T
- $\forall x \in S, f(x) = g(x)$

- Applicazione Id su un insieme X associa ad ogni elemento di X se stesso:

$\text{Id}_X: X \rightarrow X$ (funzione va da x in x)

$\text{Id}_X(x) = x \quad \forall x \in X$

$\text{Id}_X: X \rightarrow X$

es. . $f: \mathbb{R} \rightarrow \mathbb{R}$

DOM, CODOM = \mathbb{R} | IMM. di \mathbb{R} è \mathbb{R}^+ (radi > 0) | IMM. di \mathbb{N} sono i num.

$x \mapsto 3e^x$ [$f(x) = 3e^x$]

CONTROIMM. di 3 è $x=0$

3e⁰

$\cdot f: M_{2 \times 2} \rightarrow \mathbb{R}$ $f(\text{mat. diag.}) = \begin{cases} \pm 1 \end{cases} \quad f(\text{mat. inv.}) = \mathbb{R} \setminus \{0\} \quad f^{-1}(0) = \{\text{mat. non invert.}\}$

$A \mapsto \det A$ [$f(A) = \det A$]

$\cdot f: \text{insiemi esercizi umani} \rightarrow \mathbb{N}$

persona \mapsto numero di compiti

$\cdot f: \mathbb{Z} \rightarrow \mathbb{Z}$ $f(z) = 5z = \text{multipli di } 5 \quad f(3\mathbb{Z}) = 15\mathbb{Z}$ (imm.) $f^{-1}(10\mathbb{Z}) = 2\mathbb{Z}$

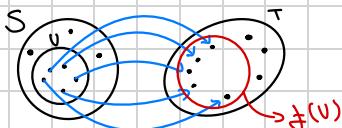
$a \mapsto 5a \quad f(a) = 5a$

IMMAGINE e CONTROIMMAGINE

Sia $f: S \rightarrow T$ sia $U \subseteq S$

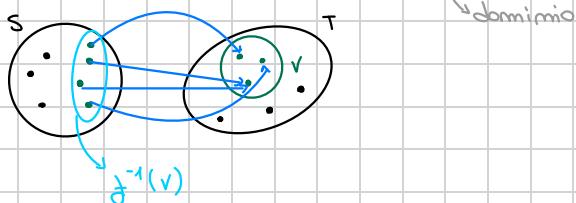
def.: d' l'immagine di U secondo f è l'insieme $f(U) = \{t \in T : \exists s \in U, f(s) = t\} \subset T$

(l'immagine sta nel codomino)



def. Se $V \subseteq T$ la composizionemagine/priamimmagine di V secondo f è l'insieme

$$f^{-1}(V) = \{s \in S \mid f(s) \in V\} \subset S$$



! Possiamo guardare l'immagine di tutto il dominio S .

INIEZIATIVITÀ e SURIEZIATIVITÀ

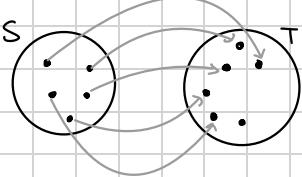
$$f: S \rightarrow T$$

def: $f: S \rightarrow T$ è iniettiva se $\forall s, u \in S$

$$s \neq u \Rightarrow f(s) \neq f(u)$$

ovvero: • $f(u) = f(s) \Leftrightarrow s = u$

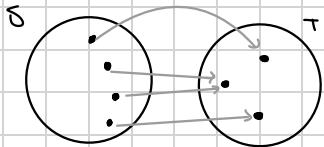
• elementi distinti di S vengono mandati in elementi distinti di T



def. $f: S \rightarrow T$ è suriettiva se $f(S) = T$

ovvero: • ogni elemento di T ha una priamimmagine in S

• $\forall t \in T \exists s \in S$ tale che $f(s) = t$



IMPORTANTE f è sia iniettiva che suriettiva si dice **BIETTIVA**.

es: riguardo gli esempi, stabilire se iniettive, suriettive o biettive

! Attenzione: Dipende da come definiamo dominio e codominio

$$\text{es } f: \mathbb{R} \rightarrow \mathbb{R}$$

$$a \mapsto |a|$$

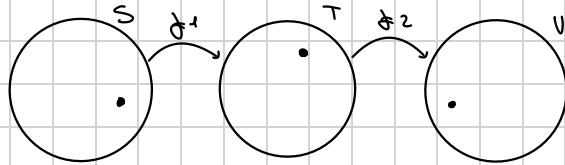
non è iniettiva perché $|a| = a$

$$f: \mathbb{R}^+ \rightarrow \mathbb{R}^+ \text{ iniettiva e suriettiva} = \text{Id}_{\mathbb{R}^+}$$

Ruolo Speciale: $f: S \rightarrow S$ da un insieme in se stesso
(endomorfismi/operatore)

Se biettive: (automorfismi/isomorfismi)

Composizione



$$f_2 \circ f_1 : S \rightarrow U$$

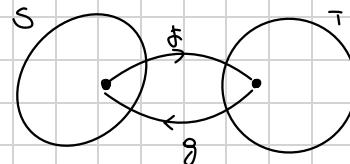
$$s \mapsto f_2(f_1(s))$$

Inversa (se esiste)

$f : S \rightarrow T$ è invertibile se $\exists g : T \rightarrow S$

talché $g \circ f = \text{Id}_S$ e $f \circ g = \text{Id}_T$

g si dice inversa di f , $g = f^{-1}$



Proposizione

Sia $f : S \rightarrow T$ sono equivalenti:

- f è invertibile
- f è biettiva
- $\forall t \in T \ \exists! s \text{ t.c. } f(s) = t$

! Attenzione: dipende dalle scelte di dom. e codom.

es. $f : \mathbb{R} \rightarrow \mathbb{R}^+ \quad f(x) = x^2$ non è invertibile

$f : \mathbb{R}^+ \rightarrow \mathbb{R}^+ \quad f(x) = x^2$ è invertibile

RECLUPERARE LEZIONE VENERDÌ

SPAZI VETTORIALI, COMBINAZIONI LINEARI



\hookrightarrow Esempio

V insieme, + somma, moltiplicazione per scalare

$$V = \mathbb{R}^m (\mathbb{C}^m)$$

$W \subset \mathbb{R}^n$ è un sottospazio se $\forall v, w \in W \cdot v+w \in W$

$$\forall v \in W, c \in \mathbb{R} \cdot cv \in W$$

COMBINAZIONI LINEARI

def Un vettore $v \in \mathbb{R}^n$ è combinazione lineare (cl) di $v_1 - v_k$ se esistono $a_1 - a_n \in \mathbb{R}$ t.c.

$$v = a_1 v_1 + \dots + a_n v_n = \sum_i a_i v_i$$

oss. dato qualunque insieme di vettori $v_1 - v_k$, posso sempre scrivere $0 = 0v_1 + \dots + 0v_k$

oss. Vedere se v è cl di $v_1 - v_k$ è la stessa cosa che chiedere se il sss. lin.

$AX = v$ ha soluzione

$\cdot a_1 - a_k$ sono le incognite

$$\cdot A = \begin{pmatrix} | & | \\ v_1 & v_k \end{pmatrix}$$

$$A = \begin{pmatrix} | & | \\ v_1 & v_k \end{pmatrix} \quad X = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

è la matrice dei coefficienti

\cdot 1° termine nulo \rightarrow se $v=0 \Rightarrow$ compatibile

per $a_i = 0 \forall i$:

esempio

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ è cl di } \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \Leftrightarrow \exists a_1, a_2 + c. \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix} = a_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix}?$$

$$\Rightarrow \begin{pmatrix} v_1 & v_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ è comp.} \Leftrightarrow \operatorname{rg} \begin{pmatrix} v_1 & v_2 \\ 0 & 1 \end{pmatrix} = \operatorname{rg} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ vero} \Rightarrow \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ è cl di } v_1, v_2$$

\Rightarrow Per vedere se v è cl di $v_1 - v_k$ scrivo $A = (v_1 - v_k)$ e confronto $\operatorname{rg} A$ con $\operatorname{rg} Av$

Cosa fondamentale: $\operatorname{rg} A$, le cui colonne sono i vettori $v_1 - v_k$

$$\cdot$$
 dati $v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ e $v_2 = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$, $v = \begin{pmatrix} -2 \\ -a \end{pmatrix}$ è cl di v_1, v_2

$$w = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \text{ non è cl di } v_1, v_2$$

Infatti

$$A = \begin{pmatrix} | & | \\ v_1 & v_2 \end{pmatrix}$$

$$\text{per } v: \left| \begin{array}{cc|c} 1 & 3 & -2 \\ 2 & 6 & -a \end{array} \right| \operatorname{rg} A \stackrel{-2}{=} 1 \quad \text{J comp.}$$

$$\operatorname{rg} A = 1$$

$$\text{per } w: \left| \begin{array}{cc|c} 1 & 3 & 1 \\ 2 & 6 & 3 \end{array} \right| \operatorname{rg} A \stackrel{-2}{=} 2 \times \text{non comp.}$$

Spazio generato

Dati $v_1 - v_k \in \mathbb{R}^m$, lo spazio generato da $v_1 - v_k$ è

$$\mathcal{L}(v_1 - v_k) = \{ v \in \mathbb{R}^m \mid v = a_1 v_1 + \dots + a_k v_k, a_i \in \mathbb{R} \}$$

= spazio delle c. di $v_1 - v_k$

• Ese. • retta im \mathbb{R}^3 passante per 0 • piano im \mathbb{R}^3 passante per 0

$$c: X = tA$$

$$c: L(A)$$



$$p: X = sA_1 + tA_2$$

numeri



Oss. lo spazio generato è sempre un ssv di \mathbb{R}^m [se $v, w \in \mathcal{L}(\dots)$ =>

$$v+w \in \mathcal{L}(\dots)$$

$$\text{Se } v \in \mathcal{L}(\dots)$$

$$c \in \mathbb{R}, cv \in \mathcal{L}(\dots)$$

def. Insieme di generatori. Sia W ssv di \mathbb{R}^m , un insieme di generatori per W è un insieme di vettori $v_1 - v_k$ t.c.

$$W = \mathcal{L}(v_1 - v_k)$$

Nell'esempio sopra • retta: trovare un insieme di generatori significa trovare un vettore direzione (definito a meno di multipli)

• piano: = trovare due vettori che generano il piano (ha molta più libertà)

Caso particolare: Quando $v_1 - v_k$ generano \mathbb{R}^n ?

$$\begin{array}{c} m \\ | \\ \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \left(\begin{array}{c} \\ \\ \\ \end{array} \right) = \left(\begin{array}{c} \\ \\ \\ \end{array} \right) \\ \text{comp \# termine nato} \\ \iff \text{rg } A = m \\ A \end{array}$$

\Rightarrow K vettori im \mathbb{R}^m generano $\mathbb{R}^m \Leftrightarrow \text{rg } A = m$

\Rightarrow Sono almeno m vettori per generare \mathbb{R}^m

Oss. Se $A \in \mathbb{M}_{m \times n}$, $\text{rg } A \leq \min(\# righe, \# colonne)$

$$\leq \min(m, n)$$

\Rightarrow se $k < m$, $\text{rg } A < m$

Esempio • im \mathbb{R}^2 sono almeno due vettori per generare \mathbb{R}^2

$$\bullet v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad v_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix} \quad A = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \quad \text{rg } A = 2$$

\Rightarrow generano \mathbb{R}^2 ✓

$$\bullet v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad v_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix} \quad v_3 = \begin{pmatrix} 3 \\ 7 \\ \sqrt{\pi} \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & -1 & 3 \\ 2 & 1 & \sqrt{\pi} \end{pmatrix} \quad \text{rg } A = 2 \Rightarrow \text{generano } \mathbb{R}^2 \quad \text{Vettore di troppo!}$$

$$\bullet v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad v_2 = \begin{pmatrix} -1 \\ -2 \end{pmatrix} \quad v_3 = \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & -2 & 3 \end{pmatrix} \quad \text{rg } A = 1 \Rightarrow \text{mom generano } \mathbb{R}^2 \quad \text{anche se sono 3 vettori e } 3 > 2$$

Vettori linearmente (Im) dipendenti

linearmente dipendenti (LD)

$\Leftrightarrow \text{im } A \subset \text{li}$

def. • $v_1, \dots, v_k \in \mathbb{R}^m$ sono LD se

$\exists a_1, \dots, a_k$ non tutti nulli t.c.

$$a_1 v_1 + \dots + a_k v_k = 0 \quad \Leftrightarrow \text{Il sl } Ax = 0 \text{ mom ha sol. unica} \quad (\Rightarrow \# \text{sol.} > \text{rg } A)$$

$$\Leftrightarrow k > \text{rg } A$$

• $v_1, \dots, v_k \in \mathbb{R}^m$ sono LI se

$$a_1 v_1 + \dots + a_k v_k = 0 \Rightarrow a_i = 0 \quad \forall i$$

(gli a_i sono tutti nulli)

$\Leftrightarrow \text{Il sl } Ax = 0 \text{ ha soluzione unica}$

$$\Leftrightarrow \# \text{sol.} = \text{rg } A$$

$$\Leftrightarrow \text{rg } A = k$$

• v_1, \dots, v_k sono LD se esistono loro a_i che danno 0, ma in cui almeno uno dei coeff è non nullo

• Sono LI se l'unica cl che dà 0 è quella con tutti i coeff nulli

OSS. v_1, \dots, v_k sono LD $\Leftrightarrow \text{rg } A < k$

Sono LI $\Leftrightarrow \text{rg } A = k$

ESEMPIO Se no 3 vettori im \mathbb{R}^2 , possono essere LI?

$$A = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} \quad \text{rg } A \leq 2 \text{ perché i vettori sono im } \mathbb{R}^2$$

Ma per essere LI serve $\text{rg } A = k = 3$

\Rightarrow mom possono essere LI

OSS Se no k vettori im \mathbb{R}^m e $k > m \Rightarrow$ mom possono essere LI

$$A = \left(\begin{array}{c|c|c|c} & & & \\ \hline & & & \\ \hline & & & \\ \hline \end{array} \right) \quad \text{rg } A \leq \min(k, m) \leq m < k$$

def. Una base per \mathbb{R}^n è un insieme di vettori tali che

• generano \mathbb{R}^n

• sono LI

\Rightarrow Ovvero ogni vettore di \mathbb{R}^n si può scrivere in maniera unica come cl dei vettori della base
generano LI

CRITERI

$$k \text{ vettori in } \mathbb{R}^m \rightarrow A = \left(\begin{array}{c|c|c|c} & & \dots & \\ \hline 1 & & & \\ \vdots & & & m \end{array} \right)^\top$$

- generano \mathbb{R}^n se $\operatorname{rg} A = n \Rightarrow k \geq n$
- sono li $\Leftrightarrow \operatorname{rg} A = k \Rightarrow k \leq n$

Per avere entrambe servono:

- esattamente n vettori
- $\operatorname{rg} A = n$

$\Rightarrow \forall_{e_i} \quad \forall_k \text{ sono una base per } \mathbb{R}^n \Leftrightarrow k = n$

$$\operatorname{rg} A = n = k$$

ESEMPIO $\bullet \mathbb{R}^3 \quad e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad n = 3 \quad k = 3$

$\mathcal{E} = \{e_1, e_2, e_3\}$ si chiama base canonica

$$A = \begin{pmatrix} e_1 & e_2 & e_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{array}{l} \text{generatore: } \operatorname{rg} A = n = 3 \\ \text{li: } \operatorname{rg} A = k = 3 \end{array} \Rightarrow \text{sono base}$$

$$\operatorname{rg} A = 3$$

• Verificare se $\begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}$ formano base di \mathbb{R}^3

$$n = 2 \quad (\mathbb{R}^2)$$

$$k = 2 \quad (\text{numero vettori})$$

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 3 \\ 1 & 1 \end{pmatrix} \quad \begin{array}{l} \text{generano: } \operatorname{rg} A = n = 2 \\ \text{li: } \operatorname{rg} A = k = 2 \end{array} \Rightarrow \text{BASE}$$

$$\operatorname{rg} A = 2$$

• $\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ formano base di \mathbb{R}^3 ?

• $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ formano base di \mathbb{R}^3 ? $k = 3 \quad n = 3$

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \begin{array}{l} \text{generano: } \operatorname{rg} A = n = 3 \\ \text{li: } \operatorname{rg} A = k = 3 \end{array} \Rightarrow \text{non sono BASE}$$

$$\operatorname{rg} A = 2$$

• $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$? $n = \quad k =$

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}$$

OSS. K vettori in \mathbb{R}^n generano $\Leftrightarrow \text{rg } A = \text{dimensione dello spazio}$

$l_i \Leftrightarrow \text{rg } A = \text{numero di vettori}$

\Rightarrow Operativamente, scivo A e confronto $\text{rg } A$ con K, m .

OSS. Se ho m vettori in \mathbb{R}^n , generare e essere l_i sono equivalenti, perch' entrambi valgono
"giusto" di vettori $\Leftrightarrow \text{rg } A = m$

OSS. se ho $K < m$ vettori possono essere l_i
non possono generare

Se ho $K > m$ vettori possono generare
non possono essere l_i

OSS. Rango di una matrice
non nulle

- # righe / matrice a scala
- massimo ordine minore non singolare
- # pivot
- # colonne l_i NEW
- # righe l_i ($\text{rg } A = \text{rg } A^\top$)

Fr. Data $A \in \mathbb{M}_{m \times n}$; quali sono le condizioni equivalenti all'aver rango massimo?

Tipi speciali di basi

• v_1, \dots, v_m sono base di $\mathbb{R}^n \Leftrightarrow A$ ha rango m , ovvero è **INVERTIBILE**.

(A invertibile \Leftrightarrow le sue colonne formano una base)

• Se A è ortogonale (\Rightarrow invertibile)

le sue colonne sono mutualmente ortogonalie di matrice 1 : formano una base ortogonale

In quest' caso, i coeff. delle l_i si trovano semplicemente con il prodotto scalare

Applicazioni lineari

\mathbb{R}^m come spazio vettoriale

$$v + w \in \mathbb{R}^m$$

$$cv \in \mathbb{R}^m$$

BASE B: insieme di vettori che generano e

sono linearmente indipendenti

dim \mathbb{R}^m = # vettori di una base

criterio: K vett. sono li $\Leftrightarrow \text{rg } A = K$

K vett. generano $\mathbb{R}^m \Leftrightarrow \text{rg } A = m$

$$\Rightarrow \dim \mathbb{R}^m = m$$

G gruppo $(G, *, e)$

G' " $(G', *, e')$

$\varphi: G \rightarrow G'$ omom.

$$\varphi(g * g') = \varphi(g) * \varphi(g')$$

$$\varphi(g^{-1}) = [\varphi(g)]^{-1}$$

$\text{Ker } \varphi, \text{ Im } \varphi \rightarrow \text{Ker } \varphi \subset G$

$\text{Im } \varphi \subset G'$

ISOM.: OMOM + INIETTIVI + SURIETTIVI

Applicazioni lineari

- def. $F: \mathbb{R}^m \rightarrow \mathbb{R}^m$ è una app. lin. se:
- $F(u+v) = F(u) + F(v) \quad \forall u, v \in \mathbb{R}^m$
 - $F(cv) = cF(v) \quad \forall v \in \mathbb{R}^m, c$ scalare
 - $F(0) = 0$

È sufficiente definire F su una base

Se $B = \{v_1, \dots, v_m\}$ base e $F(v_i) = w_i \in \mathbb{R}^m$
 $F(v_m) = w_m \in \mathbb{R}^m$

$$\Rightarrow F(v) = ? \quad v \in \mathbb{R}^m?$$

$v = a_1v_1 + \dots + a_mv_m$, a_i univocamente determinati perché la base

$$F(v) = F(a_1v_1 + \dots + a_mv_m) = a_1F(v_1) + \dots + a_mF(v_m) = a_1w_1 + \dots + a_mw_m$$

Immagine di v

ESEMPIO Se $C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Definiamo $F\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $F\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$$F\left[\begin{pmatrix} x & y \\ u & v \end{pmatrix}\right] = F\left(x\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = xw_1 + yw_2$$

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} = x\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= xF\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + yF\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = x\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + y\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$$

Caricale: Ad ogni matrice $m \times m$ corrisponde una AL da $\mathbb{R}^m \rightarrow \mathbb{R}^m$, Ad ogni AL da $\mathbb{R}^m \rightarrow \mathbb{R}^m$ corrisponde una mat. $m \times m$ (per ogni scelta di base)

ESEMPIO:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{1m} \\ & & \\ a_{m1} & & a_{mm} \end{pmatrix} \text{ deg. } L_A: v \mapsto Av$$

$$\text{UN: } A(v+w) = Av + Aw$$

$$A(cv) = cAv$$

$$\underbrace{\begin{pmatrix} & & \\ & A & \\ & & \end{pmatrix}}_{m \times m} \underbrace{\begin{pmatrix} & & \\ v & & \\ & & \end{pmatrix}}_{m \times 1} = w$$

$$\underbrace{\begin{pmatrix} & & \\ & A & \\ & & \end{pmatrix}}_{m \times m} \underbrace{\begin{pmatrix} & & \\ w & & \\ & & \end{pmatrix}}_{m \times 1} = w$$

Facciamo il conto:

$$A \begin{pmatrix} x_1 \\ 1 \\ x_m \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mm}x_m \end{pmatrix} = L_A(x_1 \quad \underset{\text{junzione}}{\text{x}_m})$$

Ogni variabile compare con la potenza uno senza l'aggiunta di costanti.

Esempio: $L(x, u) = \begin{pmatrix} x+u \\ x-u \end{pmatrix}$

$$L(0, 0) = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Tutte le AL da \mathbb{R}^n in \mathbb{R}^m sono in questa forma.

Esempio:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} \quad L_A: \mathbb{R}^4 \rightarrow \mathbb{R}^2 \quad \begin{matrix} \text{moltiplicazione vettori di } \mathbb{R}^m \text{ per una matrice li trasforma} \\ \text{in vettori di } \mathbb{R}^m \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 \\ 5 \cdot x_1 + 6 \cdot x_2 + 7 \cdot x_3 + 8 \cdot x_4 \end{pmatrix} = L_A(x_1, x_2, x_3, x_4)$$

Esempio:

$$f(x, u, z) = \begin{pmatrix} x^2 + u \\ u - z \end{pmatrix} \quad \text{NON è lin. perché } x^2$$

$$f(x, u, z) = \begin{pmatrix} x - u + z + 1 \\ x + z \end{pmatrix} \quad \text{" " " " " + 1}$$

Notazione: le AL si indicano con F, L, T

Come associamo una (m, n) mat ad una AL?

- B. CANONICA: $C = \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \dots \right\}$

$$\begin{pmatrix} x_1 \\ 1 \\ x_m \end{pmatrix} = x_1 e_1 + x_2 e_2 + \dots + x_m e_m$$

$$L: \mathbb{R}^m \rightarrow \mathbb{R}^m \quad \text{l'immagine}$$

$$L(x_1 \quad \dots \quad x_m) = x_1 L(e_1) + \dots + x_m L(e_m)$$

$$= \begin{pmatrix} 1 & | & \dots & | & 1 \\ L(e_1) & | & \dots & | & L(e_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

$\Rightarrow A_L(C, C)$ = matrice che ha per colonne l'immagine di vettori di base

Esempio:

$$L(x_1, x_2) = \begin{pmatrix} x_1 + 18x_2 \\ -x_1 \end{pmatrix} \quad \rightsquigarrow A_L = ?$$

$$L\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$L\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 18 \\ 0 \end{pmatrix} \quad \longrightarrow \quad A_L = \begin{pmatrix} 1 & 18 \\ -1 & 0 \end{pmatrix}$$

$$\begin{matrix} x_1 = 1 \\ x_2 = 0 \end{matrix}$$

Possiamo scrivere la matrice associata a $(\mathbb{R}^n, \mathcal{B})$ $B = \{v_1, \dots, v_m\}$

$(\mathbb{R}^m, \mathcal{B}')$

$$A_L(B', \mathcal{B}) = \begin{pmatrix} [L(v_1)]_{\mathcal{B}'} & \dots & [L(v_m)]_{\mathcal{B}'} \end{pmatrix}$$

Le colonne di A_L sono le immagini dei vettori della base \mathcal{B} scritti in coordinate rispetto a \mathcal{B}' .

Proprietà: Così come $A_L(c, c) \cdot v = L(v)$

$$A_L(B', \mathcal{B})[v]_{\mathcal{B}} = [L(v)]_{\mathcal{B}'}$$

Ad ogni A_L associa un'unica matrice, una per ogni possibile scelta di basi.

Come posso da una base all'altra?

Def. Data $\mathcal{B}, \mathcal{B}'$ di \mathbb{R}^n , la matrice cambio base $m(\mathcal{B}', \mathcal{B})$ è la matrice che trasforma le coordinate di un vettore rispetto a \mathcal{B} nelle sue coordinate rispetto a \mathcal{B}' , ovvero $m(\mathcal{B}', \mathcal{B})[v]_{\mathcal{B}} = [v]_{\mathcal{B}'}$.

$$\forall v \in \mathbb{R}^n \quad m(\mathcal{B}', \mathcal{B})[v]_{\mathcal{B}} \text{ coggi. di } v \text{ come } c_i \text{ dei vettori di } \mathcal{B}$$
$$[v]_{\mathcal{B}'} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \quad \text{e} \quad [v]_{\mathcal{B}} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \quad \text{e} \quad \mathcal{B} = \{v_1, \dots, v_m\}$$

Come si scrive $(\mathcal{B}', \mathcal{B})$?

$$m(\mathcal{B}', \mathcal{B}) = \begin{pmatrix} 1 & | & 1 \\ [v_1]_{\mathcal{B}'} & \dots & [v_m]_{\mathcal{B}'} \\ 1 & | & 1 \end{pmatrix} \leftarrow \text{Le colonne sono le coordinate dei vettori di } \mathcal{B} \text{ scritti rispetto a } \mathcal{B}'$$

Possiamo pensare i cambi di base come applicazioni lineari

• Se $m(\mathcal{B}', \mathcal{B}) = P$

$$m(\mathcal{B}, \mathcal{B}') = P^{-1}$$

$$\begin{array}{ccc} m(\mathcal{B}, \mathcal{B}) & & m(\mathcal{B}, \mathcal{B}') \\ [v]_{\mathcal{B}} & \rightsquigarrow & [v]_{\mathcal{B}'} \\ \Rightarrow m(\mathcal{B}', \mathcal{B}) \cdot m(\mathcal{B}, \mathcal{B}') & = & I \end{array}$$
$$\begin{matrix} "P" \\ "P^{-1}" \end{matrix}$$

Def. Una AL $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ (da uno spazio a se stesso) si dice OPERATORE

oss. Due matrici A, B che rappresentano un operatore T rispetto a basi \mathcal{B} sono simili, ovvero $\exists P$ invertibile tale che $B = P^{-1}AP$

Se A rappresenta T rispetto a \mathcal{B} in posiz. e in ordine

$$\rightarrow A[v]_{\mathcal{B}} = [T(v)]_{\mathcal{B}}$$

B rappresenta T rispetto a \mathcal{B}' , in posiz. e in ordine,

$$\rightarrow B[v]_{\mathcal{B}'} = [T(v)]_{\mathcal{B}'}$$

Si può fare anche con basi \mathcal{B} in posiz. e in ordine ma diventa più complicato

Domanda finale: In quali casi esiste una base in cui T si può rappresentare con una mat. diagonale?

CONCETTI BASI SU AL

def. $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ AL, la sua immagine è

$$\text{Im } L = \{w \in \mathbb{R}^m \mid \exists v \in \mathbb{R}^m, L(v) = w\}$$

= Spazio generato dalle colonne di A_L

mat. associata rispetto alle basi canoniche

def. $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ AL, Il nucleo/Ker del di L è

$$\text{Ker } L = \{v \in \mathbb{R}^m \mid L(v) = 0\} = \text{Sol}(A_L, 0) = \text{Sol}\{A_L, 0\}$$

Oss. $\text{Im } L$ è un ssv di \mathbb{R}^m
 $\text{Ker } L$ è un ssv di \mathbb{R}^m

| w è ssv di \mathbb{R}^m

$\Leftrightarrow \forall v, w \in W, v+w \in W$

$\forall v \in \mathbb{N}, c \in \mathbb{R}, cv \in W$

mis. base di W è un insieme di vettori

di W che • generano

• sono LI

mis. diam $\mathbb{N} = \#$ vett. di una base

Potendo $\text{Im } L$ = Spazio generato dalle colonne?

$$A_L = \begin{pmatrix} | & | \\ |(e_1) & \dots & L(e_m)| \\ | & | \end{pmatrix}$$

Se $w \in \text{Im } L \Rightarrow \exists v \in \mathbb{R}^m$ t.c. $w = L(v)$

$$v = a_1 e_1 + \dots + a_m e_m$$

$$\Rightarrow w = L(w) = L(a_1 e_1) + \dots + L(a_m e_m) = a_1 L(e_1) + \dots + a_m L(e_m)$$

colonne
di A_L

< Per calcolare $\text{Im } L$ scrivo matrice associata A_L ; $\text{Im } L = \mathcal{L}$ (colonne di A_L)

di solito si chiede di trovare una base >

def. $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ suriettiva se $\forall w \in \mathbb{R}^m \exists v$ t.c. $L(v) = w$ ovvero $\text{Im } L = \mathbb{R}^m$

$\text{Im } L = \{ \text{spazio generato dalle colonne} \} \Rightarrow L$ suriettiva $\Leftrightarrow \dim \text{Im } L = m$

ovvero

A_L ha m colonne LI (le colonne di A_L generano $\text{Im } L$; una base è formata da generatori che sono anche LI \Rightarrow mi serve che tra queste colonne ce ne siano sicuro m LI)

$\Rightarrow L$ suriettiva $\Leftrightarrow \text{rg } A_L = m = \dim \mathbb{R}^m$

Oss. $A_L = \left(\begin{array}{c|c} | & | \\ |(e_1) & \dots & L(e_m)| \\ | & | \end{array} \right)_m \rightarrow \text{rg } A_L \leq \min(m, m) = m \Rightarrow \text{rg } A_L = m$ serve $m \geq m$

\Rightarrow Se $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ suriettiva, $m \geq m$

def. $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ e' iniettiva $\Leftrightarrow \forall v \neq w \Rightarrow L(v) \neq L(w)$

prop. $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ iniettiva \Leftrightarrow

- $\ker L = \{0\}$

- $\operatorname{rg} A_L = m = \dim \mathbb{R}^m$

dim. Se iniettiva $\Rightarrow \ker L = \{0\}$

Suppongo $\ker L = \{0\}$. Sia u, v t.c. $L(u) = L(v) \Rightarrow L(u) - L(v) = 0$
 $\hookrightarrow L(u-v) = 0 \Rightarrow u-v \in \ker L \Rightarrow u-v = 0$ (cioe' $u=v$) \checkmark

• $\ker L = L^{-1}\{0\} = \operatorname{Sol}(A_L v = 0) \rightarrow \dim \ker L = \# \text{ parametri delle sol.} = \# \text{ vdc} - \operatorname{rg} A_L = m - \operatorname{rg} A_L$

\Rightarrow sol unica $\Leftrightarrow \operatorname{rg} A_L = m$

OSS.

$$A_L = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \Big|_m \Rightarrow \operatorname{rg} A_L \leq \min(m, m) \Rightarrow \text{per essere iniettiva deve avere } m \leq m$$

\Rightarrow Se $L: \mathbb{R}^m \rightarrow \mathbb{R}^m$ iniettiva, $m \leq m$

\Rightarrow Se $T: \mathbb{R}^m \rightarrow \mathbb{R}^m$ isom. $\rightarrow m = m$

(iniettiva: $m \leq m$

suriettiva: $m \geq m$)



$F: \mathbb{R}^m \rightarrow \mathbb{R}^m$ e' una AL se $F(v+w) = F(v) + F(w)$

$$F(cv) = cF(v)$$

$$\text{FAI } \xrightarrow{\text{B} \sim \text{B}'} A_F(B', B) = \left(\begin{matrix} [F(v_i)]_{B'} \\ [F(v_m)]_{B'} \end{matrix} \right) \quad \{v_1, \dots, v_m\} = B$$

$$\ker F = \{v \in \mathbb{R}^m, F(v) = 0\} = \operatorname{Sol} A_F v = 0\}$$

$$\operatorname{Im} F = \{w \in \mathbb{R}^m, \exists v \in \mathbb{R}^m, F(v) = w\} = \{ \text{colonne di } A_F \}$$

Fondamentale: $F(v) = A_F v$ base comune

$$[F(v)]_{B'} = A_F(B', B)[v]_B \quad \text{base generica } B', B$$

F iniettiva / suriettiva / isom.

$$F \rightsquigarrow A_F \quad F' \rightsquigarrow A_F' \quad F \text{ isom} \Leftrightarrow A_F \text{ quadrata invertibile}$$

es. Matrice cambia base

def. Un operatore T e' una AL da $\mathbb{R}^m \rightarrow \mathbb{R}^n$

(Rappresentato da matrici $A \in M_{m \times n}$, una per ogni scelta di base)

Q. In quali casi esiste una base di \mathbb{R}^m , in cui $A_F(B', B)$ e' diagonale?

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

(a penso come $A_F(\mathbb{C}, \mathbb{C})$ per un operatore
 $(F(e_1), F(e_2), F(e_3)) \rightsquigarrow F(e_1) = e_1, F(e_2) = 2e_2, F(e_3) = 3e_3$)

AUTONALORI e AUTOVETTORI

def. T operatore su \mathbb{R}^m , $\lambda \in \mathbb{R} \Leftrightarrow$ AUTONALORE per T se $\exists v \neq 0$ tale che

$$T(v) = \lambda v \quad v \text{ si dice AUTOVETTORE}$$

Essere autonale è speciale.

$$T(v) = \lambda v \rightsquigarrow A_T v = \lambda v \rightsquigarrow A \cdot v - \lambda v = 0 \rightsquigarrow Av - \lambda I v = 0 \rightsquigarrow (A - \lambda I)v = 0 \quad (*)$$

matrice dei coeff di un
sistema

$\Rightarrow \lambda$ autonale \Leftrightarrow il sistema $\textcircled{*}$ ha sol m m.bondi

$$\# \text{pot} = \# \text{radici} - \text{rg}(A - \lambda I) = m - \text{rg}(A - \lambda I) > 0$$

$$\Leftrightarrow \text{rg}(A - \lambda I) < m \Leftrightarrow \det(A - \lambda I) = 0$$

\Rightarrow gli autonali di A sono le radici del polinomio $\det(A - \lambda I)$

Ricorda per trovare gli autonali cerca i λ tali che $\det(A - \lambda I) = 0$

def. $\det(A - \lambda I)$ si chiama polinomio caratteristico di A, è un polinomio di grado m.

1° PROB. Su R mmt tutti i pol. di grado m hanno m radici (con molteplicità)

Anche essere autovettore è speciale: l'immagine di un autovettore è un multiplo di sé stesso. Nell'esempio

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \det(A - \lambda I) = \begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & 2-\lambda & 0 \\ 0 & 0 & 3-\lambda \end{pmatrix} = (1-\lambda)(2-\lambda)(3-\lambda)$$

Autovettori: multipli di e_1 ;

" " e_2 ; nessun altro!

" " e_3 ;

Calcolo autovettori Dopo aver trovato gli autonali, v è autovettore relativo a un autonale $\lambda \Leftrightarrow v \neq 0$ e $(A - \lambda I)v = 0$

$\Rightarrow v$ è autovettore per $\lambda \Leftrightarrow v \neq 0$ e soddisfa questo sia l'inedita.

Si definisce l'autospazio relativo all'autonale λ come

$$V_\lambda = \text{Sd } \{(A - \lambda I)v = 0\} = \{0\} \cup \{\text{autovettori relativi a } \lambda\}$$

Ad ogni autonale λ abbiamo due numeri:

$n_{\lambda}(\lambda)$ = numero di volte che

compare come radice di $p_\lambda(t) = \det(A - t I)$

$m_{\lambda}(\lambda) = \dim V_\lambda = m - \text{rg}(A - \lambda I) \geq 1$ perché λ autonale $\Rightarrow A - \lambda I$ non è invertibile

molteplicità
geometrica

Esempio

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{Calcolare autovettori: } A - \lambda I = \begin{pmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{pmatrix}$$

Calcolare autovettori:

$$V_0 = \text{Sd}(A - 0I | 0) \quad A - 0I = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{rg} = 1$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \left\{ \begin{array}{l} x+4=0 \\ x=0 \end{array} \right.$$

$$x = -4$$

$$\Rightarrow V_0 = \text{Sd} \left\{ \begin{pmatrix} 1 \\ -4 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 1 \\ -4 \end{pmatrix}, t \in \mathbb{R} \right\}$$

spazio generato

$$Bv_0 = \left\{ \begin{pmatrix} 1 \\ -4 \end{pmatrix} \right\}$$

$$V_2 = \text{Sd}(A - 2I | 0) \quad A - 2I = \begin{pmatrix} 1-2 & 1 \\ 1 & 1-2 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \quad \left\{ \begin{array}{l} -x+y=0 \rightarrow x=y \\ / \end{array} \right.$$

$$\Rightarrow V_2 = \text{Sd} \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$Bv_2 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

OK! $\text{rg} < m = 2$

ho saltato λ apposta

$$\text{rg} = 1$$

$$T: \mathbb{R}^M \rightarrow \mathbb{R}^N$$

Oss. Due matrici A, B rappresentano lo stesso operatore T rispetto a basi diverse \Leftrightarrow sono simili, ovvero $\exists P \in M_{n \times n}$ invertibile tale che: $B = P^{-1}AP$

FOTO TEL

$$\text{In coord: } \star B[\cdot]_{B'} = [\tau(\cdot)]_{B'} \quad M(B, B')[\cdot]_{B'} = [\cdot]_B$$

$$A[\cdot]_{B'} = [\tau(\cdot)]_{B'}$$

Controllo funzioni \star se $B = P^{-1}AP$

$$B[\cdot]_{B'} = (\underbrace{P^{-1}AP}_{[\cdot]_B})[\cdot]_{B'} = [\tau(\cdot)]_{B'} \quad (\star) \quad \checkmark$$

$$\begin{array}{c} [\cdot]_B \\ \hline [\tau(\cdot)]_{B'} \\ \hline [\cdot]_{B'} \end{array}$$

$$[\tau(\cdot)]_{B'}$$

oss. Gli autovettori non dipendono dalla scelta delle basi, ovvero della matrice che lo rappresenta. Infatti

prop. Due matr. simili hanno lo stesso pd. caratteristico

dim A, B suppongo $B = P^{-1}AP$ P invertibile

$$P_A(t) = \det(A-tI)$$

$$I = P^{-1}P$$

$$P_B(t) = \det(B-tI) = \det(P^{-1}AP-tI) =$$

Binet

$$= \det(P^{-1}AP - tP^{-1}IP) = \det(P^{-1}(A-tI)P) =$$

$$\Rightarrow \det P^{-1} \cdot \det(A-tI) \cdot \det P = P_A(t)$$

$$\det P \cdot \det P^{-1} = 1$$

def. Una matr. $A \in M_{n \times n}$ è diagonalizzabile $\Leftrightarrow \exists D$ diagonale, P invertibile, tale che $D = P^{-1}AP$

Formulazione equivalenti in termini di operatori:

def. $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ è diagonalizzabile $\Leftrightarrow \exists$ base B di autovettori, ovvero $A_T(B, B)$ è diagonale

Nell'esempio $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rightsquigarrow \lambda_1 = 0 \quad B_{v_0} = \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$
 $\lambda_2 = 2 \quad B_{v_2} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$

Base di autovettori: $B = \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$
 $A_T(B, B) = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} = D \quad T\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = 0\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$
 $T\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = 2\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$

\Rightarrow se voglio trovare D diagonale e P invertibile tale che

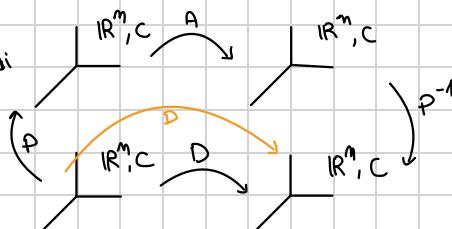
$$D = P^{-1}AP,$$

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

Che è P ? $P \in M(C, B)$
= colonne vettori di
 B scritte in
coordinate
risp. a C
= vettori di B

$$\Rightarrow P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Bose di v_0
Bose di v_2



Questa è la ragione per cui si scrive

$$D = P^{-1}AP: \text{ così } P \text{ ha come colonne gli autovettori.}$$

Se scrivessi $D = \tilde{P}A\tilde{P}^{-1}$, $\tilde{P} \in M(C, B)$ non avrebbe
per colonne i vettori cominci scritti in cost. risp.
 $a, b \rightarrow$ conti EXTRA

Riass. • Calcolo autoval.

• Calcolo base per ogni auto spazio

• Se ho abbastanza autovettori per le basi $M \rightarrow D$ mettendo gli autoval. sulla diagonale

$\rightsquigarrow D$ mettendo gli autovett.

come colonne

2° PROB: Perché non avere abbastanza autovettori

Ese.

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \quad \lambda = 2 \quad \text{Ma}(2) = 2$$

$$V_2 = \text{Sd}(A - 2I) \quad A - 2I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{rg} = 1 \quad \text{autoval. ok}$$

$$\underline{\lambda_A} \neq \text{pct} = \# \text{val} - \text{rg} = 2 - 1 = 1$$

$$\Rightarrow V_2 = \dots = \lambda \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

$$\Rightarrow B_{V_2} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

Per avere una base di autovettori per \mathbb{R}^2 , mi servono due autovettori, ma me ne ho uno solo!

Non ho altre autovetori da cui trovare autovettori e V_2 non dimensione $1 < 2$.

DA SAPERE

Fatto Una matrice A è diagonalizzabile \Leftrightarrow

1. Esistono tutte le radici di $p_A(t)$ in \mathbb{R}

Cond. necess.

2. \forall autovettore λ

$$\text{Mav}(\lambda) = \text{mg}(\lambda)$$

da C: mo prob. too fam.
algebrico

e suff.

Altri due criteri: • Se tutti gli autovetri esistono e sono distinti] criteri
 $\Rightarrow A$ è diagonalizzabile

• Se una mat. è simm. \Rightarrow è diagonalizzabile
(TEO. SPECTRALE)

suff. - ma non
necessari

Ragionevole:

ogni autoval. mi dà
un autovett., devo solo
dim. li

DOMANDA D'ESAME:
criteri diagonalibilità

Esercizi applicazioni lineari e diagonalizzazione

MINI RIASSUNTO

- \mathbb{R}^m ($V \subset \mathbb{R}^m$) è un s.v. se $v_1 + v_2 \in V \quad \forall v_1, v_2 \in V$
per \mathbb{R}^m (sottinsieme per \mathbb{R}^m) $c v \in V \quad \forall v \in V, c \in \mathbb{R}$
- base per V : insieme di vettori $\cdot L$
 - che generano V
- $\dim V = \#$ vettori di una base (non dipende dalla scelta)
- per ogni scelta di B , $v \mapsto [v]_B$ $\xrightarrow{\text{memoria}}$
 - a un vettore possiamo associare le sue coordinate
 - rispetto a questa base
- per passare dalle coordinate rispetto a B alle $\xrightarrow{\text{uso una matr. cambio base } M(B', B)}$
 - le matr. cambio base sono invertibili, e le matr. invertibili posso vederle come matr. cambio base
 - le matr. ortogonali corrispondono alle matr. che cambiano base tra C e una base orthonormale
 - $M(C, B)$ è la matr. le cui colonne sono i vettori di B
 - Per ogni scelta di base B, B'
 $M(B', B) = [M(B, B')]^{-1}$

Applicazioni lineari

$F: \mathbb{R}^m \rightarrow \mathbb{R}^m$, Per ogni scelta di basi B su \mathbb{R}^m
 B' su \mathbb{R}^m

- posso scrivere $A_F = (B', B)$
- $A_F(C, C) = (F(e_1), \dots, F(e_n))$
- $\xrightarrow{\text{immagini vettori base}}$
- $T: \mathbb{R}^m \rightarrow \mathbb{R}^m$, due matrici A, B rappresentano T
 \iff sono simili [$\exists P$ invertibile, $B = P^{-1}AP$]
- B base di autovettori per $T \Leftrightarrow A_T(B, B)$ è diagonale

Esercizi AP. lin.

- es. completo: data F a.l. calcolare:
- | | | |
|-----------------------------|------------------------------|--|
| $\text{Im } F$ | $\text{Ker } F$ | $\cdot F$ è iniettiva / suriettiva / isomorfismo |
| $\dim \text{Im } F$ | $\dim \text{Ker } F$ | |
| \cdot base $\text{Im } F$ | \cdot base $\text{Ker } F$ | |
- F può essere data in due modi: A) $F(x_1, \dots, x_m) = \dots$
B) $F(e_1) = \dots, F(e_2) = \dots$

Altre domande:

- Scrivere $F: \mathbb{R}^n \rightarrow \mathbb{R}^m$ che sia iniettiva / ecc..

ESEMPIO 1

$$F(x_1, x_2, x_3) = \begin{pmatrix} 2x_1 + x_3 \\ x_1 + x_2 \\ x_1 + x_2 + x_3 \\ x_1 - x_2 + x_3 \end{pmatrix}$$

OSSERVAZIONE: $F: \mathbb{R}^3 \rightarrow \mathbb{R}^4$
 (il vettore immagine ha 4 componenti)

Def. di Al.

Dimostrare che

$\text{ker } F, \text{Im } F$ sono ssv
 di $\mathbb{R}^3, \mathbb{R}^4$

STEP 0: Scrivere matrice associata

$$A = A_F = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}$$

copio i coeff. / posso pensare le colonne di A come $F(e_1), \dots, F(e_m)$

$$F(e_1) = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix}, F(e_2) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix}, F(e_3) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

STEP 1: calcolare il rango

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & R_2 - 2R_1 \\ 2 & 0 & 1 & R_3 - R_1 \\ 1 & 1 & 1 & R_4 - R_1 \\ 1 & -1 & 1 & \end{array} \right) \xrightarrow{\text{R2} - 2R1} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & -2 & 1 & R_4 - R_2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 1 & \end{array} \right) \xrightarrow{\text{R4} - R2} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\rightarrow \text{rg } A = 3$$

eg max

$$\dim \text{Im } F = 3$$

\Rightarrow 3 < \dim \mathbb{R}^4
 => non suriettiva

$$\dim \text{Ker } F = \# \text{ vct. rig. } - \text{rg } A = M - \text{rg } A$$

$$= \text{sol } (AX = 0)$$

$$\dim \mathbb{R}^M$$

$$= 3 - 3$$

$$= 0$$

PROPRIETÀ: una A.L. è imiettiva \iff

il suo nucleo è il vettore nullo

STEP 2: Calcolo $\text{Im } F$ (recupero la matr. originale, non quella ridotta a scalo perché l' $\text{Im } F$ è lo spazio generato dalla matr. originale)

Recupero A ($\text{Im } F$ si calcola sulle colonne di A, non sulla matr. ridotta a scalo)

$$\text{Im } F = \mathbb{L} (\text{colonne di } A)$$

$$- \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = a_1 \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix} + a_3 \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$

Il numero ottimale di col. da usare è dato dal rango, in questo caso 3

↑ SPAZIO GENERATO = SPAZIO delle C.L.

Attenzione allo spazio a cui appartengono i vettori

$B_{\text{Im } F}$ - Devo estrarre dalle colonne un insieme di vettori l.i.

In questo caso li ho già perché $\dim \text{Im } F = 3$
 $= \# \text{ col } A$

$$B_{\text{Im } f} = \left\{ \begin{pmatrix} 2 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

STEP 3: Kernel da proprietà fondamentale di A è $\forall v \in \mathbb{R}^m, F(v) = A \cdot v$

$$\text{Ker } F = \text{Sol}(Ax=0)$$

Possiamo rappresentare la matrice a scalo

In questo caso specifico $\text{Ker } F = \{0\}$

, poiché $\dim \text{Ker } F = 0$

$$B_{\text{Ker } F} = /$$

STEP 4: Non suriettiva perché $\dim \text{Im } F < \dim \mathbb{R}^4 \rightarrow$ NO isomorfismo
spazio d'arrivo

Si imiettiva poiché $\text{Ker } F = \{0\}$

$$F \text{ imiettiva} \Leftrightarrow \text{Ker } F = \{0\}$$

$$\mathbb{R}^3 \rightarrow \mathbb{R}^4$$

$3 < 4 \rightarrow$ non può essere suriettiva

$$\text{ES.2 } L: \mathbb{R}^4 \rightarrow \mathbb{R}^3 \text{ definita da } L(e_1) = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, L(e_2) = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, L(e_3) = \begin{pmatrix} 4 \\ 3 \\ -1 \end{pmatrix}$$

$$L(e_4) = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 1 & 3 & -1 \\ -1 & 0 & -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & -1 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & -1 \end{pmatrix} \xrightarrow{\substack{R_3 + 2R_1 \\ R_2 + R_1}} \begin{pmatrix} -1 & 0 & -1 & 1 \\ 0 & 3 & 3 & 3 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$R_2 - 3R_3 \quad \begin{pmatrix} -1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{rg } A = 2$$

$$\dim \text{Im } L = 2 < \dim \mathbb{R}^3 = 3$$

\Rightarrow No suriettiva

$$\dim \text{Ker } L = \dim \mathbb{R}^4 - \text{rg } A$$

$$= 4 - 2 = 2$$

\Rightarrow NO imiettiva

ARRIVO

PARTENZA

• $\text{Im } L$, tormo a uscire A

$$\text{Im } L = \text{L}\left\{ \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \right\}$$

Poiché $\dim \text{Im } L = 2$, bastano due coh. L.I.

$$= \text{Im } L = \left\{ \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \right\} = \left\{ \mathbf{x} \in \mathbb{R}^3 \mid \mathbf{x} = s \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} + t \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \right\}$$

$$B_{\text{Im } L} = \left\{ \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \right\}$$

$$\cdot \text{Ker } L = \text{Sol}(A\mathbf{x} = \mathbf{0}) = \left\{ \mathbf{v} \in \mathbb{R}^4 \mid L(\mathbf{v}) = \mathbf{0} \right\} = \mathbb{C}^4 \setminus \{0\}$$

Posso usare la matrice a scalo

$$\begin{pmatrix} -1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{cases} -x_1 - x_3 + x_4 = 0 \\ x_2 + x_3 + x_4 = 0 \end{cases} \quad \begin{cases} x_1 = -x_3 + x_4 \\ x_2 = -x_3 - x_4 \end{cases}$$

$\dim \text{Ker } L = 2 \rightarrow 2 \text{ param.}$

$$x_3 = s$$

$$x_4 = t \implies \begin{cases} x_1 = -s + t \\ x_2 = -s - t \end{cases}$$

$$\text{Ker } L = \left\{ \mathbf{x} \in \mathbb{R}^4 \mid \mathbf{x} = \begin{pmatrix} -s+t \\ -s-t \\ s \\ t \end{pmatrix} = s \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix} + t \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$B_{\text{Ker } L} = \left\{ \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

- NO suriettiva $\dim \text{Im } L = 2 < 3 = \dim \mathbb{R}^3 \Rightarrow \text{No isomorfismo}$
- NO iniettiva $\text{Ker } L \neq \{0\}$

Domanda Extra: Calcolare l'immagine di un vettore $\rightarrow L \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$

$$L(\mathbf{v}) = A\mathbf{v} = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 1 & 3 & -1 \\ -1 & 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 27 \\ 9 \\ 0 \end{pmatrix}$$

DIAGONALIZZAZIONE

- Ripassare autovettori e autovalori
- Non tutte le matrici sono diagonalizzabili
 - * possono mancare autovettori

$$R = \begin{pmatrix} \sin \theta & -\cos \theta \\ \cos \theta & \sin \theta \end{pmatrix}$$

* possono essere

